Infrastructural Sovereignty over Agreement and Transaction Data ('Metadata') in an Open Network-Model for Multilateral Sharing of Sensitive Data

Completed Research Paper

S. (Simon) Dalmolen MSc
University of Twente
Drienerlolaan 5
7522 NB Enschede
The Netherlands
simon.dalmolen@tno.nl

H.J.M. (Harrie) Bastiaansen PhD
Netherlands Organisation for applied scientific research TNO
Eemsgolaan 3
9727 DW Groningen
The Netherlands
harrie.bastiaansen@tno.nl

M. (Maarten) Kollenstart MSc
Netherlands Organisation for applied scientific research TNO
Eemsgolaan 3
9727 DW Groningen
The Netherlands
maarten.kollenstart@tno.nl

M. (Matthijs) Punter MSc
Netherlands Organisation for applied scientific research TNO
Kampweg 55
3769 DE Soesterberg
The Netherlands
matthijs.punter@tno.nl

Abstract

Organizations are becoming ever more aware that their data is a valuable asset requiring protection against mis-use. Therefore, being in control over the usage conditions (i.e. data sovereignty) is a prerequisite for sharing sensitive data in (increasingly complex) supply chains. Maintaining sovereignty applies to both the primary shared data and to the 'metadata' stemming from the data sharing support processes. However, maintaining sovereignty over this metadata creates an area of tension. Data providers must balance operational efficiency through outsourcing the data sharing support processes and the associated metadata to external, trusted, organizations against the added risk of transferring control over the metadata. At the same time, lock-in by community providers and major integration efforts due to multiple data sharing relationships need to be avoided. To address these issues, this paper elaborates an open network-model approach for maintaining sovereignty over metadata.

Keywords: Data Sovereignty, Metadata, Multi-lateral Data Sharing, Network-Model, Hub-Model, Service-Orientation, Terms-of-Use, Access and Usage Policies, Logging

Introduction

Organizations are increasingly working together to serve customers through mutually dependent and co-operative supply chains. Digitization is fundamentally changing these supply chain collaborations. As (Bharadwaj et al. 2013) state:

> "*Digital technologies are fundamentally transforming business strategies, business processes, firm capabilities, products and services, and key interfirm relationships in extended business networks.*"

Agile digital business networks are currently required to thrive competition in global markets and supply chains. However, digitization and data sharing in such business networks and supply chains pose major challenges from both an organizational and a technical/IT perspective (Luftman, Lyytinen, and ben Zvi 2017). In their transition towards more advanced digital supply chain collaboration, organizations are faced with a dichotomy. On the one hand, they are becoming ever more aware that data sharing is essential for being successful in the emerging data economy, whilst on the other hand data is recognized as a real valuable asset that should be handled by the organizations as such to prevent from mis-use (Marinagi, Trivellas, and Reklitis 2015), (Lee and Whang 2000), (Gunasekaran et al. 2017). They require that the organization's data is handled in a controlled and secure way as a prerequisite sine qua non the organization may not be prepared to share its data.

The key capabilities for (data sharing) in agile business networks have been identified as (Hillegersberg, Moonen, and Dalmolen 2012): (1) Modularization of Services, Products and Processes, (2) Coordination and Collaboration, (3) Quick Connect, and (4) Relationship Management. In this paper we address trust and data sovereignty as key aspects of the relationship management capability. Agility and flexibility in supply chains and business networks imply that trust and data sovereignty can no longer be based on long-term inter-organizational relationships. Rather, they must be governed in the digital data sharing infrastructure itself and should be incorporated by-design through integral capabilities. Advanced supply chain collaboration architectures should be built upon a 'data-centric' foundation (S. Dalmolen et al. 2015) (Nicolaou, Ibrahim, and van Heck 2013), which enables the organizations to be in control over their sensitive data.

The underlying needs and mechanisms that drive towards the inclusion of data sovereignty capabilities in data sharing infrastructures have been illustrated by an extensive (PricewaterhouseCoopers 2019) survey amongst a large set of executives of representative (German) companies. Its results indicate that main challenges and obstacles for data exchange as perceived by the survey participants are fear for security risks and worries about losing control over their data. A similar studies amongst companies in the Netherlands (Dutch Ministry of Economic Affairs and Climate Policy 2018) confirms these observations by concluding that 'Consent' (i.e. the owner being in control over his data) is one of the nine essential building blocks for data sharing initiatives.

Clearly, maintaining sovereignty by the data provider applies to sharing sensitive primary data. However, it also applies to the secondary data as required and generated by the data sharing support processes, referred to as 'metadata'. This metadata for instance includes the applicable data sharing agreement, the terms-of-use (expressed as access and usage conditions) and the logging and provenance information for specific data sharing transactions. However, maintaining sovereignty by the data provider over the metadata gives rise to operational challenges. An area of tension exists between on one hand the stringent data sovereignty requirements asking organizations to keep the control over this metadata by locally storing and processing it within their own security domain, whilst on the other hand the manageability and cost-efficiency thereof which tends organizations to transfer the management and storage of metadata to external and specialized organizations such as trusted third-party (TTP) data brokers and clearing houses. At the same time, lock-in by community providers and major integration efforts due to multiple data sharing relationships need to be avoided.

Therefore, this paper addresses the following research question: "*How can an infrastructure for multilateral data sharing optimally be developed for assuring trust and sovereignty of data and metadata for a data provider?*" Our contribution as presented in this paper encompasses an architecture based on a network-model approach with infrastructural trust and data sovereignty capabilities. It provides a solution for the data sharing challenges on trust, data sovereignty, community lock-in and minimization of integration effort as described above. Moreover it includes a service-oriented business architecture for intermediary data brokering and clearing house roles infrastructural to support sovereignty over metadata in a flexible manner. The proposed architectural approach is illustrated and elaborated for the International

Data Spaces (IDS) initiative, which is currently gaining major international attention as an open infrastructure for trusted, multi-lateral, data sharing (Otto et al. 2019).

The approach as presented in this paper extends beyond the capabilities of existing data sharing infrastructures. The current existing architectures mainly lack the required data sovereignty capabilities. Their functionality is restricted to exchanging data amongst organizations, where security mostly applies to encrypted data transactions, sometimes augmented with end-user identification and authentication functions (Otto and Jarke 2019), (Jarke, Otto, and Ram 2019). Authorization and data sovereignty across business domains are mostly lacking (Zrenner Johannes 2019).

The structure of this paper is as follows. The data sharing support processes and their associated metadata artefacts are described in the following section. The subsequent section addresses the benefits of an infrastructural data sovereignty by means of an open network-model approach for maintaining sovereignty over sensitive metadata. It is followed by a section elaborating the architecture from a technical, service and information security perspective. The subsequent sections provide (the status of) a practical case study on the architectural approach and concepts as described in this paper and provide a discussion on wide-scale adoption thereof, respectively. The final section provides the main conclusions and future work.

Data Sharing Support Processes and their Associated Metadata

Metadata is required for and generated by support processes for managing data sharing agreements and data transactions. Therefore, they form the basis for the service approach and architecture in this paper. The goal of the support processes is to enable the sharing of data and to prevent misuse of the shared data. They include the processes for data providers and consumers to comply with both internal (e.g. business) and external (e.g. regulatory) policies on data sharing. Table 1 lists and describes the main data sharing support processes, categorized according to the subsequent life-cycle stages in data sharing (Simon Dalmolen et al. 2019).

Table 1: Support Processes for Data Sharing, Categorized in Life-Cycle Stages.

Defining and publishing a data set.	
Subprocesses	• Definition of a data sharing profile • Publication of a data sharing profile
Making a data sharing agreement.	
Subprocesses	• Definition of terms-of-use, including usage and access control policies • Definition of the commercial and juridical conditions • Negotiation, acceptance and signing of the data sharing agreement
Performing a data sharing transaction.	
Subprocesses	• Clearing of the data sharing transaction, including non-repudiation • Data transfer, including binding of the transaction to an agreement • Settlement and discharging of the data sharing transaction
Logging, provenance and reporting.	
Subprocesses	• Logging and binding of data transactions to data sharing agreements • Tracking, monitoring and reporting of data transactions to stakeholders • Auditing, billing and conflict resolution

The data sharing support processes as listed in Table 1 require and generate metadata. On the one hand, the descriptions of the data to be shared and the data sharing agreements are metadata in themselves. On the other hand, the management, control and administration processes over their associated data sharing transactions are a major source of metadata. Table 2 lists and describes these metadata artefacts.

Table 2: Metadata Artefacts for the Support Processes for Data Sharing in Table 1.

Data descriptor	Description of the (type of) data available to be shared.

Data transaction	Specific data sharing instance of primary data, including the (combination of a) data request, data response, and the associated processes for management and administration thereof. It should be noted that we apply this both to the controlled sharing of data sets (e.g. inventory levels) as well as sharing of data resulting from a business transaction (e.g. data on a purchasing transaction).
Data request	Requesting by a data consumer for some data, mostly as part of a data exchange pattern, e.g. 'request–response' (in which the data request is a specific instance request a specific set of data) or 'publish-subscribe' (in which the data request is a request to be subscribed to a data topic).
Data response	Actual sharing of data by a data provider as response on a data request. As with a data request, the data response can be of a 'request–response' or 'publish-subscribe' data exchange pattern.
Data sharing agreement	Specifying the conditions under which specific data will be shared, consisting of the contractual conditions and the terms-of-use.
Access control policy	Stating which individuals, roles or systems are allowed access to the data provided
Usage control policy	Stating how the data may be used or distributed after access has been given to individuals, roles or systems.
Security profile policy	Stating the requirements on the security profile of the data consumer.
Service levels	Stating the quality parameters of the data provided, including completeness, accuracy and timeliness.
Terms-of-use	Combining the access control policies and usage control policies, expressing the data provider's internal (business) data sharing policies and the external (regulatory) policies.
Commercial conditions	Stating the commercial conditions under which the data will provided, including the costs of the data and the invoicing and payment conditions.
Juridical conditions	Stating the juridical aspects required (to avoid) conflict resolution, e.g. the IPR-conditions, the applicable law, ….
Contractual conditions	Combining the service levels, the terms-of-use, the juridical conditions and the commercial conditions.

The metadata artefacts for the data sharing support processes in Table 2 contain potentially sensitive information. As such, the data provider needs a well-defined business policy for maintaining sovereignty over this metadata. Outsourcing the enforcement of the data provider's business policy for maintaining sovereignty over his metadata to external (trusted) service providers might be an adequate approach for allowing the data provider to focus on its core business and to minimize its costs. However, such an outsourcing approach requires adequate service offerings on trust and data sovereignty enabling capabilities by external (trusted) service providers . How this can be done by means of a service-oriented business architecture in an open network-model is addressed in the following sections.

Infrastructural Sovereignty over Metadata in an Open Network-Model

Data sovereignty is the key prerequisite for data providers to share their potentially sensitive data. This applies to a multitude of data consumers and communities with which a data provider would like to share his data. However, it provides a major challenge as data sovereignty concepts are currently mainly provided by community solutions with their own specific solutions. Consequently, the data provider is faced with both a threat of customer lock-in by their community providers and with major integration efforts on defining and enforcing data sovereignty requirements in case of a multi-lateral data sharing. A single entry point for the data provider with common and agreed upon protocols for defining and enforcing terms-of-use for data sharing will give the data providers clear operational advantages in efficiency and effectiveness of managing his data sharing interconnections.

These challenges of enabling data sovereignty in a multi-lateral data sharing infrastructure are mainly due to its hub-based implementation by community solutions for trusted data sharing (Liezenberg, Chiel, Lycklama, Douwe, and Nijland, Shikko 2018), having their own specific solutions to providing data providers with data sovereignty maintaining capabilities. The hub-model is commonly used for sector specific, closed, communities. An open network-model approach for infrastructural sovereignty over (meta)data provides an attractive alternative.

The following subsections subsequently describe the design principles underlying the network-model approach, the International Data Spaces (IDS) initiative which is currently developing such a network-model approach and a the required service-oriented business architecture for providing the trust and data sovereignty capabilities in the network-model approach.

An Open Network-Model for Infrastructural Data Sovereignty

An open network-model approach is currently attracting major attention in overcoming the challenges associated to the hub-model. It provides generic infrastructural data sovereignty capabilities, enabling a single entry point for the data provider with common and agreed upon protocols for defining and enforcing terms-of-use for data sharing. Figure 1 illustrates the transition from a solution specific hub-model approach towards an open network-model approach for infrastructural data sovereignty (Liezenberg, Chiel, Lycklama, Douwe, and Nijland, Shikko 2018).

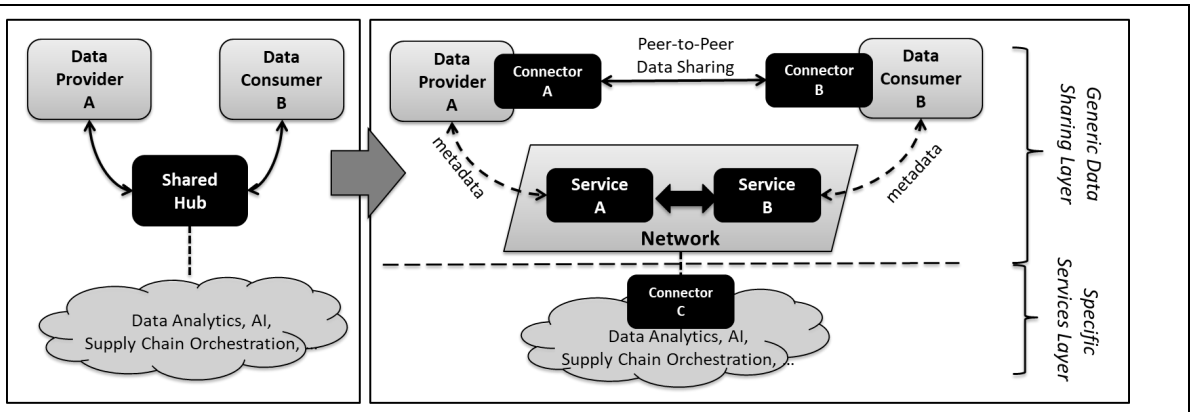


Figure 1: Transition from a Hub-Model (l) to a Network-Model (r) for Data Sharing.

The right part of Figure 1 illustrates the main leading architectural principles of the network-model approach for enabling infrastructural data sovereignty (Simon Dalmolen et al. 2019):

- Peer-to-Peer data sharing,
- Federated infrastructure for support services and Openness for wide-scale adoption.

In the network-model approach, data sharing is done on a peer-to-peer basis (decentralized/federated). Nevertheless, this peer-to-peer data sharing may be used to populate a centralized data lake to support value adding services. This is depicted as the specific services layer in the lower part of Figure 1, in which a multitude of specific value adding services can be supported, e.g. for data analytics, AI services and supply chain orchestration. This may seem contradictory and may seem to make the generic data sharing layer in the upper part of Figure 1 superfluous. It is noted however, that also in these cases there is added value in the generic data sharing layer of the network-model approach: (1) in the aligned and standardized mechanisms of communicating from data provider to service provider the terms-of-use under which the data is shared, (2) in the enforcement thereof in the domain of the service provider, and (3) in the added value of providing supporting functions for data sharing by external trusted roles as independent party.

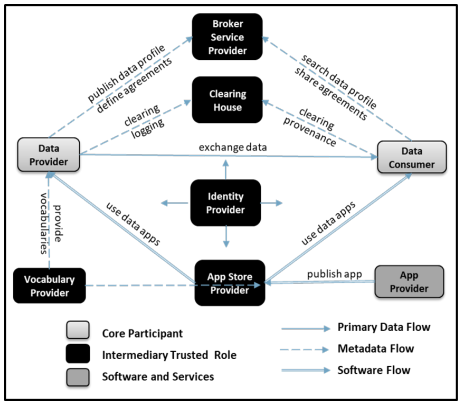
Trusted data sharing based an open network-model approach for maintaining data sovereignty is gaining major interest. A network-model approach has previously been successfully developed and realized for infrastructural service provisioning in the banking and telecommunications sector. To enable wide scale adoption and lower the barriers to participate, the network-model approach should be 'open'. It has to be noted that for the various stakeholders in the federated infrastructure 'openness' has its specific meaning (Council and Committee 1994): Open to end-users, Open to solution providers and Open to service

providers and to innovation. It does not force end-users into closed groups or deny access to any sectors of society but permits universal connectivity. This is also referred to as creating a 'level playing field'. It allows any solution provider to meet the requirements to provide enabling components in the federated and open data sharing infrastructure under competitive conditions. It provides an open and accessible environment for service providers to join and for new applications and services to be introduced (Simon Dalmolen et al. 2019).

The technological concepts and components to enable a network-model approach with infrastructural data sovereignty are currently maturing and becoming available. This is reflected in various current development initiatives. The International Data Spaces (IDS) initiative is currently gaining major international traction as such an open network-model approach. It is described in the following subsection.

International Data Spaces: An Open Business Architecture

The International Data Spaces (IDS) initiative is currently gaining major international traction for realizing an open network model approach for multi-lateral data sharing with infrastructural data sovereignty capabilities. The IDS reference architecture (Otto et al. 2019) is aimed at enabling the trusted sharing of sensitive data, whilst maintaining sovereignty, based on the network-model architectural principles as described in the previous subsection: peer-to-peer data sharing with local data storage and processing in a federated and open infrastructure for support services . Moreover, the IDS reference architecture can be considered an architectural elaboration of the Trusted Multi-Tenant Infrastructure (Trusted Computing Group 2013). Figure 2 depicts the main roles as distinguished in the IDS reference architecture, together with a high-level description of the functions they provide.



IDS Intermediary Trusted Roles	
Role	**Function**
Identity Provider	- Manage Identities of Participants - Validate Identities of Participants
Clearing House	- Clearing and settlement of data transaction - Logging of data agreements and transactions - Auditing, reporting and conflict resolution
Broker Service Provider	- Registration and publication of data profiles - Definition and negotiation of data sharing agreements
App Store Provider	- Publication and provoisioning of data apps
App Provider	- Development and mainenance of data apps
Vocabulary Provider	- Management and offering of (domain specific) vocabularies

Figure 2: Roles in the IDS Reference Architecture (l) (Otto et al. 2019) , together with a Functional Description for the Intermediary Roles (r) (Simon Dalmolen et al. 2018).

The 'Intermediary Roles' in the IDS reference architecture act as trusted entities and are assumed to be provided by trusted third parties (TTPs). The IDS-role of identity provider supports the trust function, together with an additional IDS-role for providing certification and remote attestation functions (not depicted in the figure).

The intermediary roles of 'broker service provider' and the 'clearing house' supports the data sovereignty function. Therefore, the focus in the remainder of this paper will be on these two roles. For elaboration of their data sovereignty enabling capabilities , a clear separation between the responsibilities and functions provided by both roles is needed:

- The broker service provider fulfils the functions for managing data sources and agreements to the point that a formal data sharing agreement has been agreed upon between data provider and consumer. It executes the support processes '*Defining and publishing a data set*' and '*Making a data sharing agreement*' in the initial life cycle stages of data sharing, as described in Table 1.
- The clearing house fulfils the functions for managing data sharing after a mutual data sharing agreement has been made, i.e. managing actual data sharing transactions in accordance with the data sharing agreements and logging and reporting thereof. It performs the support processes

'*Performing a data sharing transaction*' and '*Logging, provenance and reporting*' in the subsequent life cycle stages of data sharing in Table 1.

As depicted in Figure 1, in the federated architecture for the open network-model, multiple instances of these intermediary roles will coexist. The data provider and the data consumer will in general be subscribed to different instances, which may be considered as their 'home' intermediary roles.

Service Approach to Infrastructural Data Sovereignty

As described in the introduction, maintaining sovereignty over metadata in a federated and open network-model approach gives rise to operational challenges for the data provider. The data provider has to strike the right balance between - maintaining a strict data sovereignty policy requiring him to keep the storage and data sharing support processes and associated metadata under his own full-control and within his own security domain. And striving for operational efficiency through outsourcing the storage and data sharing support processes and the associated metadata to external, trusted, organizations, e.g. to broker service providers and to clearing houses, which transfers the control over the possibly sensitive metadata from the data provider to external organizations. This on the one hand may give rise to increased associated risk levels, whilst on the other hand it may yield value adding advantages of providing supporting functions for data sharing by external trusted organizations, e.g. for independent conflict resolution in case of misuse of sensitive data.

A large variety of intermediary options is feasible between these extremes. The options (strongly) depend on the user requirements. To support such a variety of options, a multitude of specific value adding services for infrastructural data sovereignty will have to be supported by the intermediary roles. As such, an attractive way forward will be a service-oriented business architecture in a network-model approach, in which the intermediary roles support data providers with an adequate service portfolio for maintaining sovereignty over their sensitive metadata.

In such a service-oriented architecture, multiple and independent participants provide and govern their own services and solutions (Nicolaou, Ibrahim, and van Heck 2013), (Heikkilä, Heikkilä, and Pekkola 2008). Nevertheless, they will have to be seamlessly interoperable in realizing and providing the overarching data sovereignty enabling capabilities. To enable wide-scale adoption with low barriers to participate, they have a joint interest in defining and adhering to an agreed-upon reference architecture, ensuring the specific functions and business interests of each participant are supported by well-defined standards for interoperability. Such an open, service-oriented, business architecture for an open network-model approach will avoid strong monolithic implementations and prevent 'lock-in', by service providers.

The architecture perspectives for maintaining sovereignty over the metadata in such a federated business architecture for the open network-model approach is elaborated in the following section.

Architecture for Maintaining Sovereignty over Metadata

The service-oriented business architecture in a network-model approach for maintaining sovereignty over metadata is addressed from the technical perspective, the service perspective and the information security perspective in the following subsections, respectively.

Technical Perspective: Interaction Topologies for Seamless Interoperability

In a federated open network-model approach for multilateral data sharing as depicted in the right side of Figure 1, the seamless interoperability is key for enabling wide scale adoption. An overarching interoperability approach is required that on the one hand serves the needs for the various roles in the network-model and on the other hand minimizes implementation complexity. Metadata role interaction topologies form the technical basis for overarching interoperability. The subsequent paragraphs describe their typology, evaluate the options and describe the run-time environment for their realization.

Typology for Metadata Role Interaction Topologies

Various interaction topologies for sharing metadata in a service-oriented manner within an open network-model for multilateral data sharing can be distinguished. These are referred to as 'Metadata Role Interaction Topologies' (MRITs) and are illustrated in Figure 3.

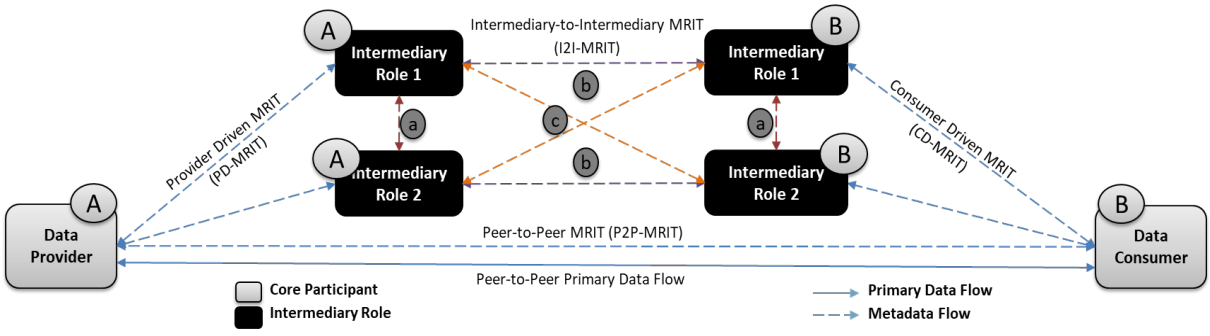


Figure 3: Four Types of 'Metadata Role Interaction Topology' (MRIT) in an Open Network-Model for Multilateral Data Sharing.

The four types of MRITs which are applicable in an open network-model as depicted in the figure, are:

- *Peer-to-Peer MRIT (P2P-MRIT),* in which the data provider and the data consumer share metadata directly without involvement of intermediary roles.

  As described previously, peer-to-peer data sharing is a leading architectural principle for maintaining sovereignty in the open network-model is. Not only can this apply to the primary data flow, also the metadata may be shared on a peer-to-peer basis between the data provider and the data consumer.
- *Provider Driven MRIT (PD-MRIT),* in which the data provider orchestrates the sharing of metadata with the intermediary roles it has subscribed to.

  For this MRIT, it is the data provider's responsibility to subscribe to (trusted) intermediary roles that provide adequate service options for the data sharing supporting processes that match the data provider's business policies. For instance, this applies to templates for (negotiation of) data sharing agreements and logging of data transactions.
- *Consumer Driven MRIT (CD-MRIT),* in which the data consumer orchestrates the sharing of metadata with the intermediary roles it has subscribed to.

  For this MRIT, it is the data consumer's responsibility to subscribe to (trusted) intermediary roles that provide adequate service options. For instance, this applies to data provenance, i.e. the (trustworthy) logging and accounting of the handling, processing and proliferation of shared data along the supply chain for conflict resolution and financial settlement.
- *Intermediary-to-Intermediary MRIT (I2I-MRIT),* in which the intermediary roles of the various data providers and consumers orchestrate the sharing of metadata amongst themselves.

  Some functions on maintaining sovereignty over metadata may not only require interactions between the data provider or consumer and their subscribed intermediary roles. Rather, they may require direct interaction between intermediary roles. For instance, this may apply to metadata related to proliferation and publication of data descriptors between broker service providers to make it searchable and available to potential data consumers connected to other broker service providers.

For maintaining sovereignty over metadata in an open network-model, the four types of MRITs are not equally suitable and applicable. Therefore, the MRIT options are evaluated in the following subsection.

Evaluation of Interaction Topology Options for Metadata Sovereignty

The applicability and suitability of the various types of MRITs for sharing metadata between roles in the federated and open architecture for multilateral data sharing are evaluated on the following criteria:

- *Maintaining sovereignty over the metadata by the data provider and consumer.*

  Maintaining sovereignty over metadata and being in control over the proliferation chain thereof is essential for data providers and consumers. Proliferation along a chain of interconnected intermediary roles by means of I2I-MRITs implies loss of such control and having to trust and rely on intermediary roles that are potentially not even known to the data provider or consumer.

Restricting proliferation of the metadata to their 'home' intermediary roles that a data provider or data consumer has subscribed to, will prevent such loss of control.

- *Complexity of the overarching interoperability architecture.*
  The widescale adoption of agreed-upon (and preferably standardized) role interaction protocols strongly depends on the implementation complexity and number of standardized interconnections to be realized between intermediary roles in in the highly federated infrastructure of the open network-model, denoted as (a), (b) and (c) in Figure 3. Having to implement and adhere to standardized interaction protocols for a multitude of types and instances of intermediary-to-intermediary MRITs may become (too) complex, both from the development and deployment perspective.
  It is to be noted, that this complexity may be technically overcome as has been demonstrated in the 'old-school' world of pre-divestiture telecommunications at the end of the previous millennium. In their regulated environment, a limited number of (mostly non-competitive) major telco's had a common interest in closely collaborating in developing standards for interoperability to achieve globally interoperable services. In the current liberalized situation for data services however, such a centrally governed development and deployment process is non-existent. Hence, definition and adoption of agreed-upon intermediary-to-intermediary interoperability protocols are a far less viable option.

On these criteria, the observation is that the PD-MRIT and CD-MRIT are to be preferred as the default-to-be-used metadata interaction topologies over the I2I-MRITs. Figure 4 illustrates how the resulting interaction topologies in federated, open, network-model approach are to be realized by means of the PD-MRIT and CD-MRIT, whilst avoiding the necessity for realizing an I2I-MRIT interaction topology.

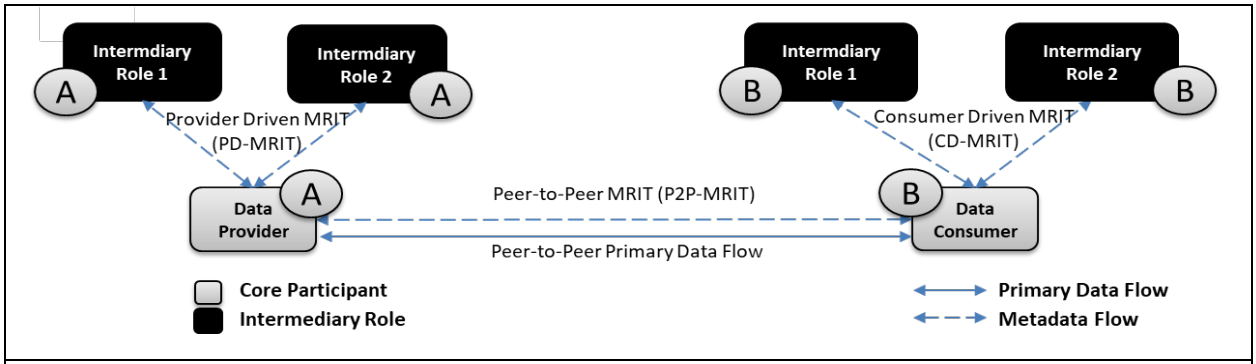


Figure 4: The Preferred 'Metadata Role Interaction Topologies' PD-MRIT and CD-MRIT for Maintaining Sovereignty in a Federated, Open, Network-Model Approach.

The figure illustrates that with the preferred provider PD-MRIT and consumer driven CD-MRIT, all sharing of metadata is through orchestration and under control of the data provider and the data consumer. This gives them the required control over their metadata for maintaining sovereignty. No direct intermediary-to-intermediary metadata sharing beyond the direct control of the data provider and data consumer is required, preventing them from having to rely on trusted third parties or requiring complex I2I-MRIT interface implementations.

The following subsection describes how the preferred PD-MRIT and CD-MRIT interaction topologies may be realized in a federated, open, network-model approach for multi-lateral sharing of sensitive data.

Runtime Environment for Metadata Flow Control in an Open Network-Model Approach

Maintaining sovereignty by data providers over their sensitive metadata requires both procedural and technical data sovereignty maintaining capabilities in the open network-model approach:

- *Procedural data sovereignty maintaining capabilities:* These include administrative capabilities such as data sharing agreements (terms-of-use expressed as access and usage control policies, commercial and juridical conditions), trust through certification and attestation, logging and data provenance, reporting and accountability.

- *Technical data sovereignty maintaining capabilities:* These include technical capabilities such as peer-to-peer data sharing, encryption and key management for data in transfer and in storage, sandboxing / containerization, and policy based admission control (Yavatkar, Pendarakis, and Guerin 1999) and enforcement.

The procedural and technical data sovereignty enabling capabilities are closely related to the concepts of legal enforceability and technical enforceability of data sharing agreements, respectively. Legal enforceability ensures that by means of automation generated digital data sharing agreements and their associated data sharing transactions are juridically correct and acceptable in legal procedures. Technical enforceability ensures for the data provider that the agreed-upon conditions under which data is shared are (securely) implemented and enforced in the open, federated, infrastructure for multi-lateral data sharing.

The combination of the procedural and technical data sovereignty enabling capabilities constitute to a data sovereignty framework for the supporting life-cycle processes for data sharing (as enumerated in Table 1) and their associated metadata artefacts (as enumerated in Table 2). They are implemented by means of the preferred PD-MRIT and CD-MRIT by means of a data sharing connector as shown in Figure 5.

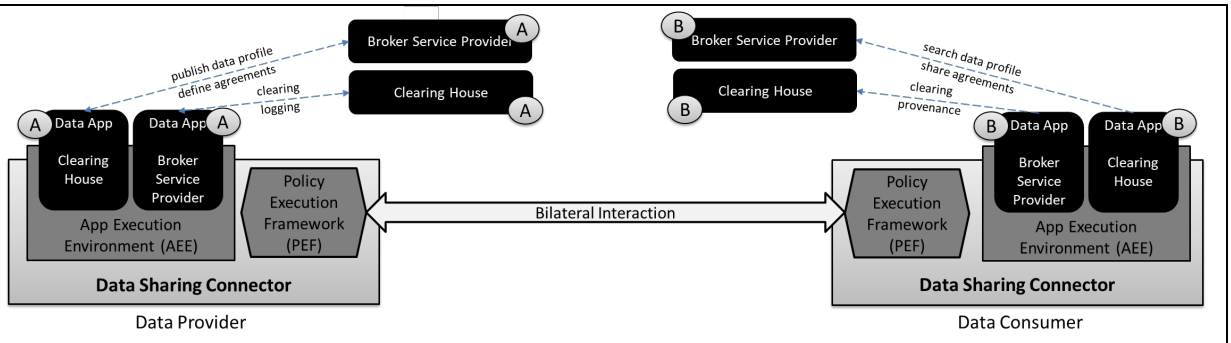


Figure 5: Runtime Environment for Metadata Flow Control based on a Data Sharing Connector with an App Execution Environment and Policy Execution Framework.

As the figure shows, a data sharing connector consists of a policy execution framework in combination with an app execution environment:

- The *Policy Execution Framework (PEF)* includes the capabilities for technical enforceability of the agreed-upon terms-of-use, access control policies and usage control policies in combination and collaboration of the PEF-instances in the connectors of the local and remote data sharing endpoints. Typically, the PEF provides the technical data sovereignty capabilities for technical enforceability as described above.
- The *App Execution Environment (AEE)* runs a set of containerized apps of which the input and output data flows are being controlled by the associated PEF. These could be the apps of the intermediary roles. Typically, the apps in the AEE provide the procedural data sovereignty capabilities for legal enforceability as described above.

For IDS, the data sharing connector is referred to as an 'IDS connector', currently being standardized under the terminology of 'Security Gateway' (DIN SPEC 27070 n.d.). It consists of an execution core container, with the AEE and PEF, that is able to retrieve certified data apps from intermediary roles from an app store. The execution core container has a data router for routing incoming and outgoing messages through the correct data apps. Furthermore, it is enabled to enforce access and usage control policies.

This runtime environment for controlling metadata flows enables a large variety of service offerings on data sovereignty, as addressed in the following subsection.

Service Perspective: Towards a Service Portfolio for Intermediary Roles

As described, a service-oriented business architecture that enables the 'intermediary' roles to offer a varying data sovereignty enabling service portfolio. This allows data providers to subscribe to those 'intermediary' roles that provide the adequate services matching data provider's specific policy on data sovereignty, ranging between having full self-control within its own domain on one end and fully outsourcing responsibility and control to 'intermediary' roles on the other end. The runtime environment architecture

as described in the previous subsection enables the intermediary role to provide brokering or clearing house services in differing and distinguishing flavors, providing them an option to distinguish in a possibly competitive market. The following paragraphs subsequently describe how this can be realized for a basic portfolio of processing and logging services of sensitive metadata.

Processing of Sensitive Metadata

The AEE in the data sharing connector (as depicted in Figure 5) enables intermediary roles to provide their services for the data sharing support processes (as listed in Table 1) by means of apps executing locally in the AEE. This allows him to maintain data sovereignty over the metadata as the metadata does not leave the local data provider's or data consumer's data sharing connector in an uncontrolled manner. Processing and storage at a central location of the intermediary role can be circumvented.

The supporting subprocess for definition of terms-of-use as described in Table 1 provides an illustrative and representative scenario on how this can be done. This subprocess is to be provided by an intermediary broker service provider role. A main added value and distinguishing factor for a specific broker service provider can be in minimizing the complexity for defining and configuring the applicable terms-of-use for their subscribed data providers, thus minimizing the required skills and IT-savviness for the data provider, lowering the barriers of adoption and allowing data providers to focus on their core functions. As such adequate broker services will increase overall efficiency throughout the overarching role and service-oriented business architecture.

In the scenario, the broker service provider offers its subscribed data providers a set of data sharing agreement templates for defining and configuring the applicable terms-of-use (expressed as access and usage control policies), together with the applicable commercial and juridical conditions. The quality and ease-of-use of the templates will be a main competitive distinguisher. The templates are provided as data brokering app executing locally in the AEE of the data provider's connector. The app fulfills the role of the delegated data brokering service running within the data provider's trust domain and under control of its local PEF. It manages the data sharing agreement negotiation and signing process, based on the easy-to-use templates of the broker service provider. As part of the app installation and configuration process, its associated terms-of-use (expressed as access and usage control policies) are instantiated within the data provider's PEF, preventing from misuse or data leakage of the associated metadata and enabling technical enforcement thereof. This pattern of locally executing data apps of intermediary roles to enable sovereignty over metadata is applicable to and representative for a broad set of support processes as listed in Table 1.

It is to be noted that the implementation of the services of the intermediary roles as data-app in the AEE of the data provider's connector will enable data sovereignty without the need for both the data provider and the data consumer to install and execute the same data app. As such, there is no cross-dependence of the data providers and consumers with their independently subscribed intermediary roles as prescribed by the preferred PD-MRIT and CD-MRIT interaction topologies the open and federated infrastructure.

Logging of Sensitive Metadata

For the 'Logging, provenance and reporting' subprocesses as listed in Table 1, a broad variety of logging and storage service options may be enabled by a clearing house intermediary role in a federated business architecture in an open network-model approach by means of a data-app executing locally within the AEE of the data provider's connector. This approach enables various service alternatives, differentiating between locally logging of metadata (i.e. in the data app within the data provider's or consumer's connector) versus centrally logging of metadata (i.e. within the domain of the clearing house):

No centrally logging of metadata. This reflects the strictest approach to maintaining data sovereignty in which the data provider or consumer keeps the data sharing support processes and associated metadata logging and storage under his own full-control and within his own security domain.

Centrally logging of hashed metadata. In this approach, the data provider keeps the data transaction metadata within his own security domain, whilst providing hashed metadata to its subscribed clearing house. In case of conflict resolution, the clearing house acts as trusted third party by verifying the validity and consistence of the logged data hashes with the data provider's loggings.

Centrally logging of encrypted metadata. In this case, the data provider does not log metadata in his own security domain. The metadata is only logged by his subscribed clearing house, preferably in an encrypted format. Management of the encryption keys may remain under control of the data provider.

These various flavors of logging and storage of metadata are relevant for both the data provider and the data consumer. For the data provider this may apply for instance for logging the metadata on data transactions for the case of conflict resolution (non-repudiation). For the data consumer this may apply for instance for logging data provenance metadata to report on compliance to the agreed upon data sharing agreement and terms-of-use.

Information Security Perspective: Confidentiality, Integrity, Availability and Non-Repudiation

The implementation for maintaining sovereignty in a federated, open, network-model approach by means of data sharing connectors consisting of a combination of AEE and PEF as described previously must conform the key concepts of information security as described in Table 3.

Table 3: Key Concepts of Information Security(Wikipedia 2019).	
Integrity	The property of assuring the accuracy and completeness of data over its entire lifecycle. Data cannot be modified in an unauthorized or undetected manner.
Availability	The property that information must be available when it is needed. Ensuring availability also involves preventing denial-of-service attacks.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Non-repudiation	The property that the data consumer cannot deny having received the data, nor can the data provider deny having sent the data.

For the key concepts of information security as listed in Table 3, the following observations can be made in the context of the open network model approach for maintaining sovereignty as described in this paper:

- *Integrity of the metadata*. In the service-oriented business architecture, integrity of the metadata associated to individual data transactions is addressed in several ways. With the preferred PD-MRIT and CD-MRIT interaction topologies, both the data provider and consumer are in control over logging the associated metadata according to its own policy and preference, either locale or through is subscribed clearing house. This prevents from (dependence on) a single, potentially non-trusted provider. Moreover, a pivotal core values for the subscribed clearing house is in being trustworthy with respect to administering and reporting on the data transactions. Therefore, the options for ensuring metadata integrity are included by design in the network model approach.
- *Availability of the metadata*. In a similar manner as for 'Integrity', the options for ensuring metadata availability are included by design in the network model approach, through the support of the preferred PD-MRIT and CD-MRIT interaction topologies and the service-oriented business architecture for trusted and independent clearing houses.
- *Confidentiality of the metadata*. This applies to both the sharing and the logging of metadata. In the network-model approach (such as IDS) this is implemented by means of: (1) the trust capabilities provided by the combination strong identity provider functions / roles and a certification and remote attestation function, and (2) the highly secure (and standardized) connector and communication protocols.
- *Non-repudiation of the metadata*. In a federated, open, network model approach as described in this paper, the design for non-repudiation is complex and requires special. Therefore, it is described further elaborated in the remainder of this paragraph.

In the runtime environment for metadata flow control based on a data sharing connector (as illustrated in Figure 5), the PEFs play an important role for realizing non-repudiation. The PEFs ensure that the data consumer and the data provider follow the required and correct process for non-repudiation. Essential for the role of the PEF is that the PEFs can be trusted by all parties as they are part of the certification and remote attestation process. Hence, this also applies to the PEF within the data consumer's connector .From

the data provider's perspective also its subscribed clearing house (including its clearing house data app executing within the AEE of the data provider's connector) can be trusted.

However, the data apps running in the AEE of the remote data consumer's connector are not to be trusted a priori by the data provider as they are outside this overarching, certified, security framework. Nevertheless, non-repudiation may be ensured with the service-oriented business architecture in the network-model approach, based preferred PD-MRIT and CD-MRIT interaction topologies. This is illustrated through the sequence diagram for the non-repudiation process of a specific data transaction as depicted in Figure 6 (Zhou and Gollmann 1997). It starts from the premises that the entities (intermediary roles) have been authenticated and have a secure channel for communication.

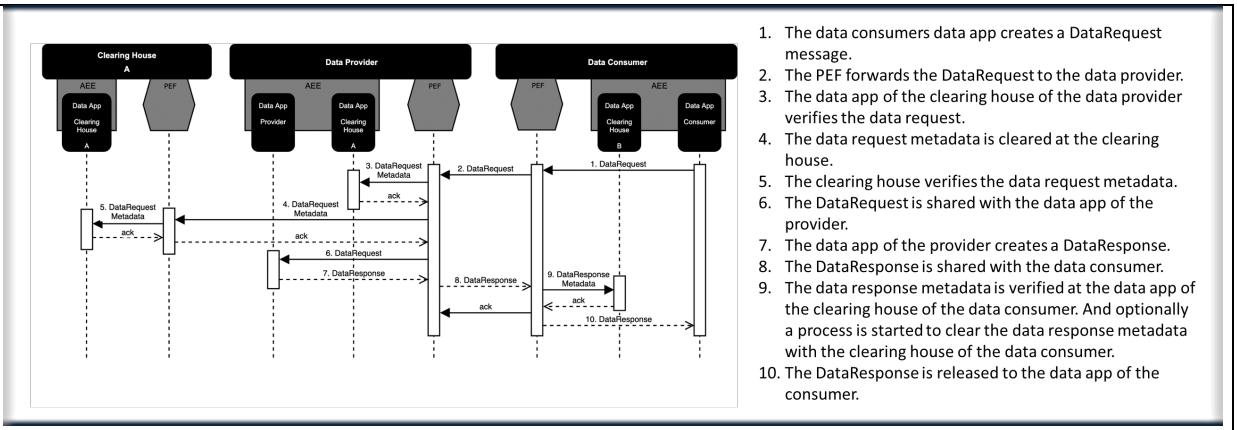


Figure 6: Sequence Diagram of the Non-Repudiation Subprocess.

As the figure shows, the PEF of the data consumer safeguards the process flow of sending the data request and receiving the data response. The most important task is to ensure the non-reputability of both sending the data request and receiving the data response by making sure the reception of the data response is acknowledged to the data provider, which ensures the data consumer actually received the data response it requested. Only after the reception of the data response has been acknowledged, the data is released and transferred to the data app of the data consumer for further processing. The PEF of the data provider handles the release of the data request metadata to the data provider's clearing house. If, and only if, a positive acknowledgement is received from the clearing house, the data request is released to the data app of the data provider. Consequently, the interactions with the clearing house only stem from the data provider, not the data consumer. As such, this process adheres to the PD-MRIT as a preferred interaction topology. Moreover, the (encrypted) payload of the data transaction is not shared with the centralized location of the clearing house. Only the metadata with the (encrypted) keys and references to the applicable data sharing agreement are shared with the clearing house, which is the fundamental metadata as required for clearing a specific data transaction with non-repudiation.

Case studies: iSHARE and the Smart Connected Supplier Network

The iSHARE initiative has been initiated by the logistics in the Netherlands. It has the same goals for a network-model approach with infrastructural trust and data sovereignty capabilities. The iSHARE initiative (https://www.ishareworks.org/en/) is considered as powerful initiative with low barriers to participate for organizations through an easy onboarding process. Differences between iSHARE and the IDS-approach (as addressed in this paper) are in the scope and in the technical implementation. It doesn't support the security features by means of data sharing connectors at the communications level together with its technical enforcement features for data sovereignty in the data sharing connectors. iSHARE is currently commercially operational and gaining business traction. The iSHARE and IDS initiatives recognize the potential of alignment and strive for an interoperable and complementary approach in which the strengths of both initiatives reinforce each other.

In the Smart Industry sector, the procurement of products is increasingly being done based on just-in-time replenishment of stocks, tailored to varying specific customer demands. This coincides with an increasing demand for specialty products (specific size, quality, etc.). Industrial companies can improve their

competitiveness by meeting these demands whilst maintaining mass-production pricing levels. In enabling such improvements in the supply chain digital information exchange is a critical enabler. Its requirements include:

- *Agreed semantics,* allowing organizations to effectively use the data in their systems and processes.
- *Easy and secure connectivity,* for seamless interconnection and easy integration when adding partners to the network, with little set-up costs.
- *No re-invention of the wheel,* enabling re-use of existing systems (e.g. for ERP) and standards.
- Flexibility, meeting the increasingly importance for manufacturing companies to work with customers in various domains (e.g. automotive, aerospace, construction, electronics, …) each with their own specific semantics and data infrastructures.
- *Assurance,* providing each partner a sufficiently level of confidence in data sharing to prevent from mis-use of his sensitive data through trust capabilities (e.g. on identity management and certification) and data sovereignty maintaining capabilities (e.g. on both the procedural and technical data sovereignty maintaining capabilities as described in the previous section).

To meet these requirements, the Smart Connected Supplier Network (SCSN) field lab has been developed. It is currently operating with manufacturing companies and integrators in a high-tech smart industry supply network, with a specific focus on low volume, high mix and high complexity production processes.

Within this SCSN field lab the IDS reference architecture (as illustrated in Figure 2) has been introduced to meet the above requirements. Furthermore, an messaging standard (also referred to as SCSN) has been developed and implemented. In short, this messaging standard specifies ordering, bill-of-materials, logistics, forecast and invoicing messages for the Smart Industry sector.

Through many interviews with the partners, a clear need has been identified for data sovereignty capabilities as part of the SCNS field lab. Sharing data in a controlled and secure manner across domain boundaries is seen as very important in the coming decade to operate successfully for small and medium enterprises. Therefore, the exploratory phase for the usefulness and necessity of data sovereignty maintaining capabilities for both the sensitive primary data and secondary metadata has been endorsed by the partners in the SCSN field lab. Its next phase has towards implementation has started, namely the implementation of standardized security gateways by means of the DIN SPEC conforming IDS-connectors (DIN SPEC 27070 n.d.), (DIN SPEC 16593-1 n.d.). The communication is done according to the IDS handshake regarding identification and authentication. The actual shared information is based on SCSN messages.

As part of the SCSN field lab development process, a technological experiment on the preferred MRIT interaction topology for metadata control as described in Figure 3 is currently running. This will test the hypotheses as described in this paper. In the technical simulation, the MRIT interaction topologies as described in Figure 3 and Figure 4 are technically working. However, a real practical pilot in the SCSN field lab is required and foreseen to prove the current hypothesis of being in control and sovereignty over both the sensitive organizational data and the secondary metadata.

Standardization and Cooperation for Wide-Scale Adoption

As the technical components of the data sharing and metadata sovereignty concepts as described in this paper become more and more available, adequate governance needs major attention to stimulate wide scale adoption and prevent from a lack of uptake. This applies to both governance of the development and of the deployment. Openness and interoperability through standardization are major governance enablers for success.

Standardization in the open network-model must focus on interoperability between the data providers and data consumers and with the supporting intermediary roles. To optimally enable service-orientation for infrastructural sovereignty over metadata as described in this paper, standardization should not be (too) prescriptive with respect to the service options that can be supported by these intermediary roles. As such, conforming to the architectural considerations as described in this paper, standardization should focus on and be limited to standardization of:

- the (information models for the) metadata artefacts as listed in Table 2,
- the interaction messages for conveying specific information (metadata) artefacts between the roles in the open network-model, e.g. DataRequest, DataResponse, …, and

- protocols for the orchestration of interactions between components and roles.

The standardization of protocols applies to both the exchange of term-of-use and maintaining sovereignty (expresses as access and usage control polices) and to the interaction protocols at the underlying technical layer for securely connecting between data providers and data consumers. It is to be noted that the main concepts of the IDS architecture and their interoperability protocols as described in this paper are currently being standardized as DIN SPEC standards, (DIN SPEC 27070 n.d.), (DIN SPEC 16593-1 n.d.).

Standardization of the main architectural concepts is key for openness and cross-sector interoperability. Leaving the uptake to individual commercial users or sectors may not be an adequate approach as it may not be contributing to their core business, vision and ambition. Moreover, within Europe the industry exists of only a few big players and a highly fragmented market with many small and medium enterprises. Therefore, the vision and ambition of governments and authorities to take a leading position in standardization is crucial in preventing from vendor lock-in or a winner-takes-all-solution. Public-private cooperation may provide a good option for success. Support by governments and authorities in jointly developing the data sharing infrastructure into a broadly available public utility may be envisioned, supported by adequate commercial implementations and marketing power to develop, deploy and exploit the infrastructure, e.g. by independent service providers or telecommunication operators.

Conclusions and Future Work

A primary objective of this paper has been to describe the need and architectural approach for infrastructural data sovereignty over (meta)data for multi-lateral sharing of sensitive data. A technical, service and information security perspective have been elaborated on a service-oriented business architecture for transferring (outsourcing) data sharing support processes and their associated metadata to external, trusted, and specialized organizations, whilst maintaining sovereignty by the data provider over his (meta)data . This approach gives data providers flexibility and agility in balancing manageability and cost-efficiency of outsourcing to external organizations against the increased risks of misuse of their (meta)data.

The concepts as described in this paper will provide data provider with more options and flexibility in realizing its business policy for maintaining sovereignty and control over both their sensitive primary data and secondary metadata, in a world that is ever more realizing that data is a real valuable asset to be protected. It may lower the barriers for organizations for sharing their data in the transition towards a data-centric global information society. However data sovereignty isn't easy to implement in agile business networks where short-term relationships and ad hoc collaboration are becoming the standard. Widescale adoption of the proposed architecture requires adequate governance, both for development and deployment.

With the service and architectural approach for maintaining sovereignty by the data provider over their metadata as presented in this paper, data sovereignty can become a constructive and powerful concept for data providers to overcome the barriers to share their data. As such, it may improve supply chain collaboration, whilst preventing misuse of potentially sensitive shared data. Moreover, the recent EU regulation regarding General Data Protection Regulation (GDPR) has major impact for may core business processes. The solution proposed may help organization to get grip on its GDPR mitigation measures in the context of their interorganizational data sharing.

Future work on the concepts as described in this paper will include:

- Development of a user-oriented implementation that makes the large diversity of service options for infrastructural data sovereignty in an open network-model approach available and configurable in a user-friendly and manageable manner. An adequate overarching user-friendly, architecture will spur wide scale adoption. Value adding roles on integration and service packaging will arise that provide service and application portfolios for brokering and clearing house functionality according to the service-oriented approach as described in this paper are foreseen. Additionally large scale, cloud-based, connector infrastructures may emerge that provide high-performance and user-friendly facades to data providers and consumers for easily connecting to the multilateral data sharing infrastructure.
- Performance assessment (e.g. in terms of throughput, processing power and overhead) of the interaction topologies for maintaining sovereignty over metadata as proposed within this paper. As

part of the performance assessment, the feasibility and performance of light-weight implementations may be considered, e.g. for IoT applications and ARM-processor environments.'

- Applicability in a hybrid environment, for instance for interconnectivity and interoperability of the network-model approach as described in this paper with existing community solutions operating in a hub-model approach. This may for instance be applicable for port community systems, which are currently mainly operating with a centralized data lake in a hub-model approach.
- Embedding of the architectural concepts within a reference architecture for multi-lateral data sharing, for instance the International Data Spaces (IDS) architecture as described in this paper.

Acknowledgements

The work as presented in this paper has been supported and co-financed by the Dutch Top consortia for Knowledge and Innovation 'Institute for Advanced Logistics' (TKI Dinalog, www.dinalog.nl) of the Ministry of Economy and Environment in The Netherlands.

In addition, this paper builds upon the work done within the Dutch NWO Research project 'Data Logistics for Logistics Data' (DL4LD, www.dl4ld.net), supported by TKI Dinalog and the Dutch Commit-to-Data initiative (https://commit2data.nl/).

References

Bharadwaj, Anandhi, Omar A. El Sawy, Paul A. Pavlou, and N. Venkatraman. 2013. "Digital Business Strategy: Toward a next Generation of Insights." *MIS Quarterly* 37 (2): 471–482.

Council, National Research, and NRenaissance Committee. 1994. *Realizing the Information Future: The Internet and Beyond*. National Academies Press.

Dalmolen, S., H. M. Moonen, J. van Hillegersberg, A. J. R. Stoter, and E. Cornelisse. 2015. "Supply Chain Orchestration and Choreography: Programmable Logistics Using Semantics." In *Advanced Logistics and Transport (ICALT), 2015 4th International Conference On*, 76–81. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7136596.

Dalmolen, Simon, Harrie Bastiaansen, Somers, Erwin, Djafari, Somayeh, Maarten Kollenstart, and Matthijs Punter. 2019. "Maintaining Control over Sensitive Data in the Physical Internet: Towards an Open, Service Oriented, Network-Model for Infrastructural Data Sovereignty." In *International Physical Internet Conference. London*.

Dalmolen, Simon, Harrie Bastiaansen, Hans Moonen, Wout Hofman, Matthijs Punter, and Erik Cornelisse. 2018. "Trust in a Multi-Tenant, Logistics, Data Sharing Infrastructure: Opportunities for Blockchain Technology." In *5th International Physical Internet Conference, IPIC 2018*, 299–309. University of Groningen.

DIN SPEC 16593-1. n.d. DIN SPEC 16593-1 RM-SA - Reference Model for Industrie 4.0 Service Architectures - Part 1: Basic Concepts of an Interaction-based Architecture; Accessed April 30, 2019. https://www.en-standard.eu/din-spec-16593-1-rm-sa-reference-model-for-industrie-4-0-service-architectures-part-1-basic-concepts-of-an-interaction-based-architecture-text-in-english/.

DIN SPEC 27070. n.d. DIN SPEC 27070: 'Reference Architecture for a Security Gateway for Sharing Industry Data and Services. Accessed April 30, 2019. https://www.din-mitteilungen.de/de/din-spec-27070-und-kuenftige-din-spec-27072-standardisiertes-security-gateway-und-security-anforderungen-fuer-iot-geraete-im-small-business-home-umfeld-272902.

Dutch Ministry of Economic Affairs and Climate Policy. 2018. "Generiek Afsprakenstelsel Voor Datadeelinitiatieven Als Basis van de Digitale Economie." https://www.rijksoverheid.nl/documenten/rapporten/2018/12/30/generiek-afsprakenstelsel-voor-datadeelinitiatieven-als-basis-van-de-digitale-economie.

Gunasekaran, Angappa, Thanos Papadopoulos, Rameshwar Dubey, Samuel Fosso Wamba, Stephen J. Childe, Benjamin Hazen, and Shahriar Akter. 2017. "Big Data and Predictive Analytics for Supply Chain and Organizational Performance." *Journal of Business Research* 70: 308–317.

Heikkilä, J., M. Heikkilä, and S. Pekkola. 2008. "Coordinating and Boundary Spanning Roles of Business Networks." *In: Vervest, P., Van Heck, E. & Preiss, K.,(Eds.): Smart Business Networks a New Business Paradigm*.

Hillegersberg, Jos, Hans Moonen, and Simon Dalmolen. 2012. "Coordination as a Service to Enable Agile Business Networks." In *The Dynamics of Global Sourcing. Perspectives and Practices*, edited by Julia Kotlarsky, Ilan Oshri, and LeslieP. Willcocks, 130:164–74. Lecture Notes in Business Information Processing. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-33920-2_10.

Jarke, Matthias, Boris Otto, and Sudha Ram. 2019. "Data Sovereignty and Data Space Ecosystems." *Business & Information Systems Engineering*, August. https://doi.org/10.1007/s12599-019-00614-2.

Lee, Hau L., and Seungjin Whang. 2000. "Information Sharing in a Supply Chain." *International Journal of Manufacturing Technology and Management* 1 (1): 79–93.

Liezenberg, Chiel, Lycklama, Douwe, and Nijland, Shikko. 2018. *Alles transactie*. LannooCampus.

Luftman, Jerry, Kalle Lyytinen, and Tal ben Zvi. 2017. "Enhancing the Measurement of Information Technology (IT) Business Alignment and Its Influence on Company Performance." *Journal of Information Technology* 32 (1): 26–46.

Marinagi, C., P. Trivellas, and P. Reklitis. 2015. "Information Quality and Supply Chain Performance: The Mediating Role of Information Sharing." *Procedia-Social and Behavioral Sciences* 175: 473–479.

Nicolaou, Andreas I., Mohammed Ibrahim, and Eric van Heck. 2013. "Information Quality, Trust, and Risk Perceptions in Electronic Data Exchanges." *Decision Support Systems* 54 (2): 986–96. https://doi.org/10.1016/j.dss.2012.10.024.

Otto, Boris, Sebastian Steinbuß, Andreas Teuscher, and Steffen Lohmann. 2019. "International Data Spaces: Reference Architecture Model Version 3." https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf.

Otto, Boris, and Matthias Jarke. 2019. "Designing a Multi-Sided Data Platform: Findings from the International Data Spaces Case." *Electronic Markets*, August. https://doi.org/10.1007/s12525-019-00362-x.

PricewaterhouseCoopers. 2019. "Data Exchange as a First Step towards Data Economy." https://www.pwc.de/en/digitale-transformation/data-exchange-as-a-first-step-towards-data-economy.pdf.

Trusted Computing Group. 2013. "Trusted Multi-Tenant Infrastructure Work Group - Reference Framework."

Wikipedia. 2019. "Information Security." In . https://en.wikipedia.org/w/index.php?title=Information_security&oldid=894427340.

Yavatkar, Raj, Dimitrios Pendarakis, and Roch Guerin. 1999. "A Framework for Policy-Based Admission Control."

Zhou, Jianying, and Dieter Gollmann. 1997. "An Efficient Non-Repudiation Protocol." In *Proceedings 10th Computer Security Foundations Workshop*, 126–132. IEEE.

Zrenner Johannes. 2019. "Usage Control Architecture Options for Data Sovereignty in Business Ecosystems." Edited by Möller Frederik Oliver. Translated by Eitel Andreas and Otto Boris. *Journal of Enterprise Information Management* 32 (3): 477–95. https://doi.org/10.1108/JEIM-03-2018-0058.