User-Centric Network-Model for Data Control with Interoperable Legal Data Sharing Artefacts

Improved Data Sovereignty, Trust and Security for Enhanced Adoption in Interorganizational and Supply Chain IS Applications

Dr. H.J.M. (Harrie) Bastiaansen
S. (Simon) Dalmolen, MSc
M. (Maarten) Kollenstart, MSc
Prof. Dr. T.M. (Tom) van Engers

Logistics Data
Data Logistics

Rigor & Relevance

- In the emerging **_data economy_**, advanced supply chain collaboration architectures are ever more built upon a **_data-centric foundation_**.

- Various studies indicate that main challenges and obstacles for data sharing are fear for security risks and worries about losing control over their data, i.e. **_data sovereignty is key_**.

- Recent studies amongst companies in the Netherlands identifies **_nine essential building blocks_** for controlled data sharing, whilst the data owner maintains data sovereignty.
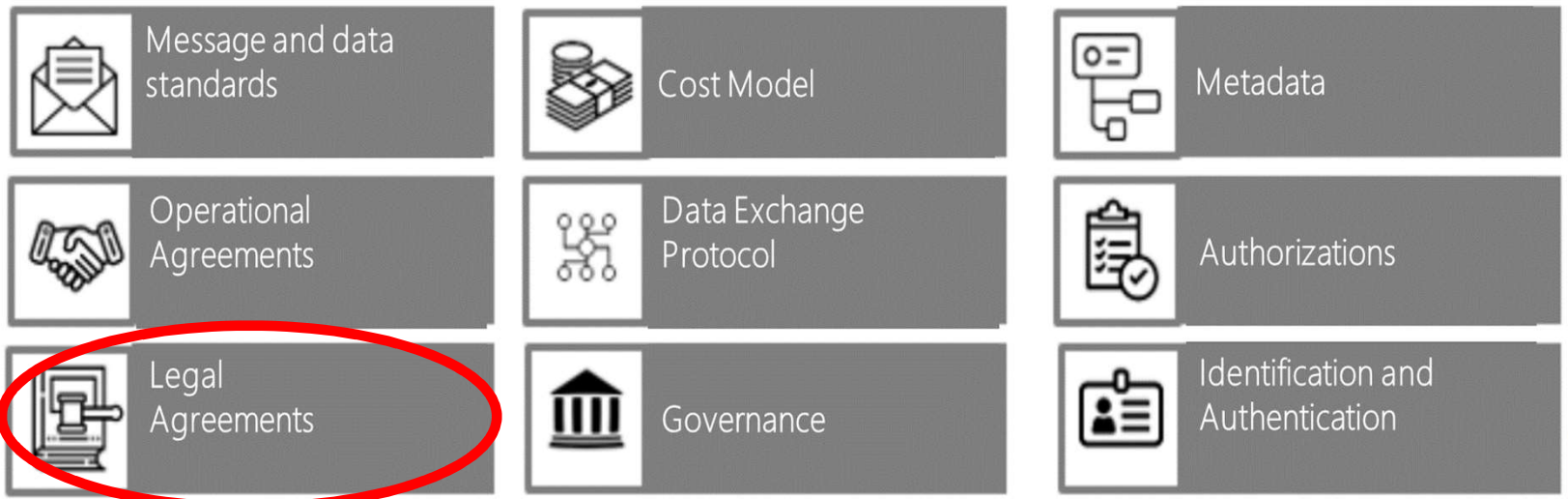
# A more user-centric approach is needed

Currently, data control capabilities are mainly provided within closed sector-specific ecosystems, with specific solutions, giving challenges for end-users that share data in multiple ecosystems :

- Threat of vendor lock-in
- Major integration efforts to manage data sovereignty, trust and security

A network-model approach may offer significant advantages from the end-user perspective

- Providing generic and re-usable infrastructural capabilities for defining and enforcing data sovereignty, trust and security in multi-lateral data sharing:
  - Various initiatives are currently emerging
  - The International Data Spaces (IDS) initiative has major international attention
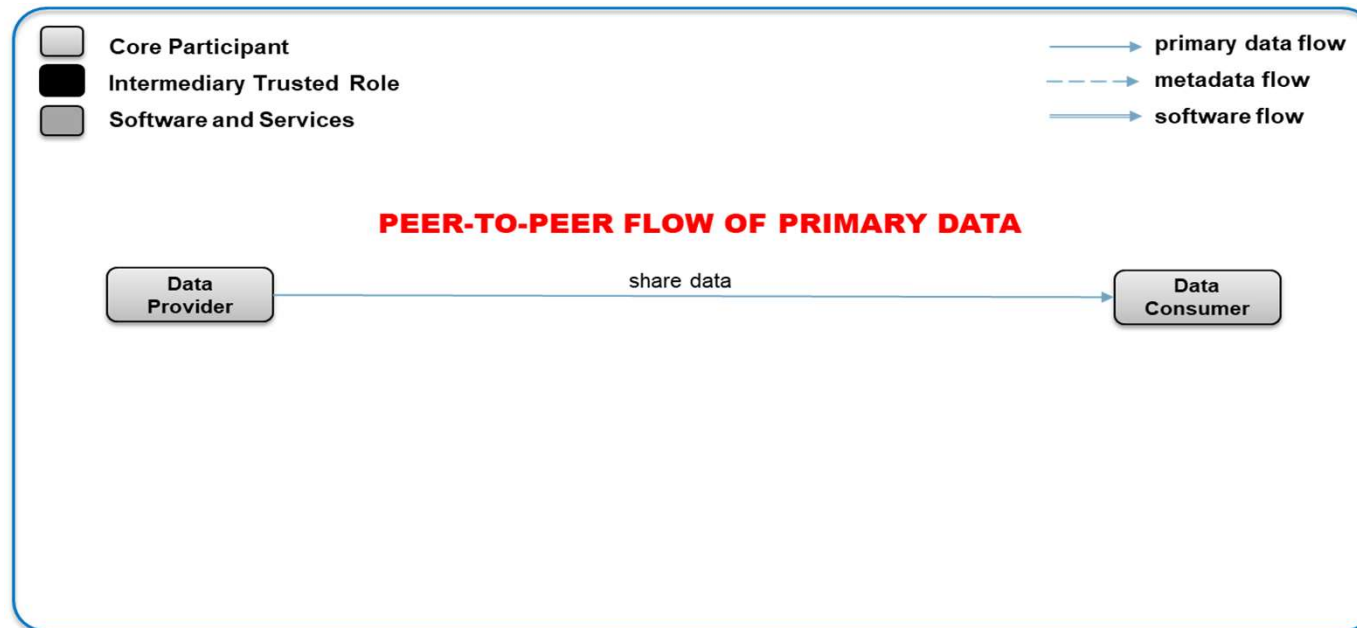   - https://www.internationaldataspaces.org/

Towards An Open Network-Model

Hub-Model
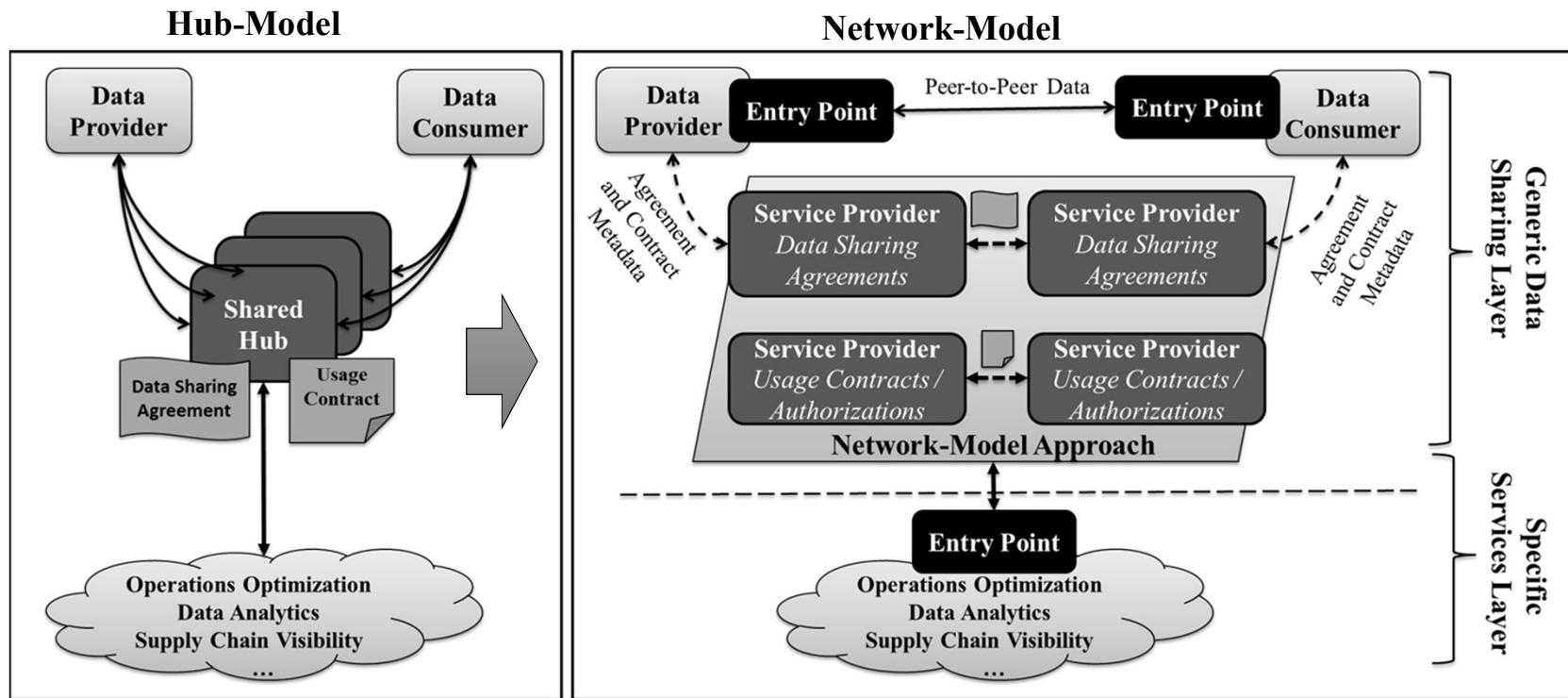
Network-Model

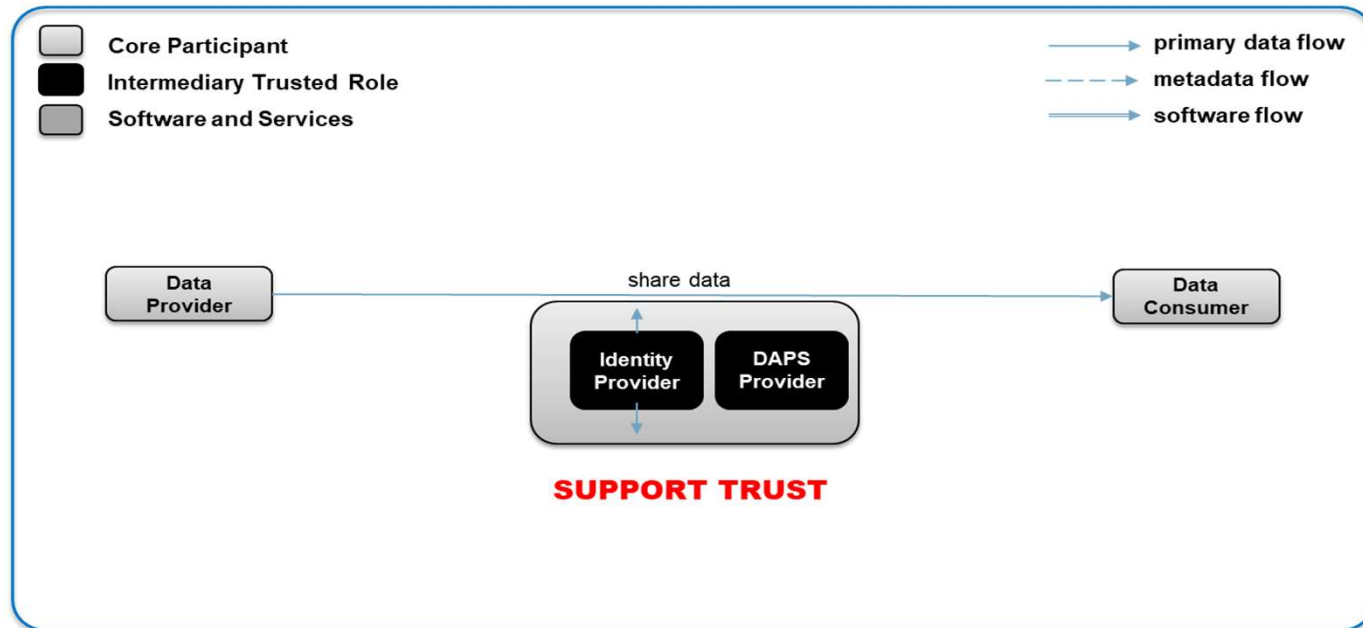Transition from a Hub-Model to a Network-Model for Data Sharing.

International Data spaces (IDS)
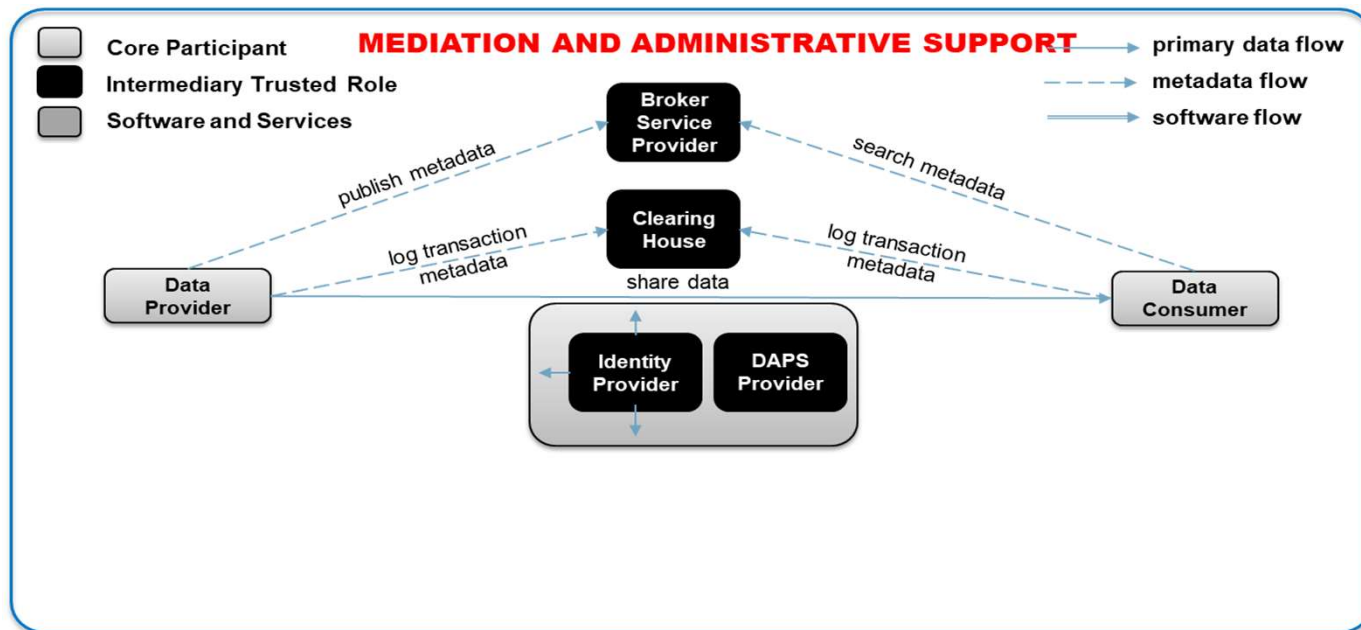## A reference architecture for an open network model approach

International Data spaces (IDS)
A reference architecture for an open network model approach

International Data spaces (IDS)
A reference architecture for an open network model approach

International Data spaces (IDS)
A reference architecture for an open network model approach

International Data spaces (IDS)
A reference architecture for an open network model approach

International Data spaces (IDS)
A reference architecture for an open network model approach
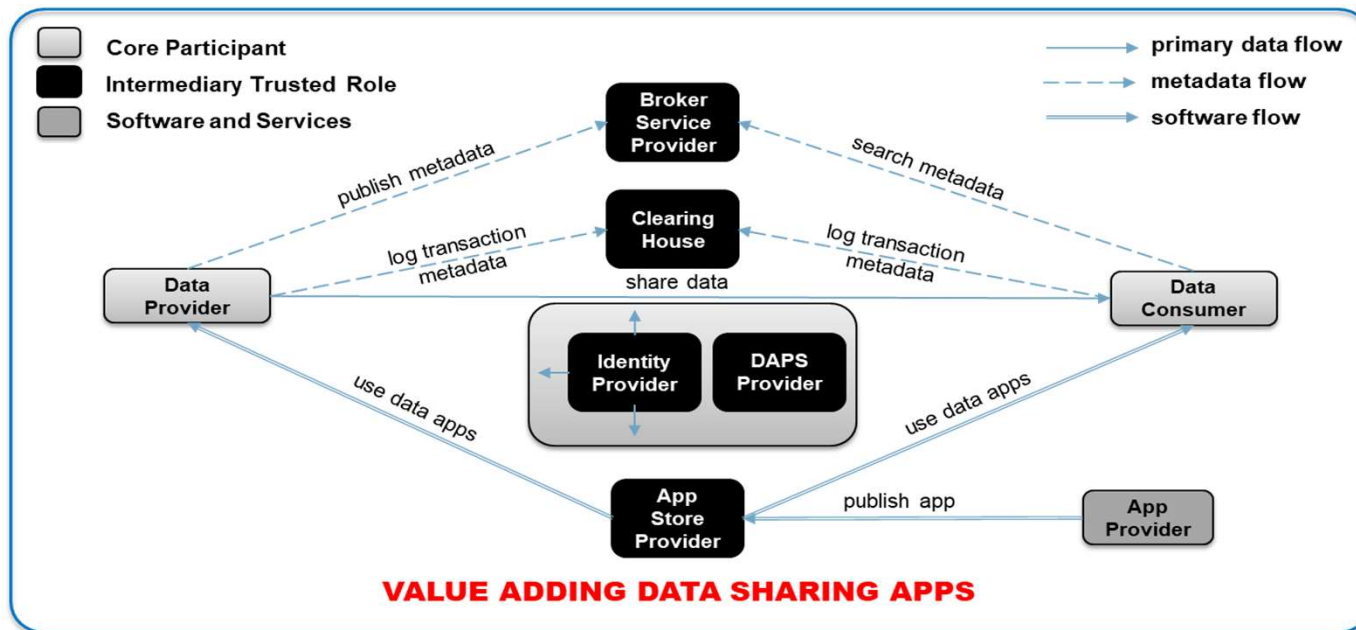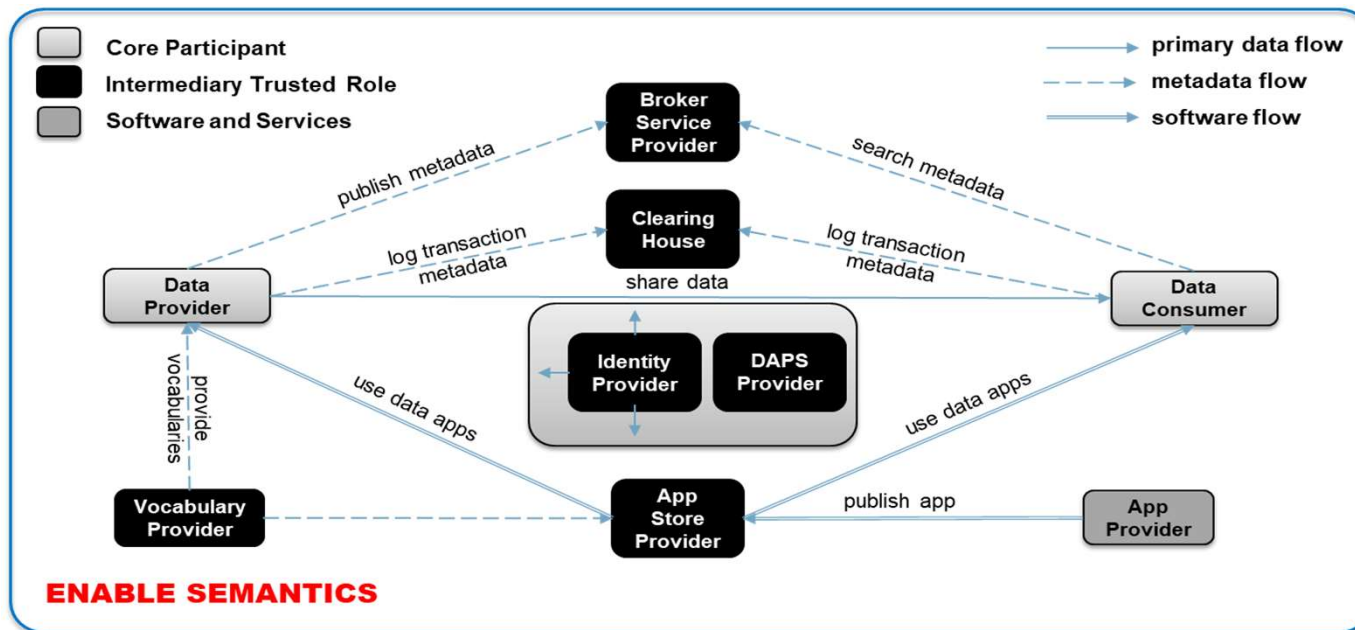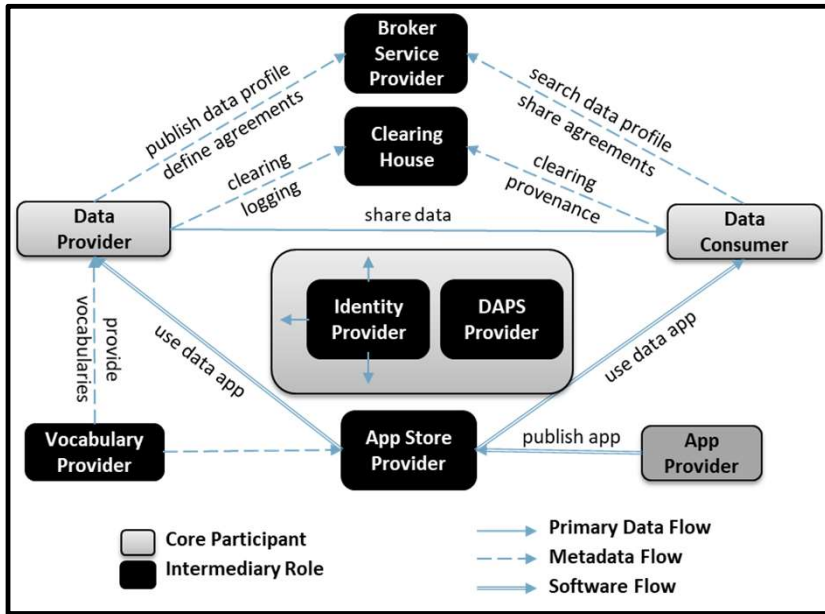
Broker Service Provider

Clearing House

publish data profile
define agreements

clearing
logging

search data profile
share agreements

clearing
provenance

Data Provider

share data

Data Consumer

Identity Provider

DAPS Provider

provide vocabularies

use data app

use data app

Vocabulary Provider

App Store Provider

publish app

App Provider

Core Participant
Intermediary Role

Primary Data Flow
Metadata Flow
Software Flow

IDS Intermediary Trusted Roles	
Role	**Function**
Identity Provider	- Manage Identities of Participants - Validate Identities of Participants
DAPS Provider	- Provide attribute information on participants and connectors - Manage and register security profiles
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, negotiation and signing of data sharing agreements
App Store Provider	- Publication and provoisioning of data apps
App Provider	- Development and maintenance of data apps
Vocabulary Provider	- Managing and offering of (domain specific) vocabularies

The network-model approach provides user-centric advantages

The network-model approach provides end-users and organization (user-centric) advantages:

- A single entry-point for simultaneously controlling data sharing over multiple relationships:
  - Based on agreed upon and standardized architectures and protocols
    - For IDS: DIN SPEC 27070: *"Reference Architecture for a Security Gateway for Sharing Industry Data and Services,". DIN Standardization Body*, https://www.din.de/en

- Operational advantages in terms of:
  - User-friendliness
  - Reduced complexity
  - Improved operational efficiency,
  - Lower costs

The user-centric network-model approach poses interoperability challenges

However, the network-model approach for controlled data sharing poses interoperability challenges.

- It is implemented in a federation of multiple intermediary roles by independent organizations
    - Providing data sharing support functions: identity provisioning, data brokering, clearing house, ….

- This also applies to interoperability for the legal concepts:
    - Data sharing agreements
    - Usage contracts, also referred to as 'terms-of-use' .

Research Question for the Paper

"How can an open model approach for data sharing with interoperability of data sharing agreements and usage contracts be developed for wide scale multi-organization adoption?"

Data sharing agreements and usage contracts

|	
Data sharing agreement: Specifying the conditions under which specific data will be shared, consisting of the contractual conditions and the usage contract.	
	Commercial conditions: Stating the commercial conditions under which the data will provided, including the costs of the data and the invoicing and payment conditions.
	Legal conditions: Stating the legal aspects required (to avoid) conflict resolution, e.g. the IPR-conditions, the applicable law, …
	Service level: Stating the quality parameters of the data provided, including completeness, accuracy and timeliness.
Usage contract: Combining the access control policies and usage control policies, expressing the data provider's internal (business) data sharing policies and the external (regulatory) policies.	
	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.

Interoperability
Role Interaction Topologies (RITs)
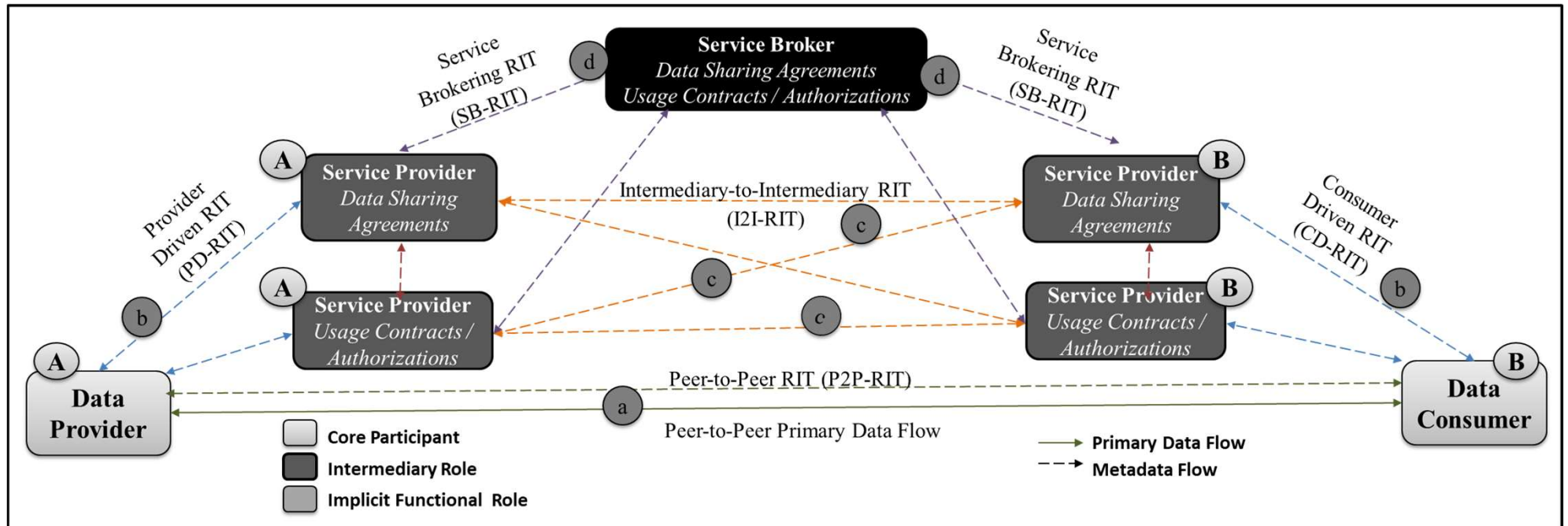
(b) Provider and Consumer Driven RIT (PD-RIT / CD-RIT)
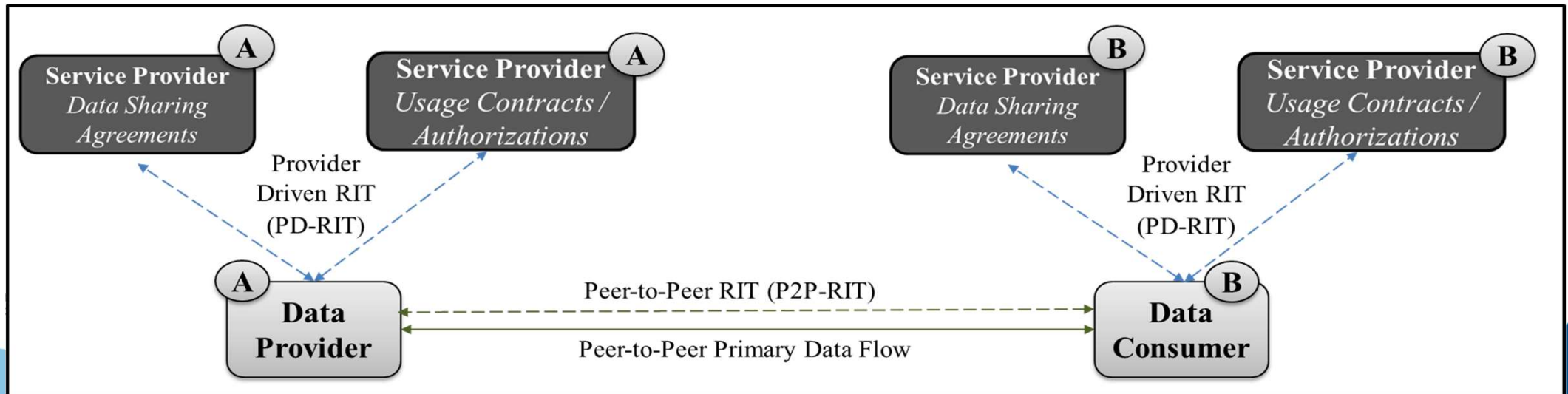(c) Intermediary-to-Intermediary RIT (I2I-RIT)
(d) Service Broker RIT (SB-RIT)

Interoperability
Role Interaction Topologies (RITs)

Evaluation criteria:

- Maintaining sovereignty over the legal concepts by the data provider and consumer

- Complexity of the overarching interoperability architecture

To be preferred: Provider and Consumer Driven RIT (PD-RIT / CD-RIT)

Conclusions and Discussion

- There is a big need for data sovereignty

- From a user-centric perspective, an open network model is preferable:
  - To enable single point of entry and prevent from vendor lock in.
  - As such, the International Data Spaces (IDS) initiative is currently attracting major interest

- The network-model approach poses an interoperability challenge on the multiple (intermediary) roles:
  - This specifically applies to data sharing agreement and the usage contract
  - The Provider and Consumer Driven Role Interaction Patterns (PD-RIT / CD-RIT) are preferred

- A machine-readable interpretation of the data sharing agreement and the usage contract is required
  - This enables automatic reasoning on the complex system of rules and obligations.
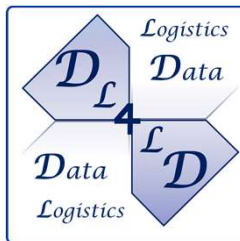 - For usage contracts within IDS, this is ODRL-based and currently being tested

Thank you for your attention

TIME FOR QUESTIONS

HARRIE.BASTIAANSEN@TNO.NL