REFERENCE GUIDE FOR INTRA AI DATA SPACE INTEROPERABILITY

Developing individual AI data space instances

Working group Data Sharing

NL AI Coalition

March 2023

Content

MANAGEMENT SUMMARY

The ambition of the Netherlands AI Coalition (NL AIC) is to position the Netherlands at the forefront of knowledge and application of AI for prosperity and well-being. To achieve this goal, it is deemed crucial to make data widely available to train and fuel the AI-algorithms. This is why the NL AIC working group Data Sharing has set the goal of the creation of trustworthy and interoperable AI data spaces. This will be done in alignment with the European data strategy, in short summarised as '*Towards a Federation of Interoperable (AI) Data Spaces*'. Therefore, in 2021, it has described the overarching AI data space reference guide [1], in which two developments lines are introduced: the intra and the inter AI data space interoperability development line. This report address the former, i.e. the development line for intra AI data space interoperability. The latter is addressed in the companion report [2].

The ambition of the reference guides for both intra and inter AI data space interoperability is to support organisations in developing interoperable AI data spaces to address the data sharing challenges to optimally support AI with its variation in collaboration models as introduced in the overarching AI data space reference guide [1]. They elaborate the architecture and building blocks, providing a rich set of capabilities to support data sharing and to ensure trust and interoperability within and between different AI data spaces.

The intra AI data space reference guides in this report address two distinct scenarios, i.e.: (1) the '*homogenous*' intra AI data space interoperability scenario in which the participants within an AI data space adopt an agreed upon and aligned architecture and trust interaction framework, e.g. such as described in this report, and (2) the '*heterogenous*' intra AI data space interoperability scenario in which participants within an AI data space do not all need to adopt an aligned architecture and trust interaction framework, and in which a hybrid security gateway absorbs the variation in protocols.

The subsequent parts of this report address the ecosystem, the building block and the trust architecture for intra AI data space interoperability, with the ecosystem architecture describing the main strategic, organisational and data space ecosystem principles, the building block architecture defining and elaborating the individual building blocks, and the trust architecture addressing the interaction patterns and protocols to assure that data and AI processing services and resources are shared in a trustworthy manner. In addition, this report contains a part on the reference implementation, roadmap and conclusions for intra AI data space interoperability.

Both the work on the intra and inter AI data space interoperability development line report on work-in-progress. Based on the input, know-how and expertise of the participants of the NL AIC working group Data Sharing the reports provide the foundation for data spaces for AI in the Netherlands. The collaborative development of the AI data space architecture, its building blocks, the sharing of best practices and the management of the roadmap from proofs-of-concept towards operationalisation paves the way to the successful introduction of a federation of operational and interoperable AI data spaces in the Netherlands.

Moreover, it is to be noted that the Netherlands with the NL AIC working group Data Sharing and adjacent data sharing initiatives has a good starting position to make data sharing for AI work and to take a leading role in Europe for realising the European

Data Strategy [3]. As such, the work and knowledge of the NL AIC working group Data Sharing will be provided transferred to the various Dutch and EU initiatives working on a common goal and strategy for realising the European Data Strategy of the '*federation of interoperable data spaces*', specifically to (1) the Data Sharing and Cloud Centre-of-Excellence as joint follow-up effort of the work for the Data Sharing Coalition, the NL AIC working group Data Sharing and the Gaia-X Hub in the Netherlands and to (2) the EU Data Spaces Support Centre (DSSC) project as part of the Digital Europe program addressing the aligned development of data spaces for and across various sectors in Europe.

Founded in 2019, the NL AIC has been set up to support well-being and welfare in the Netherlands by putting it in a front-runner position in terms of AI knowledge and applications. The NL AIC is a public-private partnership in which the government, business sectors, educational and research institutions, as well as civil society organisations collaborate to accelerate, implement, encourage and connect AI activities [4].

1. INTRODUCTION

One of NL AIC's building blocks is 'Data Sharing' [4], for which the NL AIC working group Data Sharing has been started in 2020. This introductory chapter describes the goal, scope and structure of this reference guide for intra AI data space interoperability in the context of the overarching work and deliverables of the NL AIC working group Data Sharing.

1.1 The NL AIC working group Data Sharing: goals and deliverables

A dedicated working group, the NL AIC working group Data Sharing, is tasked with providing the community knowledge, guidance and resources around responsible data sharing for AI, taking due note of Dutch and European developments and values.

As preparatory work, in 2020 the NL AIC working group Data Sharing has (1) identified the specific challenges for data sharing for advanced data analytics and provided an overview of technologies and architectures that can be used in addressing these challenges [5][6], (2) outlined the process of how companies can share data for AI, from experimental ("first-time engineering") phase to a phase of daily practice ("operationalisation") [7], (3) developed three proofs-of-concepts to demonstrate the architectural and technical concepts for controlled data sharing for AI, using three illustrative and representative cases from the sectors 'government', 'health' and 'energy' [8], (4) done a 'GAP-analysis' on the system operations gaps and the governance gaps to be bridged between the architectures and technology as demonstrated in the proofs-of-concepts and the large-scale deployment and adoption thereof [8], and (5) caried out a quick scan to validate that a data space approach is in line with international developments [9].

Starting in 2021, the NL AIC working group Data Sharing has initiated the structural work on the interrelated set of deliverables as graphically depicted in **Figure 1**.

As the figure shows, the NL AIC working group Data Sharing has provided the overarching reference guide for AI data spaces ('Towards a Federation of AI Data Spaces') in 2021 [1]. It sets the development direction towards federated and interoperable AI data spaces, aligning with the European data strategy and adhering to the European values of trust and data sovereignty. It introduces the developments lines for intra and inter AI data space interoperability, which are reported in their corresponding reference guides.

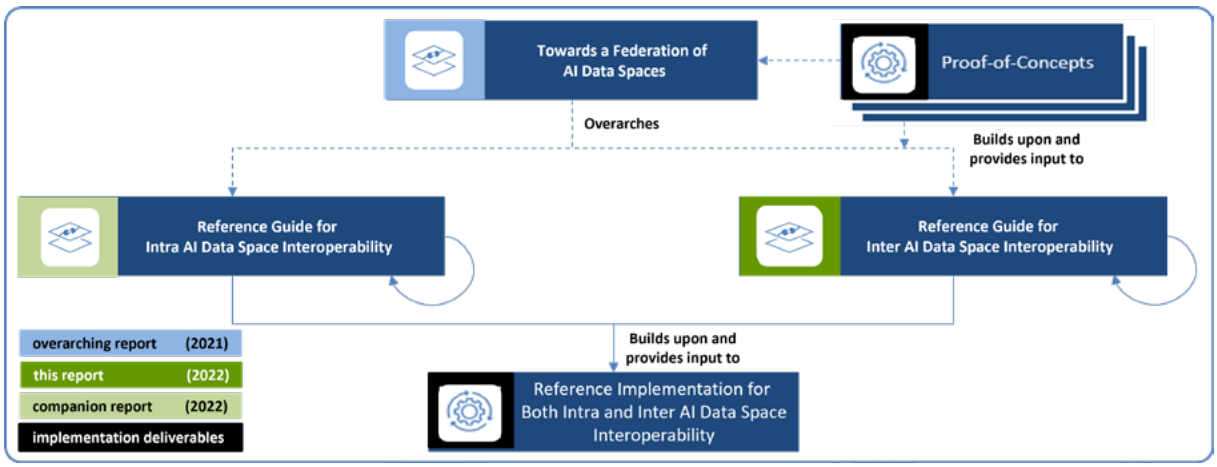

Figure 1 - Deliverables of the NL AIC working group Data Sharing and their interrelationship.

Moreover, to show the potential and to identify lessons learned, their architectural concepts and technologies have been demonstrated by means of use cases and demonstrators in close collaboration with participants the NL AIC working group Data Sharing [10] and are further developed by means of illustrative and representative scenarios in the NL AIC reference implementation as described in chapter 8 and annex B of the companion report [2].

1.2 Reference guides for intra and inter AI data space interoperability: goals

As described in [1], AI data spaces provide the ecosystem and building blocks for sharing data and AI algorithms, for processing AI algorithms and data apps and for managing trust, data sovereignty and (legal) agreements. In view of the European ambition of federation of interoperable European data spaces, adequate governance is required to realize interoperability of the AI data space building blocks, both within individual AI data spaces and between multiple AI data spaces. Therefore, the NL AIC working group Data Sharing distinguishes two development lines for AI data spaces:

- *Intra AI data space interoperability*, focussing on a reference architecture, building blocks, guidelines and solutions for interoperability between building blocks within a single AI data space.
- *Inter AI data space interoperability*, focussing on a reference architecture, building blocks, guidelines and solutions for interoperability between multiple AI data space instances.

The work on the inter AI data space interoperability development line is reported on in this report. It elaborates the overarching architecture, building blocks and roadmap for inter AI data space interoperability. The goal is to serve as reference guide for realising interoperability between multiple data space instances, jointly providing overarching data sharing capabilities whilst ensuring trust and interoperability between AI data spaces.

The work on the intra AI data space interoperability development line is reported in the companion report '*Reference guide for intra AI data space interoperability*' [2].

1.3 Transfer of results

The results of the NL AIC working group Data Sharing on architecture, building blocks and roadmap (as described in the previous section) are transferred to and followed up both within the relevant data space development initiatives, both within the EU and within the Netherlands:

- *Within the EU context*: hand-over of the results is done to the Digital Europe programs (under the responsibility of EU DG Connect) addressing the aligned development of data spaces for and across sectors, specifically the EU Data Spaces Support Centre programme [11] aimed to facilitate common data spaces that collectively create an interoperable data sharing environment in Europe, executing from October 2022 until March 2026 and the EU SIMPL initiative [12] aimed at procuring the open-source development of the smart middleware building blocks that will enable cloud-to-edge federations and support all major data initiatives funded by the European Commission, such as the common European data spaces.

- *Within the Dutch context*: the Centre-of-Excellence Data Sharing and Cloud as currently being defined as joint effort in the Netherlands of the work of the Data Sharing Coalition [13], the NL AIC working group Data Sharing [14] and the Gaia-X Hub in The Netherlands [15].

With the transfer of the work of the NL AIC working group Data Sharing as described in this report, its results will be firmly embedded in strong national and international initiatives.

1.4 Structure of this report

This report has three parts, subsequently addressing the ecosystem architecture, the building block architecture and the trust architecture of the intra AI data space development line, followed by a concluding part describing the reference implementation, the roadmap and the overarching conclusions. The initial two parts follow the phases for developing ICT architectures, i.e. the architecture design phases of the Open Group's Architecture Development Method (TOGAF ADM [15]) as depicted in Figure 2.

- *PART A: The ecosystem architecture*

  The ecosystem architecture describes the main strategic and organisational principles that provide the foundation for developing AI data spaces. It is 'overarching' as it provides the foundation for both the intra and inter AI data space interoperability architecture. It encompasses the phases A and B of the TOGAF ADM, i.e. the architecture vision in chapter 2 (including the AI-collaboration models and the business role model for AI data spaces) and the business architecture in chapter 3 (expressing the architecture vision in terms of business architecture principles).

- *PART B: The building block architecture*

  The building block architecture provides a decomposition of the ecosystem architecture into a set (generic) building blocks, jointly providing the capabilities for realising the architecture vision and the business architecture. It encompasses the phases C and D of the TOGAF ADM, i.e. the information systems architecture (ISA) in chapter 4 (providing the overarching set of building blocks) and the technology architecture in chapter 5 (with their technical elaboration).

- *PART C: The trust architecture*

  The trust architecture encompasses the governance, management and monitoring activities to assure that both the (potential sensitive and valuable) pri-mary data and AI algorithms and their associated metadata being shared are trustworthy. Moreover, it ensures data sovereignty to the entitled parties over their data, services and assets. It overarches the phases A through D of TOGAF ADM. As such, chapter 6 elaborates the trust architecture for the data space authority, the identity management and the policy management capabilities. Chapter 7 elaborates the trust interaction model to ensure trustworthiness of metadata sharing between building blocks.

- *PART D: The reference implementation, roadmap and conclusions*

  The basic technology for the individual building blocks for AI data spaces is currently maturing. However, the development of the overarching ecosystem architecture of the federation of interoperable AI data spaces is still in its infancy, requiring further guidelines and a roadmap for development. Therefore, chapter 8 provides a reference implementation to demonstrate the potential and to identify lessons learned for developing towards large

scale adoption. Subsequently, chapter 9 provides the development roadmap for intra AI data space interoperability, after which chapter 10 provides the overarching conclusions.

In addition, this report includes three annexes. Annex A describes an illustrative and representative usage flow for each of the four AI-collaboration models to be supported by AI data spaces [1], i.e. the Data Sharing AI-collaboration model, the Algorithm Sharing AI-collaboration model, the Third Party Processing AI-collaboration model and the Network Processing AI-collaboration model, respectively. annex B describes the high level reference implementation in the domain of geriatric health care, with representative story lines on the network processing AI collaboration model, on data sovereignty and technical (trust) interoperability and on semantic interoperability. Finally, annex C elaborates the security gateway building block, including a description of a TNO open source implementation thereof.

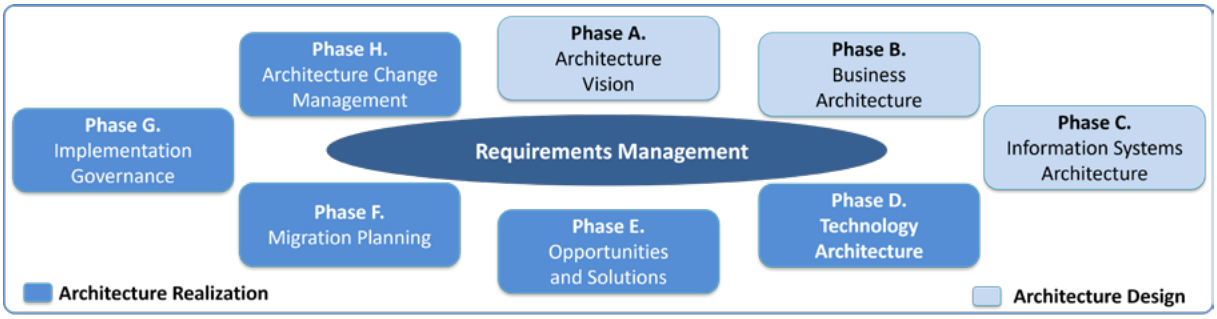

Figure 2 - TOGAF ADM phases [15] for architecture design as basis for the Part A and Part B of this report.

PART A: ECOSYSTEM ARCHITECTURE

The ecosystem architecture describes the main strategic and organisational principles that provide the foundation for developing AI data spaces. The ecosystem architecture encompasses the phases A and B as defined in the TOGAF Architecture Development Method (TOGAF ADM [15]): i.e. the architecture vision and the business architecture. These are addressed in chapter 2 and chapter 3, respectively.

2. ARCHITECTURE VISION

The architecture vision builds upon the ambition of the European Data Strategy as previously described in the overarching reference guide for AI data spaces '*Towards a Federation of AI Data Spaces*' [1]. As such, the sections in this chapter recapitulate from this the overarching reference guide the vision, the AI-collaboration models and the business role model as foundation for the development of AI data spaces.

2.1 European Data Strategy: federation of interoperable data spaces

Data sharing and data spaces are clearly on the radar of the European Commission. Its release of the European Data Strategy [16], the Data Governance Act [17] and the additional input sought on data spaces through the Open DEI initiative [18][19] illustrate the importance the EU attributes to data sharing for society and economy. Moreover, various (European and national) initiatives are exploring the potential, architectures and implementations for federative data sharing and data spaces. An extensive overview on federative data sharing initiatives is given in [20].

The ambition on federative data sharing as expressed in the EU Data Strategy can be summarised as:

'Towards a federation of interoperable data spaces'

As motivated and described in the overarching reference guide for AI data spaces '*Towards a Federation of AI Data Spaces*' [1] the development of AI data spaces as pursued by the NL AIC working group Data Sharing adheres and builds upon this ambition. The federation of interoperable AI data spaces allows entitled parties to maintain of sovereignty over their (potentially sensitive) through the support of various AI collaboration models, and enables an open business role model to federative data sharing between data services providers and consumers, i.e. without centrally storing the data by means of a 'data lake'. A value proposition for AI data spaces has recently been developed by the NL AIC working group Data Sharing [21].

2.2 AI-collaboration models

Data sharing for AI encompasses the enabling for AI algorithms to access data from various sources to realize an AI-result. However, the various data sources for AI algorithms cannot always simply be brought together. This may be the case when the amount of data to be transferred is too large or due to confidentiality, ethical or legal issues, e.g. the GDPR or company confidentiality policies. In such cases, data should remain with its provider or administrator and not to be transferred to other organisations for AI processing: only access to data is provided instead of sharing the data.

Therefore, four collaboration models (or archetypes) have been identified that need to be enabled by AI data spaces [1] to support the various interaction patterns between providers of data and providers or executers of AI algorithms:

1. *Data Sharing*, in which the data is transferred from the data services provider to the organisation executing the AI algorithm.
2. *Algorithm Sharing*, in which the AI algorithm is transferred and executed in the security domain of the data services provider.

3. *Third Party Processing*, in which both the data and the AI algorithm are transferred and executed in the security domain of a (trusted) third party.

4. *Network Processing*, in which the execution of the AI algorithm is done in a distributed manner by a network of parties, e.g. in the case of Federated Learning or secure Multi-Party Computation.

It is to be noted that these four AI-collaboration models have overlap and commonalities in their requirements on sharing either data or (parts of) AI algorithms between individual organisations. Illustrative usage scenarios for each of the four AI-collaboration models are described in annex A.

2.3 Business role model for intra AI data space interoperability

A business role fulfils a primary (business) activity in the overarching processes for data sharing for AI as enabled by the AI data spaces, which may be performed by an independent organisation. The business role model for AI data spaces builds and extends upon the work of the EU Open DEI initiative, which has further elaborated the ambition as expressed in the EU Data Strategy. It has defined a data space as "*a decentralised infrastructure for trustworthy data sharing and exchange in data ecosystems based on commonly agreed upon principles*", requiring the following elements [19]:

- *building blocks such as data platforms*, providing support for effective data sharing and exchange as well as for engineering and deployment of data exchange and processing capabilities;
- *building blocks such as data marketplaces*, where data services providers can offer and data services consumers can request data, as well as data processing applications;
- *building blocks ensuring data sovereignty*, i.e. the ability for each stakeholder to control their data by making decisions as to how digital processes, infrastructures, and flows of data are structured, built and managed, based on an appropriate governance scheme enabling specification of terms and conditions.

Based on this work of the EU Open DEI initiative, the business role model for AI data spaces has been defined in [1] and is depicted in **Figure 3**. Where applicable, the roles in the business role model align with the roles (and their naming) as defined for the IDS role model in the IDS Reference Architecture Model [22][23].

As the figure shows, each business role can be assigned to one of four categories:

1. the data space *core roles*,
2. the data space *intermediary roles*,
3. the data space *software and services roles*, and
4. the data space *governance roles*.

The data space core roles in the business role model for AI data spaces have been defined in [1]. Moreover, it has identified the relation of the business role model for AI data spaces with the 12 building blocks in the soft infrastructure stack as defined by the EU Open DEI initiative [19].

Table 1 describes the four categories of business roles for AI data spaces and the individual roles.

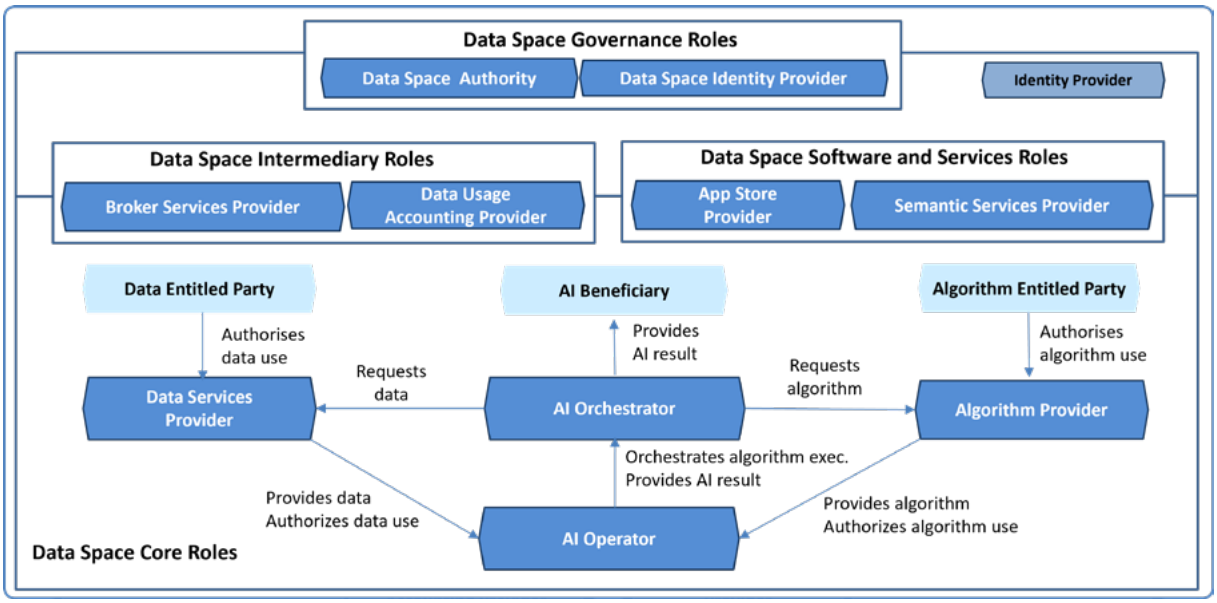

Figure 3 - TOGAF ADM phases [15] for architecture design as basis for the Part A and Part B of this report.

Table 1: The four categories of business roles for intra AI data space interoperability ([1], paragraph 6.1.4).
Data Space Core Roles The data space core roles are involved and required every time data or an AI algorithm is shared or executed in the AI data space. The role of a core participant can be fulfilled by any organisation that owns, wants to provide, consume/use or execute data or an AI algorithm.
AI Beneficiary The AI Beneficiary is interested in a result of AI interaction. The AI Beneficiary receives the results that are requested from the AI Orchestrator. The AI Beneficiary is responsible for initiating an AI interaction via an AI Orchestrator.
AI Orchestrator The AI Orchestrator orchestrates the intended AI interaction and ensures that the AI algorithm yields the intended results for the AI Beneficiary. The AI Orchestrator properly manages the policies for what it orchestrates. The AI Orchestrator understands what core modules for AI are required and is tasked with bringing these together (i.e. orchestration), e.g. on identifying and bringing together relevant data and AI algorithms. The AI Orchestrator is also responsible for properly assessing policies that are relevant to the intended AI result. A main added value of the AI Orchestrator is in being a single-point-of-contact for the AI Beneficiary in orchestrating and integrating the interactions with all core business roles and the services/building blocks they provide.
AI Operator The AI Operator is responsible for providing an environment for execution of algorithms on the data. As such, it provides a capability (building block) that is referred to as the 'Application Container Environment (ACE)' in which the security gateway and the AI algorithms are executed with the required data in order to produce the intended results of the AI algorithm. Moreover, the AI Operator is responsible for properly assessing policies that are relevant during the execution.

Data Services Provider Data Services Providers hold data in the data spaces and makes the data available in a controlled manner for AI algorithms. The Data Services Provider manages policies for the data it is holding, e.g. it manages and enforces access and usage policies and provides additional policies to the AI Operator. The Data Services Provider also manages the quality and availability of data on behalf of Data Entitled Parties.
Data Entitled Party Data Entitled Parties have one or more entitlements, e.g. having control over or being the subject of the data as provided by a Data Services Provider. The Data Entitled Party has the right to define the terms and conditions of use of data to which it is entitled.
Algorithm Provider Algorithm Providers hold the AI algorithm in the data spaces. The Algorithm Provider properly manages policies for the AI algorithms it is holding. It manages and enforces access and usage policies and shares the policies with the AI Operator. The Algorithm Provider also manages the quality and availability of algorithms on behalf of Algorithm Entitled Parties.
Algorithm Entitled Party Algorithm Entitled Parties have one or more entitlements to the AI algorithm as provided by an Algorithm Provider. The Algorithm Entitled Party has the right to define terms and conditions of use of the algorithm to which it is entitled.
Data Space Intermediary Roles The data space intermediary roles enable the processes for interaction between the core roles by establishing providing metadata, support services and establishing trust.
Broker Services Provider A Broker Services Provider provides capabilities to register, manage and expose information about the resources available in a data space, e.g. data services, AI algorithms and computing resources. Moreover capabilities can be provided to support the offering of data resources and services under defined terms and conditions, which clearly describe the rights and obligations for data and service usage, and access to data and services.
Data Usage Accounting Provider The Data Usage Accounting Provides manages and provides the basis for accounting access to and/or usage of resources (e.g. data, algorithms) by various participants. It includes the important capabilities for registering data transactions that have taken place, also as basis for clearing, billing and conflict resolution.
Data Space Software and Services Roles The data space software and services roles comprises IT companies providing software and/or services (e.g., in a software-as-a-service model) to the participants of the AI data space.
App Store Provider The App Store Provider provides data apps which contain applications (e.g. AI algorithms) that may be deployed within the secure processing environments of the data space, e.g. in a participants security gateway or the Application Container Environment (ACE) and related execution environment of an AI Operator. The data apps facilitate data processing workflows. The App Store Provider is responsible for managing metadata on the data apps it provides.

Semantic Services Provider The Semantic Services Provider provides services to manage semantics within the data space, including a registry of vocabularies (i.e., ontologies, reference data models, or metadata elements) and semantic mappings that can be used to annotate, describe and transform data sets. Moreover, the transformation of data sets can be provided as a separate service.
Data Space Governance Roles The data space governance roles coordinate the set of commonly agreed principles within an AI data space and manage the compliance of data space participants to these agreed principles. The data space governance roles provide the capabilities as associated to the 'agreement framework', which are sometimes also referred to as the 'trust framework'.
Data Space Authority AI data spaces, comprising of the previously described roles, may potentially grow very large. In these larger data space environments, in which not all participants may directly know each other, capabilities are needed to ensure that data sharing transactions between participants are according to an agreed upon protocol/approach and can be 'trusted'. The Data Space Authority is responsible for the (legal and operational) agreements within a data space and for certification of participants and components used within the data space.
Data Space Identity Provider The Data Space Identity Provider offers a service to create, manage, maintain, monitor, and validate identity information of participants and/or components in a data space. This is imperative for secure operation of the data space and to avoid unauthorised access to and usage of data.

It is to be noted that **Figure 3** also depicts the role of 'Identity Provider'. It provides the capabilities to identify and authenticate natural persons, organisations or software components as legal entities. This is a generic capability to be used by multiple business roles. As such, the role of 'Identity Provider' will not further be elaborated in the remainder of this report.

3. BUSINESS ARCHITECTURE

The business architecture encompasses a translation of the architecture vision architecture vision for AI data spaces (as described in the previous chapter) into business architecture principles, an interoperability framework and a business process framework for AI data spaces as addressed in the following sections, respectively.

3.1 Business architecture principles

The business architecture principles for AI data spaces are derived from the European ambition on federation of interoperable data spaces as expressed in the European Data Strategy [3] and the Open DEI guidelines therefore [19].

BA.1. Data is provided in a FAIR manner within AI data spaces

To stimulate the (re-)use of available data and to reduce the manual actions necessary to share and use data within and across AI data spaces, the FAIR principles [24] are adopted (to improve the Findability, Accessibility, Interoperability, and Re-usability of data assets). These principles are currently gaining major traction.

BA.2. Data can be a valuable asset and must be managed as such by means of both access and usage control

Data is an asset that has value to the enterprise and is managed accordingly. Data may be protected from unauthorised use and disclosure. Entitled parties are sovereign in determining who, how and when their data is shared and under which conditions. To this end, both access control (managing which participants are allowed access to the data) and usage control (managing what participants are allowed to do with the data) capabilities are supported.

BA.3. Full stack integrity is provided within AI data spaces

To ensure data sovereignty by the data entitled party, an AI data space provides full stack integrity. This means that it can be guaranteed (including possible certification of software) that data access and usage policies can be technically enforced while sharing data and all elements involved in the sharing and processing of data are sufficiently secured (e.g. using encryption and isolation).

BA.4. Various AI-collaboration models may be supported within an AI data space

AI data spaces can be enabled to simultaneously support the processes and interactions between the participants in the business role model for the four AI collaboration models as described in the overarching AI data space reference guide [1], section 6.3, and re-enumerated in paragraph 2.1: Data Sharing, Algorithm Sharing, Third Party Processing and Network Processing.

BA.5. AI data spaces enable its participants to share and (locally) run data apps

The support of data apps (e.g. for semantic transformations or data pre-processing) is an integral part of an AI data space. Therefore an AI data space should enable its participants to share and execute data apps. It must be possible

to execute data apps locally, e.g. within the security domain of the data services provider or the AI operator. Data apps can be shared and provisioned by the App Store Provider.

BA.6. A single point of entry provides access to each data service in the federation of AI data spaces

To prevent the major integration efforts from having to connect to multiple data sharing environments, a single entry point gives participants access to *each data service provided* by a participant within any AI data space instance of the overarching federation. The single point of entry improves user friendliness and lowers the barriers for adoption.

3.2 Data space interoperability framework: intra and inter data space interoperability

As the ambition of the European Data Strategy ('*Towards a federation of interoperable data spaces*', see section 2.1) expresses, both interoperability within individual data spaces and interoperability between multiple data spaces need adequate governance, architectures and building blocks. These are referred to as intra and inter data space interoperability, respectively:

- *Intra data space interoperability*: Individual data spaces have a high degree of autonomy in developing and deploying their own internal agreements and architecture. Intra data space interoperability focusses on the alignment of the various capabilities (building blocks) within an individual data space.
- *Inter data space interoperability*: Interoperability between multiple data spaces is key for the federation of data spaces as expressed in the ambition of the EU Data Strategy. Inter data space interoperability requires alignment and guidelines for individual data spaces to ensure interoperability between them.

Figure 4 illustrates the concepts of intra and inter data space interoperability.

Data space interoperability is more than merely the interoperability of technical modules. As described in the overarching reference guide report [1]. An approach to systematically categorize the interoperability aspects is provided by the new European Interoperability Framework (EIF) as developed by the European Commission [25]. As **Figure 5** depicts, the EIF distinguishes four interoperability levels (technical, semantic, organisational and legal) under an overarching integrated governance approach.Each of the four EIF interoperability levels needs to be addressed in developing the interoperability architecture for data spaces, both for intra and inter data space

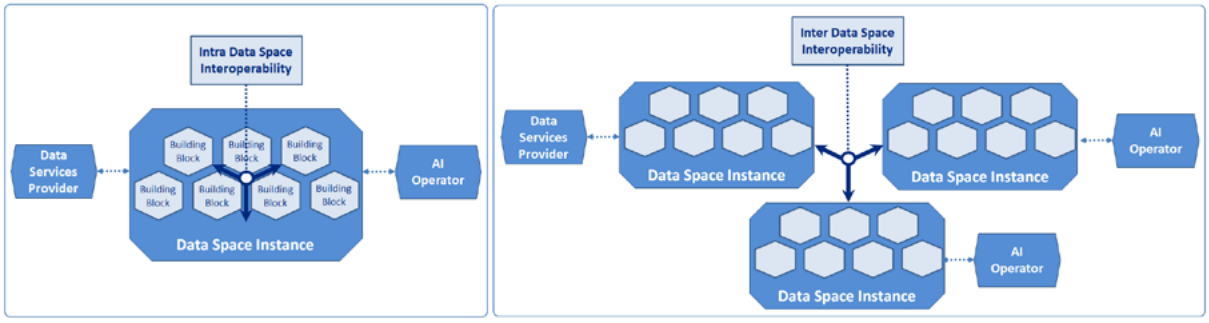

Figure 4 - Intra (l) and inter (r) data space interoperability.

interoperability. Moreover, multiple interoperability aspects can further be distinguished within each of the four levels of the EIF, as described in the right column in the figure and described in the following paragraphs.

3.2.1 Technical level

The technical level covers the software and hardware modules for controlled, sovereign and secure sharing of data. It consists aspects that require adequate governance:

- *Secure (peer-to-peer) connectivity*

  The secure communication protocol handles aspects such as encrypted message exchange, session management between end-points and remote attestation of end-points. It is also referred to as the handshake protocol. A security gateway (or connector) may be used for realising Secure (peer-to-peer) connectivity.

- *Identity, authentication and authorisation (IAA)*

  Within an AI data space, identification and authentication are done at two levels:

  - As *legal identities,* to identify and authenticate natural persons, organisations or software components as legal entities.

  - As *AI data space members*, to administer actual membership of legal entities of a data space and (as such) adhere to its (legal) agreements. At run-time, a data sharing transaction may include a process for verification of legal identity and status of participants, including its AI data space membership.

  Authorisation encompasses the management of (*access and usage control*) policies, including their definition, registration and enforcement. The access control policy states which organisations, roles or systems are allowed access to the data provided. The usage control policy states what participants are allowed to do with the data provided. The policies can express both the data services provider's or data entitled party's internal (business) data sharing policies and the external (regulatory) policies.

- *Generic data space information model*

  The data space information model defines the semantics used as basis for communicating between data space participants. It is the basic semantic model used by data space participants to model metadata. It enables the security gateway for controlled and secure data sharing with (security gateways) of other data space

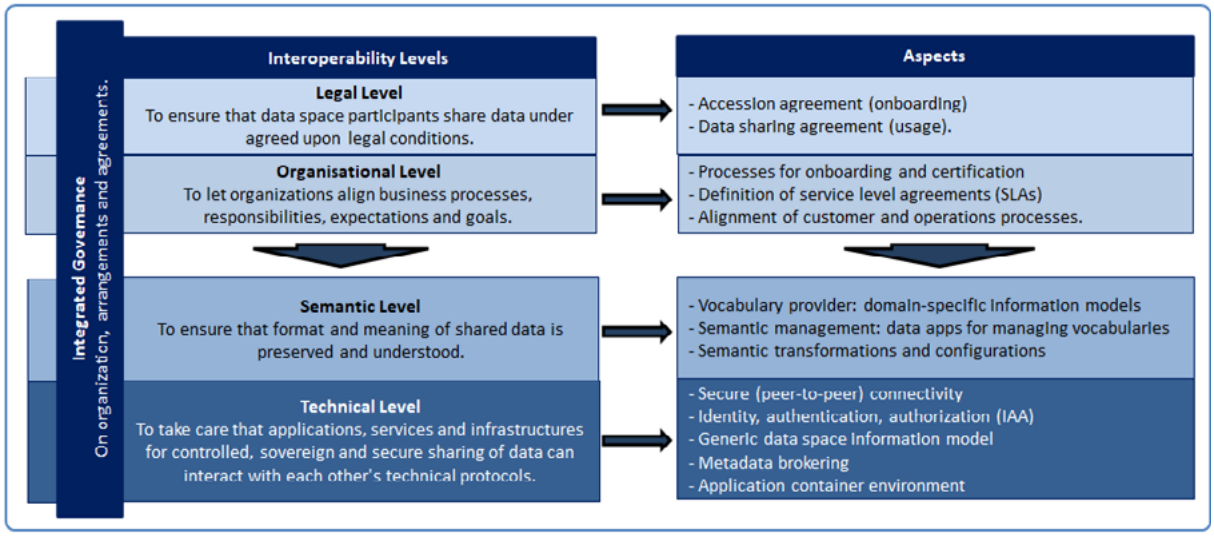

Figure 5 - Intra (l) and inter (r) data space interoperability.

participants. Moreover, it allows the security gateway to publish the provided data service in a metadata broker using self-description capability.

- *Metadata brokering*

  Metadata brokering entails the management, registration and publication of the resources available in a data space (e.g. data sets, data services, algorithms and computing capabilities) and to make these registered resources searchable and available within and across data spaces. *A metadata broker* provides these capabilities within a single data space instance. Through federation, the metadata brokers can be virtually acting as a 'single' overarching broker across multiple data space instances.

- *App enabling*

  To enable ease of deployment of (third party) data apps, an Application Container Environment (ACE) is needed together with a capability for automated data app deployment orchestration (which can be controlled by orchestration functionality provided by the security gateway). The deployment orchestration capability should interwork with the security gateway's framework to manage data usage policies. ACE can for instance be implemented on top of cloud/edge processing capabilities with capabilities for advanced data control and data sovereignty. It may be used for deploying the (local workers) for the network processing collaboration model as described in section 2.2.

3.2.2 Semantic level

Individual AI data spaces instance may enrich the (generic) data space information model with *domain-specific information models*. In general, such domain-specific information models will be provided by domain-specific *Vocabulary Providers*.

At the semantic level, it may be obvious that a common semantic model (e.g. a common domain-specific information models) used by both data services providers and data services consumers has major advantages in minimising complexity for interconnection and collaboration. However, such a jointly used common semantic model will appear to be an utopia. Therefore, capabilities for *semantic management* need to be supported in the data space architecture. This may be taken care of by means of a vocabulary hub (to manage, register and publish vocabularies, i.e. ontologies, reference data models, or metadata elements) and semantic transformation apps enabling easy-to-use mappings between semantic models.

3.2.3 Organisational level

The organisational level refers to the way in which the agreements, processes and expectations are aligned, monitored and managed to achieve the common goals for controlled data sharing within a data space instance. This includes the processes for *onboarding and certification* (according to common and accepted criteria), definition of service level

agreements (for realising overarching expectations and quality control) and alignment of operations and *customer processes* (for improved operating efficiency and enhanced customer experience).

3.2.4 Legal level

Within the legal framework of an AI data space, in general both an accession agreement (i.e. a contract between all participants and the scheme owner of the AI data space) and transaction specific legal agreements (further referred to as '*data service transaction agreements*').

By signing the accession agreement, a party becomes a participant of the data space and has to adhere to the overarching legal agreements as part of its scheme. The accession agreement may refer to terms-of-use which define the rights and obligations of every participant and the scheme owner. They state the requirements that participants should comply with at any time, and from which they will not be able to deviate. These are the requirements that deal with the proper functioning of the data space and its scheme.

The data service transaction agreements apply to the conditions and (access and usage) policies under which specific data sharing transactions are executed. These polices may be defined by the entitled party in a policy registry. Under the accession agreement, the data sharing parties are legally bound to adhere to the agreed upon policies for specific data sharing transactions as expressed by means of these data service transaction agreements. In this manner, a hierarchical construction of legal agreements applies.

Currently, legal aspects are mainly dealt with (within a specific data space instance) by pre-defining these (multi-lateral) legal accession when on-boarding a data space. Alternatively, international architecture initiatives on federative data sharing (e.g. IDSA, Gaia-X) consider capabilities for negotiation of legally binding agreements per data sharing transaction[1]. An architecture for contract negotiation of legally binding agreements per data sharing transaction and policy enforcement to manage usage policies is developed. These developments still have to prove their technical and market viability for large scale deployment.

3.3 Towards a business process framework for AI data spaces

The wide-scale adoption of data sharing for AI can be facilitated and stimulated with an aligned and accepted overarching AI data space process framework. For instance, the enhanced Telecommunications Map (eTOM) business process framework [26] has previously been successfully developed and applied for aligned development of support and management capabilities for offering (other) telecommunication services.

There are various potential benefits of a business process framework for AI data spaces. Firstly, it helps to create overview and completeness in identifying all capabilities for data sharing for AI and as such provides guidance to the development of a 'logical' modular IT architecture for data sharing for AI in terms of the capabilities to be provided to be supported by each of the AI data space roles and its constituting building blocks. Secondly, it paves the way to interoperability by providing the requirements

1 To be legally valid, the Dutch law prescribes three steps that have to be gone through when engaging into a data sharing agreement in an electronic manner. It starts with an offer that the data services provider makes to the data services consumer. That offer may subsequently be accepted and that acceptance must on its turn be confirmed by the data services provider. As long as the confirmation has not been received, the data services consumer may cancel the agreement. Failure to confirm an offer in time counts as a rejection thereof. In case the data services consumer doesn't accept the offer, he may return a new. This process is referred to as the 'contract negotiation process'.

for the definition of the Application Programming Interfaces (APIs) exposing the capabilities of each of the building blocks in AI data spaces, and thereby reduces the costs of integration.

Within the context of the business role model for AI data spaces as depicted in **Figure 3**, the processes as defined and elaborated in the business process framework should enable and support the four AI-collaboration models as have been identified in section 2.2. As **Figure 3** depicts, the following main high-level processes are distinguished as being part of the AI data space process framework:

- *authorisation management,*
- *orchestration of AI algorithm execution,*
- *AI algorithm result sharing,*
- *data sharing*, and
- *AI algorithm sharing.*

It is noted that the initial three of these main high-level processes for AI data spaces are expected to be applicable to each of the four AI-collaboration models, whereas the applicability of the latter two (in italics) depends on the AI-collaboration model that is actually being implemented.

The business process framework for AI data spaces contributes to efficient and cost-effective development and deployment of AI data spaces. This may apply to both the usage (i.e. run-time execution of data sharing and processing transaction) and operations (i.e. management and onboarding) behaviour of AI data spaces.

The business process framework for AI data spaces is out-of-scope of this report and is considered in the roadmap for AI data spaces in chapter 9 for future development

PART B: BUILDING BLOCK ARCHITECTURE

The building block architecture provides a decomposition of the ecosystem architecture into a set of IT-modules, referred to as building blocks. It encompasses the phases C and D of TOGAF ADM [15]. Chapter 4 addresses the information systems architecture, providing a breakdown of the inter AI data space interoperability architecture into building blocks. Chapter 5 addresses the technology architecture for the individual buildings blocks.

4. INFORMATION SYSTEM ARCHITECTURE

The Information Systems Architecture (ISA) gives a breakdown of the intra AI data space interoperability architecture into building blocks, jointly implementing the capabilities for realising the AI-collaboration models and the business role model for AI data spaces (as elaborated in the architecture vision in chapter 2) and the business architecture principles and approach (as defined in chapter 3).

4.1 Information System Architecture principles

The Information System Architecture (ISA) deploys a set of principles for realising the business vision and business architecture principles for intra AI data space interoperability as defined in the previous chapters. Moreover, these principles are aligned with the Open DEI design principles for data spaces [19]:

ISA.1. AI data space capabilities are provided by means of interoperable building blocks

Building blocks implement the capabilities as provided by the core and enabling business roles. The building blocks in an AI data space are interoperable at each of the interoperability levels introduced in section 3.2.

ISA.2. The capabilities of building blocks are exposed as services by means of Application Programming Interfaces (APIs), providing a service-oriented approach for AI data space capabilities

A variety in options exists for realising the capabilities of the building blocks in an AI data space. The options (strongly) depend on varying user needs. To support various options, a service-oriented architecture is to be adopted, with options to provide an adequate service portfolio for maintaining sovereignty by the entitled parties over their sensitive (meta) data.

ISA.3. The ISA and its building blocks is based on the IDS Reference Architecture Model (IDS RAM)

International Data Spaces (IDS) is currently gaining major international traction for realising federated and interoperable data spaces. In a previous assessment by the NL AIC WG Data Sharing [9], the selection of the IDS Reference Architecture Model (RAM) [22][23] as basis for AI data spaces has been motivated.

ISA.4. Data sovereignty and control are based on standardised frameworks

Data sovereignty requires the definition, management and support of adequate data sharing policies and the enforcement thereof. Standardised frameworks are required for interoperability in a federation of interoperable AI data spaces.

ISA.5. ICT-resource sharing policies (e.g. on data and AI algorithms) are defined by entitled parties and can be managed by means of the capabilities (building blocks) in the AI data space

AI data spaces allow entitled parties to administer usage policies for sharing ICT-resources (e.g. data, AI algorithms, data apps) in the system in a machine and human readable format. They make it possible to take policy enforcement decisions during the dynamic sharing process, based on the administered usage policies and to trigger actions in the case policies are violated, Moreover, it should be possible to delegate responsibilities on definition of usage policies to other participants.

ISA.6. The metadata of ICT-resources within an AI data space is managed and may be exposed

AI data spaces contain metadata on available IC- resources such as data space participants, data sources, data sharing policies, delegation information, AI algorithms, data apps, processing capabilities and data transactions loggings. This metadata can be managed and exposed, e.g. by means of (various types of) registries. The registries should provide APIs for easy registration and discovery of relevant metadata.

For the definition of metadata of available ICT-resources the IDS Information Model is used within an AI data space, where possible and applicable. This will enable the participants to easier find and share their resources and helps in the interoperability.

ISA.7. Transaction logging

All performed data sharing transactions should be logged for analysis, maintenance, audit and billing purposes.

4.2 Demarcation of AI data spaces

The business vision and architectural principles for AI data spaces (as described in the previous sections) form the basis for developing the AI data spaces. They provide the basis for realising interoperability and trust in a federation of AI data spaces, both within (intra) and across (inter) data spaces.

The demarcation of an AI data space and intra AI data space interoperability starts with the definition of a data space. A multitude of definitions of data spaces is currently available. For the NL AIC working group Data Sharing, we adhere to the definition of a data space as provided by the Open DEI initiative [18] in its design principles for data spaces report [19]. It defines a data space as a '*decentralised infrastructure for trustworthy data sharing and exchange in data ecosystems based on commonly agreed principles*'.

Figure 6 depicts the demarcation of an AI data space and intra AI data space interoperability in relation to the internal data pipeline of a data services provider and inter AI data space interoperability.

The middle part of the figure shows an AI data space by means of its business role model as described in paragraph 2.1. It shows the following demarcation features:

- *Demarcation of an AI data space with the internal data pipeline of a data services provider*

  A data services provider exposes its data as a data service through a well-defined API. Preparing the data for sharing over the data service API is a data services provider responsibility. As such, the data service API provides the point of demarcation between the data services providers domain and the AI data space. This demarcation should not be interpreted as demarking different ICT

environments. The internal data pipeline of the data services provider is out-of-scope for the intra AI data space reference guide in this report.

Making use of a common and agreed upon (semantic) API to expose data for AI will make integration more efficient and provide opportunities for improved machine-to-machine (M2M) automation.

- *Demarcation of an AI data space with other data spaces: intra and inter AI data space interoperability*

  As the Open DEI definition (as cited above) states the basis of a data space is formed by a set of commonly agreed principles. Furthermore, as described in [1] and depicted in the figure, such a set of commonly agreed principles cover more than merely the technical aspects. To achieve interoperability by means of a set of commonly agreed principles, an approach is provided by the new European Interoperability Framework (EIF) as developed by the European Commission [25]. The framework distinguishes four interoperability levels (technical, semantic, organisational and legal interoperability) under an overarching integrated governance approach.

For the elaboration of AI data spaces we adhere to this approach:

- *Intra data space interoperability* describes the set of commonly agreed principles for developing AI data spaces, including each of the four interoperability levels (technical, semantic, organisational and legal interoperability) of the EIF.

The reference guide for intra AI data space interoperability is elaborated in the remainder of this report.

- *Inter data space interoperability* addresses the cases in which interoperability for AI data spaces conforming to the set of commonly agreed principles (as described in this report) needs to be realised with an organisation or building block that doesn't adhere to these principles, either at the technical, semantic, organisational or legal level.

The reference guide for inter AI data space interoperability is elaborated in the companion report [2].

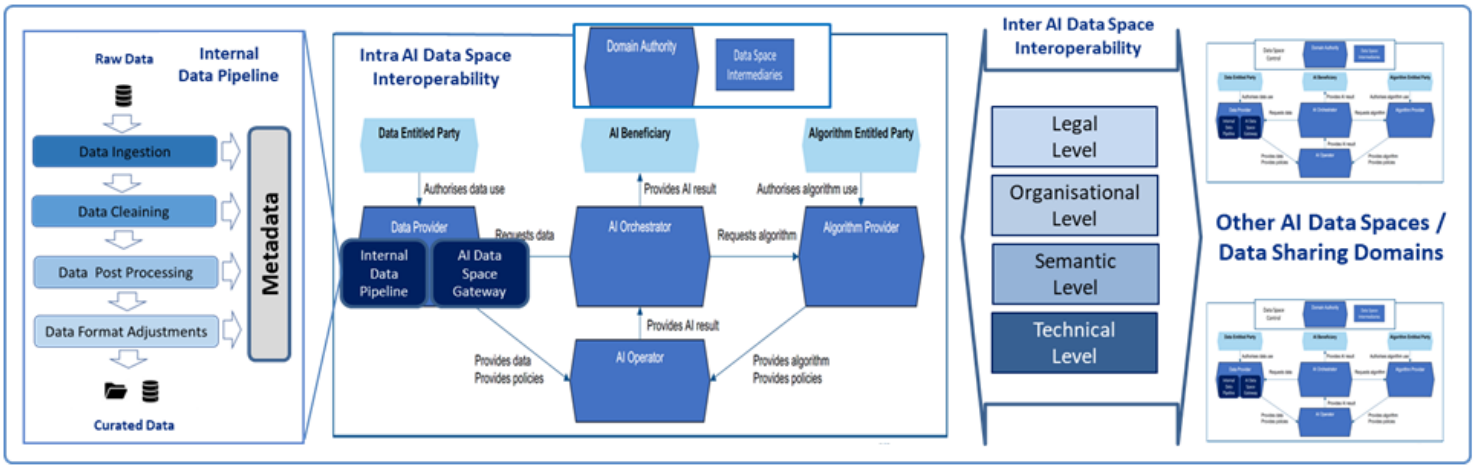

Figure 6 - Demarcation of an AI data space and intra AI data space interoperability (middle) in relation to the internal data pipeline of a data services provider (left) and inter AI data space interoperability with other AI data spaces (right).

4.3 Building blocks

In the ISA, the building blocks required for realising the capabilities for the various roles in the business role model are defined. A building block provides a generic software implementation of a capability to be performed by a role in the business role model for intra AI data space interoperability.

The Open DEI initiative [18] distinguishes three types of building blocks as part of the soft infrastructure in its design principles for data spaces report [19]:

- building blocks such as *data platforms*, providing support for effective data sharing and exchange as well as for engineering and deployment of data exchange and processing capabilities;
- building blocks such as *data marketplaces*, where data services providers can offer and data services consumers can request data, as well as data processing applications;
- building blocks *ensuring data sovereignty*, i.e. the ability for each stakeholder to control their data by making decisions as to how digital processes, infrastructures, and flows of data are structured, built and managed, based on an appropriate governance scheme enabling specification of terms and conditions.

Moreover, the Open DEI soft infrastructure use categorisation of technical building blocks into the verticals 'Interoperability', 'Trust' and 'Data Value' (see **Figure 8**). Aligned with this categorisation, Table 2 provides the categorised overview of the building blocks in the ISA for intra data space interoperability.

Table 2: Building Blocks in the ISA for Intra Data Space Interoperability.

Data Space Trust Architecture Building Blocks: Data Sovereignty Management Capabilities enabling data sovereignty for the entitled party of data or AI algorithms, guaranteeing that data sharing policies (i.e. access and usage control policies) can be defined and technically enforced.
Security Gateway Provides the fundament for a data space. It enables (standardised) data sharing capabilities between data space participants with a secure environment to find and execute data apps, whilst maintaining data sovereignty for entitled parties.
Policy Enforcement Framework Technically enforces the applicable policy conditions (e.g. specific access and usage policies) within the security environments of the (combination of) Data Services Provider and/or Data Services Consumer.
Policy Registry Manages and registers the applicable policy conditions, i.e. the specific access and usage rights for data space participants as attributed by entitled parties to data services or AI algorithms, including delegation thereof to other data space participants.

Application Container Environment Provides the capabilities to deploy and execute data apps and/or AI algorithms in a secure and controlled manner. This may be either in the security environment of the Data Services Provider or Data Services Consumer or in a secure environment provided by a third party (e.g. an AI Operator).
Data Space Trust Architecture Building Blocks: Identity Management Capabilities to manage the various types of identities within a data space, jointly providing the foundation for the trust architecture.
Data Space Membership Certificate Authority System: DS CAS Provides certificates for participants and/or software components involved in data sharing within a data space, e.g. to be used for verifying data space membership when performing a data sharing transaction.
Dynamic Attribute Provisioning Service: DAPS Manages and registers the dynamic attributes of software modules implemented by means of a security gateway, including the security profiles, certification status, …
Participant Information System: ParIS Manages and registers the attributes of the participants, specifically for natural persons or organisations as legal entities, including the name and address details, chamber of commerce number, …
Data Space Semantic Interoperability Architecture Building Blocks Capabilities to define, expose, find and manage the ICT-resources within and between data spaces, including for managing semantics transformations.
Data Space Metadata Broker Manages, registers and publishes the ICT-resources available within a data space, e.g. data services, AI algorithms and computing resources.
App Store Manages, registers and publishes data apps. These can be deployed within a security gateway. data apps facilitate data processing workflows.
Vocabulary Hub Registry service providing facilities for publishing, editing, browsing and maintaining vocabularies and related documentation. Vocabularies incl. ontologies, reference data models, schema specifications, mappings and API specifications that can be used to annotate and describe data sets and data services. The vocabulary hub can mirror a set of third party vocabularies ensuring availability and resolution.
Semantic Transformation Engine Provides semantic transformation services between data formats. It uses vocabularies and mapping specification as provided by the vocabulary hub. The component can be integrated at the data services consumer or data services provider implementation or offered as a service in a data space.
Data Space Connector Semantics Configurator Service to enable data space participants to use vocabularies to configure the semantic interoperability of data space connector implementations. This is primarily done by creating ontology based API specifications to specify the semantic interface between data services provider and data services consumer. Additionally the data space connector configurator can assist in creating mapping specifications if needed. These can be used in the semantic transformation engine.

Data Space Value Creation Architecture Building Blocks Capabilities to create value from data sharing in a data space and to valorize data transactions through registration of data sharing contracts and transactions and through accounting and monetisation thereof.
Contract Manager Provides capabilities to support the offering of data resources and services under defined terms and conditions, including the management of processes linked to the creation and monitoring of smart contracts, which clearly describe the rights and obligations for data and service usage, and access to data and services.
Clearing House Handles all required pre-conditions before (sensitive and/or valuable) data can be shared. These pre-conditions may include both confidentiality aspects (e.g. for non-repudiation) or financial aspects (e.g. financial settlement). As such, a specific capability for the clearing house can be event-driven (real-time) data flow control, e.g. based on smart contracting. Moreover, the clearing house may also register and monitor data sharing transactions, e.g. as input for conflict resolution.
Billing Engine Provides the capabilities for the billing process associated to data sharing transactions, e.g. generate invoices and manage the payment process.

Figure 7 shows how the building blocks can be attributed to each of the roles in the business role model for intra AI data space interoperability for deployment.

It is noted that a security gateway as building block in the data space core roles has a different shading than the security gateway as building block in the data space intermediary and the data space software and services roles. Moreover, it is not included as building block in the data space governance roles. This illustrates that (1) the actual added value and use of the security gateway building block differs per category of roles and (2) that the capability it provides may differ per category of roles. The considerations and guidelines on the role and deployment of a security gateway building block for each of the (categories of) business roles are further elaborated in chapter 7 on the trust interaction model.

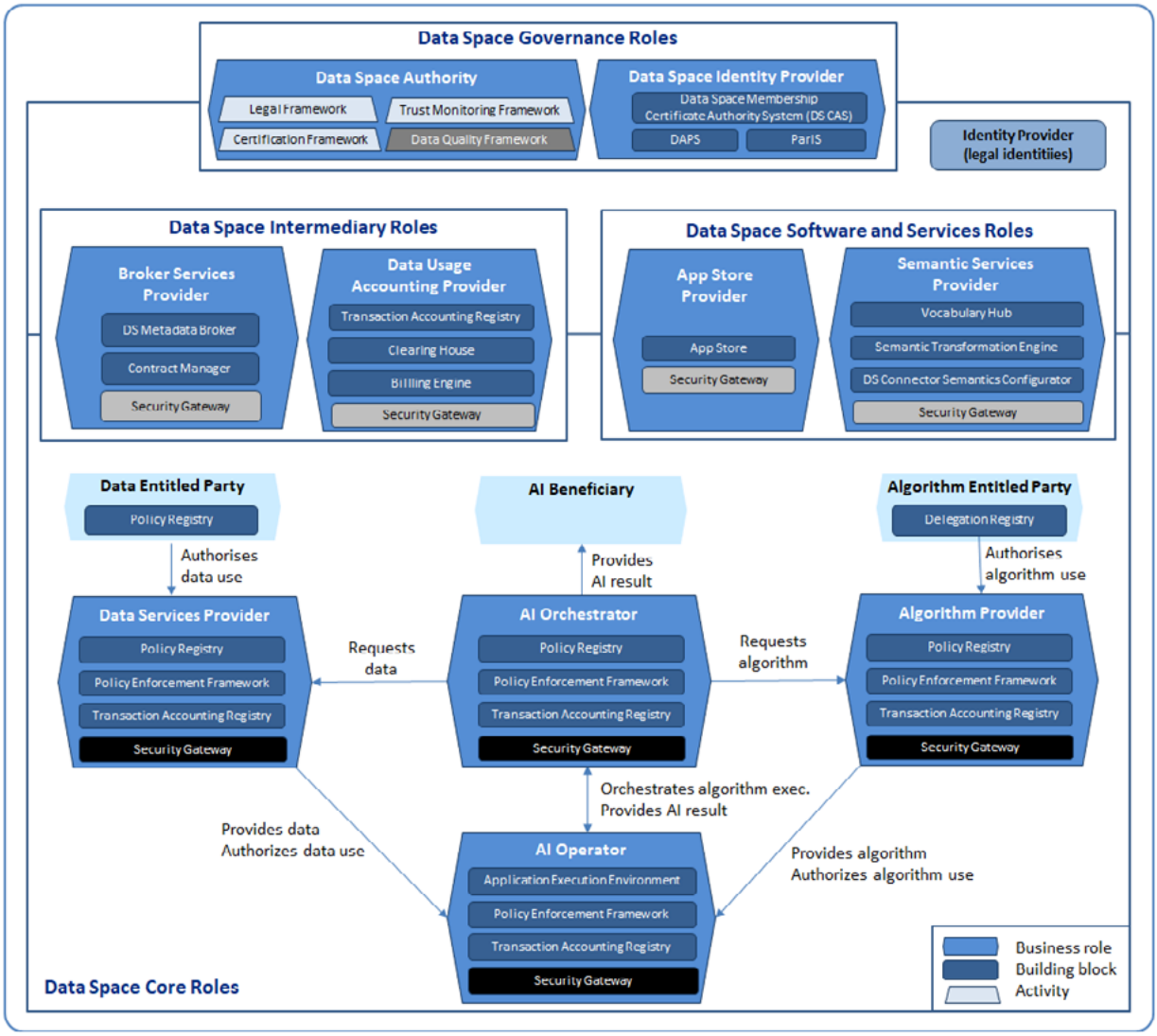

Figure 7 - Attributing building blocks to the roles of the business roles for intra AI data space interoperability.

5. TECHNOLOGY ARCHITECTURE

The technology architecture describes the architecture development and the design approach for each of the buildings blocks as defined in the ISA. After addressing the technology architecture development approach in the following section, the subsequent sections in this chapter elaborate the architecture and design for each of the categories of building blocks for each of the building blocks as listed in Table 2, i.e. the trust architecture building blocks for data sovereignty management, the trust architecture building blocks for data identity management, the semantic interoperability architecture building blocks and the value creation architecture building blocks, respectively. Each of these sections addresses both the functionality of the building blocks, the alignment with EU reference architecture initiatives and the implementation aspects (in terms of architecture, design and open-source modules).

5.1 Technology architecture development approach

The technology architecture development approach is elaborated in the following paragraphs in terms of the technology architecture principles, the alignment with EU reference architectures on federative data sharing and data spaces and a development proposal for the individual building blocks from the perspective of the NL AIC working group Data Sharing.

5.1.1 Technology architecture principles

For the realisation of the building blocks defined in the Information System Architecture (ISA) in the previous chapter, the following set of technology architecture principles is used:

TEC.1. The building blocks as described in ISA expose their capabilities by means of well-defined Application Programming Interfaces (APIs)

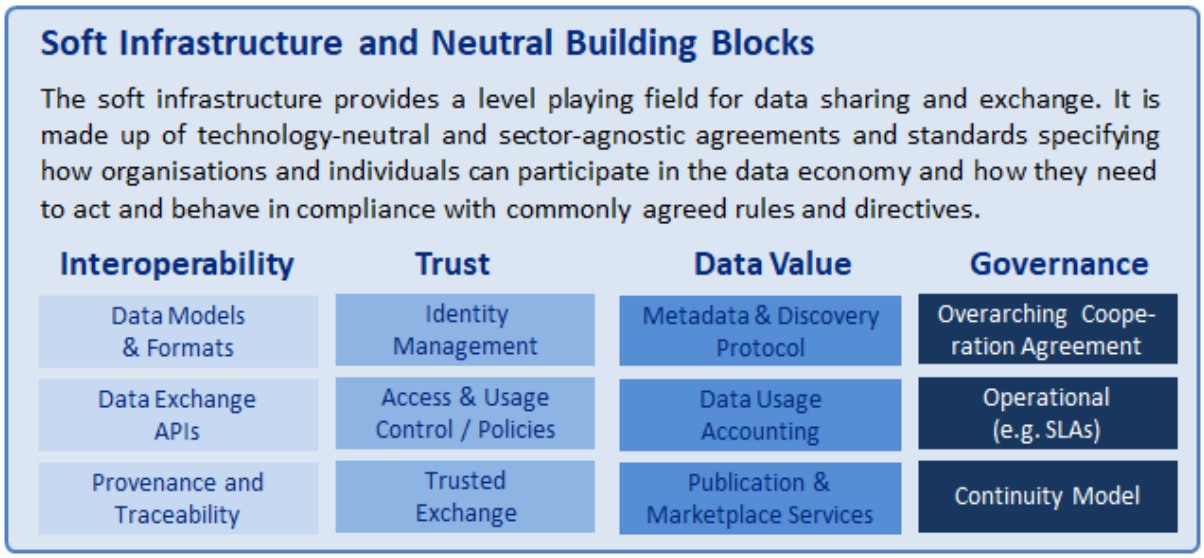

Figure 8 - Attributing building blocks to the roles of the business roles for intra AI data space interoperability.

As also addressed by the ISA architecture principles in section 4.1, a service-oriented architecture is to be adopted with services being exposed as well-defined APIs on their associated building blocks. As such, the building block APIs form the basis for the technology and solution of AI data spaces, with the building blocks providing realisations of these APIs.

TEC.2. For maintainability, the set of interoperability APIs for AI data spaces should be limited

By limiting the set of prescribed APIs for AI data spaces the governance and management efforts for maintaining the AI data space architecture and guidelines can remain under control. Moreover, it limits the technological diversity to be controlled and minimizes the non-trivial cost of maintaining expertise on interoperability between AI data spaces.

TEC.3. Reference implementations of AI data space building blocks should be open source and future proof

Usage of widely used and actively updated open source software will help to reduce cost of development and maintenance. Furthermore, the tools used as part of the reference implementations of AI data space building blocks should be future proof. It is therefore important to only select software modules that are well maintained, widely used and expected to be widely adopted within the market.

TEC.4. The IDS Information Model is used for metadata support within AI data spaces

For the description of ICT-resources such as data space participants, data sources, data sharing policies, delegation information, metadata will be used that can describe not only the syntax and serialisation, but also the semantics of the involved data. By default (and when possible) the IDS Information Model is used to describe the metadata.

TEC.5. Multiple versions of metadata standards for ICT-resources should be supported and manged

Participants of the data space will metadata on ICT-resources in different versions of the information model, which should be simultaneously supported, maintained and managed as such.

TEC.*6. Building blocks should be developed to be federable over multiple AI data spaces*

To allow AI data spaces to be easily connected, it is important that building blocks (where applicable) are developed to be federable over multiple AI data space instances. The aspect of federable building blocks is further addressed in the companion report [2].

5.1.2 Alignment with EU reference architectures on federative data sharing and data spaces

The European Data Strategy [16] (see also section 2.1) and various associated EU initiatives work on defining and aligning federative data sharing and data space reference architectures and developing reference implementations for their enabling building blocks.

A main initiative defining the policy, approach and building blocks is the EU Open DEI initiative [18]. With the aim to support the creation of common data sharing infrastructures based on a unified architecture and an established standard, it has defined (the scope of) a data space in the context of

the European Data Strategy and has elaborated the data space concept in terms of a soft infrastructure consisting of 12 building blocks [19] as depicted **Figure 8**.

As the figure shows, the Open DEI soft infrastructure distinguishes between technical building blocks (in the verticals 'Interoperability', 'Trust' and 'Data Value') and governance building blocks (in the vertical 'Governance').

The figure shows that trust and its associated building blocks are a key and integral part of the data space concept. Jointly they can be referred to as a trust framework. Open DEI defines a trust framework as '*a structure that lets people and organisations do business securely and reliably online*'. Typically, a trust framework includes capabilities for overarching legal agreements between participants in a data space, for transaction specific legal agreements (further referred to as '*data service transaction agreements*') and for data sovereignty management. The trust architecture for AI data spaces is further addressed in Part C of this report.

The Open DEI soft infrastructure and its building blocks have been identified and described at a high abstraction level. Technical specification and elaboration of the building blocks are done by various European initiatives on reference architectures and implementations. The most noteworthy of these EU initiatives are:

- The *International Data Spaces Association (IDSA) initiative*, having developed a reference architecture model for data spaces [22][23]. The IDS data space architecture leverages existing standards and technologies as well as governance models for the emerging data economy. It facilitates secure and standardised data exchange and data linkage in a trusted (business) ecosystem, thereby providing a basis for creating smart service scenarios, while at the same time guaranteeing data sovereignty for data owners. The IDSA GitHubs provide both a repository with the specifications for the IDS components [27] and an overview of repositories with IDS open source components [28].
- The *Gaia-X initiative* having the goal to establish an ecosystem in which data is made available, collated and shared in a trustworthy environment in which entitled parties always retain sovereignty over their data [29]. It develops a software framework of control and governance and implements a common set of policies and rules that can be applied to existing cloud/edge technology stacks to obtain transparency, controllability, portability and interoperability across data and services. The Gaia-X architecture aims at a set of interconnected data and infrastructure ecosystems, enabled by a set of Gaia-X Federation Services (GXFS) [30]. The Gaia-X Federation Services are services used for the operational implementation of a Gaia-X Data Ecosystem. They are categorised into four groups: Identity & Trust, Data Sovereignty Services, Federated Catalogue and Compliance.
- The *FIWARE initiative* brings a curated framework of open source software platform modules, building around the FIWARE Context Broker. A suite of complementary open source FIWARE Generic Enablers is available, dealing with (amongst others) the building blocks for 'Context Data/API management, publication, and monetisation' for the support of usage

control and the publication and monetisation part of managed context data. An overview of FIWARE open source modules (i.e. the FIWARE Generic Enablers) can be found at [31].

- The *iSHARE initiative* provides a trust framework for data spaces. iSHARE originates from the logistics sector in the Netherlands [32] and is expanding towards other sectors and application areas as well. Moreover, iSHARE provides trust framework capabilities for sharing data both within a single data space and across multiple data spaces [33], i.e. for both 'intra' data space interoperability and for 'inter' data space interoperability (as addressed in the companion report [2]). For enabling data spaces iSHARE currently provides legal framework, trust registration and administration, discovery and inter data space interoperability capabilities [33].
- The *Data Space Business Alliance (DSBA) initiative* [34] that has recently started and in which the International Data Spaces Association (IDSA) and Gaia-X work together with the Big Data Value Association (BDVA) and the FIWARE Foundation towards an aligned and coherent architecture for data spaces. As such, the work of the DSBA has resulted in a technical convergence proposal [35]

These reference architecture initiatives are developing towards fully distributed trust framework capabilities for identity, authentication and authorisation (IAA), contract negotiation and usage control. They are expected to provide an alternative for the more centralised building block definitions for the data space trust framework as described in the following sections. Moreover, it is to be expected that these various approaches and solutions for realising these data space building blocks will coexist. In view of these developments it is advised that further development of the (building blocks) for the AI data space architecture is accompanied by:

1. a vision and roadmap on whether and how develop and align its trust framework capabilities with the developments on alternative, fully distributed, trust framework capabilities, and
2. migration scenario's providing data space participants a smooth and seamless (service and technical) evolution trajectory for these developments.

Finally, the EU has recently started the SIMPL initiative [36] under its EU DIGITAL Work Programme. The goal of SIMPL is to develop an open source cloud-to-edge middleware platform, supporting all major data initiatives funded by the European Commission, such as common European data spaces. An architecture vision document [37] has been developed for SIMPL as part of its preparatory work in view of the procurement of the open source cloud-to-edge middleware platform.

5.1.3 Elaborating the building blocks

In the following sections, each of the individual building blocks as listed in section 4.3 is elaborated, addressing both the functionality, the alignment with EU reference architectures and the (open-source) implementation, respectively:

- *Functionality: capabilities and APIs*
  This paragraph describes the main capability as provided by the building block. Each of the building blocks as listed in section 4.3 exposes its capabilities by means of well-defined Application Programming Interfaces (APIs). The APIs for each of the building blocks are distinguished into:

- Usage APIs, exposing the capabilities of the building block to be used part of a data transaction process flow.

- Federation API, allowing separate instances of a building block to mutually interconnect such that they jointly act as a single instance towards the users thereof. Federation is part of the ambition to evolve towards federated and interoperable AI data spaces and is further addressed in the reference guide for inter AI data space interoperability [2].

- Management API, exposing the capabilities for managing the building block, e.g. for configuration, onboarding and monitoring.

A building block managed by either a management API (for machine to machine interfacing) or a user interface (UI). The management API may be based on the Simple Network Management Protocol (SNMP), a widely used protocol for management of machines, servers and software. Both the management API and the UI are not elaborated as part of the building block as (1) they do not contribute added value to AI data space functionality or architecture, (2) they are solution and service provider specific and (3) their definition provides competitive advantages to the building block supplier.

- *Alignment with EU reference architecture initiatives*

  This paragraph assesses and proposes how the main capability of the building block for intra data space interoperability can and will be provided taking into account and adhering to the requirements, guidelines and/or reference implementations as being developed by the various EU initiatives on reference architectures for federative data sharing and data spaces, as enumerated in paragraph 5.1.2.

- *Implementation: architecture, design and open-source modules*

  This paragraph provides a high-level architecture overview of the building block. Where applicable, links to more detailed specifications and designs are included. In addition, links to open source open-source implementations may be provided.

5.2 Data space trust architecture building blocks: data sovereignty management

To ensure data sovereignty by the data entitled party implies that it can be guaranteed that data sharing policies (i.e. access and usage control policies) can be defined and technically enforced while all elements involved in the sharing and processing of data are adequately secured.

The paragraphs in this section subsequently describe the data space trust architecture building blocks for data sovereignty management, i.e. the security gateway, the policy enforcement framework, the policy registry and the application container environment, respectively.

5.2.1 Security Gateway

A security gateway provides the fundament for an AI data space. It provides capabilities for (standardised) data sharing between data space participants and a secure environment to execute data apps.

The security gateway is further elaborated in detail in annex C.

5.2.1.1 Functionality: capabilities and APIs

The security gateway provides the following capabilities:

- Manage and execute (containerised) data apps as part of its associated application container environment (ACE, see paragraph 5.2.4).
- Host a data app to read and write data from the local backend of a data services provider.
- Route the shared data to and from data apps executed within the application container environment (see paragraph 5.2.4).
- Route and thereby share data with the (security gateways of) other participants in the AI data space using standardised communication protocols.
- Encompass a policy enforcement framework (PEF, see paragraph 5.2.2) to enforce the data sharing policies as registered in the policy registry (see paragraph 5.2.3).
- Provide security and avoid unwanted interactions by assuring that data apps and the security gateway itself can only use specified and secure APIs.

Not all of the listed capabilities may be required for every security gateway. An extensive overview of the modules of a security gateway to support these capabilities is included in annex C.

A security gateway is a building block that can be deployed within the security domain of a data space participant (on local IT systems). It may be embedded software on devices/machines for IoT or smart industry applications or deployed on mobile devices or in a cloud (under the condition that the cloud can offer a sufficiently trusted IT environment).

5.2.1.2 Alignment with EU reference architecture initiatives

Within the IDSA's Reference Architecture Model (IDSA RAM) for data spaces [22][23], the security gateway is a key component, also referred to as IDS connector. It uses the standardised IDS Communication Protocol (IDSCP) interface for data sharing with the security gateway of participants, using the IDS Information Model. The IDS Information Model is an RDFS/OWL-ontology used for the generic description of ICT-resources such as data sets, data apps and data sharing policies.

Within the Gaia-X initiative, there is no concept of a security gateway. Nevertheless, it builds upon the so called Trust Services as part of the Gaia-X Federation Services [30]. Its Trust Services perform similar capabilities as provided by the security gateway. The most relevant is the Policy Decision Engine of Gaia-X that matches the policy enforcement framework as part of the security gateway capabilities as described in paragraph 5.2.2. Furthermore Gaia-X defines 'Resources' (as the end-points involved in data sharing) and 'Service Offering' (combining Resources and Assets) which could be a data set or a computational node. The resources are described by means of self-descriptions which can be exposed in a Gaia-X Federated Catalogue. As the security gateway supports self-descriptions, it will be important to align the IDS self-descriptions (as being managed and published in the data space metadata broker, see paragraph 5.4.1) with the Gaia-X self-descriptions (as being managed and published in a Gaia-X Federated Catalogue).

The iSHARE initiative doesn't specifically contain a separate security gateway building block. The iSHARE Authorisation Registry may be used to specify data sharing policies and can be integrated with the policy registry and/or the policy enforcement framework implemented inside the security gateway.

5.2.1.3 Implementation: architecture, design and open-source modules

In beginning 2023, alignment has started between two main developments for security gateways, i.e. for the IDS connector and the Eclipse Dataspace Connector (EDC [38]). It is expected that through the joint definition of the 'Data Space Protocol' in 2023, the implementations of both types of security gateways will become interoperable. In the remainder of this report, the IDS connector is used as reference.

For AI data spaces, the IDS connector as defined in the IDSA RAM can be used to implement the security gateway. **Figure 9** depicts the high-level architecture of an IDS connector as basis for the security gateway [22][23].

The individual modules of the IDS connector architecture as depicted in the figure:

- *Application Container Management*: In most cases, the deployment of the Connector Core Service(s) and data apps is based on application containers. Data apps are isolated from each other by containers in order to prevent unintended interdependencies. Using Application Container Management, extended control of data apps and containers can be enforced. In the reference architecture for AI data spaces as described in this report, the Application Container Management together with the Operating System and Virtual Machines/Hardware correspond to the Application Container Environment (ACE) building block as described in paragraph 5.2.4.
- *A Custom Container* provides a self-developed data app. Custom containers usually require no certification.
- *A Certified App Container* is a certified container providing a specific data app to be deployed in an ACE of the security gateway. The container with the data app may be provided by an app store as described in paragraph 5.4.2.
- *A Certified Core Container* contains a Connector Core Service which provides capabilities like data management, metadata management, contract and policy management, data app management, IDS protocols authentication, and many more. A more detailed elaboration of the modules within the core container are provided in annex C.

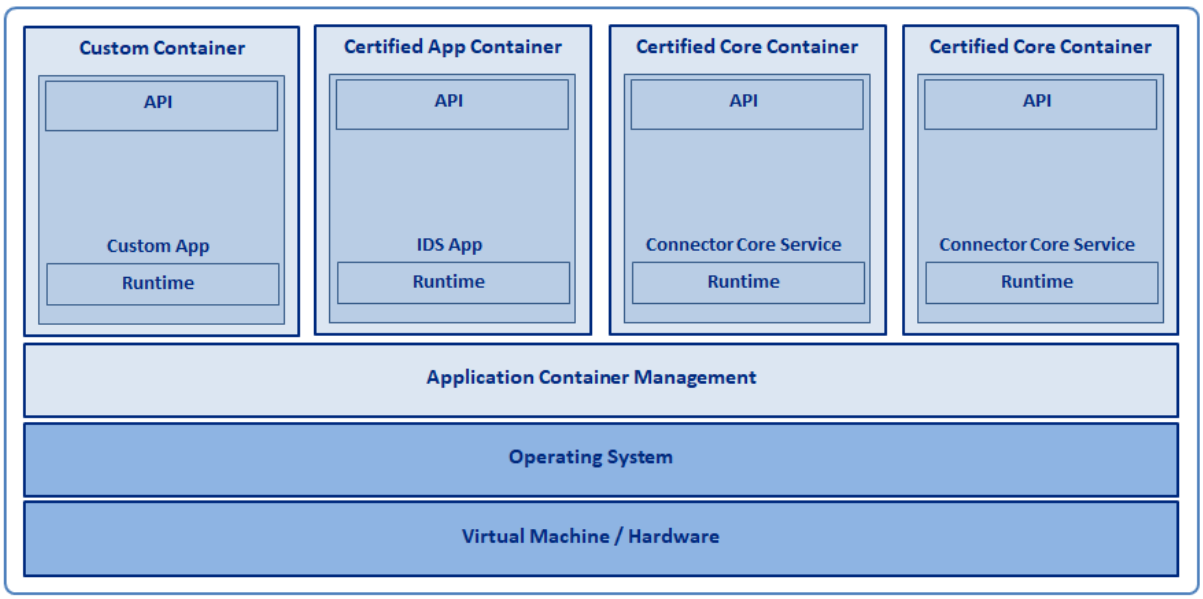

Figure 9 - Attributing building blocks to the roles of the business roles for intra AI data space interoperability.

- *An IDS App* defines a public API, which is invoked from the security gateway. This API is formally specified in a meta-description that is imported during the deployment phase of an IDS App. IDS Apps can be implemented in any programming language and target different run-time environments. Existing components can be reused to simplify a migration from other integration platforms.
- The *Run-time* of a custom or certified app/container depends on the selected technology and programming language. The Run-time, along with the application, constitutes the main part of a container. Different containers may use different run-times. From the run-times available, a service architect may select the one deemed most suitable.

Based on the architectures, standards and specifications as provided by the IDSA, organisations should be able to develop their own security gateways that may be used for AI data spaces. This may be done by re-using existing open source implementations. An up-to-date overview of open source IDS components is provided at the IDSA GitHub [28].

TNO has made an open source security gateway implementation with build-in features to support the architecture and building blocks of the AI data spaces as described in this report, which is referred to as the TNO Security Gateway (TSG). It is further described in annex C.

5.2.2 Policy Enforcement Framework (PEF)

5.2.2.1 Functionality: capabilities and interfaces

The Policy Enforcement Framework (PEF) building block in the security gateway manages and enforces data sharing policies to ensure data sovereignty and to increase trust between participants. It protects the involved participants in the sharing of data or AI algorithms against unintended and unauthorised usage of data and AI algorithms.

The eXtensible Access Control Markup Language (XACML) standard [38] is used to implement the PEF. The XACML standard defines a declarative fine-grained, attribute-based access control policy language. Furthermore, it includes an architecture and a processing model describing how to evaluate access requests according to the rules defined in policies. The XACML architecture for policy enforcement distinguishes a set of capabilities (and associated APIs) for managing and enforcing data sharing policies:

- the Policy Enforcement Point (PEP),
- the Policy Decision Point (PDP),
- the Policy Information Point (PIP),
- the Policy Retrieval Point (PRP), and
- the Policy Administration Point (PAP).

These capabilities and the associated APIs are further elaborated in paragraph 5.2.2.3.

5.2.2.2 Alignment with EU reference architecture initiatives

Although their implementation in modules differ, XACML based policy enforcement is included in both the IDS, Gaia-X, iSHARE and FIWARE architectures. Alignment will be required on the interfaces between the XACML capabilities and the definition language used for the policies. IDS has adopted the Open Digital Rights Language (ODRL) as policy definition language. ODRL is a powerful, flexible, semantics based standard for definition of policies. The various EU initiatives should align on ODRL for the definition of data sharing policies.

For assuring policy enforcement Gaia-X describes to the so called Continuous Automated Monitoring (CAM) capability, required for the highest assurance level called "High Gaia-X Assurance". This capability can be compared with the policy enforcement framework as part of the security gateway.

5.2.2.3 Implementation: architecture and open-source modules

Figure 10 depicts the PEF architecture as adopted by IDS. It introduces some extensions to the original XACML standard [39] as described in paragraph 5.2.2.1. It is similar to the IN2DUCE framework as proposed by Fraunhofer [41] and as aligned with the IDSA position paper on usage control [41]. The capabilities as depicted in the figure include:

- *Policy Enforcement Point (PEP)*: The triggering point in the flow of data where policy decisions should be enforced and an event can be forwarded to the PDP for policy decision, e.g. using an subscribe mechanism.
- *Policy Decision Point (PDP)*: The central module in the policy enforcement framework responsible for taking the decision for the usage of data, based on the applicable data sharing policies. It is able to reason on the data sharing policies and the received triggering event;
- *Policy Information Point (PIP)*: It provides additional policy information/attributes relevant for the decision making by the PDP. This could for example be relevant context information.
- *Policy Execution Point (PXP)*: It is responsible for corrective actions or notifications for detective enforcement based on information received from the PDP, e.g. in case of violation of policies.
- *Policy Retrieval Point (PRP)*: It provides secure policy storage, protected against malicious modification and accessible by the PMP for policy management and the PDP for policy retrieval.

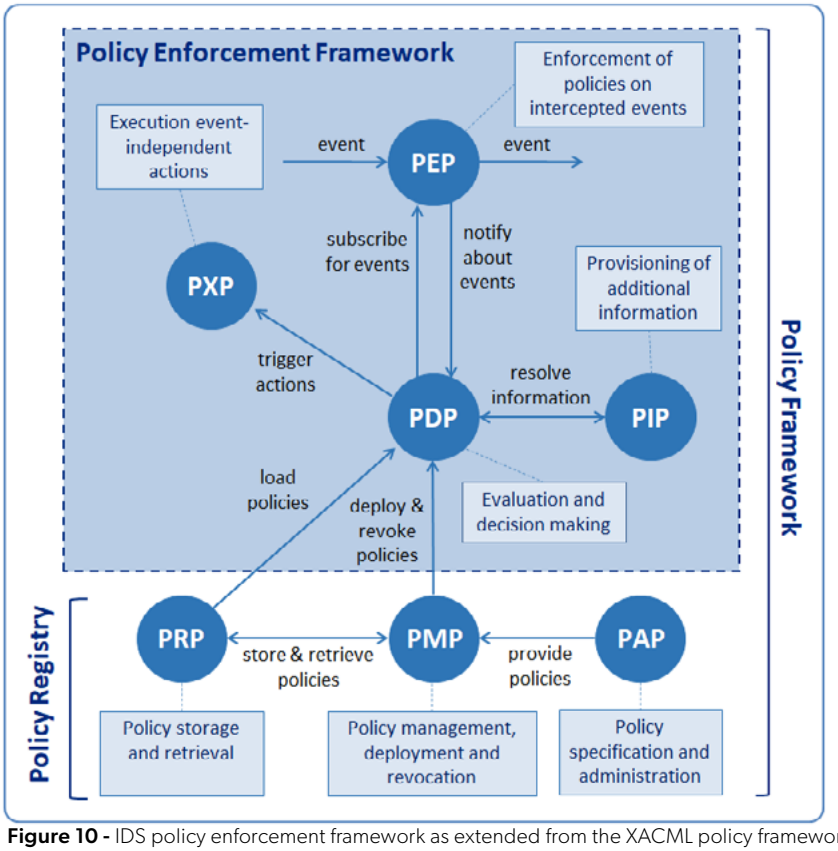

Figure 10 - IDS policy enforcement framework as extended from the XACML policy framework.

- *Policy Administration Point (PAP)*: It is used for the administration of the data sharing policies (i.e. the access and usage control policies). The PAP provides human readable policy information to the user and transforms this into a machine readable format that can be shared with the PMP.
- *Policy Management Point (PMP)*: It is responsible for the management of policies and related interaction with the PDP (deploying and revoking used policies) and PRP (for the secure storage and retrieval of policies).

The security gateway handles all data sharing transactions according to defined data sharing policies. As such, it implements the PEF with it capabilities for administering, enforcing and deciding on usage policies as depicted in **Figure 10**. More specifically, the PEF in the security gateway implements the PEP, PDP PIP and PXP capabilities, whereas the PRP, PMP and PAP capabilities may be provided by an internal policy registry within the PEF as well. Alternatively, the PAP, PMP and PRP capabilities may be implemented by a separate policy registry building block (see paragraph 5.2.3). In this case the data sharing policies may be synchronised between the internal and external policy registries to optimize performance.

Integration of the IDS Application Container Management concept with Gaia-X cloud processing is to be addressed, thereby enabling data apps (and the security gateway itself) to be deployed within a Gaia-X cloud, while maintaining all policy enforcement capabilities and related security measures to protect the data sharing processes. To this end, the app orchestration and workflow management capabilities in the application container environment building block needs to be aligned with the workflow management capabilities in Gaia-X to ensure overarching data sharing policy enforcement.

5.2.3 Policy Registry

5.2.3.1 Functionality: capabilities and interfaces

The policy registry building block is the registry for formal data sharing policies, containing the specific access and usage conditions for ICT-resources to be shared. In addition, the policy registry can act as delegation registry, allowing an entitled party to delegate access and usage rights to other data space participants.

The policy registry includes the Policy Administration Point (PAP), Policy Management Point (PMP) and Policy Retrieval Point (PRP) as defined in the XACML policy framework [38], as described in paragraph 5.2.2. As such, it provides the following APIs:

- a *Policy Administration Point* (PAP) API for definition, storage, updates and retrieval of policies in the PAP of the policy registry,
- a *Policy Management Point* (PMP) API for deploying and revoking policies in the Policy Decision Points (PDPs) and for storing and retrieving policies in the policy registry Points (PRPs) of the policy enforcement framework of a security gateway, and
- a *Policy Retrieval Point* (PRP) API for retrieval of policies stored in the policy registry, to be used by the PDP in the security gateway.

The PAP capability in the policy registry may contain human readable data sharing policies and transform these into a machine readable formal data sharing policies which can be used by the PDP capability of the policy enforcement framework. In the formal data sharing policies, a distinction can be made between access and usage control policies:

- *Access control policies* describe who can access an ICT-resource, e.g. a data service. For instance, a data services provider may choose to only grant access to its data service to requests from a connector with a specific identity.
- *Usage control policies* pose restrictions on how the data can be used after access has been granted. For instance, access to a data service may be granted under the condition that the shared data is not used for commercial purposes.

It is to be noted that the data sharing policies in the policy registry have to comply with all legal regulations. The policy registry with its authorisation and delegation capabilities must be fully transparent to the data entitled parties, in the sense that any authorisation policy that applies to the respective data entitled party must be visible and authorisations should be mutable at any moment[2].

Any changes in the data sharing policies should be propagated directly throughout the data spaces. Any policies referring to a data sharing policy should immediately be invalidated and consequently rebuilt according to the new data sharing policies. Data sharing using contracts based on the invalidated policy are also invalidated, which implies that the data can no longer be legally used for any task. Any information extracted from the data while the contract was valid, remain valid.

5.2.3.2 Alignment with EU reference architecture initiatives

Both IDS, Gaia-X and iSHARE use an XACML based architecture for policy control. IDS identifies the policy enforcement framework (see paragraph 5.2.2) for managing and enforcing data sharing policies, without identifying and defining a policy registry as part of its architecture. In iSHARE policies are included in the Authorisation Registry (AR). Different than in IDS the iSHARE AR also performs the actual policy decisions (as an PDP), where the policy registry only stores the policy data. Similar as in iSHARE, the policy registry could be shared between parties which will reduce complexity for parties that would like to use data that could be provided by multiple parties (and thus only need to consider policies contained in one policy registry). The benefit of the iSHARE AR is the fact that the actual policies themselves do not need to be shared between parties as the interactions in most cases involve policy decisions without sharing the policy data itself. In this aspect the role of the policy registry is different as policy decisions are performed in the security gateway and only parties which are allowed to see or modify the actual policies will get access to the policy registry. When the policy registry is shared between many parties that want to share data (using security gateways), all parties will need to get access to the policies in the policy registry. In iSHARE this is not required. Where the iSHARE AR maintains audit trails for all policy decisions, the IDS security gateway and the clearing house will log transaction which can be used as audit trails. To possibly integrate the iSHARE AR and policy registry, possible integration of both mechanisms could best be investigated (e.g., supporting different scenarios using same the registry).

2 This definition of Policy Registry is broader than (but not in contraction with) the definition as provided by the GDPR, which defines six lawful grounds for processing of personal data: Consent (the consent of a data subject to the processing of her/his personal data), legitimate interest (there is a weighed & balanced legitimate interest where processing is needed), public interest (public authorities and organisations in the scope of public duties and interest), contractual necessity (processing is needed in order to enter into or perform a contract), legal obligations (controller is obliged to process personal data for legal obligation) and vital interests (it is vital that specific data are processed for matters of life and death).

The policy enforcement framework of IDS can be compared with the Gaia-X Federation Service Compliance (policies and rules) document and the Trust Services of Gaia-X. For the definition of policies Gaia-X also suggests ODRL to be used as a standard.

In line with Gaia-X, IDS already adopted ODRL for the definition and description of policies. It would be good when all initiatives would align on the usage of ODRL for policy description, so policies can be easily shared between the various architectures.

The policy registry needs to support both access and usage control policies. A recommended W3C standard for formal policy description is the Open Digital Rights Language (ODRL) [42].

5.2.3.3 Implementation: architecture and open-source modules

The policy registry is a database which contains the (ODRL based) data access rights and usage control policies to be enforced by the policy enforcement framework. The policy registry can be seen as combination of the Policy Administration Point (PAP), Policy Management Point (PMP) and Policy Retrieval Point (PRP) capabilities as elaborated in paragraph 5.2.2 and depicted in **Figure 10**. The policy registry will provide an interface to store and retrieve data usage policies to be applied in the data transaction processes. Data usage policies are specified in ODRL using RDF/OWL format according to the IDS Information Model. As the policy registry is not yet considered as separate component but as internal functionality of the IDS connector, the interface is not yet standardised in IDS RAM [22][23]. The policy registry is used to store ODRL usage policies. As a basis a database could be used that supports storage of RDF/OWL and possibly a SPARQL end point as API to other modules (for semantic analysis and resolution of the stored policies). An example of an open source database that supports SPARQL is Apache Jena.

Various open source XACML policy framework implementations are available. As such, it has also been included as part of the TNO Security Gateway as described in annex C.2. However, to support the policy delegation capabilities and make it into a generic, re-usable, service to be used by multiple participants in an AI data space, the corresponding PAP, PMP and PRP capabilities need to be externalised and accessible through a well-defined API.

5.2.4 Application Container Environment (ACE)

5.2.4.1 Functionality: capabilities and interfaces

The Application Container Environment (ACE) building block provides the environment for the execution of data apps that may use the data as provided by a data services provider as input. The AI operator is the role which will provide and manage the ACE building block. Other participants of the data spaces may take on this role as well. For instance, in the Algorithm Sharing AI-collaboration model and the Network Processing AI-collaboration model (as described in section 2.2 and illustrated in annex A), a data services provider may not want or be allowed to share sensitive data with other participants and it needs to fulfil the AI operator role as well, for which it deploys the ACE building block as well to locally run data apps in its own security domain. For discovery and retrieval of available data apps, an app store can be used.

The ACE is responsible for secure, trustworthy, stable and scalable execution of data apps and processing of the data. It provides a controlled environment in which multiple data apps can be deployed and

executed which can use data provided by the data services providers. Examples of data apps that could run on the ACE would be anonymisation and pseudonymisation (jointly 'de-identification') data apps, semantic management (e.g. transformation) data apps, data quality management data apps, data pre-processing/cleaning data apps or distributed AI algorithm data apps (e.g. for Federated Learning and secure Multi-Party Computation). The ACE provides the basic capabilities to support the four AI collaboration models as defined in section 2.2.

As apps may require data from other apps as input, the ACE should provide a form of app orchestration, with which input and output data flows can be configured and forwarded between data apps. To avoid unwanted app interaction, shielding is provided by using software containers. Furthermore it should be possible to scale the data processing capability, e.g. for example by distributing multiple instances of the apps on multiple servers and splitting data in multiple streams or by using a (trusted) cloud environment. As software modules deployed by the ACE will be containerised, the ACE should provide standard Docker Engine APIs to deploy and execute containers.

5.2.4.2 Alignment with EU reference architecture initiatives

As depicted in **Figure 9**, the IDS connector architecture includes the Application Container Management capability, corresponding to the ACE building block. It is used for extended control over the deployment and execution of data apps and containers.

Gaia-X has the concept of computational resources which can be used to perform data app and security gateway deployment and processing tasks. The Gaia-X Federated Catalogue will include these computational resources and processing environments (with a metadata model to define and describe them, e.g. on computing capacity, location, costs, …). The Federated Catalogue could also indicate security levels of the provided computational resources, which can for example be used to determine if computational resources are adequate to deploy a specific security gateway handling sensitive data.

The iSHARE initiative doesn't contain an ACE building block.

5.2.4.3 Implementation: architecture and open-source modules

The ACE provides deployment, management and execution capabilities to run data apps and security gateways on an execution environment, e.g. servers, virtual servers or clouds. As data apps in the data space are containerised and can be controlled and managed as such, open-source Docker Engines and Kubernetes tools for automating deployment, scaling, and management of containerised applications can be used to implement the ACE, either as (cloud) services provided by a third party or as private (cloud) implementation. Participants providing an ACE building block can describe and expose its specifics and characteristics (e.g. processing capacity, memory available, type of hardware (GPU,CPU), security level, cost, geographic location, etc.) through self-description in the data space metadata broker or a federated catalogue.

Figure 11 provides the high-level functional architecture for the ACE building block.

As the figure shows, the ACE will contain:

- A *Data Sharing Execution Core* (DSEC) which provides the routing capabilities between the locally hosted data apps on the ACE. To ensure data sharing can be done securely, the DSEC will act as the orchestrator of all data apps and main router of data shared between the data apps and between the (security gateways of the) data services provider and AI orchestrator. The DSEC will implement Policy Enforcement Point (PEP) in the managed data flows.
- The *Policy Enforcement Framework* (PEF) that will provide the Policy Decision Point (PDP) capabilities, receiving triggers from the PEP (as implemented in the DSEC but also part of the PEF) and policies from the policy registry (via the PMP and PRP, see paragraph 5.2.2).
- The *data apps* hosted on the ACE that will be able to receive and send data through the security gateway. As the security gateway is in full control of the data shared with the data apps, policy enforcement is also applied on the data sharing and processing by data apps.

To ensure the policies are enforced on the relevant data sharing transactions, the DSEC must implement triggers to initiate the PEP capability on all the points where data sharing or app usage must be validated by the PEF. For the collection of additional information needed to make accurate usage policy decisions, Policy Information Points (PIPs) can be implemented (e.g. capabilities that can provide additional information relevant for policy decisions not available at the PEP or PDP). The PDP can also trigger a Policy Execution Point (PXP) when activation of capabilities are required for specific policy decisions (like logging and validation of the transaction by the clearing house, which can also forward relevant information to the billing engine for billing of the transaction). The PEP capability in the ACE and the PDP capability in the PEF will need to support the specific policy enforcement rules defined in the policy registry. Initially some of the policies will need to be validated via static mechanisms, like data app certification, as it might for example be very difficult (or impossible) to correctly define, implement and dynamically validate all required policies using ODRL.

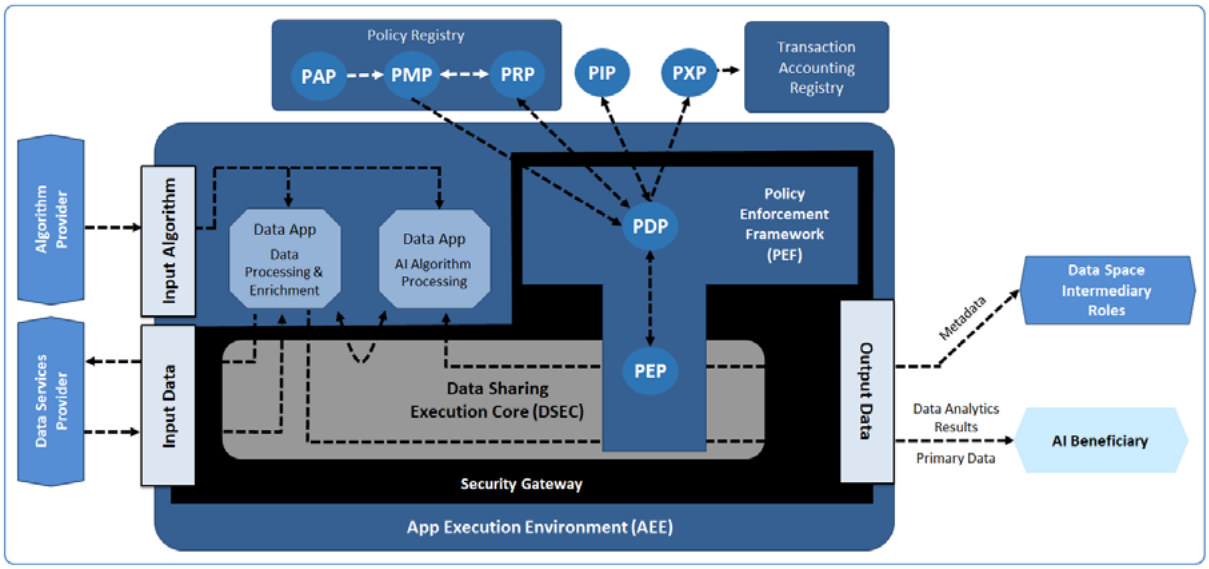

Figure 11 - App enabling approach in the data sharing security gateway architecture.

Furthermore, the ACE should support the logging APIs towards the clearing house to log specific application execution transactions that are relevant for monitoring, maintenance and billing, e.g. the starting and stopping of data apps and the processing resources consumed by the data apps. This allows providers of an ACE to perform usage based pricing. Furthermore the ACE will need to provide interfaces that produce information needed for operation of the environment.

5.3 Data space trust architecture building blocks: identity management

To ensure identities used within the data space can be trusted, secure and trusted identification and authentication of participants and/or components in the data spaces is needed. A participant can be a legal organisation, a component can be representing a participants machine or data service provided by means of a data app within the Data Services Provider's ACE.

The paragraphs in this section subsequently describe the data space trust architecture building blocks for identity management, i.e. the data space membership certificate authority system, the dynamic attribute provisioning service and the participant information system, respectively.

5.3.1 Data Space Membership Certificate Authority System (DS CAS)

5.3.1.1 Functionality: capabilities and interfaces

Participants and/or components of a data space need certification by the data space authority by means of the certification framework. When certification is granted, the Data Space Membership Certificate Authority System (DS CAS) will generate, manage and store certificates for them as being member of the specific AI data space.

The DS CAS has:

- a user interface for generating certificates for participants and/or components for membership of the data space,
- an interface to derive status and validity of issued certificates,
- an interface to the DAPS to store, update and revoke the security gateway certificates for verification at run-time, and
- an interface to the ParIS to store, update and revoke participant certification status.

5.3.1.2 Alignment with EU reference architecture initiatives

IDS uses X.509 certificates as the basis for the OAuth 2.0 based authentication mechanism provided by the DAPS. Gaia-X uses both OAuth 2.0, OpenID Connect (OIDC) and Self Sovereign Identity (SSI) as authentication mechanisms. iSHARE uses OAuth 2.0 and OIDC for authentication.

As the DS CAS provides X.509 certificates, an aligned approach for the IDS, Gaia-X and iSHARE approaches may be followed which also use X.509 certificates as the basis for their OAuth 2.0 mechanisms.

5.3.1.3 Implementation: architecture and open-source reference implementation

The DS CAS is a separate building block for generating X.509 certificates for data space membership of participants and/or components (e.g. security gateways). This entails generically available IT functionality, for which various open-source Certificate Authority system software solutions are available.

5.3.2 Dynamic Attribute Provisioning Service (DAPS)

5.3.2.1 Functionality: capabilities and interfaces

The (validity of the) data space membership registration of the participants and/or components is managed by the data space authority for which certificates are provided and managed by the DS CAS. The certificates are stored in the Dynamic Attribute Provisioning Service (DAPS) for verification at run-time. The DAPS will create, maintain and manage identity information and provide an authentication capability for validating identities. For the creation, maintenance and management of identities, certificates will be used that can contain both static and dynamic attributes. The certificates are used for creation and authentication of the identities, for authorisation and for the encryption of data traffic from and towards the participant holding the certificate.

The DAPS can provide, update and validate identities and their attributes in a dynamic way to ensure trustworthiness and security are guaranteed during the operation of the system. It is possible to dynamically revoke security status of an identity when a vulnerability is detected.

The DAPS interfaces include:

- *DAPS Registration interface* to register received certificates to use for authentication and issuing of tokens.
- *DAPS Notification interface* to notify successful (X.509) certification.
- *DAPS Identification & Authentication interface*: an OAuth interface using token requests (including annotated additional properties from the IDS Information Model) to authenticate if a specific identity belongs to the data space.

5.3.2.2 Alignment with EU reference architecture initiatives

The IDS DAPS uses X.509 certificates and OAuth 2.0 authentication mechanism as a Public Key Infrastructure (PKI) infrastructure. It extends on standard PKI solutions by sharing additional IDS attributes in Dynamic Attribute Tokens (DATs). As IDS is mainly based on data sharing and trust between components (not the end users) and the transfer of possibly large amounts of data, concepts like OIDC do not seem to be appropriate authentication mechanism for IDS.

Gaia-X uses both OAuth 2.0, OpenID Connect (OIDC) and Self Sovereign Identity (SSI) as authentication mechanisms. OIDC is a protocol that adds usage of an authentication server and user identity information to the standard OAuth 2.0 protocol. SSI is based on Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs). SSI is used as the mechanism for fully user controlled (self-sovereign) data sharing. As certificates Gaia-X uses eIDAS, X.509 and Verifiable Credentials (VCs).

The iSHARE solution uses OAuth 2.0 and OIDC for authentication and uses eIDAS certificates for authentication. The OAuth 2.0 mechanism used in iSHARE differs from the IDS mechanism used by the DAPS.

Hence, alignment is needed to integrate the concept of the DAPS in IDS in the SSI and OAuth 2.0 based mechanism currently provided by Gaia-X and iSHARE. IDS does not contain or require user related authentication so only alignment on organisation and component level authentication is required.

5.3.2.3 Implementation: architecture and open-source modules

For the IDS DAPS, open source implementations are available, e.g. the IDS DAPS by Fraunhofer AISEC [43].

Alternatively, a generically available and trusted identification and authentication solution that is able to handle X.509 certificates and tokens may be used.

5.3.3 Participant Information System (ParIS)

5.3.3.1 Functionality: capabilities and interfaces

The Participant Information System (ParIS) is the central registration and information point for the (status of the) participating roles within a data space. It includes master data and information on the security profiles, certification status, domain membership status and applicable legal agreements.

The data and information on the participant as registered in ParIS is based on information provided by other participants, e.g. from a Data Space Authority (for legal agreement status for Data Services Providers joining a data space) or certification bodies (for certification status of participants and/or components such as data apps).

Realisation of the ParIS within a data space requires a trusted Data Space Membership Certification Authority System (DS CAS) to validate organisations for participation in the specific data space and for issuing (and revoking) X.509 certificates.

The ParIS uses a Participation API, which is a HTTPS REST API for sharing participant information (including metadata relevant for other participants) and requesting (X.509) certification status of participants of the data space.

5.3.3.2 Alignment with EU reference architecture initiatives

In Gaia-X there is no separate registry for participants information in a data space, but instead the Federated Catalogue supports definition of self-descriptions of the involved participants. There is however no automatic update of the status of the participant as it is expected the participant will update their own self-descriptions. Integration effort is needed to fully include the ParIS capability in the Federated Catalogue as used in Gaia-X.

In iSHARE authentication is done on participant level using iSHARE Satellite and eIDAS certificates, whereas the IDS approach (as adopted for the AI data spaces) uses X.509 certificates for components, e.g. the security gateway. In future the ParIS (or an integrated module) could possibly be used for participant authentication using eIDAS, like is currently done in iSHARE Satellites.

5.3.3.3 Implementation: architecture and open-source modules

An open source version for the Participant Information Service (ParIS) from Fraunhofer AISEC is available [44].

5.4 Data space semantic interoperability architecture building blocks

The ambition of the European Data Strategy ('*Towards a federation of interoperable data spaces*', see section 2.1) expresses the need for semantic interoperability capabilities for the ICT-resources being shared within and between multiple AI data spaces.

The paragraphs in this section subsequently describe the intra data space interoperability architecture building blocks, i.e. the data space metadata broker, the app store, the vocabulary hub, the semantic transformation engine and the data space connector semantics configurator, respectively.

5.4.1 Data Space Metadata Broker

5.4.1.1 Functionality: capabilities and interfaces

The data space metadata broker building block contains metadata about the ICT-resources that are available in a data space. It is a registry in which providers can publish resource self-descriptions -or 'offerings'- to make them discoverable and available to other data space participants consumers.

The metadata broker can contain self-descriptions of any type of resource. While the core of the metadata model must be specified (standardised), a metadata broker may extend the metadata model to manage additional metadata elements.

To support AI, the following types of resources are foreseen as part of an AI data space and to be registered in a metadata broker by means of self-descriptions:

- *Data services*, for data sets accessible by means of a well-defined data service interface (API). Data services are accessible by means of API endpoints that provide data. The data services self-descriptions in the metadata broker contain the information to describe the data service as well as the technical information to consume the data service.
- *Data apps*, which are deployable images of applications that can be used to instantiate and access data services or to process data . The metadata broker contains self-descriptions of the data apps with a reference to the actual deployable image, which may be stored in an app store. Data apps may include distributed (local workers of) AI algorithms to support the various AI collaboration models as described in section 2.2, e.g. for Privacy Enhancing Technologies (PETs) such as Federated Learning (FL) and Multi Party Computation (MPC).
- *Processing/compute resources*, with the specifics and characteristics of available processing environments where data apps can be deployed by data space participants, e.g. processing capacity, memory available, type of hardware (GPU,CPU), security level, cost, geographic location, etc..

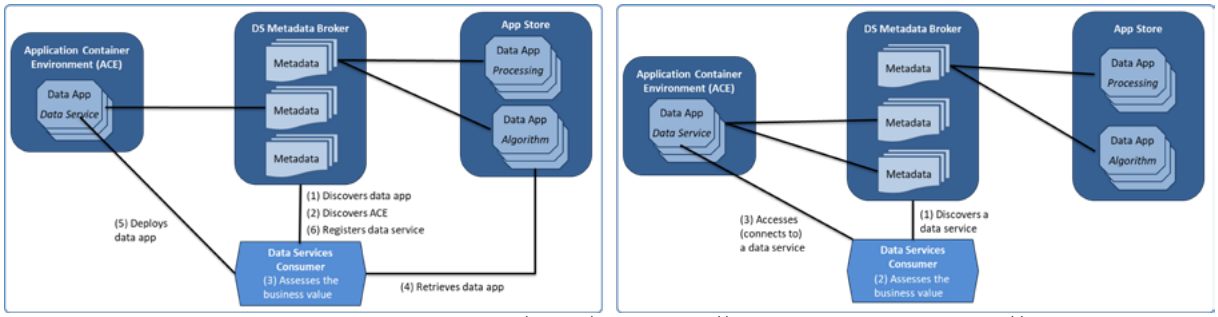

Figure 12 - The data space metadata broker for data app (service) deployment (l) and for data service discovery (r).

The processing/compute resources will mainly be provided by data space participants acting as AI operator, by means of their Application Container Environment (ACE) building blocks. The processing/compute resources as described by self-descriptions in the metadata broker contain the technical information that is required to deploy data apps in an ACE.

The metadata broker has two facilitating capabilities, i.e. for deployment and for discovery of ICT-resources. These are schematically depicted in the left and right side of **Figure 12** for the case of data apps.

The left side of **Figure 12** shows the high-level activities of the metadata broker for data service deployment: a data services provider queries the metadata broker to (1) discover a data app (e.g. for exposing a data service, for processing the data or for executing an AI algorithm) and to (2) discover an ACE. Based on the returned self-descriptions, the data services provider is able to (3) assess the business value of both the data app and the ACE, as well as their compatibility. The data app self-descriptions contain a reference to the actual location of the data app and how it can be retrieved. Once retrieved (4) the data services provider can (5) deploy the data app in the ACE and (6) register the data service in the metadata broker.

The right side of **Figure 12** shows the high-level activities of the metadata broker for data service discovery: (1) a data services consumer discovers a data service in the metadata broker, (2) the metadata broker provides the data service self-description to the data services consumer with which the data services consumer and (3) can access (connect to) the data service.

The metadata broker has the following interfaces:

- *Publication API* for storage of annotated ICT-resource self-descriptions and metadata on available data services, data apps and processing/compute resources in the data space;
- *Discovery API* for discovery of data services, data apps and processing/compute resources in the data space. For discovery and retrieval, SPARQL can be used to perform the query on the metadata broker and the results can be returned in JSON-LD format.

5.4.1.2 Alignment with EU reference architecture initiatives

IDS defines a component called 'Metadata Broker' [22][23], which is a registry for IDS connector (security gateway) self-description documents.

The Gaia-X reference architecture describes the concept of 'Federation Services', which are (intermediating) services that are required to implement a data space or federation. One such service is a catalogue that contains resource offerings, called a Federated Catalogue, enabling the matching between resource providers and consumers [45].

As the IDS security gateway supports self-descriptions, it is important to align the self-descriptions (and governance thereof) in the metadata broker with the IDS information model and standards of the IDS security gateway. Similarly, the self-descriptions in the metadata broker should align with self-description definitions in Gaia-X, which use W3C Verifiable Credentials [46] to describe (among others) participants, resources and service offerings from providers.

Furthermore, the DCAT Application Profile for data portals in Europe (DCAT AP) [47] could be used to provide the required self-description specifications for data services and data sets. At the time of writing, no self-description specification is provided by the DCAT AP for data apps. The reference architectures and information model for the IDS metadata broker and the Gaia-X Federated Catalogue should be aligned to ensure the solutions will remain compatible with currently developed standards.

5.4.1.3 Implementation: architecture and open-source reference implementation

The IDSA has released an open source version of the IDS Metadata Broker [48]. An open source implementation of the Gaia-X Federated Catalogue is being developed as part of the Gaia-X Federation Services initiative [30].

5.4.2 App Store

5.4.2.1 Functionality: capabilities and interfaces

The app store contains all resources required to describe, expose, discover, retrieve and deploy data apps in an Application Container Environment (ACE). In the information model, the data apps are formally described as 'App Resources'. The metadata broker can contain descriptions of the deployed (instantiated) data apps, whereas the app store contains the deployable data apps for retrieval by data space participants. As such, the app store itself also includes a registry with the formal descriptions of available data apps, referred to as its metadata store.

Data apps must be represented as web services in OCI (Open Container Initiative)-compliant images (for instance Docker images) to be deployable within an ACE. OCI images conform to open-source and widely-adopted industry standards. The app store is facilitated by an OCI-compliant image registry to hold all versions of the data apps, and the metadata store for the semantic self-descriptions of the data apps.

The app store facilitates the uploading of new data apps and enables retrieval and deployment of data apps when queried or requested by a data space participant. Data apps that are registered in the app store must be accompanied with a sufficiently unique self-description, and suitable access and usage policies. The app store must provide all available versions of the data apps. Policies may be enabled to allow filtered access to upload data apps. This may enable the deployment of some certified data apps by any security gateway, or restrict access to certain data apps to a select group. A connection from the app store to a clearing house (see paragraph 5.5.2) may be used to log all data app retrievals.

The app store has the following interfaces:

- *App Registration API* to register, upload and publish new data apps.
- *App Retrieval API* to query for and download data apps from the app store, to be executed in an ACE building block. Security gateways can use this interface to securely retrieve new data apps. To enable successful transfer of binary code, binary-to-text encoding (like Base64) of the data app can be applied.

Additionally the app store may provide a user interface to manually upload data apps.

5.4.2.2 Alignment with EU reference architecture initiatives

The IDSA Reference Architecture Model [22][23] identifies the app store as a building block with which the app store will be aligned.

The Gaia-X architecture and the Gaia-X Federation Services (GXFS) [30] don't distinguish a separate app store building block. Through the ongoing alignment of the IDSA and Gaia-X reference architectures, the app store building block is however to be expected in their overarching, coherent, architecture as being developed by the Data Space Business Alliance (DSBA) initiative [29].

5.4.2.3 Implementation: architecture and open-source reference implementation

Fraunhofer FIT has provided an open source version of the app store [49].

TNO currently develops an app store implementation containing interfaces to both an OCI-compliant image registry and the app stores metadata store. It is possible to query the metadata store of the app store for data apps (app resources) using SPARQL to obtain single-use access tokens to the image registry to retrieve the actual data apps.

5.4.3 Vocabulary Hub

5.4.3.1 Functionality: capabilities and interfaces

As semantic models (also called vocabularies) are at the heart of semantic interoperability, these models need to be findable, accessible, and usable for users and services in the data space. The vocabulary hub is a catalogue service for the design-time models that semantically describe the run-time assets in the data space. This includes ontologies, reference data models or metadata elements that define the data itself, annotate the assets or define a semantic data transformation and validation.

The vocabulary hub must at least provide capabilities to store and publish vocabularies and enable collaboration. Collaboration may comprise search, selection, matching, updating, request for changes, version management, deletion, knowledge sharing, Q&A and additional supporting capabilities.

Various vocabulary hub instances may be federated to enable effective collaboration across multiple data spaces by offering a single point of entry to find and use semantic models.

5.4.3.2 Alignment with EU reference architecture initiatives

IDS identifies the vocabulary hub as a building block in the IDSA RAM [22][23]. In Gaia-X, the vocabulary hub is a part of the Gaia-X Federated Catalogue and provides part of the capability of a Gaia-X node's self-description. ISHARE doesn't distinguish a vocabulary hub building block.

The vocabulary hub as deployed in the AI data spaces should be aligned with IDS and develop towards computability with the Gaia-X vision.

5.4.3.3 Implementation: architecture, design and open-source modules

Currently there are only a few implementations of vocabulary hubs available to be used as building block within an AI data space:

- *Vocol*, which is an integrated environment for collaborative vocabulary development as developed by Fraunhofer IAIS [50]. Linked Data vocabularies are a crucial building block of the semantic data web and semantic-aware data value chains. Vocabularies reflect a consensus among experts in a certain application domain. They are thus implemented in collaboration between domain experts and knowledge engineers. Particularly the presence of domain experts with little technical background requires a low-threshold

vocabulary engineering environment.

Inspired by agile software and content development methodologies, the VoCol methodology and tool environment addresses this requirement. VoCol is implemented without dependencies on complex software modules, it provides collaborators with comprehensible feedback on syntax and semantics errors in a tight loop and gives access to a human-readable presentation of the vocabulary. The VoCol environment is employing loose coupling of different modules for syntax validation, documentation generation, visualisation, etc. on top of a standard Git repository.

- *Semantic Treehouse*, which is an online community platform for semantic data models developed by TNO [51].

  The platform combines the publication, maintenance, and governance for data models in one place. Semantic Treehouse is based on more than 10 years of experience with developing, maintaining, and sharing data standards. The platform can be branded and styled to a specific corporate identity for a recognizable user experience.

  Various standardisation bodies in the Netherlands already use the platform for their community management and maintenance of semantic specifications.

  TNO will open source the Semantic Treehouse platform.

5.4.4 Semantic Transformation Engine

5.4.4.1 Functionality: capabilities and interfaces

When dealing with a large number of different participants in a data space, there is a need to handle and combine many different heterogenous data sets in different syntactical formats from or to different systems and APIs. Although shared semantic models allow every system to implement and speak the same language, this is not a realistic prerequisite in many cases. In practice, differences will continue to exist due to legacy implementations, different context/domains or (for historical reasons) competing standards. Furthermore, there is not always a positive business case for users to adapt a new semantic model in their IT systems and interfaces. As such, a semantic transformation is needed for converting from one data model to another, which can quickly be used at run-time and be configured with a variety of models, allowing semantic transformations when needed.

At the core of the semantic transformation engine lies the usage of declarative rules using the RDF Mapping Language (RML) [52]. Through the execution of these rules, knowledge graphs are created from corresponding data sources using annotations provided through vocabulary terms. These vocabulary terms are derived from an ontology. The original data source remains unchanged. Since it is declarative, RML rules are separated from the software that executes them, so the latter does not need to be updated when the rules are updated.

For designing RML specifications, open source tools like Matey or YARRML are available. They provide a more user-friendly way of writing transformation specifications. The data space connector semantics configurator building block (as described in the following paragraph) can assist in creating such specifications using existing vocabularies.

5.4.4.2 Alignment with EU reference architecture initiatives

Although semantic interoperability for heterogenous data is a common problem identified by multiple European data sharing initiatives, most initiatives suggest defining a common data model used by all data sharing participants. Facilitating semantic interoperability by converting data sets at run-time is not yet included in reference architectures or design principles. This also applies to the IDSA, Gaia-X and iSHARE reference architectures.

However, as described in paragraph 3.2.2, when applied to the real world getting all data sharing members to adopt a single data model proves difficult or even an utopia. As such, a successful usage of the semantic translation engine may feed back into reference architectures and design principles for data spaces in multiple European initiatives.

5.4.4.3 Implementation: architecture, design and open-source modules

TNO develops a Semantic Translation Engine building block based on the open RML mapping logic, for which multiple implementations are available. The addition made to include this module is in exposing this RML logic as an IDS data app, which is done using a generic convertor from the IDS information model to the REST calls understood by most RML implementations.

TNO will open source the Semantic Translation Engine.

5.4.5 Data Space Connector Semantics Configurator

5.4.5.1 Functionality: capabilities and interfaces

The data space connector semantics configurator enables data space participants to use vocabularies to configure the semantic interoperability of connector (data app) implementations. This is primarily done by creating Ontology-based API Specifications (OAS) to specify the interface between data services provider and data services consumer. Additionally the configurator can assist in creating mapping specifications.

The configurator is a design-time building block that is used by domain experts and IT specialists; together named as interface designer. The configurator takes existing (or extended) vocabularies as input and provides a "wizard" approach to select the relevant subset for a specific data sharing use case. The configurator is able to generate syntax specific schema that shape the semantic foundation of the API specification, i.e. the request and/or response body.

5.4.5.2 Alignment with EU reference architecture initiatives

The data space connector semantics configurator is not explicitly part of the current reference architecture models (IDS, Gaia-X, iSHARE) yet.

5.4.5.3 Implementation: architecture, design and open-source modules

Currently, an implementation of the data space connector semantics configurator is available as part of the Semantic Treehouse [53], i.e. a vocabulary hub as described in paragraph 5.4.3. It may be used to create ontology based schema and mappings for API specifications using a three step approach:

- For the first step the interface designer creates a message model specification, adds metadata describing the use case, imports vocabularies that are needed and selects a class that serves as root type for the information that will be exchanged (e.g. Organisation, Person, Order or Measurement).
- In the second step, the interface designer selects the type of information that is to be exchanged, which the configurator collects into an abstract message tree (AMT). The module allows interface designers to 'cherry pick' the relevant classes and properties from the imported ontologies;
- Finally, in the third step, the configurator generates a technology-specific syntax binding between the AMT and a syntax format of the user's choice, e.g. XML or JSON and generates RML specifications if needed.

The configurator is available as generic service for the data space participants to design, publish and share the data sharing interactions and interfaces based on vocabularies. The resulting schema can be used directly in Open API specifications (OAS) that provide for standardised APIs to be used by the data apps that will be deployed within an ACE (see paragraph 5.2.4) of a security gateways. RML can be used to configure a semantic transformation engine, see paragraph 5.4.4.

5.5 Data space value creation building blocks

To create value from data sharing in a data space and for valorising data transactions, (administrative) capabilities are required for registration data sharing contracts and transactions, for accounting and for monetisation thereof.

The paragraphs in this section subsequently describe the data space value creation building blocks, i.e. the contract manager, the clearing house and the billing engine, respectively.

5.5.1 Contract Manager

5.5.1.1 Functionality: capabilities and interfaces

The contract manager provides capabilities to support the offering of ICT resources (e.g. data services or AI algorithms) under defined terms and conditions. This encompasses the management of processes linked to the creation and monitoring of contracts which clearly describe the rights and obligations for data and service usage and access to data and services. The support offered can also include verification of GDPR requirements when applicable.

The contract manager will also play a central role to document and store the legally binding contracts for the participants of a data space. Participants of a data space (specifically data services providers and AI algorithm providers) need to ensure that legally binding contracts are in place before services are delivered. The contract manager can support such a process and ensure that both the providers and consumers of services have access to the defined contracts and that these are signed before the actual sharing of data or AI algorithms takes place. For this the contract manager could for example provide an API to interact with the clearing house to validate presence of legally binding contracts for specific data sharing transactions.

5.5.1.2 Alignment with EU reference architecture initiatives

Gaia-X has policy rules and compliance and labelling criteria to govern and establish controls over individual transactions. An important element of these policy rules is the usage of a contractual

framework between 'provider' and 'customer' and the governance of this contractual framework. It would be good to align activities of the contract manager with the governance framework defined by the Gaia-X.

5.5.1.3 Implementation: architecture, design and open-source modules

The implementation of the contract manager will mainly be focussed on processes on creating and sharing legally binding acts/contracts and less on actual technologies or interfaces to store and monitor the contracts.

It will be helpful however to see to what extend the legal contracts used can be aligned with contracts used in iSHARE, Gaia-x and IDSA.

5.5.2 Clearing House

5.5.2.1 Functionality: capabilities and interfaces

The clearing house provides clearing and settlement services for data sharing transactions. As such, the clearing house plays an important role in providing legal, financial and technical support capabilities both prior to actually sharing the data (i.e. 'clearing') and after the data has been shared (i.e. 'settlement').

As part of a data sharing transaction the metadata needs to be logged in the security gateways but also in the clearing house in case clearing, logging and/or billing is required. The clearing house acts intermediate party in case the sensitivity of the data shared requires non-repudiation capabilities, such that for example the AI Orchestrator cannot deny having received the data. The clearing house can also validate signatures in a contract of the parties involved in the data sharing and verify payment conditions and policies. It will bind the transaction to an instance of a data sharing agreement and usage contract and thereby enable execution of a transaction. The clearing house can provide additional reports on the performed (logged) transactions for billing, conflict resolution, etc. The clearing house will also be involved during the data sharing transaction where it collects additional metadata and finally the discharge of a transaction. By storing policy verifications and other transaction data, the clearing house will create an audit trail (which could optionally be implemented using blockchain technologies) for auditing and to help solve conflicts between parties of the data space involving specific transactions.

The clearing house has the following interfaces:

- *Clearing House API* for:
  - receiving and validating transaction requests (with metadata information on contract agreements), optionally using external sources like policy registries, the metadata broker r or other sources,
  - logging of metadata information of the transactions, and
  - receiving and handling discharge requests for data-sharing transactions.
- *Monitoring API* for monitoring and reporting of data-sharing transactions handled by the clearing house;
- *Billing API* for providing billing information as input for a billing engine.

For the collection of relevant information to perform validation, the clearing house can interact with other components in the data space, like the contract manager, the policy registry, the ParIS and the metadata broker, for which additional APIs might be provided.

5.5.2.2 Alignment with EU reference architecture initiatives

The clearing house is a role within the IDSA's Reference Architecture Model (IDSA RAM) for data spaces [22][23]. As such alignment with the IDS clearing house is necessary.

A specific capability for the clearing house can be event-driven (real-time) data flow control, for which a specific data app to be deployed in the clearing house may need to be developed.

5.5.2.3 Implementation: architecture, design and open-source modules

Fraunhofer AISEC already implemented an open source version of the clearing house [54][55], which could be used as starting point for the clearing house component.

The capabilities for the clearing house building block encompass generic IT capabilities which are not specific for data spaces. It is expected that generic, commercial-off-the-shelve (COTS) implementations are available. Therefore, the elaboration of the clearing house building block implementation is further out of scope.

As parties that perform similar billing capability already exist in the market, it may also be possible to request an existing clearing house party to perform requested capability based on transaction and policy data from the data space.

5.5.3 Billing Engine

5.5.3.1 Functionality: capabilities and interfaces

As part of a data sharing transaction, metadata is logged in the clearing house, which can be used to bill the data sharing transactions, possibly using additional billing information, e.g. from the metadata broker, the contract manager and/or the ParIS. The billing engine will translate the data sharing transaction metadata to generate billing information and to perform required payment and invoicing.

The billing engine has a Billing Engine API for collecting transaction data from the clearing house.

5.5.3.2 Alignment with EU reference architecture initiatives

The billing engine has been out-of-scope for the EU reference architecture initiatives.

5.5.3.3 Implementation: architecture, design and open-source modules

The capabilities for the billing engine building block encompass generic IT capabilities which are not specific for data spaces. It is expected that generic, commercial-off-the-shelve (COTS) implementations are available. Therefore, the elaboration of the billing engine building block implementation is further out of scope.

As parties that perform similar billing capability already exist in the market, it may also be possible to request an existing billing party to perform requested capability based on transaction and policy data from the data space.

PART C: TRUST ARCHITECTURE

The trust architecture addresses the governance, policies, architecture and management and activities to assure that both the (potential sensitive and valuable) primary data and AI algorithms and their associated metadata being shared within and between AI data spaces are trustworthy. Moreover, the trust architecture ensures data sovereignty to the entitled parties over their data, services and assets.

As part of the trust architecture, chapter 6 addresses the trust agreement framework describing the trust capabilities and building blocks, after which chapter 7 elaborates the trust interaction patterns to ensure trustworthiness of the metadata being exchanged between building blocks in an AI data space.

6. TRUST FRAMEWORK: CAPABILITIES AND BUILDING BLOCKS

As Figure 8 (paragraph 5.1.2) on the Open DEI soft infrastructure shows, trust and its associated building blocks are a key and integral part of the data space concept. Moreover, Open DEI identifies the importance of a trust framework, defining it as 'a structure that lets people and organisations do business securely and reliably online'. The various aspects of a trust agreement framework for intra AI data space interoperability are subsequently distinguished in the following sections, i.e. data space authority trust management, data space identity management and data space policy management.

6.1 Data space authority trust management

The AI data space authority trust management encompasses the legal framework, the certification framework and the trust monitoring framework activities as depicted in **Figure 7** (section 4.3) as being part of the Data Space Authority role. These are addressed in the subsequent paragraphs of this section[3].

6.1.1 The legal framework

The legal framework ensures that data space participants can share ICT-resources under common, agreed-upon and legally bounding conditions. Legal agreements provide the legal basis for the sharing of data between organisations. To support legal agreements at a large scale between organisations, across sectors and areas of application, it may be preferable to manage them electronically, i.e. by means of an electronic data sharing agreement[4][5].

In a data sharing agreement, the participants in a data sharing transaction acknowledge that data is being exchanged, with both participants recognising and committing to their own responsibility, whilst adhering the applicable law. Data sharing agreements and legal interoperability present a major challenge.

Currently, legal aspects are mainly dealt with within a single data sharing domain by pre-defining the set of multi-lateral legal agreements to which individual data services providers and consumers are bound to adhere to when signing up for joining the data space. This approach with a hierarchy of legal agreements has been described in paragraph 3.2.4.

3 It is noted that the data quality framework as depicted in Figure 7 (section 4.3) is not considered as part of the trust framework (and the intra and inter AI data space reference guides) as it is not part of the data sharing environment.

4 The legal aspects of (electronic) data sharing have previously been addressed by the NL AIC working group Data Sharing in [5] (appendix C.2), the Data Sharing Coalition's Data Sharing Canvas ([57], section 7.1, Figure 19) and in paragraph 3.2.4 of this report, explaining the hierarchical legal construction with data space accession agreements and data service transaction agreements.

5 To be legally valid, paragraph 3.2.4 has described the three steps that the Dutch law prescribes that have to be gone through when engaging into a data sharing agreement in an electronic manner. Moreover, for an electronic data sharing agreement to be (legally) equivalent to a written data sharing agreement, Article 6:227a of the Dutch Civil Code (Burgerlijk Wetboek) imposes four requirements [5]: (1) the data sharing agreement is equally accessible (consultable) by both parties, (2) the authenticity of the data sharing agreement can sufficiently be guaranteed, (3) the time of creation of the data sharing agreement can be established with sufficient certainty, and (4) the identity of both parties can be established with sufficient certainty. In addition to these mandatory rules for an electronic data sharing agreement there are some optional parts that can be included in the data sharing agreement [5], (appendix C.2.3): the processing agreement, an interpretation of parties, the legal qualification, the confidentiality criteria, the intellectual property conditions, liability statements, privacy and security agreements, dispute settlement, agreement duration and termination, purpose binding, and third parties involved.

However, the (inter-)national environment of federative data sharing and data spaces are rapidly developing. This applies to both EU regulations and reference architectures. As such, the Data Governance Act [17] provides the legal framework for federative data sharing whereas the main European initiatives on federative data sharing and data spaces (IDSA, Gaia-X, ….) are developing more distributed contract negotiation protocols in which data services providers and data services consumers bilaterally negotiate the legal conditions under which they share data. This results in a two-stage approach in which (1) a data sharing contract is negotiated between a data services provider and a data services consumer, based on which (2) the data services provider shares the data with the consumer. This is enabled by a strong and formalised semantic fundament to ensure that participants (possibly operating in different sectors and jurisdictions) unambiguously understand the legal conditions. A machine-readable interpretation of the legal data sharing agreements and usage contracts is required to enable automated reasoning on the complex system of policies, rules and obligations.

To support AI data spaces, the former approach is simples to realize in the short term, also to support AI data sharing over multiple domains. It may therefore be considered by the NL AIC as initial step. On the medium to long term, the possibilities that the latter approach on distributed contract negotiation capabilities provide should be further developed and deployed, both in the context of intra and inter AI data space interoperability. Moreover, it is to be expected that both approaches will coexist and need to be (simultaneously) supported.

6.1.2 The certification framework

To establish trust among all participants in the ecosystem of federated and interoperable AI data spaces, the certification framework includes both:

- participant (organisation) certification,
- building block (technical) certification.

Certification expresses compliance of a participant or building block with the criteria and the evaluation method for the AI data space as agreed upon under the coordination of the data space authority.

When executing data sharing transactions, run-time support of activities for requesting and verifying certification status and validity of certificates of participants and building blocks are needed as part of the identity management processes and building blocks.

6.1.3 The system monitoring framework

To assure trustworthiness of the overall ecosystem of federated and interoperable AI data spaces and the data sharing transaction processes that they enable, it is important that the building blocks provide adequate monitoring capabilities to (automatically) detect, prevent and possibly (help to) resolve potential trust or security breaches. To this end, an AI data space may provide capabilities for:

- *Remote Attestation*, i.e. the verification of the integrity of security gateways at run-time, e.g. as being defined for security gateways as part of the IDS Communication Protocol (IDSCP) [56], and
- *Dynamic Trust Monitoring*, i.e. the verification of integrity for a longer period of time with possibility to trigger actions (in case of validations) and/or revocation of AI data space membership certificates.

6.2 Data space identity management

Identifying participants and components, both as legal identities and as AI data space members is fundamental to the trust framework for AI data spaces. This has also been addressed in paragraph 3.2.1.

As shown in **Figure 7** (section 4.3), the Information System Architecture for AI data spaces includes three types of identity management building blocks as part of the data space governance roles:

1. the Data Space Membership Certificate Authority System (DS CAS) building block,
2. the Dynamic Attribute Provisioning Service (DAPS) building block and
3. the Participant Information Service (ParIS) building block.

For executing data sharing transactions, these three identity management building blocks need to support the activities to request and to identify and authenticate natural persons, organisations or software components as legal entities.

6.3 Data space policy management

The data space policy management capabilities provide the data services providers and entitled parties with the capability to express their requirements on how to share and handle their data and/or AI algorithms by means of 'policies' and the enforcement thereof.

As shown in **Figure 7** (section 4.3), the Information System Architecture for AI data spaces includes three types data space policy management building blocks:

1. the policy registry building block,
2. the policy enforcement framework building block, and
3. the contract manager building block.

How these building blocks can be used to support the processes for defining and enforcing data sharing policies, has been addressed in the elaboration of the policy enforcement framework building block in paragraph 5.2.2.

7. TRUST INTERACTION PATTERNS

Trust interaction patterns elaborate how the various building blocks in the AI data space can interact to ensure trustworthiness of the metadata being exchanged, e.g. the metadata on identification, authentication and authorisation (IAA) and on data sharing contracts and policies. The following sections in this chapter subsequently address the various AI data space trust interaction patterns, the guidelines for deploying trust interactions for intra AI data space interoperability and the trend towards fully distributed trust interaction patterns as currently being pursued by the main European initiatives on federative data sharing and data spaces, respectively.

7.1 Intra and inter AI data space trust interaction patterns: homogeneous and heterogeneous

Various patterns may be developed to ensure trustworthiness of the metadata being exchanged between the building blocks in an AI data space. A categorisation thereof can be based on the distinction between homogeneous and heterogeneous trust interaction patterns, both being applicable for intra and inter AI data space interoperability. Table 3 briefly lists and describes this categorisation.

This categorisation is visually depicted in **Figure 13**.

The (homogeneous and heterogeneous) trust interaction patterns are elaborated in the following paragraphs for both intra and inter AI data space interoperability.

Table 3: Categorisation of data space trust interaction patterns
Trust interaction patterns for intra AI data space interoperability To ensure trustworthiness of metadata exchange between building blocks within a single AI data space.
Homogeneous trust interaction pattern: aligned security gateway The building blocks within an AI data space adopt an aligned architecture, e.g. the (IDS-based) architecture as described in this report with alignment on using the (same) security gateways and their associated trust interaction protocols.
Heterogeneous trust interaction pattern: hybrid security gateway The building blocks within an AI data space do not need to follow the same and aligned architecture. A hybrid security gateway absorbs the variation in protocols to be supported and provides and enforces a (variation in) trust interaction patterns, accordingly.
Trust interaction patterns for inter AI data space interoperability To ensure trustworthiness of metadata exchange between building blocks over multiple AI data spaces.
Homogeneous trust interaction pattern: full harmonisation by means of federable building blocks The individual AI data spaces adhere to an aligned architecture, e.g. the (IDS-based) architecture as described in this report. Each of the (relevant) building blocks of the AI data space is developed to be 'federable' over multiple AI data spaces, by means of a building block federation API as depicted in Figure 13.
Heterogeneous trust interaction pattern: partial harmonisation by means of data space proxies The individual AI data spaces don't adhere to an aligned architecture. Various (implementation types of) enabling building blocks may be used in different AI data spaces. Data space proxies are used to translate data space specific transactions to their harmonised equivalents, thereby facilitating interoperable transactions and creating an understanding of concepts like trust and security across data spaces. A data space proxy itself is part of the individual data spaces. The data space proxy APIs exposes the capabilities of the individual data spaces.

7.1.1 Intra AI data space interoperability: trust interaction patterns

For intra AI data space interoperability, the homogeneous and heterogeneous trust interaction patterns are addressed in the following sub-paragraphs, subsequently.

7.1.1.1 Homogeneous trust interaction pattern: uniform (aligned) security gateway

In the homogeneous trust interaction pattern for intra AI data space interoperability all participants within the same AI data space adhere to the same reference architecture, e.g. as described in this report for intra AI data space interoperability. This specifically (but not only) applies to deployment of the security gateway building block as described in section 5.2.1 and the policy registry and the policy enforcement framework building blocks as described in section 5.2.2.

With this homogeneous trust interaction pattern the most advanced features on access and usage control for data sharing within an AI data space can be developed and supported, as described in the IDSA position paper on usage control [41].

The homogeneous trust interaction pattern for intra AI data space interoperability is the initial and main pattern that is used as basis for the reference implantation for AI data spaces as described in the following chapter 8. Moreover, it form the basis for elaboration into interaction guidelines for a trustworthy AI data space in the follow-up section 7.2.

7.1.1.2 Heterogeneous trust interaction pattern: hybrid security gateway (connector)

From a data services provider perspective, it is noted that the same high level of security will not be required for sharing of data with all data services consumers. By supporting various and differing interaction patterns, a data services provider can make his data available in an easy manner to a larger set of data services consumers. For instance, when open data is shared or when data has been anonymised it may already be used by a broad set of data services consumers without all 'heavy-weight' control and security measures of IDSCP and an IDS trusted connector being required. A 'light-weight' interaction pattern may be sufficient for being allowed to access the data. Therefore, in the heterogeneous interaction pattern for intra AI data space interoperability not all participants within the same AI data space have to adhere to same protocols and interfaces of the common reference architecture, e.g. as described in this report for intra AI data space interoperability. Moreover, allowing heterogenous interaction patterns for different participants in an AI data space enables a smooth migration trajectory for data spaces. For example, it allows OAuth 2.0 based data spaces to gradually migrate to an IDS based AI data space, without all data services providers and data services consumers needing an all at once 'big bang' technical migration step for enabling the full-fledged advanced features of a data space as described in the report.

A data services provider in an AI data space can handle such variations in interaction pattern by means of a hybrid connector that allows for various interaction patterns is to be simultaneously

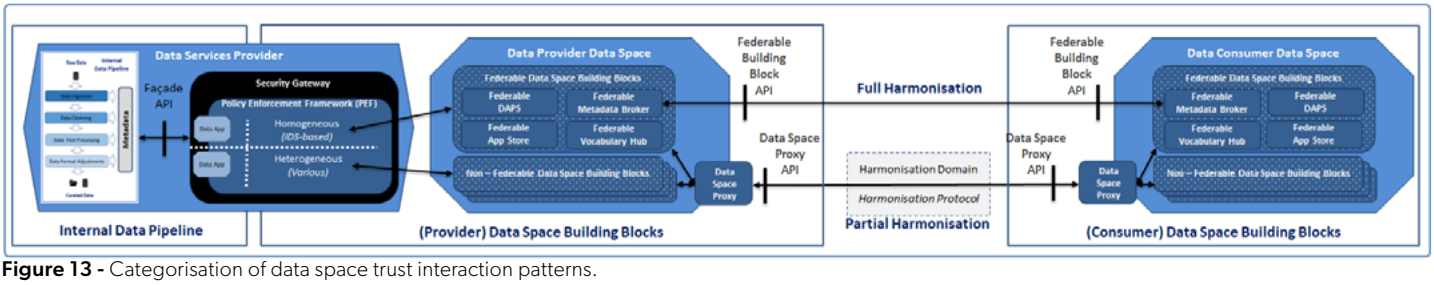

Figure 13 - Categorisation of data space trust interaction patterns.

supported. Dependant on the interaction pattern with which a data services consumer requests access to its data service, the data services provider can deploy different data sharing policies by means the (XACML) framework capabilities as part of the security gateway and aligned with the IDSA position paper on usage control [40], see section 5.2.2. Moreover, this policy enforcement framework allows the access to individual data services as provided by a data services provider to be shielded by means of a so-called 'façade' from the manner in which it is invoked by varying interaction patterns deployed by data services consumers in the AI data space.

7.1.2 Inter AI data space interoperability: trust interaction patterns

Interoperability between data spaces is a key aspect of the EU Data Strategy. The Data Sharing Coalition (DSC) addresses interoperability between multiple data spaces in its Data Sharing Canvas [58]. It introduces the concept of 'harmonisation', which is defined as '*the establishment of agreements, standards, and requirements between participants to enable data sharing between them*'.

As the Data Sharing Canvas describes, interoperability between multiple data spaces can be achieved via full or partial harmonisation. As Table 3 and **Figure 13** show, full harmonisation corresponds to the homogeneous trust interaction pattern for inter AI data space interoperability, whilst partial harmonisation corresponds to the heterogeneous trust interaction pattern for inter AI data space interoperability.

The full and partial harmonisation mode for the homogeneous and heterogeneous trust interaction pattern for inter AI data space interoperability are further elaborated in the companion report on inter AI data space interoperability [2].

7.2 Interaction guidelines for a trusted ecosystem for intra AI data space interoperability

The intra AI data space interoperability architecture is based on building blocks that expose their capabilities as services through well-defined APIs by the various enabling roles in the NL AIC business role model, as defined in section 2.1 and depicted in **Figure 3**. Controlled access to these services is fundamental for realising data sovereignty and a trusted overarching ecosystem. Such controlled access to the APIs applies both for:

- the data services and data processing services as provided by the core roles in the NL AIC business role model as described in section 2.3, and
- the services of the individual building blocks as provided by the enabling roles (i.e. the data space intermediary roles, the data space software and services roles, and the data space governance roles) in the NL AIC business role model as described in section 2.3.

The following interaction guidelines for intra AI data space interoperability are applied for controlled access to core and enabling roles in the NL AIC business role model:

- *By default, core role participants deploy a security gateway based on a trusted IDS-connector.*

  A trusted IDS-connector (using the IDSCP interaction pattern) is initially foreseen for those participants in core roles that require (1) stringent usage policy enforcement on the sharing of (valuable or sensitive) data and/or (2) support of the IDS information model for message exchange.

Different core role participants may use different trust interaction patterns within an AI data space, allowing for migration and 'hybrid' data spaces.

This is referred to as the heterogeneous interaction pattern as addressed in subparagraph 7.1.1.2. A hybrid security gateway (connector) can be used by data services providers to simultaneously handle various interaction patterns. The hybrid security gateway (connector) is implemented within the policy enforcement framework of the security gateway. In this manner, e.g. both authorisation protocols based on access tokens and on contract negotiation may be simultaneously supported by a data services provider.

As described in subparagraph 7.1.1.2, this guideline enables a smooth migration trajectory for a multitude of existing data sharing domains that are not (yet) based on the capabilities provided by the AI data spaces as described in this report.

- *Data and processing services are shielded by means of a 'façade' API, preventing providers from having to implement a variation of access authorisation protocols.*

  As depicted in **Figure 13**, a 'façade' API is used to shield the internal implementation of a data services provider from the variations of protocols being used within a 'hybrid' AI data space. These variations specifically apply to identification, authentication and authorisation (IAA). The policy enforcement framework in the hybrid security gateway (connector) handles variations in supported IAA protocols. This allows the (data and processing) services exposed by core role participants to be implemented independently of the IAA protocols to be supported and enables providers of these services to simultaneously handle multiple authorisation protocols and an efficient implementation thereof.

- *Authorised access to enabling services is based on access tokens.*

  For interactions by core role participants with AI data space services (as provided by intermediary and software and services roles as described in section 2.1 and depicted in **Figure 3**), only access policies need to be supported by the enabling services. Usage policies are not required. Therefore, an authorisation protocol based on access tokens (e.g. OAuth 2.0) can be deployed. The use of IDSCP is optional as interaction protocol[6].

- *ODRL is preferred as language to express usage policies.*

  ODRL is the preferred language to express usage policies for policy registries as it can be used for expressing both access and usage control policies. Mappings from XACML (which is commonly used to express access policies) to ODRL, and vice versa, can be made.

  Apart from storage in policy registry, the usage policies are also shared within IDSCP messages between participants. By using ODRL all participants will be able to share and read policies defined by other participants (preferably automatically using the PEF in their security gateway).

6 IDSCP is not mandatory between security gateways (connectors) according to IDS standards. IDSCP is only mandatory if highest trust level is needed, using remote attestation. However, usage of the IDS information model is mandatory. So, also when IDSCP is not used between security gateways (connectors), the use of the IDS information model for exchanging metadata needs to be supported on the interfaces. The HTTP MIME is mostly used between security gateways (connectors) whilst support of HTTP REST as protocol between security gateways (connectors) is planned for. Metadata is formatted according to the IDS information model.

- *Both participants and technical components (security gateways) in AI data space can be identified and authenticated as AI data space participant.*

  Identification and authentication of both participants and technical components forms the basis for a broad set of use cases and scenarios to be supported and lays the foundation for interoperability between data spaces. It may be implemented in the combination of the Data Space Membership CA, the DAPS and the ParIS building blocks.

- *In authorisation processes of AI data spaces, identification as AI data space participant is used.*

  Within an AI data space, authorisation identification of participants is based on AI data space membership as administered in the data space membership certification authority system (DS CAS), the DAPS and the participant registry (ParIS) building blocks.

  The identification as legal entity is not used in the authorisation processes within AI data spaces. The manner of identification as legal entity is open for individual AI data spaces to agree upon.

- *Data sharing role interactions and data sharing transactions are logged.*

  To manage and monitor the AI data spaces, both the data sharing role interactions and data sharing transactions should be logged and monitored, e.g. to detect and solve possible errors occurring, track and trace individual data transactions and to support conflict resolution.

- *Whenever possible the data services and data processing services should be published in the data space metadata broker.*

  To stimulate use of data and processing services within the data space, it should be stimulated to publish metadata on the data services and data processing services in the data space metadata broker. For automatic publishing of the metadata the IDS defined self-description interfaces could be used. Gateways are often already equipped with a self-description interface for publishing, updating and removing metadata form the data space metadata broker.

7.3 Towards fully distributed trust interaction patterns

The (inter-)national environment of federative data sharing and data spaces is still in development. This also holds for trust framework capabilities. Specifically, the main European initiatives on federative data sharing and data spaces (IDSA, Gaia-x, DSBA, ...) are developing towards fully distributed trust framework capabilities for identity, authentication and authorisation (IAA), contract negotiation and usage control. These developments still have to prove their technical and market viability for large scale deployment in AI data spaces. As described in paragraph 5.1.2, it is therefore advised that further development of the trust interaction patterns and associated building blocks for AI data spaces is accompanied by (1) a vision and roadmap on whether and how develop and align its trust framework capabilities with the developments on alternative, fully distributed, trust framework capabilities, and (2) migration scenario's providing data space participants a smooth and seamless (service and technical) evolution trajectory for these developments.

Moreover, the technical options for evolving and migrating towards a fully distributed federative data sharing architecture and trust interaction patterns should be accompanied by an adequate legal framework to ensure that data space participants can share ICT-resources (such as data and AI algorithms) under legally bounding conditions, even without a pre-defining and signed multi-lateral legal agreement for joining a specific AI data space, for which the EU Data Governance Act [17] is expected to provide the legal basis (see also paragraph 6.1.1).

PART D: REFERENCE IMPLEMENTATION, ROADMAP AND CONCLUSIONS

The technology for realising the individual building blocks for intra AI data space interoperability as described in this report is rapidly maturing. Nevertheless, the deployment of (the overarching federation of) AI data spaces is still in in its infancy. Therefore, guidance is needed, both on the architectural development and on adoption. To this end, chapter 8 describes the reference implementation to demonstrate the potential and to identify lessons learned for development and large scale deployment of AI data spaces according to the intra and inter AI data space interoperability approach as described in this report and the companion report [2]. Subsequently, chapter 9 provides the further development roadmap for intra AI data space interoperability, after which chapter 10 provides the overarching conclusions.

8. REFERENCE IMPLEMENTATION

To demonstrate the potential and to identify lessons learned for developing towards large scale adoption, the architectural concepts and building blocks for intra and inter AI data space interoperability (as described in this report and in the companion report [2]) are demonstrated by means of an illustrative and representative reference implementation. The reference implementation shows how the various building blocks for intra and inter AI data space interoperability work together and can be integrated to implement the overarching architecture for a federation of interoperable AI data spaces as pursued by the NL AIC working group Data Sharing in alignment with the EU Data Strategy.

The scenario and story lines for the reference implementation focus on geriatric health care. Geriatric health care is used as it covers the various complexities and concepts of data sharing for AI, both applicable to intra and inter AI data space interoperability. It is considered both illustrative and representative due to:

- the privacy and sensitive nature of the data needed as input for AI processing, and
- the diversity in participants in providing and processing of geriatric data.

Health care carries major societal cost. As such, improved digitisation and AI may contribute to better treatments, higher efficiency and reduction of costs. In the Netherlands, approximately a quarter of government expenditure goes to the health care sector.

Within health care, the focus of the reference implementation is on the case of dementia or Alzheimer disease. One in five people suffers from a form of dementia or Alzheimer disease during their life [57]. Most of these people use various forms of structured car. In view of the major (and rising costs) of medical treatment, small improvements can lead to large societal advantages, or more pressing: if no improvements are made there is a risk of health care costs becoming overwhelming and too high for society to bear.

However, the data containing the potential insights on improved treatments are currently hidden in and dispersed over multiple health care organisations, e.g. hospitals, general practitioners, elderly and nursing homes and government agencies. The relevant data is expressed by different data models and data sharing is only possibly under various legal frameworks per application area. As such, up until now it has been difficult to share and process geriatric data on a large scale. The reference implementation will demonstrate how this can made possible and provides lessons learned on how this can be improved.

Although the reference implementation applies to geriatric health care, it is considered to be similarly applicable to a broad range of data sharing use cases in other sectors and application areas as well. Two main (generically applicable) lines of thought are reflected in the scenario and story lines for the reference implementation, reflecting the 'Data Sharing' and 'Algorithm Sharing' collaboration models (or archetypes) to be enabled by AI data spaces as previously identified and described in [1] and summarised in section 2.2 of this report:

The *Data Sharing collaboration model*, which focusses on situations in which the data itself is of interest for sharing, for example when an external participant needs the actual data to do its analysis, i.e. the sensitive data has to be shared between participants. As such the risk related to data sharing has to be minimised, whilst adhering to the conditions of data sovereignty by the entitled party.

The *Algorithm Sharing collaboration model*, which focusses on the capabilities needed to execute an AI algorithm in case the data services consumers are only interested in its end result and the entitled parties are reluctant to share the (sensitive) patient data with other organisations. In this case, an AI algorithm can be deployed at the location where the sensitive data resides, i.e. within the (security) domain of the data services provider. In this manner, the sensitive data is not shared between organisations, circumventing the confidentiality issues. Currently, Privacy Enhancing Technologies (PETs) are considered very promising as such, with Federated Learning (FL) and Multi Party Computation (MPC) important representatives.

The reference implementation demonstrates and validates the architectural approach and building blocks for both intra and inter AI data space interoperability as described in this report and in the companion report [2]. The reference implementation, its geriatric health care scenario and associated story lines and the architectural approach and building blocks for intra and inter AI data space interoperability are further elaborated in annex B of this report.

9. DEVELOPMENT ROADMAP

The development roadmap for intra AI data space interoperability distinguishes the three main views as used within this report: the ecosystem architecture, the building block architecture and the trust architecture. Figure 14 shows the overarching development roadmap for intra AI data space interoperability for the time period 2023 - 2025[7].

The figure shows how the individual activities are grouped in various topics. The following sections address the specific development activities and their topics for the ecosystem architecture, the building block architecture and the trust architecture view, respectively.

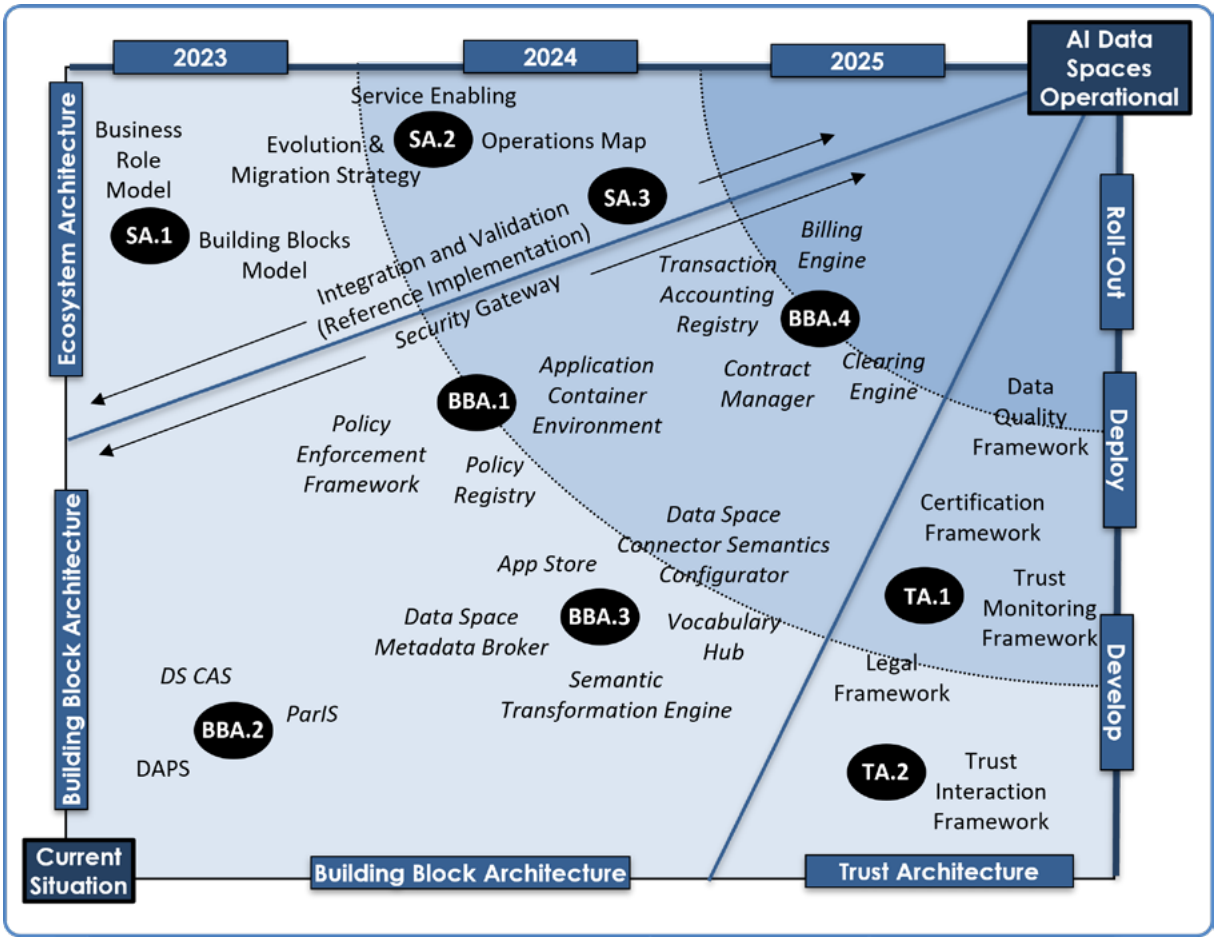

Figure 14 - Roadmap for intra AI data space interoperability: ecosystem, building block and trust architecture.

7 Disclaimer: It is to be noted that the actual realisation of this development roadmap by the NL AIC working group Data Sharing in the time period 2023 – 2025 strongly depends on the opportunities and resources made available, which at the time of writing are not clear yet.

9.1 Developing the ecosystem architecture

The ecosystem architecture view includes the activities for the system decomposition architecture (SA.1), for the service and process architecture (SA.2) and for integration and validation (SA.3).

The activity for the system decomposition architecture (SA.1) considers the decomposition of AI data spaces into business roles and technical building blocks as addressed in section 2.3 and in section 4.3, respectively. It is to be expected that the business role model will remain stable. The building block model is expected to evolve over the coming years due to the ongoing trend towards more fully distributed trust interaction patterns as described in section 7.3.

The activity for the service and process architecture (SA.2) includes the service enabling, the migration and evolution strategy and the operations map. The service enabling topics should address the alignment with and support of the data space architectures with the various types of AI service providers as currently emerging and the development and deployment of services, data apps and user interfaces for data services providers and consumer for easily connecting with (and shielding of) the complexity of the inner working of data spaces. The operations map addresses the roles and processes developing and operating the various roles, building blocks and associated processes in the federation of AI data spaces. The service enabling and operations map topics should be addressed in 2023 – 2024 timeframe.

The activity for integration and validation (SA.3) must be an is continuously ongoing activity in which the AI data space architecture and building blocks are assessed by the NL AIC working group Data Sharing on technical and market viability, e.g. by means of use case development and reference implementations.

9.2 Developing the building blocks

The activities in the building block architecture view address the further development of the building blocks according to the grouping as introduced in Table 2, section 4.3, i.e. activities for the development of building blocks for the data space trust architecture on data sovereignty management (BBA.1), for the data space trust architecture on identity management (BBA.2), for the data space interoperability architecture (BBA.3) and for the data space value creation architecture (BBA.4).

- The activity for the further development of the building blocks in the data space trust architecture on data sovereignty management (BBA.1), includes the work on the security gateway, the policy registry, the policy enforcement framework and the application container environment building blocks. The work on these building blocks is continuously ongoing in the subsequent years as it provides key data sovereignty capabilities. Specifically the development of building blocks in alignment with the main EU reference architecture initiatives working towards more fully distributed data sovereignty architectures as described in section 7.3 (IDSA, Gaia-x, DSBA, …) should be included, closely together with the development on the (open source implementation of) the security gateway.

- The activity for the further development of the building blocks in the data space trust architecture on identity management (BBA.2), encompasses the management of various aspects of identities of AI data space participants, based on the (combined) capabilities of the data space membership certificate authority system building block, the dynamic attribute provisioning service building block and the participant information system building block. Specifically the potential, role and positioning of distributed identity architectures and protocols (e.g. Self Sovereign Identity (SSI) based on Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs)) should be assessed and developed as part of the trend towards a more fully distributed federative data sharing architecture and trust interaction patterns as described in paragraph 5.1.2 and section 7.3.
- The activity for the further development of the building blocks in the data space interoperability architecture (BBA.3) develops (in combination and coherence) the building blocks as required for exposing, finding and using various ICT-resources available in the ecosystem of federated AI data spaces. This encompasses the building blocks for the data space metadata broker and app store. Moreover, it contains the building blocks for managing semantics, i.e. the vocabulary hub, the semantic transformation engine and the data space connector semantics configurator. The initial version for these building blocks have been realised in 2022 and demonstrated as part of the reference implementation as described in chapter 8 and elaborated in annex B. These should be further developed in the timeframe 2023-2024 with specific focus on defining and standardising the interfaces of their associated building blocks.
- The activity for the further development of the building blocks in the data space value creation architecture (BBA.4) targets the building blocks to enable the administrative processes for valorising, monetising and logging/monitoring actual data sharing transactions. It includes the building blocks for the contract manager, the clearing house and the billing engine. To a major extend, the capabilities that these building blocks provide may be available as generic, common-of-the-shelf, IT-solutions.

The status and development proposal for each of the building blocks is provided in Table 4.

Table 4: Building Blocks: Status and Development Proposal.		
Building Block	**Status**	**Proposal for Further Development**
Data Space Trust Architecture Building Blocks: Data Sovereignty Management		
Security Gateway	Open source solution available, e.g. as TNO Security Gateway (TSG, see annex C).	
Policy Enforcement Framework	Completed, open source solution available within the TNO Security Gateway (TSG).	Further extend offered capabilities, e.g. types of policy enforcement.
Policy Registry	First research version available.	Consider further development to mature the policy registry building block.
Application Container Environment	Available.	Further extend offered capabilities, e.g. improve orchestration controlled via security gateway.
Data Space Trust Architecture Building Blocks: Identity Management		
Data Space Membership Certificate Authority System: DS CAS	Not available yet.	Consider usage of existing CA solutions.
Dynamic Attribute Provisioning Service: DAPS	Available.	Investigate integration with Gaia-X initiatives, e.g. usage of SSI.
Participant Information System: ParIS	Open source solution available.	Consider usage of open source solution and/or usage of/integration with existing iSHARE satellite.
Data Space Interoperability Architecture Building Blocks		
Data Space Metadata Broker	Initial open source solution available.	Consider usage of open source solution and usage of GAIAX Federated Catalogue solutions.
App Store	First research version available.	Consider further development to develop the app store component.
Vocabulary Hub	Initial open source solutions available.	Extend specification in the next IDSA RAM release and consider and extend existing solutions like the Semantic Tree House of TNO.
Semantic Transformation Engine	Initial solutions available to be open sourced in 2023.	Consider usage and extension of existing open source solution.
Data Space Connector Semantics Configurator	Initial version developed as part of the semantic treehouse vocabulary hub.	Consider usage and extension of solution.
Data Space Value Creation Architecture Building Blocks		
Contract Manager	Not available yet	To be investigated.
Clearing House	Initial open source solutions available.	Consider usage of existing open source solution and investigate available COTS products.
Billing Engine	Not available yet.	Consider and investigate usage of available COTS products.

9.3 Developing the trust architecture

The activities in the trust architecture view address the further development of the intra AI data space authority architecture (TA.1) and the trust interaction framework (TA.2).

The intra AI data space authority architecture (TA.1) develops the legal framework, the trust monitoring framework, the certification framework and the data quality framework to assure trustworthiness of participants and/or components in the AI data spaces. These frameworks operate both on the organisational level of the AI data spaces and on the technical level. The work on these aspects of the AI data space authority architecture should start in 2023 as part of the broader community development.

The trust interaction framework (TA.2) providing the trust, security and controlled access capabilities to ensure trust in the data sharing infrastructure, the metadata being shared and the data sharing transations. It encompasses the capabilities to enable hybrid environments with both homogeneous and heterogeneous trust interaction patterns as described in section 7.1 and to support the trust interaction guidelines as addressed in section 7.2. The work on the trusted interaction framework has started in 2022. It needs continuation with strong emphasis on both evolution and migration aspects and with interoperability between multiple AI data spaces.

10. CONCLUSIONS

This reference guide report has elaborated the architecture, building blocks and development roadmap for intra AI data space interoperability. It builds upon the lessons learned from the work of the NL AIC working group Data Sharing as done in 2021/2022, pursuing the goal of evolving towards a 'federation of interoperable data spaces' as defined as ambition of the EU Data Strategy. It has addressed both the ecosystem architecture, the building block architecture and the trust architecture.

In a federated approach for AI data spaces, individual data space instances may have their own specific internal implementation of the architecture and building blocks. As such, the guidelines as elaborated in this report must be interpreted as a reference for developing individual AI data space instances, providing a rich set of features to support the challenges and requirements of AI. Nevertheless, adhering to these guidelines for individual AI data space instances will yield major benefits in both development efficiency and being prepared for interoperability with other AI data space instances.

The adoption of AI data spaces based on the reference guidelines as presented in this report is still in in its infancy. Nevertheless, the required basic technology is rapidly maturing. Therefore, to optimally take advantage of these newly available architecture, concepts and technologies further guidance is needed both on the uptake (including introduction, evolution and migration) by data sharing communities and organisations and on the architectural and technical deployment. At the same time, it is to be realised that standards are still in development. Hence, this reference guide may help organisations with their initial steps towards AI data spaces, whilst being aware fact that the environment, architecture, concept and standards are evolving. Moreover, data sharing communities and organisations can contribute to their further development by implementing proof-of-concepts and use cases for (federated) AI data spaces providing feedback and input for extension and improvement to the reference guides.

In the further development of the architecture, concepts and technologies as described in this reference guide for intra AI data space interoperability, alignment with the main (inter-)national reference architecture initiatives on federative data sharing should be a focal point, especially the Open DEI, IDSA, Gaia-X, FIWARE and the DSBA initiatives (as described in paragraph 5.1.2). These reference architecture initiatives are developing towards fully distributed trust framework capabilities for identity, authentication and authorisation (IAA), contract negotiation and usage control. They still have to prove their technical and market viability for large scale deployment in AI data spaces. Nevertheless, striving for alignment could already prevent from incompatible standards and implementation of similar capabilities in different technology silos, which may complicate the required interoperability in and migration to a federation of interoperable AI data space considerably. Hence, the work as presented in this report on intra AI data space interoperability is work-in-progress. The know-how and expertise of the participants of the NL AIC working group Data Sharing can provide a major contribution to the collaborative development, roadmap and operation introduction of a (federation of) AI data spaces in the Netherlands and the EU.

REFERENCES

[1] The Netherlands AI Coalition working group Data Sharing (2021). "Towards a federation of AI data spaces - NL AIC reference guide to federated and interoperable AI data spaces". URL: https://nlaic.com/wp-content/uploads/2021/11/NL_AIC_Towards_a_federation_of_AI_data_spaces.pdf.

[2] The Netherlands AI Coalition working group Data Sharing (2022). "Reference guide for inter AI data space interoperability - Inter data space development line". URL: https://nlaic.com/wp-content/uploads/2023/04/reference-guide-for-inter-ai-data-space-interoperability.

[3] The Netherlands AI Coalition working group Data Sharing (2022). "Key insights AI use cases and demos - Report of NLAIC Data Sharing Working Group serving as inspiration for further development of AI data spaces". Available for NL AIC Community Member. URL: https://community.nlaic.com/groep-media/data-delen/221223-publication-version-nlaic-use-case-summaries.

[4] The Netherlands AI Coalition. "About NL AIC". URL: https://nlaic.com/en/about-nl-aic.

[5] The Netherlands AI Coalition working group Data Sharing (2020). "Verantwoord datadelen voor AI". URL: https://nlaic.com/wp-content/uploads/2020/03/Verantwoord-datadelen-voor-AI.pdf.

[6] The Netherlands AI Coalition working group Data Sharing (2020). "Responsible data sharing in AI". URL: https://nlaic.com/wp-content/uploads/2020/10/Responsible-data-sharing-in-AI.pdf.

[7] The Netherlands AI Coalition working group Data Sharing (2020). "Van First-time-Engineering naar Operationalisatie". URL: https://nlaic.com/wp-content/uploads/2020/08/NL-AIC-Naar-First-time-Engineering-en-Operationalisatie.pdf.

[8] The Netherlands AI Coalition working group Data Sharing (2021). "GAP-analysis- From data sharing proofs-of-concept towards operationalisation of the system architecture". URL: https://nlaic.com/wp-content/uploads/2021/03/NL-AIC-GAP-Analysis.pdf.

[9] The Netherlands AI Coalition working group Data Sharing (2021). "AI Ecosystem & Market Analysis - Quick scan of data sharing market to validate blueprint of the NL AIC". February 2021. URL: https://nlaic.com/wp-content/uploads/2021/02/AI_Ecosystem_and_Market_Analysis_Data_Sharing_4-feb-2021.pdf.

[10] EU Digital Europe Programme. "Data Spaces Support Centre (DSSC)". URL: https://dssc.eu.

[11] EU Digital Europe Programme, "SIMPL: cloud-to-edge federations and data spaces made simple". URL: https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple.

[12] The Data Sharing Coalition. "Unlocking the true value of data". URL: https://datasharingcoalition.eu.

[13] The Netherlands AI Coalition working group Data Sharing. "Data Sharing Building Block". URL: https://nlaic.com/en/building-blocks/data-sharing.

[14] Gaia-X. "Gaia-X Hub - The Netherlands". URL: https://gaia-x.nl/en.

[15] The Open Group. "TOGAF 9.1". URL: https://pubs.opengroup.org/architecture/togaf91-doc/arch.

[16] European Commission (2020). "A European strategy for data". URL: https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

[17] European Commission (2022). "European Data Governance Act". URL: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act.

[18] EU Open DEI project. "Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitising European Industry". URL: https://www.opendei.eu.

[19] EU Open DEI project (2021). "Design Principles for Data Spaces – Position Paper". URL: https://design-principles-for-data-spaces.org.

[20] Protium. "Overzicht Internationale Ontwikkelingen – Federatief Zakelijk Data Delen". URL: https://www.slideshare.net/gerardvanderhoeven/220222federatiefdatadelentopsectorlogistiekpdf.

[21] The Netherlands AI Coalition working group Data Sharing (2022). "AI data space value proposition - Clarifying the added value of launching a scalable and interoperable AI data space". URL: https://community.nlaic.com/groep-media/data-delen.

[22] International Data Spaces Association (IDSA) (2019). "International Data Spaces: Reference Architecture Model Version 3". URL: Error! Hyperlink reference not valid..

[23] International Data Spaces Association (IDSA) (2022). "International Data Spaces: Reference Architecture Model Version 4". GitHub URL: https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0.

[24] Go-Fair. "FAIR Principles". URL: https://www.go-fair.org/fair-principles.

[25] European Union (2017). "New European Interoperability Framework (EIF) – Promoting seamless services and data flows for European public administrations". URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.

[26] International Telecommunications Union (ITU) (2004). "Enhanced Telecom Operations Map (eTOM) - Using B2B inter-enterprise integration with the eTOM". ITU-T Recommendation M.3050.4.

[27] International Data Spaces Association (IDSA). "IDS-G on GitHub". URL: https://github.com/International-Data-Spaces-Association/IDS-G.

[28] International Data Spaces Association (IDSA). "Overview on the IDS Repositories on GitHub". URL: https://github.com/International-Data-Spaces-Association/idsa/blob/main/overview_repositories.md.

[29] EU Gaia-X Initiative. "A Federated and Secure Data Infrastructure", URL: https://www.gaia-x.eu.

[30] EU Gaia-X Initiative. "Gaia-X Federation Services - GXFS", URL: https://www.gxfs.eu/specifications.

[31] FIWARE. "Components". URL: https://www.fiware.org/catalogue.

[32] Dutch Neutral Logistics Information Platform (NLIP). "iSHARE Data Sharing Initiative". URL: https://www.iSHAREworks.org/en.

[33] iSHARE Foundation. "(Benefits) For Data Spaces", URL: https://ishare.eu/ishare/benefits/for-data-spaces.

[34] Data Space Business Alliance (DSBA). "Unleashing the European Data Economy", URL: https://data-spaces-business-alliance.eu.

[35] Data Space Business Alliance (DSBA). "Technical Convergence Discussion Document". URL: https://data-spaces-business-alliance.eu/dsba-releases-technical-convergence-discussion-document.

[36] European Commission (2022). "Simpl: cloud-to-edge federations and data spaces made simple". URL: https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple.

[37] European Commission (2022). "Architecture vision document - Preparatory work in view of the procurement of an open source cloud-to-edge middleware platform". URL: https://ec.europa.eu/newsroom/dae/redirection/document/86241.

[38] Eclipse Organisation. "Eclipse Dataspace Components". URL: https://projects.eclipse.org/projects/technology.edc.

[39] OASIS (2013), "eXtensible Access Control Markup Language (XACML) Version 3.0", OASIS Standard. URL: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[40] Jung, C., Eitel, A. & Schwarz, R, "Enhancing Cloud Security with Context-aware Usage Control Policies", C. Fraunhofer Institute for Experimental Software Engineering IESE, Informatik 2014. URL: https://cs.emis.de/LNI/Proceedings/Proceedings232/211.pdf.

[41] IDSA (2021). "IDSA Position Paper: Usage Control in the International Data Spaces". URL: https://internationaldata spaces.org/data-sovereignty-updated-position-paper-on-data-usage-control-in-the-ids.

[42] World Wide Web Consortium (W3C) (2018), "ODRL Information Model 2.2", W3C Recommendation. URL: https://www.w3.org/TR/odrl-model.

[43] GitHub. "omejdn-daps". URL: https://github.com/International-Data-Spaces-Association/omejdn-daps.

[44] GitHub. "ParIS Open core". URL: https://github.com/International-Data-Spaces-Association/ParIS-open-core.

[45] EU Gaia-X Initiative. Gaia-X - Architecture Document - 22.04 Release. URL: https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-X-Architecture-Document-22.04-Release.pdf.

[46] W3C. "Verifiable Credentials Data Model v1.1". URL: https://www.w3.org/TR/vc-data-model/#presentations.

[47] EU. DCAT Application Profile for data portals in Europe Version 2.1.0. URL: https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/dcat-application-profile-data-portals-europe/release/210.

[48] GitHub. "IDS Metadata Broker Core". URL: https://github.com/International-Data-Spaces-Association/metadata-broker-open-core.

[49] GitHub. "IDS AppStore". URL: https://github.com/International-Data-Spaces-Association/IDS-AppStore.

[50] VOCOREG. "VoCol Service". URL: https://www.vocoreg.com.

[51] Semantic Treehouse. URL: https://www.semantic-treehouse.nl.

[52] RML.io. "RDF Mapping Language (RML)". URL: https://rml.io/specs/rml.

[53] Berg, van den W. etc al (2022) "The Vocabulary Hub to configure data space connectors". Position paper Workshop Data Spaces & Semantic Interoperability, Vienna. URL: https://www.trusts-data.eu/data-spaces-semantic-interoperability/workshop-report-pictures-slides.

[54] GitHub. "IDS Clearing House Core". URL: https://github.com/International-Data-Spaces-Association/ids-clearing-house-core.

[55] GitHub. "IDS Clearing House Service". URL: https://github.com/International-Data-Spaces-Association/ids-clearing-house-service.

[56] Deutsches Institut für Normung (2019). "DIN SPEC 27070: Reference Architecture for a Security Gateway for Sharing Industry Data and Services". URL: https://www.beuth.de/de/technische-regel/din-spec-27070/319111044.

[57] Data Sharing Coalition (2021). "Data Sharing Canvas - A stepping stone towards cross-domain data sharing at scale". URL: https://datasharingcoalition.eu/app/uploads/2021/04/data-sharing-canvas-30-04-2021.pdf.

[58] Alzheimer Nederland. "Factsheet cijfers en feiten over dementie". URL: https://www.alzheimer-nederland.nl/factsheet-cijfers-en-feiten-over-dementie.

[59] IDSA. "International Data Spaces Information Model". URL: https://w3id.org/idsa/core.

[60] IDSA. "International Data Spaces Information Model". URL: https://international-data-spaces-association.github.io/InformationModel/docs/index.html.

[61] W3C. "W3C Recommendation: ODRL Information Model 2,2". URL: https://www.w3.org/TR/odrl-model.

[62] ISO/IEC 27002 - Information technology — Security techniques — Code of practice for information security controls. URL: https://www.iso.org/standard/54533.html.

[63] ISO/IEC 27001 - Information technology — Security techniques — Information security management systems — Requirements. URL: https://www.iso.org/isoiec-27001-information-security.html.

[64] IEC 62443 standard on the secure industrial automation and control systems, URL: https://www.iec.ch/blog/understanding-iec-62443.

[65] TNO. "TNO Security Gateway (TSG) – Architecture and Documentation". URL: https://tno-tsg.gitlab.io.

[66] TNO. "TNO Security Gateway (TSG) – Code". URL: https://gitlab.com/tno-tsg.

[67] YAML Framework. URL: https://yaml.org.

ANNEX A: AI COLLABORATION MODELS: ILLUSTRATIVE USAGE FLOWS

The building blocks in the Information System Architecture (ISA) have in section 4.3 (Figure 7) been introduced and attributed to the roles in the business role model for intra AI data space interoperability. The business roles and their associated building blocks can support the four AI-collaboration models as described in section 2.2. The subsequent sections in this annex provide an illustrative usage flow for each the four AI-collaboration models, i.e. the Data Sharing AI-collaboration model, the Algorithm Sharing AI-collaboration model, the Third Party Processing AI-collaboration model and the Network Processing AI-collaboration model, respectively.

A.1 Data Sharing AI-collaboration model

In the Data Sharing AI-collaboration model, the data is transferred from the data services provider to the organisation executing the AI algorithm, i.e. an AI operator in the business role model for AI data spaces as depicted in **Figure 3**. Depending on the usage policies for the data, the AI operator can either use the data freely in its own security domain or is only allowed to perform some specific algorithm processing on the data. In the latter case the AI operator will need to enforce the agreed upon policies, e.g. by running certified AI algorithms as data apps on the shared data within its own security gateway. This allows for policy enforcement that can be 'proven', for example through remote attestation of the AI operator's security gateway configuration and/or transaction logging on the data transactions in the security gateways.

Figure 15 illustrates the high level usage flows in the Data Sharing AI-collaboration model in which the data services provider shares data with an AI operator, which uses its security gateway to process the data in a trustworthy and controllable manner, according to the policies defined by the data services provider. The app orchestration capability in the security gateways manages, monitors, starts and stops the various data apps.

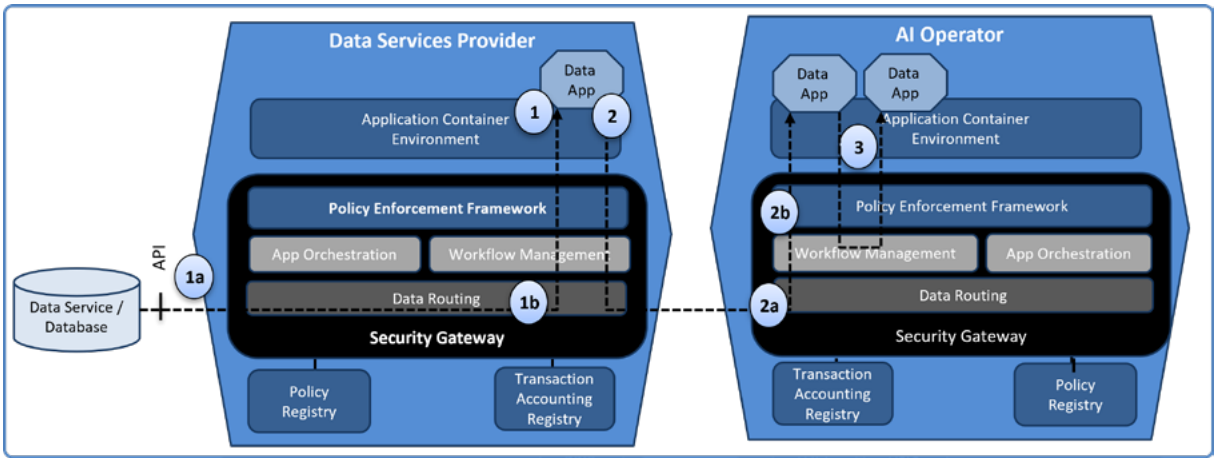

Figure 15 - Illustrative usage flow for the Data Sharing AI-collaboration model.

The figure shows the high level flow of interactions between the security gateways, excluding the interactions with the other AI data space building blocks (e.g. for identification, authentication and authorisation):

1. The data services provider retrieves a data set from its backend systems

   a. using a data retrieval data app running in its application container environment (security domain) over a predefined data service API for accessing the data services/database, and

   b. routing the data to the data app, controlled by the security gateway's workflow management capability (to manage data flows to and from the data app) and the policy enforcement framework building block (PEF, to validate data sharing policies).

2. The data app forwards the data to a data app on a security gateway of the data AI operator where

   a. the security gateway of the data services provider will route the data through the security gateway of the AI operator towards the appropriate data app by means of the workflow management capability (to manage data flows to and from the data app), and

   b. the security gateway of the AI operator will control the received data flow by applying the agreed-upon policies through the policy enforcement framework building block (PEF, to validate data sharing policies).

3. On the security gateway of the AI operator multiple data apps may be used to process the data, where the security gateway will control the data apps and the data flows using its workflow management and the PEF building block.

Additional supporting capabilities on the security gateway will ensure that the data being shared is augmented with the proper metadata (conforming to the standardised information model). Furthermore, the security gateway performs the required actions to identify and authenticate itself within the AI data space and requests other building blocks to do the same as part of the controlled data transaction process.

A.2 Algorithm Sharing AI-collaboration model

In the Algorithm Sharing AI-collaboration model, the AI algorithm is transferred from the AI algorithm provider to the organisation executing the AI algorithm. The organisation executing the AI algorithm may be a data services provider simultaneously being/acting as AI operator in the business role model for AI data spaces as depicted in **Figure 3**. The AI algorithm provider could for example be an organisation that develops AI algorithms as data apps to be executed within the application container environment (ACE) of a security gateway. As it is important within an AI data space that data is processed in a controlled and trustworthy manner, the AI algorithm provider will have its data apps certified to assure that data is processed as specified.

Figure 16 illustrates the high level usage flows in the Algorithm Sharing AI-collaboration model in which an AI algorithm provider shares its AI algorithm data app with a data services provider (also being an AI operator) to be executed within the ACE in the data services provider's security domain. In this example the AI algorithm provider is in full control of the sharing of its data apps and uses its own security gateway to share the policies for usage of the data apps and to manage the associated sharing transaction thereof.

The figure shows the high level flow of interactions:

1. The data services provider (also being an AI operator) retrieves an AI algorithm data app from the AI algorithm provider which:

   a. retrieves the AI algorithm data app from its local app registry, and

   b. forwards the data app to the security gateway of the data services provider using its data routing and workflow management capabilities and the PEF building block

2 The data services provider (also being an AI operator) deploys the data apps in the ACE by means of the app orchestration capability in its security gateway, i.e.:

   a. the AI algorithm data app as received from the AI algorithm provider, and

   b. the data retrieval data app for accessing its data services/database over a predefined data service API.

3. The data retrieval data app in the ACE of the data services provider (also being an AI operator) provides data to the AI algorithm data app by:

   a. retrieving a data set from the data services providers backend systems using a predefined data service API for accessing the providers data services/database, and

   b. routing the data to the AI algorithm data app, controlled by the workflow management capability (to manage data flows to and from the data app) and the PEF building block (to validate data sharing policies).

An alternative option would make the data apps of the AI algorithm provider available through an external app store provider business role as depicted in **Figure 3**. The app store provider may offer data apps developed by various algorithm providers. AI operators can download the data apps from the app store provider. This alternative option is elaborated as part of the Third Party Processing AI-collaboration model in the following section.

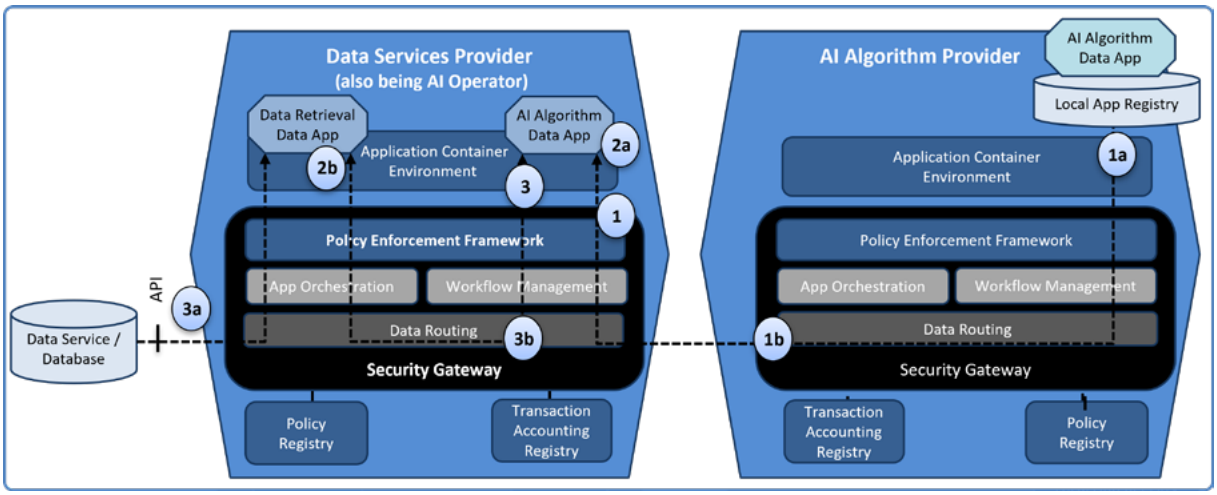

Figure 16 - Illustrative usage flow for the Data Sharing AI-collaboration model.

A.3 Third Party Processing AI-collaboration model

In the Third Party Processing AI-collaboration model, an AI orchestrator brings together data from a data services provider and AI algorithm data apps from an app store provider to be executed on the processing capabilities (i.e. the application container environment) of a third party AI operator. The AI orchestrator takes the responsibility for orchestrating the data sharing and AI algorithm execution process in such a manner that the applicable policies from each of the involved participants for sharing data, sharing AI algorithm data apps and executing AI algorithms are enforced. In this illustrative usage flow, the AI orchestrator and the AI operator are closely linked, as depicted in **Figure 17**.

Figure 17 illustrates the high level usage flows in the Third Party Processing AI-collaboration model:

1. The data services provider (as data entitled party) manages the sharing of its data by:

   a. using a data retrieval data app running in its ACE over a predefined data service API for accessing the providers data services/ database, and

   b. defining the data usage policies in its policy registry, and allowing an AI orchestrator (acting as data services consumer) to delegate its policies to AI operators,

2. The AI operator retrieves an AI algorithm data app from the app store provider where:

   a. the app store provider manages (on behalf of the algorithm entitled party) the sharing of AI algorithms by means of the AI algorithm usage policies in its policy registry, and allowing an AI orchestrator to delegate its policies to AI operators,

   b. the app store provider forwards the data app to the ACE of the AI operator using its data routing and workflow management capabilities and the PEF building block based on the AI algorithm usage policies, and

   c. the AI operator deploys and configures the received AI algorithm data app in the ACE within its security domain.

3. The AI algorithm data app executing in the AI operators ACE retrieves data from the data services provider where:

   a. the workflow management capability and the PEF building block in the data services provider the AI operator retrieve the data from the data services provider's data base and route it to the AI algorithm data app in the ACI of the AI operator, which may locally store the data in a secure local database [1],

   b. the AI algorithm data app executes on the data provided and shares the result with the AI-orchestrator.

   c. The AI orchestrator may share the results of the AI algorithm with the AI-beneficiaries, using the generic process for controlled and trusted data sharing between two participants of the AI data space.

It is noted that the use of delegation of polices in this scenarios for both the data services providers and the AI algorithm providers enable dynamic policy enforcement during the sharing and processing of the data. Their policies ae not shared with the AI orchestrator or AI operator, allowing for dynamic updating of policies and policy retraction in their own associated policy registry.

1 The mechanism implemented at the AI operator might differ from the example given here. In the described example a local data app was used to retrieve data form the local database, avoiding the need for data apps from the app store to implement database specific retrieval or storage APIs. Instead, they can use an API in which data is shared between data apps, which also matches the need of a more complex data pipeline with a consecutive flow of various data processing and AI algorithms executing data apps.

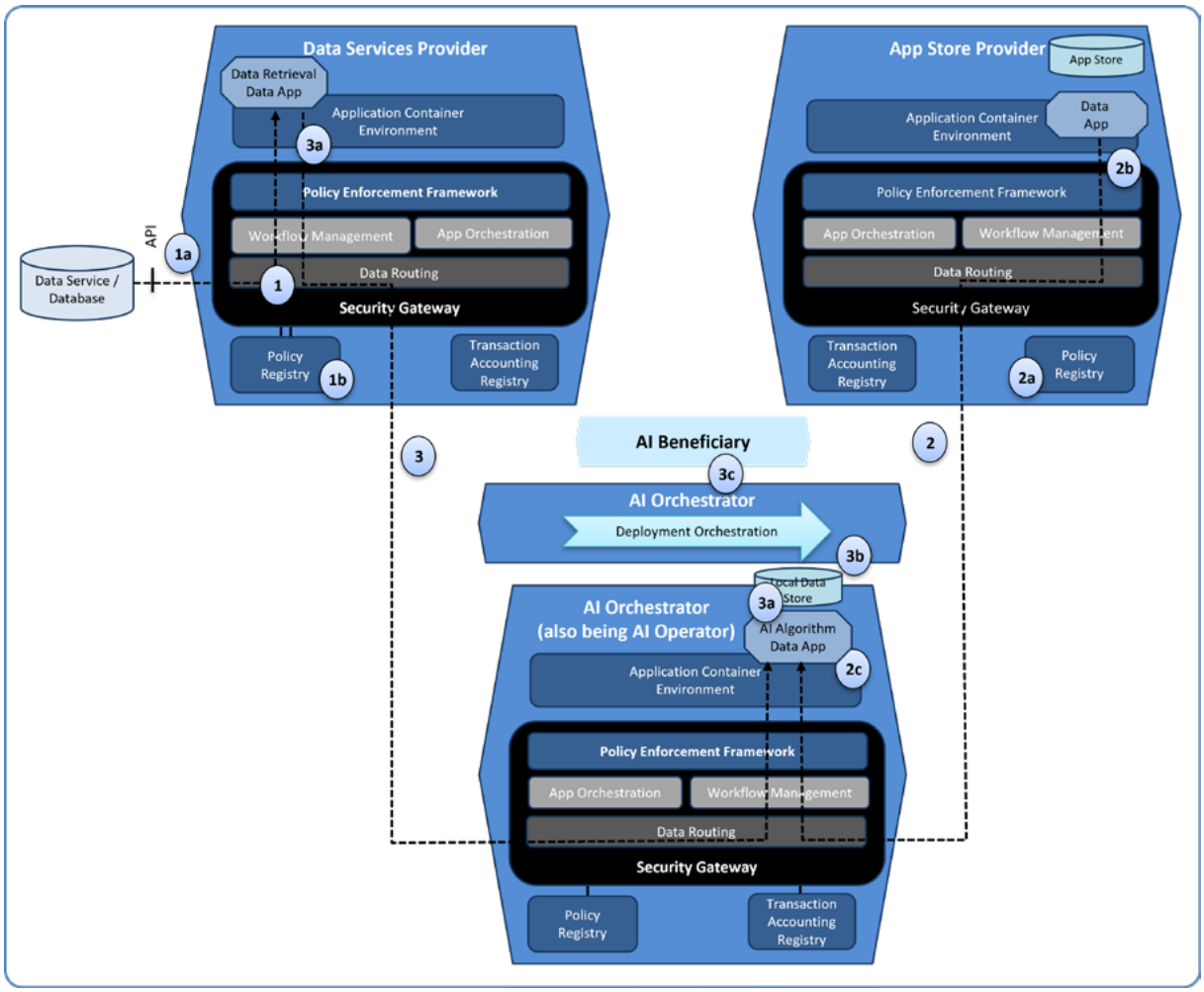

Figure 17 - Illustrative usage flow for the Data Sharing AI-collaboration model.

A.4 Network Processing AI-collaboration model

In the Network Processing AI-collaboration model, the execution of the AI algorithm on the data is done in a distributed manner by a network of participants, e.g. to enable Federated Learning (FL) or secure Multi-Party Computation (MPC). Access to data of various data services providers is required and multiple AI operators may be involved. As such, the Network Processing AI-collaboration model reflects a (complex) combination of the Data Sharing, the Algorithm Sharing and the Third Party Processing AI-collaboration models as illustrated in the previous sections. Therefore, it is referred to the previous sections for the illustrative (high level) usage flows of interactions the Network Processing AI-collaboration model. These are not further elaborated in this section.

A good example for using the Network Processing AI-collaboration model is for the case of FL where multiple data sets provided by different data services providers are used to train a model. In this case, the model may be trained using the initial data set of a specific data services provider, after which the (partially) trained model is forwarded to a next data services providers for further training on its data set.

For this FL example, as for the Algorithm Sharing AI-collaboration model, the data services providers take on the role of AI operator. They locally run the AI algorithm data app (in this case a local 'FL worker') on their data set and forward the results (i.e. the partially trained FL model) to the next data services provider. The AI algorithm data app on this next data services provider can take the partially trained model as input and further train the FL model with its own data. On its turn, it forwards the updated (partially) trained model again to subsequent data services provider. The whole process could be much more complex involving more than one data app to process the data. The workflow script processed at each of the data services providers might differ slightly but together will form the complete FL process.

An AI Orchestrator is in the lead to configure the (execution) of the workflow scripts for the individual workflow management capabilities in the security gateways for each of the participants into the complete data sharing and execution process for Federated Learning with the handovers between the (security gateways of the) participants. Each of the data services providers can have its own policy registry and policy enforcement framework to ensure data and AI algorithms are shared according to the policies as defined by the entitled parties. Moreover, a validation process is required at the data services providers to ensure the workflows (as configured by an AI orchestrator) are defined according to its policies for data app execution and routing of data sets and are enforced accordingly.

ANNEX B: REFERENCE IMPLEMENTATION: SCENARIO, ENVIRONMENT, STORY LINES

The reference implementation validates and demonstrates the potential of the architectural concepts and technologies for intra and inter AI data space interoperability and identifies lessons learned for developing towards large scale adoption. It uses a geriatric health care case as illustrative and representative scenario, but is equally well applicable for other sectors and application areas.

The initial sections in this annex describe the high level reference implementation scenario of geriatric health care and its associated data sharing environment, after which the subsequent sections elaborate its illustrative and representative story lines on the network processing AI collaboration model, on data sovereignty and technical (trust) interoperability and on semantic interoperability, respectively.

B.1 Reference implementation scenario: geriatric health care

As described in chapter 8, the reference implementation scenario focusses on geriatric health care. Geriatric health care is used as it covers the various complexities and concepts of data sharing for AI, both applicable to intra and inter AI data space interoperability. It is considered both illustrative and representative due to:

1. the privacy and sensitive nature of the data as input for AI processing, and
2. the diversity in participants in the processing of geriatric data, e.g. hospitals, general practitioners, elderly and nursing homes and government agencies.

The architectural concepts and technologies as validated and demonstrated in the reference implementation are considered to be similarly applicable to a broad range of AI data sharing use cases in other sectors and application areas as well.

B.2 Reference implementation environment: participants, data spaces and building blocks

The data sharing environment for the reference implementation emulates:

- Two hospitals, being participants of separate AI data space instances, both adopting the reference guides as described in this report.

  The hospitals provide patient data with CT-scans of brains and patient medications.

A home care organisation for elderly patients, being participant of an OAuth 2.0 -based data space, for which an iSHARE data space is chosen.

The home care organisation serves their patients with medicines and treatments on Alzheimer disease. It wants to share the information on patient's medicine use and treatments with the hospitals for research and development of improved Alzheimer treatments.

The hospitals in the reference implementation aim to bundle their data and find new treatments to Alzheimer disease. They set out to better recognize Alzheimer patients. Their hypothesis is that this should be possible by training a neural network on the available data sets to better recognize patients with early onset dementia. However, neither of the hospitals has a large enough data set to train an accurate network on its own. Moreover, due to privacy-sensitivity, the hospitals are not willing or allowed to share their patient data. As such, they decide to deploy a federated learning algorithm which is trained locally, i.e. within the hospital's own security domain. In this manner, a better trained model is obtained without having to share sensitive data between the hospitals or with third parties.

In addition, to further research potential new treatments to Alzheimer disease, one of the hospitals decides to ask for help from home care organisations, which have detailed insight into the medicine usage of a large set of elderly citizens. If they can correlate the medication of elderly patients with the progression of Alzheimer, or lack thereof, a new treatment using an existing drug may be discovered. For this the hospital requests the data of the patients medicine usage at home care organisation. The hospital can then correlate this information on medication usage with their already known disease progression data.

As stated, the three participants in the reference implementation are each member of a different data space. The system architecture of the reference implementation with the three data space instances and their associated building blocks is enumerated in Table 5, jointly demonstrate the capabilities for both intra and inter AI data space interoperability as described in this report and in the companion report [2].

Table 5: The reference implementation consisting of three data spaces and their building blocks

Hospital 1 (in AI data space A)	**Hospital 2** (in AI data space B)	**Home Care Organisation** (in OAuth2 data space, i.e. iSHARE)
• *Security Gateway* *- Incl Policy Enforcement Framework (PEF)* • *DAPS (Federable)* • *DS Metadata Broker (Federable)* • *Vocabulary Hub* • *Semantic Transformation Engine* • *Data Space Connector Semantics Configurator* • *App Store (for Distributed/Network Processing Collaboration Model Capabilities)*	• *Security Gateway* *- Inc. Policy Enforcement Framework (PEF)* • *Policy Registry* *- Both as internal PAP of the PEF (initial) and as external building block* • *DAPS (Federable)* • *DS Metadata Broker (Federable)*	• *iSHARE Authorisation Registry`* • *iSHARE Satellite*

As the table shows, not all building blocks are implemented in each AI data space of the reference implementation. In this manner, also the inter AI data space interoperability capabilities can be demonstrated. For example, the app store building blocks is positioned in AI data space A, while the data apps that it exposes and provides may be deployed in data space B. This demonstrates the sharing of data apps between AI data spaces (\as part of the inter AI data space interoperability architecture.

Additional remarks on the system architecture of the reference implementation as enumerated in Table 5:

- Providing certificates for data space membership to AI data space participants (i.e. capability of the Data Space Membership Certificate Authority System - DS CAS)) is done manually, i.e. not by a software building block.
- The ParIS building block is not included in the reference implementation as its capability is not essential for the story lines.
- The policy enforcement framework (PEF) has been implemented as part of the TNO security gateway (as described in paragraph 5.2.2 and annex C.2) and has not been included as separate building block.
- The policy registry corresponds to the capabilities of the Policy Administration Point (PAP) the, Policy Management Point (PMP) and the Policy Retrieval Point (PRP) of the PEF as described in paragraph 5.2.2. Therefore, it is also part of the TNO security gateway as elaborated in annex C.2. However, to support policy delegation capabilities and to make it into a generic building block for multiple participants it needs to be externalised as generic service, accessible through a well-defined API. In the initial version of the reference implementation, the internal PAP, PMP and PRP of the PEF in the TNO security gateway are used for policy registration, whilst a prototype of an externalised policy registry service/building block has been developed as well.
- The data value creation architecture building clocks (e.g. the clearing house and the billing engine as elaborated in section 5.5) are out of scope for the reference implementation as they are generic IT-modules which are not specific and essential for data sovereignty and secure data sharing in AI data spaces. Rather, they provide generic capabilities for monitoring, conflict resolution and monetisation of data and data sharing.

The various building blocks for AI data spaces as elaborated in the reference guides and enumerated in Table 5 are demonstrated and validated by means of the story lines of the reference implementation scenario as described in the following sections: (1) the story line on the network processing AI collaboration model, (2) the story line on data sovereignty and technical (trust) interoperability and (3) the story line on semantic interoperability.

B.3 Story line: network processing AI collaboration model

This story line addresses the optimisation of work flow management and data app deployment for easy setup of the data sharing environment to support the 'Network Processing' AI collaboration model as described in section 2.2 and illustrated in annex A.4.

In the 'Network Processing' AI collaboration model, the execution of the AI algorithm is done in a distributed manner by a network of participants, e.g. by means of Federated Learning (FL) or secure Multi-Party Computation (MPC). Both are considered as promising Privacy Enhancing Technologies (PETs)

to be used for cases in which (privacy or otherwise) sensitive data needs to be processed without this data leaving the security domain of the data services provider. Only processed data is being shared.

In this AI collaboration model, the local 'workers' for FL or MPC algorithms are developed as (third party) data apps to be deployed within application container environment of the security gateway of the data services providers. To enable ease of deployment of these (third party) data apps an app orchestration capability is needed within the security gateway to orchestrate (i.e. manage, monitor, start and stop) the execution. The app orchestration capability must interwork with the policy enforcement framework in order to validate data usage policies during the data sharing process. Moreover, a specialised 'networking data app' is needed for the configuration of virtual data sharing networks between the 'worker' data apps that are deployed at different data services providers and to orchestrate the interaction flow between them. To this end, the TNO Security Gateway (TSG) has been extended with the add-on capabilities for app orchestration and workflow management that declaratively describe the work flows, see also annex C. These app orchestration, workflow management and networking capabilities of the security gateway can not only improve ease-of-deployment of distributed FL and MPC algorithms but can also be used for many other complex orchestration and workflow management scenarios of AI data sharing and AI algorithm execution processes.

The following paragraphs further describe the illustrative health care cases of the network processing AI collaboration model for federated learning for horizontally partitioned data and multi-party computation for vertically partitioned data, respectively.

B.3.1 Case: federated learning for horizontally partitioned data

Not every patient with the same symptoms, complaints or illness visits the same hospital or health care provider. Because of this information about a particular illness is often spread over many health care providers, e.g. hospitals. Hence, each individual health care provider only has a partial view on the data about an illness. This partial view could be too small to be representative for the entire population. This disadvantages especially influences the successfulness of training AI algorithms, as these need sufficient data to be representative for the complete population of patients.

It is thus desirable to apply AI algorithms to more data that is available in a distributed manner over more health care providers. However, simply sharing all data with one centralised third party that applies the AI algorithm is undesirable – and often not allowed – due to the highly sensitive nature of patient data.

Fortunately, various approaches exist for training AI algorithms over distributed data without sharing this sensitive data. One such approach, that has proven itself in practice is Federated Learning (FL), in which data providers locally execute a 'worker' to compute a version of the FL model on its local data. Subsequently, they jointly compute an aggregate combined model and repeat the process. After several iterations of local computations and aggregations, the combined model is trained without any of the local data leaving the respective data providers' security domain.

This case demonstrates how the app orchestration, workflow management and networking capabilities of the security gateway can improve easy-of-deployment of distributed FL models to train a distributed FL model over a data set that is distributed over several data services providers. The data of each

data services provider has exactly the same features, but the data entries belong to different patients. This is called a horizontally partitioned data set. The FL process consists of the following interactions between the various roles in the business role model for AI data spaces as depicted in **Figure 3** (see also annex A.4):

1. an AI orchestrator initializes the FL process by distributing the FL worker data apps to the data services provider (also being AI operator),
2. the app orchestration capability in the data services providers security gateways deploy the FL worker data apps in the application container environment in its own security domain,
3. each data services provider (acting as AI operator) computes a local model update over its own data set,
4. each data services provider sends the parameters of the updated local model to the AI-orchestrator, i.e. without the sensitive patient data being shared,
5. the AI orchestrator aggregates the parameters of all updated local models as received from each data services provider to obtain an aggregated FL model, and
6. the AI orchestrator sends the updated parameters to the data services provider (acting as AI operator) for the next iteration.

In the reference implementation environment as described in section B.2, the case of federated learning for horizontally partitioned data is demonstrated and validated to train a FL model on two hospitals' patient data sets.

B.3.2 Case: secure multi-party computation for vertically partitioned data

Data of a specific patient is often stored in a fragmented manner at several health care providers. E.g., a general practitioner will have different data on a specific patient from a hospital. Moreover, different patient data is often spread over multiple hospitals. When data on specific patients is stored in a fragmented manner over multiple health care providers applying AI algorithms over the aggregated data sets becomes complex, especially when sharing of the (highly sensitive) patient health data is undesirable or not allowed.

This challenge seems very similar to the case of FL for horizontally partitioned data as described in the previous paragraph. Nevertheless, there is a difference in how the data is fragmented over the different data services providers. In the case of FL on horizontally partitioned data, all data services providers have data sets with the same features, but for different patients. In the current case, all data services providers have data sets on the same patients, but with different features. In other words, the data is partitioned vertically instead of horizontally, which causes problems for most FL approaches. However, there do exist other techniques that can handle computations on vertically partitioned data. In the current case a simple secure Multi-Party Computation (MPC) algorithm is used on vertically partitioned data.

Specifically, the case considers two data services providers that both have a patient data set, of which some patients are included in both data sets. However, both data services providers have different features of these patients in their data set.

The two data services providers (also acting as AI operators), together with a third party helper (acting as AI orchestrator), deploy an MPC-worker as local data app that jointly compute the aggregate over the features on the patients that are included in both data sets. In this distributed execution process the helper only learns the number of patients that is included in both data sets. Both data services providers (acting as AI operators) also learn this intersection size and also discover the aggregates. No participant learns anything about the features or patients included in a data set other than its own.

In this story line, both the data services providers (also acting as AI operators) and the third party helper (acting as AI orchestrator) leverage the app orchestration, workflow management and networking capabilities in the security gateway for ease-of-deployment of the MPC interactions. The sensitive patient data stays safely confined within the security domain of the data services providers. It only leaves the premises in an encrypted manner. The workflow management capability in the security gateways ensures that all interactions of the MPC-flow are followed in order and that the (encrypted) data is shared with the correct participants.

As for the FL case described in the previous paragraph, this case demonstrates how the app orchestration, workflow management and networking capabilities of the security gateway can improve easy-of-deployment of a distributed MPC workflow over multiple participants. The separation of the configuration of the MPC workflow and interaction network from the data apps that implement the distributed workers and helper of the MPC algorithm results in a considerably less complex deployment process. Especially for MPC, which is algorithmically complex by nature, this provides major advantages.

In the reference implementation the case of MPC for vertically partitioned data has not been implemented. However, the case of combining MPC with (IDS-based) data space architectures is currently elaborated in other data sharing projects.

B.4 Story line: data sovereignty and technical (trust) interoperability

Data sovereignty and trust represent key European values for data sharing. They are fundamental in the design of AI data spaces. A main aspect is the management of data sharing policies (i.e. usage- and access control policies), including the processes between data services providers and AI operators for defining- and agreeing upon policies and enforcing them. In the system architecture for AI data spaces these processes are enabled by various building blocks (see section 4.3 and section 5.4): the security gateway, the policy registry and the policy enforcement framework. This story line demonstrates the use of these three building blocks. The policy registry is used to register and manage the applicable data sharing policies, i.e. the specific access and usage conditions on data services or AI algorithms for data space participants as attributed by entitled parties. This may include delegation of access rights to other data space participants. The applicable (access and usage) policies in the policy registry are used by the policy enforcement framework in the security gateways of the various participants for technical enforcement.

Two commonly used approaches for governance of (usage- and access) policies are policy management with access tokens and policy management with contract negotiations. The main EU reference architecture initiatives on federative data sharing and data spaces (see paragraph 5.1.2: IDSA, Gaia-X, DSBA, ….) are developing towards distributed trust framework capabilities based on bilateral

contract negotiation and policy management and enforcement. These initiatives are still in development and have to prove their technical and market viability. Therefore, this story line will (initially) focus on the approach with access tokens.

Moreover, this story line addresses how this may be used when sharing the data between the participants being member of different data spaces, i.e. for inter data space interoperability. Interoperability between AI data spaces is key in extending the reach and scope of accessible data to be used for AI over individual data spaces. As described in section 3.2, interoperability has to be taken care of at each of the four levels of the European Interoperability Framework (EIF). For interoperability on the data sovereignty aspects, especially the interoperability aspects at the technical level as described in paragraph 3.2.1 are relevant. For this story line on data sovereignty through (access and usage) policy management, the aspects of identification, authentication and authorisation (IAA) across data spaces is relevant.

Specifically, in the reference implementation it is demonstrated how a hospital may limit access to its data to a specific data services consumer. Besides this, the reference implementation also supports sharing a data set with another data space participant, while including metadata on the allowed usage which can contractually be enforced, as well as including policies in the metadata.

B.5 Story line: semantic interoperability

As described in paragraph 3.2.2, a jointly used common semantic data model will (for many sectors and communities) appear to be an utopia. Therefore, capabilities for semantic transformation need to be supported in the system architecture for AI data spaces, for which the vocabulary hub, the semantic transformation engine and the data space connector semantics configurator building block have been identified as three semantic building blocks in section 4.3 and elaborated in section 5.4.

In the reference implementation, these three semantic building blocks jointly provide the capabilities to for semantic interoperability by enabling the use of different data models by data services providers and AI operators, either being member of the same or of different data space instances, without the need for customize data apps to be developed. In combination, they allow data and data sharing messages to be translated at run-time to another message structure using a different data model, using only a configuration file defined in a standard language. The required mapping files have to be defined only once. Separation between the mapping file definition and the execution thereof allows reusing the same application logic for different translations.

The combination of the data space approach and the translation engine provides a secure method of sharing data in which different data models may coexist, as long as a one-time mapping file is created between participants. It lowers integration cost and prevents providers from having to update their own internal system to be compatible with those of (multiple) other participants. The vocabulary hub building block provides the registry service for publishing, editing, browsing and maintaining vocabularies and related documentation. It can mirror a set of third party vocabularies ensuring availability and resolution, as provided by the vocabulary provider role in the IDSA business role model. The vocabularies and mappings from the vocabulary hub enable data space participants to use vocabularies to configure the semantic interoperability of data space connector implementations (i.e. data apps). This is done by creating ontology based

API specifications to specify the semantic interface between a data services provider and a data services consumer (e.g. an AI operator). Additionally the data space connector configurator can assist in creating mapping specifications if needed. These can subsequently be used and imported in the semantic transformation engine which provides run-time transformation between data formats as a generic service within the data space. Its transformations are based on the vocabularies and mapping specification as provided by the vocabulary hub. Alternatively to being deployed as a generic service within the data space, the semantic transformation engine building block can be integrated as data app in the application container environment of a data services consumer or a data services provider.

This story line demonstrates the use of the three semantic building blocks for data transformation at run-time as part of data sharing transactions. The three semantic building blocks are used in the reference implementation when sharing data by the home care provider with a hospital. Hospital 1 (acting as AI operator and data services consumer) first has to find and retrieve an appropriate data set from the data services provider (i.e. the home care provider), for which the federated metadata broker or federated catalogue is used. The home care provider uses a different data model and structure which has to be made understandable for the hospital so it can be analysed. To this end, the hospital uses the three semantic building blocks to do the transformation between both data models at run-time. It searches for an available semantic translation engine to convert the acquired data set to its internal data model, which is found on the app store and configured using a mapping file at the vocabulary provider. This allows the hospital to locally translate the data set within its own application container environment and use it for further analysis.

ANNEX C: THE SECURITY GATEWAY

This annex describes the capabilities, the functional design and the technical design of a security gateway, based on the reference architecture for IDS connectors. The following sections in this annex describe the generic security gateway architecture, the security aspects for the security gateway itself and the TNO open source implementation of a security gateway (referred to as the TNO Security Gateway - TSG), respectively. The TSG has built-in capabilities to interact with the building blocks for AI data spaces as described in this report, with additional network and app orchestration capabilities to support AI-collaboration models as described in this report (section 2.2).

C.1 Security gateway architecture

A security gateway provides the fundament for an AI data space. It provides capabilities for (standardised) data sharing between data space participants and a secure environment to execute data apps. As stated in paragraph 5.2.1, the IDS connector architecture, as defined in the IDSA RAM [22][23], can be used to implement the security gateway.

As such, the following paragraphs in this section build upon the architecture of the IDS-connector as basis for the security gateway for AI data spaces.

C.1.1 IDS Connector architecture

The IDS connector architecture as described in this paragraph stems (is copied) from its description in the IDSA RAM [22][23].

The IDS Connector must include some essential capability in its *Connector Core Service(s)*. The capabilities can be implemented in individual micro services or as a single comprehensive software block. In addition, the services do not have to be deployed in the same infrastructure.

The individual capabilities of the Connector Core Service(s) are shown in the figure. The figure intentionally does specify the external interfaces of modules but not the internal ones as these vary from implementation to implementation. The individual modules are:

- The *Authentication Service* holds the necessary information to authenticate the IDS Connector from/to other backend systems and/or authorize the system access from/to the IDS Connector from other IDS participants. For security reasons, a clear separation of the internal and external access credentials is recommended. The Authentication Service provides interfaces for configuration and to connect custom authentication services. In order to authorize incoming and outgoing connections it holds

  - the Key/Trust Store for the IDS Protocol(s),

  - the credentials for the access of the Data Management and Data Exchange to external systems, and

  - the information for the access control of the Data Exchange and Data Management to the IDS. This is shown via the solid line inside the IDS Connector.

- The *Data Exchange module* provides or requires interfaces to exchange data with other IDS Participants (providers/consumers). It can be deployed on another infrastructure than the IDS Protocol(s) module and it is possible to have more than one Data Exchange module

to support multiple protocol bindings. The Data Exchange module does not support IDS-specific interfaces nor does it interpret the IDS Information Model.

- The *IDS Protocol(s) module* supports at least one IDS specific interface defined in IDS-G to realize the processes defined in the Section 3.3. All modules interact with the IDS Protocol module as shown by the dashed lines.
- The *Remote Attestation module* is used to increase the trust between the participating modules. It can be used to detect whether the software has been modified at the other party's end (see Section 4.1 for more information). The module is needed for certification level 2 or higher (see Section 4.2.4).
- The *(Audit) Logging Service* is responsible for the logging of all relevant information during the operation of the module. For example, changes to settings, error messages, data accesses, and policy implementations should be logged. The information can also be passed on to corresponding systems that take over the (auditable) logging. Therefore, the module provides or requires an interface to this systems.
- The *Monitoring Service* is used to monitor the status of the module. It can be used to check, e.g., if the IDS Connector is running, remains in an error state, or is offline.
- The *Data App Management* module supports the download, deployment, and integration of IDS Apps in the IDS Connector.
- The *Policy Engine* summarizes all modules used for enforcing the IDS Usage Control Policies (part of an IDS Contract). These cover the Policy Administration Point (PAP), the Policy Enforcement Point (PEP), the Policy Information Point (PIP), the Policy Execution Point (PXP), the Policy Management Point (PMP), and the Policy Decision Point (PDP). All are described in detail in Section 4.1.6.
- The *Contract Management* module is responsible for managing the contract negotiation between Participants (see Section 3.3.3) and storing the IDS Contract Agreements afterwards. Contract management can be seen as part of _Metadata Management. However, it is visualised as a separate module due to the importance of Usage Control in IDS.
- The *Metadata Management module* holds the metadata of provided and consumed data assets. The metadata is mainly defined by the IDS Information Model, however, it can be further enriched with additional information. The metadata is coupled with the contracts from the Contract Management module and the data from the Data Management module.
- The *Data Management module* holds the data assets itself or holds a link to the data sources, data sinks, or IDS Apps to get or send the data assets to their interface dynamically.
- The *Configuration Management module* contains the configuration parameters for the IDS Protocols and all modules in general.
- The *User Management module* is responsible for providing user authentication for every interface of the modules. Therefore, the User Management can use external Identity Services or provide this service by itself. It also can be configured via an interface.

IDS Connectors are distinguished according to their certification level, which indicates, among other things, which security and data sovereignty criteria the IDS Connector implements.

There may be different types of implementations of an IDS Connector, based on different technologies and depending on what specific capability is required regarding the purpose of the Connector. As such, the TNO open source implementation of an IDS connector (referred to as the TNO Security Gateway - TSG) is described in the following section C.2.

C.1.2 IDS Information Model

The main role of the security gateway as IDS connector is to help participants to model their metadata according to the IDS Information Model [59], to enable them to share their data via IDS connectors of other participants in the data space. The IDS Information Model [60] uses ODRL [61] to model the usage policies for resources and uses RDF/OWL standards for the actual description of the metadata. The security gateway contains capabilities to define and append all necessary metadata of the IDS Information Model to the resources (data/ messages) transferred via the IDSCP interface with

By describing the data to be shared in the IDS Information Model, the security gateway will also be able to publish the provided data in the data space metadata broker (see paragraph 5.4.1) by means of self-descriptions.

The data apps running on the security gateway do not need to internally use the IDS Information Model but only need to encapsulate the shared data with IDS modelled metadata in the API towards the security gateway so it can be handled by other participants in the data space. It is optimal that all data shared by the participants in the data space uses the same (possibly domain specific) semantics and ontologies. If this is not the case, semantic building blocks (see paragraphs 5.4.2, 5.4.4, and 5.4.5) to support semantic transformations may be used to bridge the semantic gap.

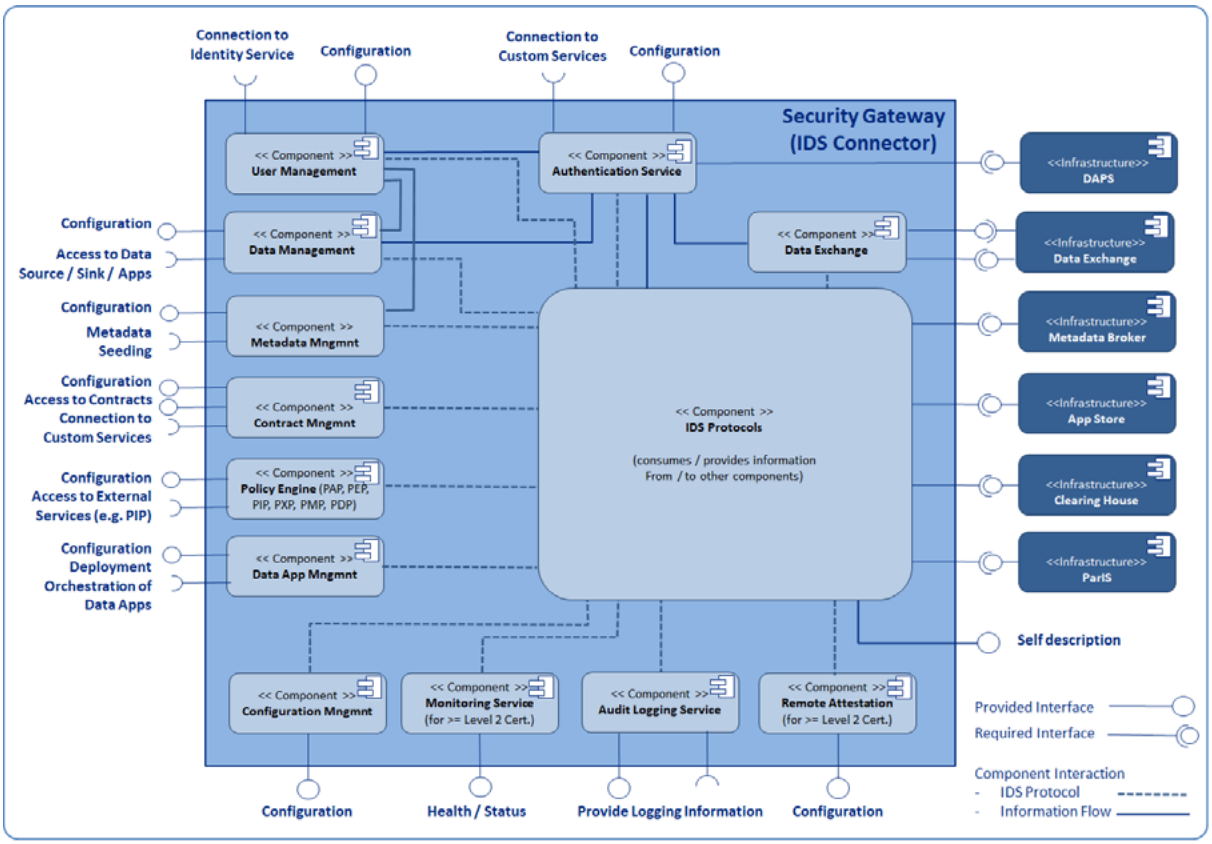

Figure 18 - IDS connector: functional view [22][23].

C.2 Security for the security gateway

The security gateway is a key module in providing trust between all modules in a data space. To ensure overarching trust within the data space it is important that all participants implement a minimum set of measures for securing the security gateway itself (as illustrated in **Figure 19**):

- The security architecture defines the *IDS Communication Protocol (IDSCP)*, which must be supported by all trusted security gateways. The purpose of the IDSCP is to establish confidential, authenticated communication, exchange data between the data space participants and allow for remote attestation (if supported by the Connectors involved);
- *Containerisation* (encapsulation) of the IDS connecter software to prevent unwanted interactions or interference with other software executed on the same server. Containerisation will prevent usage of any other interface with the software that the ones defined for access, thereby ensuring data no data can be leaked via other interfaces than allowed and other software cannot access the security gateway in any other way than the formally defined interfaces;
- *Encryption* on all interfaces with the security gateway so none of the communicated information is visible for unauthorised apps/ software. This not only includes encryption of the interfaces with IDSCP and the policy registry but also interfaces with the data apps

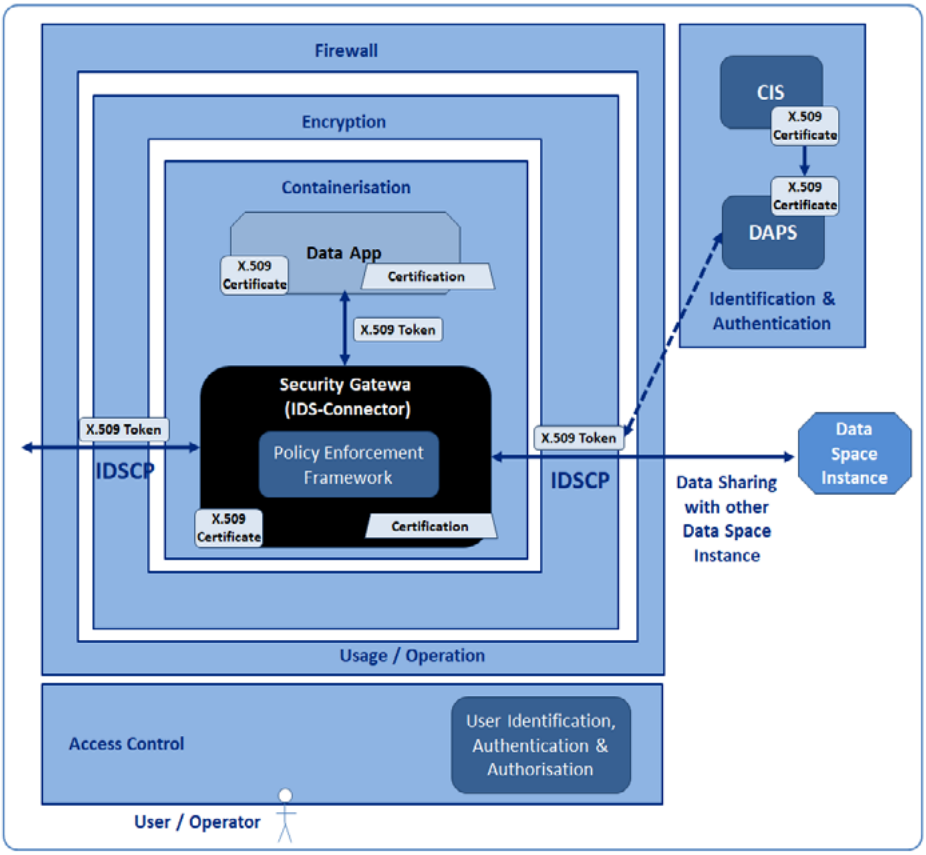

Figure 19 - Security architecture of the security gateway.el.

controlled by the security gateway. For initiation of the encryption (e.g. using TLS) the X.509 tokens are used (as part of the identification & authentication capability);

- Although outside the scope of the security gateway, usage of proper *firewalling* is advised to prevent unauthorised access to the security gateway and defend the software against security attacks;
- *Access control* for users and operators that need to access the security gateway. It is assumed that IT environment in which security gateway is executed is equipped with access control system that will provide a secure identification, authentication and authorisation mechanism on user/operator level;
- *Application of best practices* (e.g. ISO/IEC 27002 [62]) for the overall software security (e.g. systems are cleaned (unused software removed), all software regularly updated, especially with known security patches (e.g. for OS) and checked on viruses) and physical security (e.g. only authorised personnel have access, servers are protected against theft and other threats, etc.) of the used IT environment.
- For the *security of the IT environment* in which the security gateway are deployed, implementation measures as proposed in the ISO/IEC 27000 standards, like implementation of an Information Security Management System (ISMS) [63], adoption of best practices [62] and (parts of) the IEC 62443 standard [64] on secure industrial automation and control systems can be considered. This is the responsibility of each of the data space participants.

Some of these measures are intrinsic part of the proposed security gateway technology module, but most are measures that should be set as requirements for the IT environment in which the module is to be executed (like firewalling, access control and software/physical security).

C.3 TNO Security Gateway (TSG)

The TNO Security Gateway (TSG) is an implementation of a security gateway based on the IDS-connector. The TSG has built-in capabilities to interact with the building blocks for AI data spaces as described in this report, with additional capabilities to support the various AI-collaboration models such as for network and app orchestration.

The TSG is open-source available [65][66].

The functional design of the TSG is based on the Information System Architecture and the Technical Architecture as described in section 4 and in chapter 5, respectively. It builds upon the architecture of the IDS connector as described in paragraph C.1.1. **Figure 20** depicts the functional design of the TSG.

As the figure shows, the functional design defines a number of interacting modules that clearly separate capabilities and allows for a modular realisation of the TSG, including:

- *Data Routing*: capability to technically route all messages handled by the connector (between security gateways, to/from data apps, to/from database) and provide framework for integrating routing with other capabilities in the connector (e.g. the Route Manager, the PDF and the Token Manager) to manage and possibly adapt the shared data, queue data, trigger capability on received data (e.g. one of the other functional modules) and perform the required data routing;

- *Policy Enforcement*: capability of the XACML framework (especially the Policy Decision Point (PDP)) to ensure that defined data sharing policies are enforced for all shared/handled data. The PDP will make use of polices from the policy registry (as Policy Administration Point (PAP)) to decide if data can be shared. To receive, manage and store the policies from the policy registry, the PEF also contains the Policy Management Point (PMP) capability for management and deployment of policies and the Policy Retrieval Point (PRP) capability for secure storage and retrieval of policies. The PDP will be triggered using Policy Enforcement Points (PEPs) from other modules, like the Routing Management capability. The policies themselves are defined in ODRL as description format. The PMP will receive policies and revocations via the Policy Administration Point (PAP), implemented by the policy registry. Optionally PIP and PXP capabilities could be included if needed (e.g. for retrieval of context information external to connector or triggering policy violations to external systems);
- *Remote Attestation*: capability to remotely verify integrity of another security gateway (which for example will handle shared data and will also need to enforce set usage policies);
- *Artefact Management*: capability to manage the shared artefacts (data instances);
- *Route management*: capability to manages all data routes within the connector and responsible for initiating the PDP at the appropriate PEP, while connecting data routes;
- *Resource management*: capability to manage IDS metadata of resources (data, processing, data apps) offered by the connector;
- *Self-Description*: responsible for constructing self-descriptions and interact with the metadata broker;
- *Application Orchestration*: capability within the security gateway to manage, control (start and stop) and monitor (on successful execution) data apps in the application container environment (ACE) building block;
- *Workflow Management*: capabilities to automatically manage and control data workflows between data sources and data apps in the application container environment, where app control is delegated to Application Orchestration. The idea behind the Workflow Manager is that the flow/routes of data between data apps, including the possible sequence of data packets exchanges between the data apps and the starting and stopping of data apps , could be made explicit using for example a YAML script [67]. Instead of hardcoding the sequencing in the data apps, defining rigid routed between the data apps and starting of data apps at the start of the data sharing process, the workflow could be automated using a script and a Workflow Manager that can interpret this script and execute the actions. The Workflow Manager is able to dynamically configure needed routes according to the defined workflow in the script and trigger Application Orchestration to start and stop required data apps. The additional benefit is that the whole process becomes more transparent and easier to adapt as the flow of data processing is made explicit using a script. A complete workflow or set of workflows of data apps on one or multiple connectors can be seen as "Data Analytics Engine" as mentioned in Open DEI position paper [19];

- *Token management*: responsible for the interaction of authentication tokens between the security gateway and the DAPS (see IDS RAM [22][23]) to ensure trusted communication between all participants and/or components in the data space;
- *Transaction verification and logging*: responsible for the verification of transactions at the clearing house and logging of all transactions relevant for billing of transactions with other ecosystem participants (e.g. for the sharing/usage of data and the execution of data apps);
- *Management*: the overall management of the security gateway. This will include required configuration of the different modules, connectivity to other modules in the ecosystem, connectivity the local Backend System and monitoring and maintenance capability;
- *Graphical User Interface*: capability for the user interaction with the IDS component to perform configuration, monitoring and management of the connector.

The TSG itself is containerised and executed under the full control of the Application Container Environment (ACE) component provided by the environment in which the TSG (and its data apps) is executed. Similarly the data apps that communicate with the TSG are also containerised. The Application Orchestration function of the TSG communicates with the ACE component to perform the actual app orchestration.

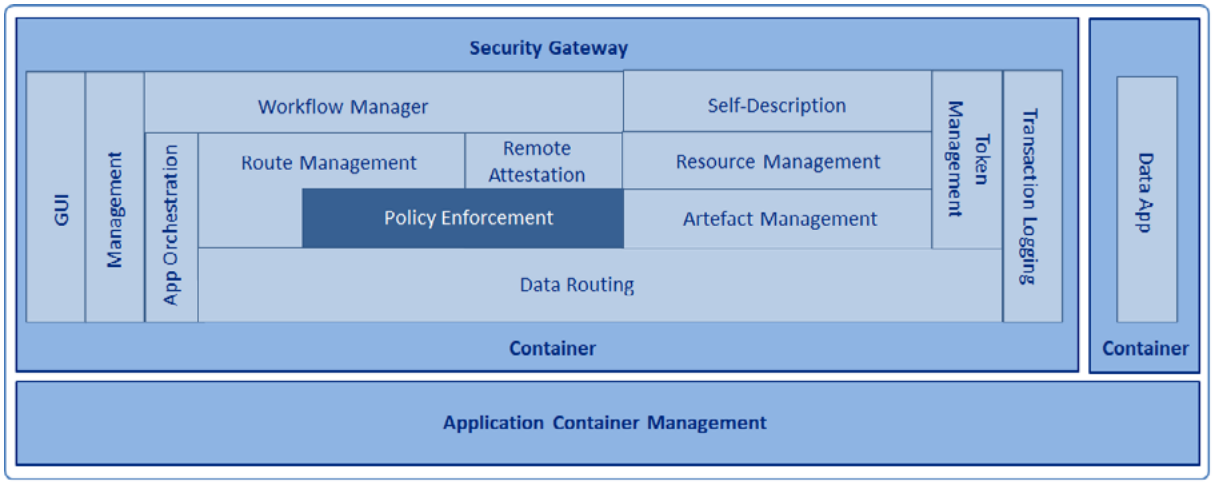

Figure 20 - Functional design of the TSG.

Colophon

This report is a result of the work of the NL AIC working group Data Sharing.

In conjunction with the overarching AI data space reference guide '*Towards a Federation of AI Data Spaces*' [1] and the companion report 'Reference Guide for Intra AI Data Space Interoperability' [2]. This report provides guidelines for realising the ambition of the NL AIC working group Data Sharing of providing the data sharing foundation for AI in the Netherlands in alignment with the interoperable data space approach as pursued by the EU Data Strategy [16].

Both the intra and the inter data space reference guide report on work-in-progress.

Contributors

Participants in the NL AIC working group Data Sharing
TNO (editors)

Review

Advisory Board of the NL AIC working group Data Sharing

Contact:
The Netherlands AI Coalition
E-mail — info@nlaic.com
Website — nlaic.com

March 2023