MAINTAINING CONTROL OVER SENSITIVE DATA IN THE PHYSICAL INTERNET

TOWARDS AN OPEN, SERVICE ORIENTED, NETWORK-MODEL FOR INFRASTRUCTURAL DATA SOVEREIGNTY

TNO innovation for life

S. DALMOLEN, H. BASTIAANSEN, E. SOMERS, S. DJAFARI, M. KOLLENSTART, M. PUNTER

IPIC 2019 CONFERENCE, LONDON, THURSDAY JULY 11TH 2019

DL4LD Logistics Data Data Logistics

TKI DINALOG Dutch Institute for Advanced Logistics

NWO Netherlands Organisation for Scientific Research

Commit 2 Data connecting business and science

MAINTAINING CONTROL OVER SENSITIVE DATA IN THE PHYSICAL INTERNET

TOWARDS AN OPEN, SERVICE ORIENTED, NETWORK-MODEL FOR INFRASTRUCTURAL DATA SOVEREIGNTY

CONTENTS

- Sovereignty in data sharing
- From a hub to a network model approach
- IDS: A reference architecture
- Sovereignty over metadata

GOALS FOR TODAY / THE PAPER

- What is data sovereignty?
  - What?
  - Why
  - How?
- What is IDS (International Data Spaces)?
  - What is the IDS approach and architecture?
  - What is its status of technology?
- How to approach sovereignty on metadata?
  - ….

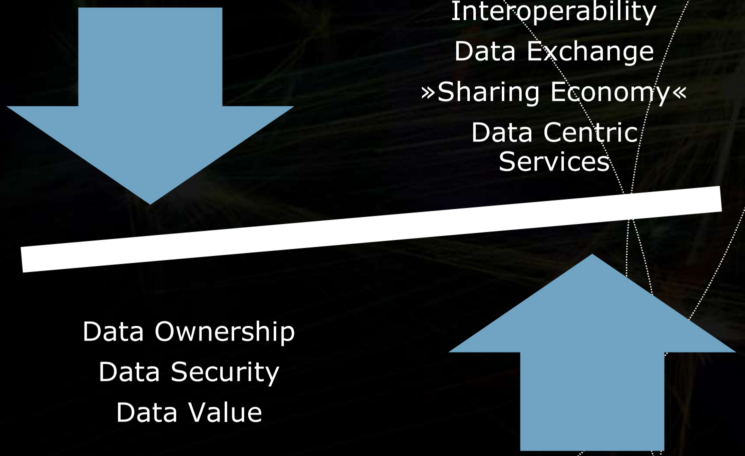
BACKGROUND

- For logistics companies being data providers in Physical Internet supply chains maintaining data sovereignty over their sensitive data applies to a multitude of data consumers, e.g. other logistics companies, logistics service providers, authorities.
  - a major challenge as data sovereignty concepts are currently mainly provided by (closed) communities with their own specific solutions.
  - Consequently, the data provider is faced with both a threat of consumer lock-in by their community providers and with major integration efforts on defining managing and enforcing data sovereignty requirements for a multitude of data sharing relationships with different data consumers.

Research question:

- How to design an overarching technical, service and business architecture for a network-model approach for infrastructural data sovereignty?

DATA SOVEREIGNTY AS BASIS
FOR TRUST BETWEEN ECOSYSTEM PARTNERS



Interoperability
Data Exchange
»Sharing Economy«
Data Centric Services

Data Ownership
Data Security
Data Value

DIGITAL SOVEREIGNTY

is the ability of a natural or legal person to exclusively and sovereignly decide concerning the usage of data as an economic asset.

SOVEREIGNTY IN DATA SHARING

DATA SOVEREIGNTY, TRUST AND SECURITY

DATA SOVEREIGNTY AND TRUST

Functional design aspect:

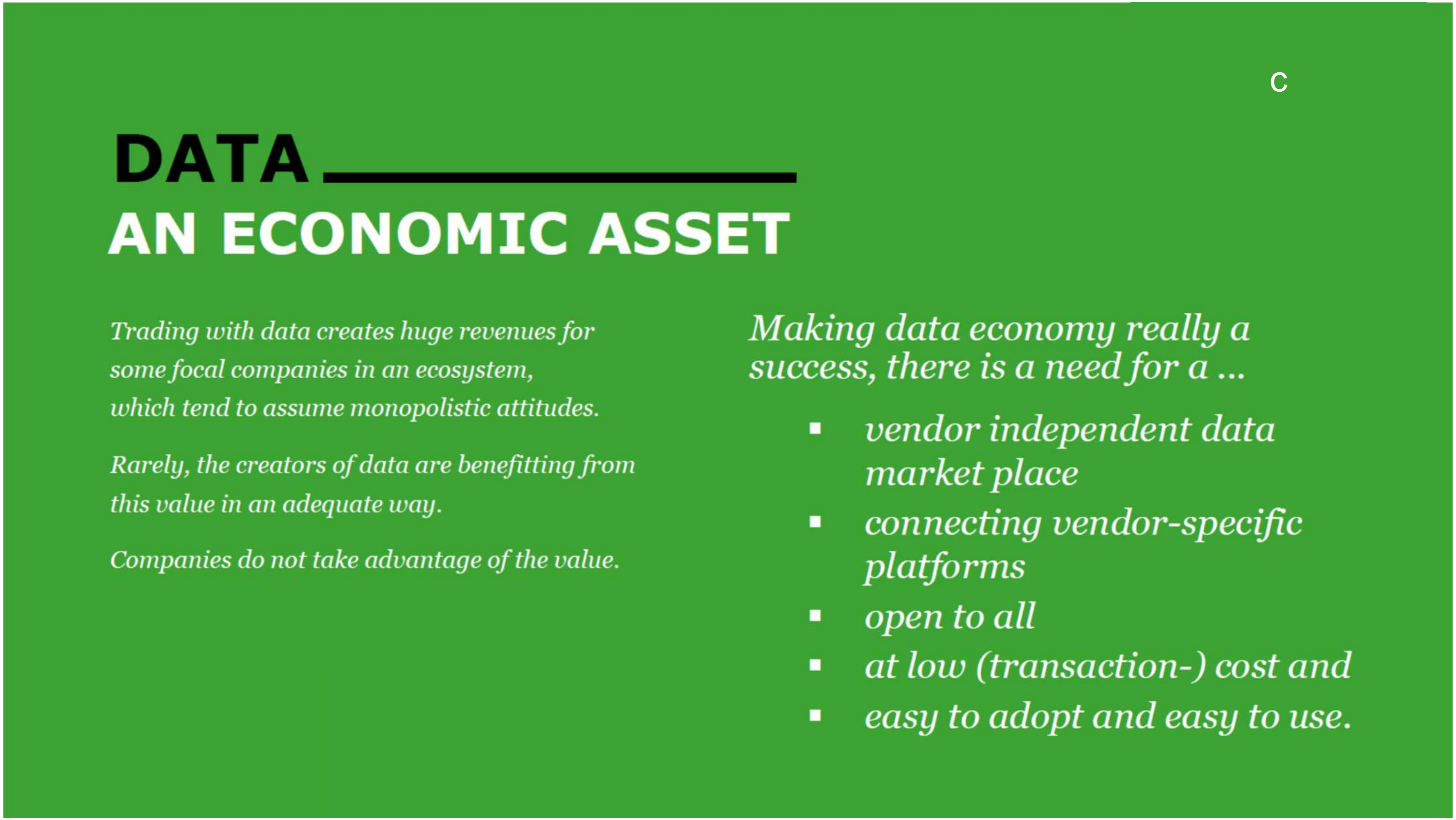
- **Data sovereignty**
- Data sharing agreements
- Enforcement of data sharing agreements
  - *legal enforceability*,
  - *implementation enforceability*
- Data provenance, logging, reporting
- System integrity monitoring

SECURITY

Non-functional design aspect:

The implementation of an IT-system must comply to its security level requirements as defined at system design and protect agains malicious or unintentional security breaches.

- Confidentiality, Integrity, Availability (CIA), …
- All ICT-systems must be secure



C

DATA

AN ECONOMIC ASSET

Trading with data creates huge revenues for some focal companies in an ecosystem, which tend to assume monopolistic attitudes.

Rarely, the creators of data are benefitting from this value in an adequate way.

Companies do not take advantage of the value.

Making data economy really a success, there is a need for a ...

- *vendor independent data market place*
- *connecting vendor-specific platforms*
- *open to all*
- *at low (transaction-) cost and*
- *easy to adopt and easy to use.*

OBSTACLES CONCERNING EXTENSIVE SHARING OF DATA

Today

57%

worry about revealing valuable data and business secrets.

59%

fear the loss of control over their data.

55%

feel inconsistent processes and systems as a (very) big obstacle.

32%

fear that platforms do not reach the critical mass, so that data exchange will be interesting.

More Data Security

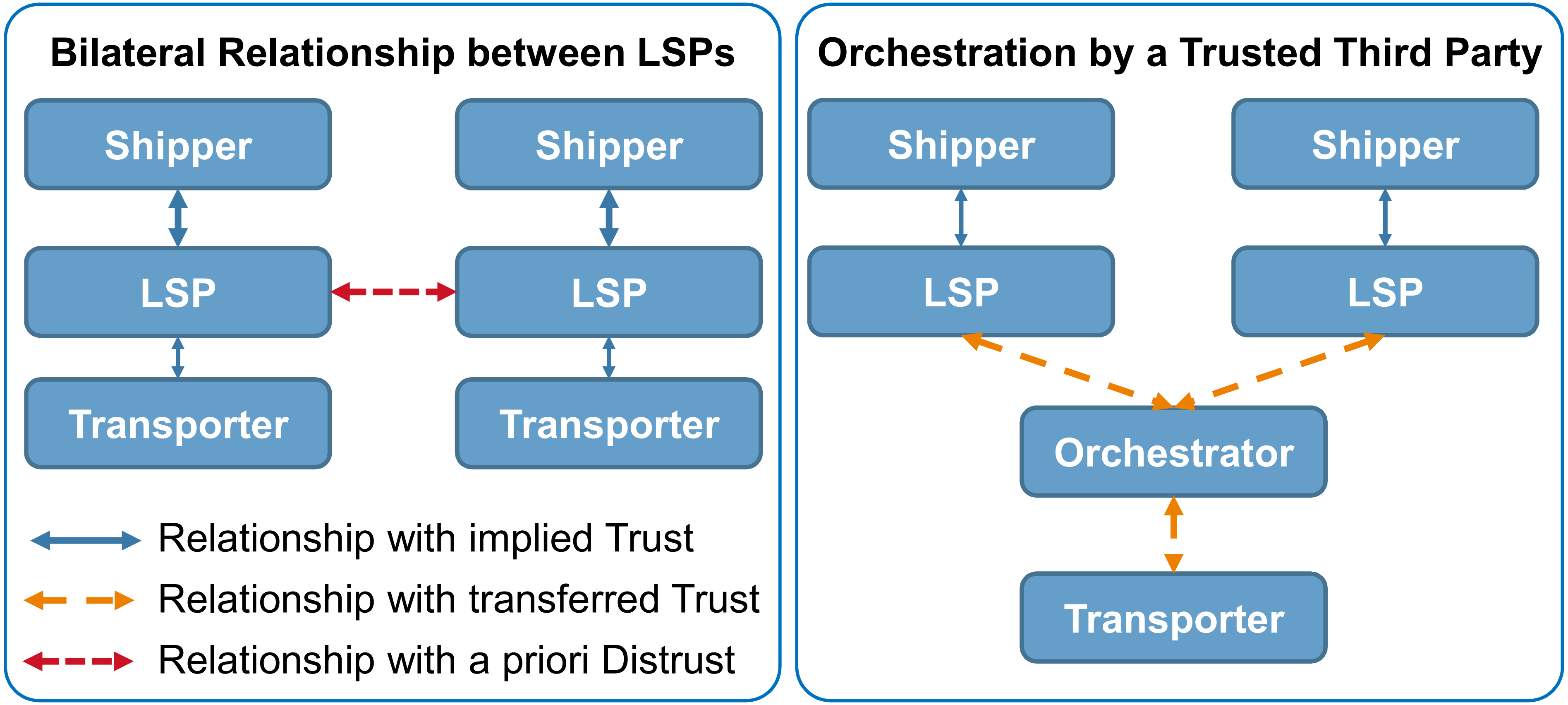
Improvement of Sovereignty

Optimising Processes and Cost Structures

Join us!

© PwC-Study on "Industrial Data Space"

TRUST RELATIONSHIPS FOR TYPICAL COLLABORATION SCENARIOS



Bilateral Relationship between LSPs

Shipper

LSP

Transporter

Shipper

LSP

Transporter

⟷ Relationship with implied Trust

⇠ ⇢ Relationship with transferred Trust

⇠--⇢ Relationship with a priori Distrust

Orchestration by a Trusted Third Party

Shipper

LSP

Shipper

LSP

Orchestrator

Transporter

DATA SOVEREIGNTY MAINTAINING CAPABILITIES

- *Procedural data sovereignty maintaining capabilities:* these include administrative capabilities such as data sharing agreements (terms-of-use and conditions), certification and attestation, logging and data provenance, reporting and accountability.
  - Legal enforceability ensures that by means of automation generated digital data sharing agreements and their associated data sharing transactions are correct and acceptable in legal procedures.

- *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 and containerization and policy-based admission control (Yavatkar et al. 1999) and enforcement and blockchains.
  - Technical enforceability ensures for the data provider that the agreed-upon conditions under which data is shared are (securely) implemented in the open infrastructure for multi-lateral data sharing

SOVEREIGNTY OVER METADATA

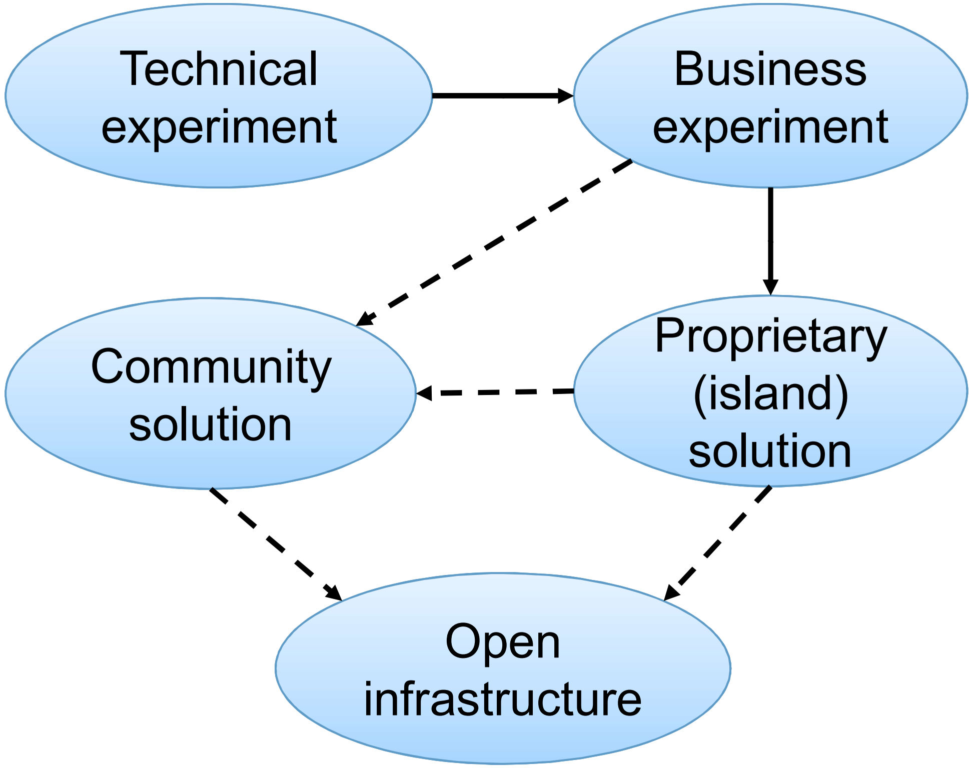
METADATA ARTEFACTS FROM DATA SHARING SUPPORT PROCESSES

Support processes for data sharing	Metadata artefacts
Definition and exposure of an available data set. • Definition and publication of a data set • Definition of a data sharing profile • Publication of a data sharing profile	• Data descriptor • Data transaction • Data request • Data response • Data sharing agreement • Access control policy • Usage control policy • Security profile policy • Service level • Terms-of-use • Commercial conditions • Juridical conditions • Contractual conditions
Making a data sharing agreement. • Definition of terms-of-use, incl. usage and access control policies • Definition of the commercial and juridical conditions • Negotiation, acceptance and signing of a data sharing agreement	
Performing a data sharing transaction. • Clearing of data sharing transactions, including non-repudiation • Data sharing, including binding of transactions to an agreement • Settlement and discharging of data sharing transaction	
Logging, provenance and reporting. • Logging and binding of data transactions to agreements • Tracking, monitoring and reporting of data transactions to • Auditing, billing and conflict resolution	

EXAMPLES OF (CLASSES) OF ACCESS AND USAGE RESTRICTIONS

Access control restrictions (access control policy) **Stating which individuals, roles or systems are allowed access to the data provided.**	**Usage control restrictions (usage control policy)** **Stating (limitations on) how data may be used after it has been shared.**
• **Provide or restrict data access to specific users** • **Provide or restrict data access for specific systems** • **Allow access to data** • **Inhibit access to data**	• Provide or restrict data access for specific purposes • Delete data after X days/months • Use data not more than N times • Use data in a specific time interval • Log data access information • Share data only if it is encrypted • Control printing shared data

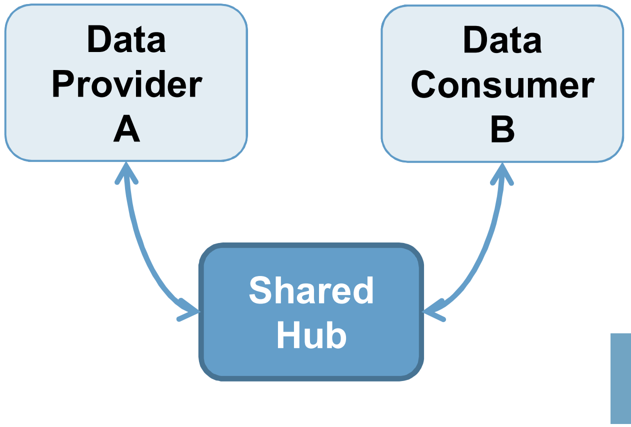
TOWARDS TO AN OPEN INFRASTRUCTURE



Otherwise **vendor-lockins** and the **legacy of the future!**

FROM A (CLOSED) HUB MODEL TO AN (OPEN) NETWORK MODEL

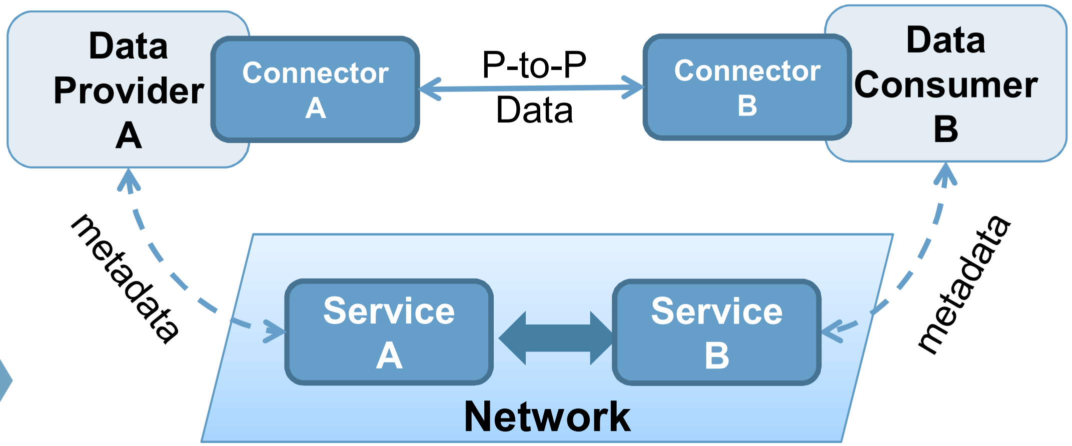
A (CLOSED) HUB MODEL



Features

- Closed communities
- Sector specific
- No single entry point for users

AN (OPEN) NETWORK MODEL

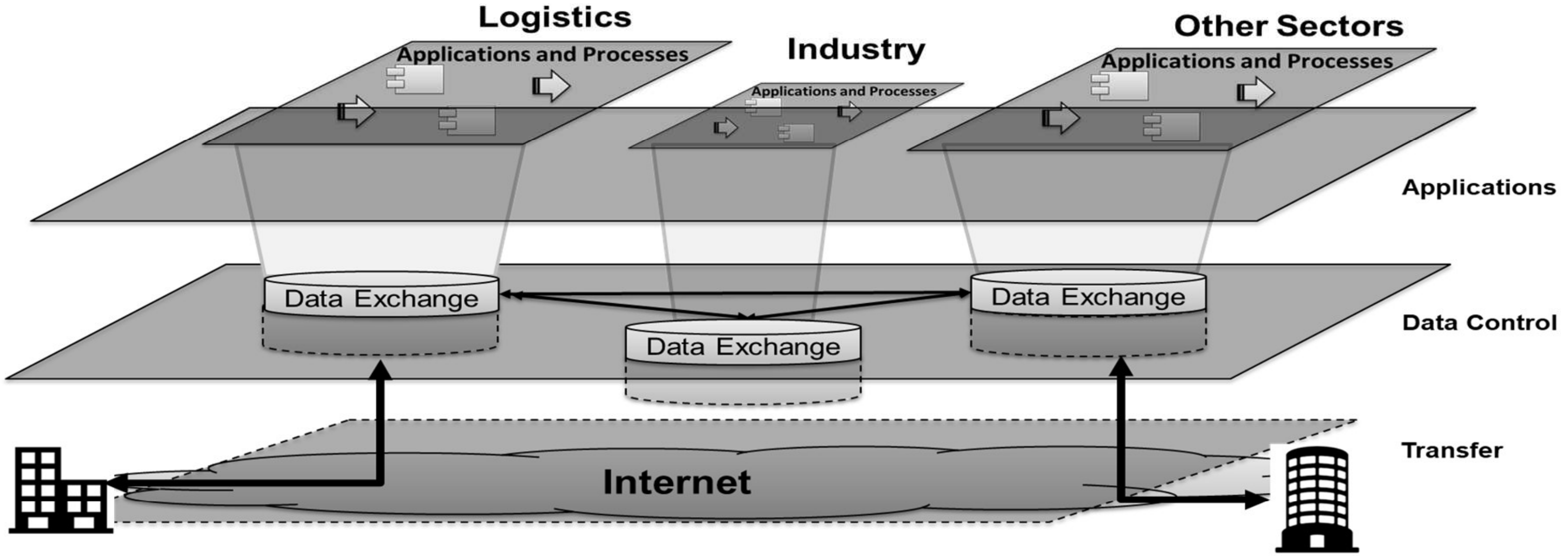


Features

- Peer-to-Peer data sharing
- Infrastructural trust
- Interoperability
  - *Examples*: banking, telecommunication, ….

THE AMBITION

OPEN INFRASTRUCTUE FOR TRUSTED SUPPLY CHAIN DATA EXCHANGE



Key requirements:

- Trust, trust, trust,…
- 'Open' infrastructure

REQUIREMENTS FOR TRUSTED DATA SHARING USING THE NETWORK-MODEL APPROACH

- *Peer-2-Peer data sharing:* local data is processed and sent directly to the data consumer
- *Distributed infrastructure for support services*
- *Openness for wide-scale adoption.*
  - *Open to end-users:* 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’.
  - *Open to solution providers:* it allows any solution provider to meet the requirements to provide enabling components in the distributed and open data sharing infrastructure under competitive conditions.
  - *Open to service providers and to innovation:* it provides an open and accessible environment for service providers to join and for new applications and services to be introduced.

IDS – A REFERENCE ARCHITECTURE

ORGANIZATION: IDS ASSOCIATION & IDS DEVELOPMENT

TNO innovation for life

IDS ASSOCIATION (IDSA)

INTERNATIONAL DATA SPACES ASSOCIATION

Objectives:

- To foster conditions and governance towards an **international standard** for the IDS architecture
- To **develop and continue** the work on standards for the IDS based on use cases
- To support **certifiable software solutions** and business models

15+
Countries
25+
Use Cases
1
Ecosystem
Allianz
TATA
Atos
BAYER
Logata
UNITY
Boehringer Ingelheim
CERTH
eccenca
Cybus
ADVANEO
Audi
Fraunhofer
DATATRONIQ
CTU
Deloitte.
HUAWEI
Insight
i2cat
denodo
mtc
SIEMENS
IK4
SAP
GateHouse
FIWARE
koppermann
komsa
DB SCHENKER
pwc
minnosphere
REWE
ENGINEERING
universität Witten/Herdecke
SETLOG
UNIKLINIK RWTHAACHEN
SICK
QuinScape
tecnalia
nicos AG
SINTEF
SALZGITTER AG
SCHAEFFLER
DXC.technology
TÜV
VOLKSWAGEN
TNO innovation for life
palbox
LSEC
RITTAL
ZVEI
thyssenkrupp
TÜV NORD GROUP
LOGENIOS
UNISCON
VTT
UNIVERSITY OF PATRAS
POLITECNICO MILANO
A!
VDMA
.msg
CHALMERS
Fastems
CAICT 中国信通院

Status Mid 2018

IDS DEVELOPMENT

Objectives:

- Create a blueprint for the data space
  - Consisting of a business, data & service, software and security architecture
  - Safe data exchange and the efficient combination of data
  - Configurable for individual use cases / scenarios

Endless **Connectivity**

Trust between security domains

Governance for the data economy

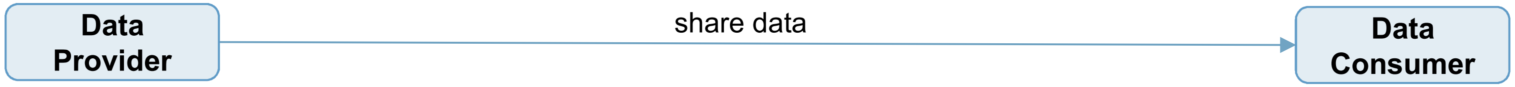
IDS – A REFERENCE ARCHITECTURE

OPEN NETWORK MODEL OF TRUSTED INTERMEDIARY ROLES

- ▢ Core Participant
- ▨ Intermediary Trusted Role
- ▧ Software and Services

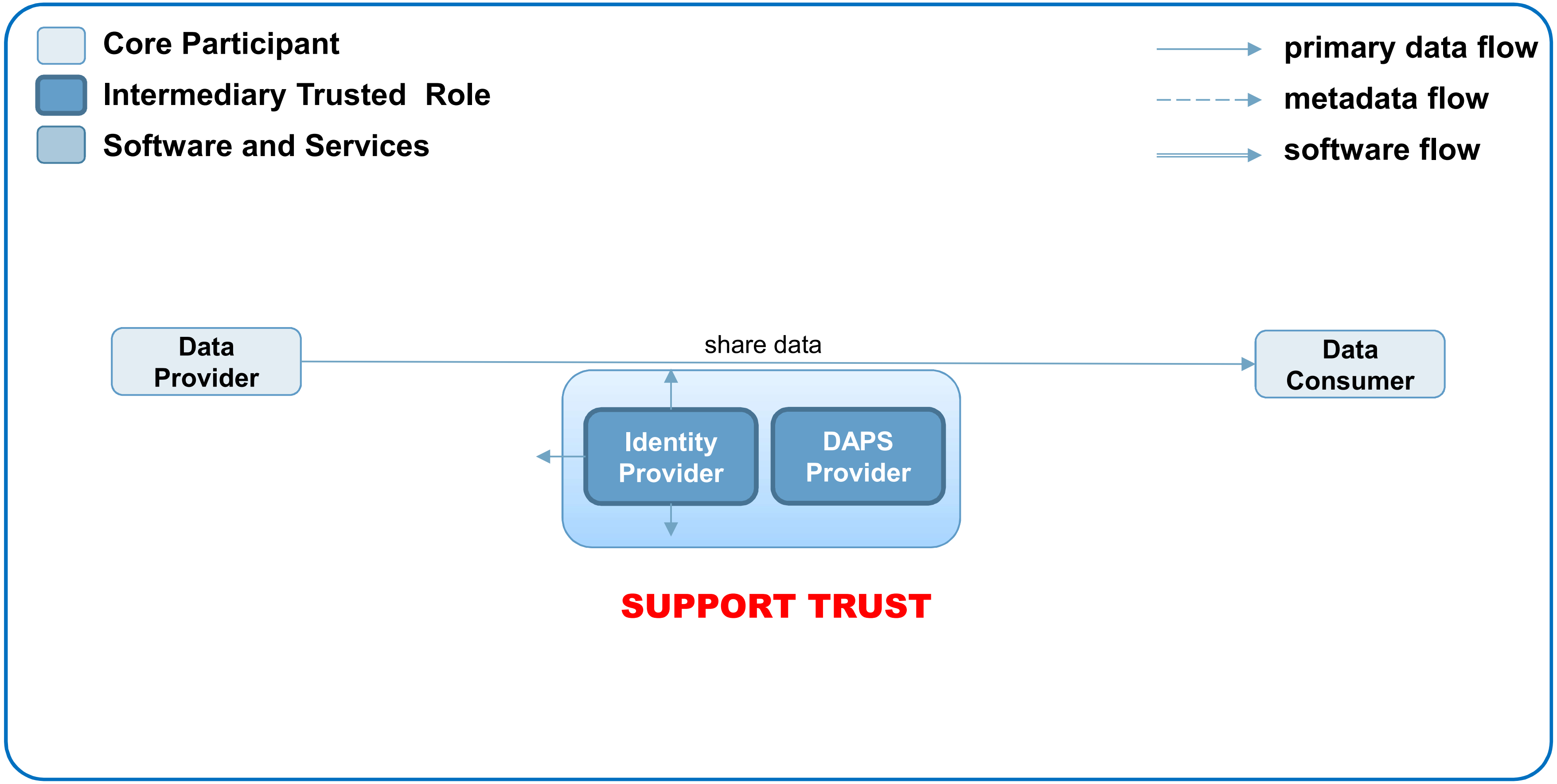
- → primary data flow
- ⇢ metadata flow
- ⇒ software flow

PEER-TO-PEER FLOW OF PRIMARY DATA



IDS – A REFERENCE ARCHITECTURE

OPEN NETWORK MODEL OF TRUSTED INTERMEDIARY ROLES



Core Participant

Intermediary Trusted Role

Software and Services

primary data flow

metadata flow

software flow

Data Provider

share data

Data Consumer

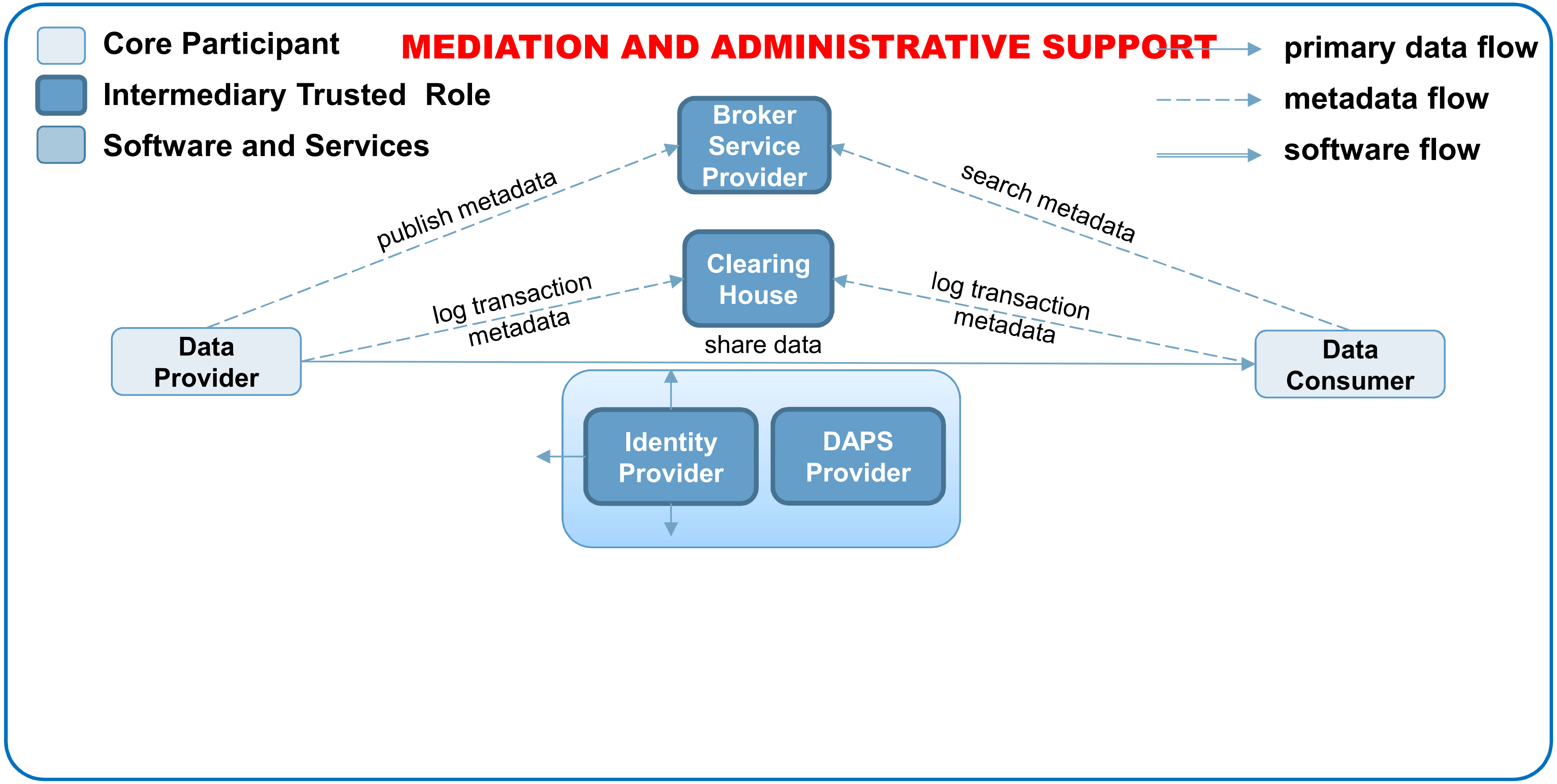
Identity Provider

DAPS Provider

SUPPORT TRUST

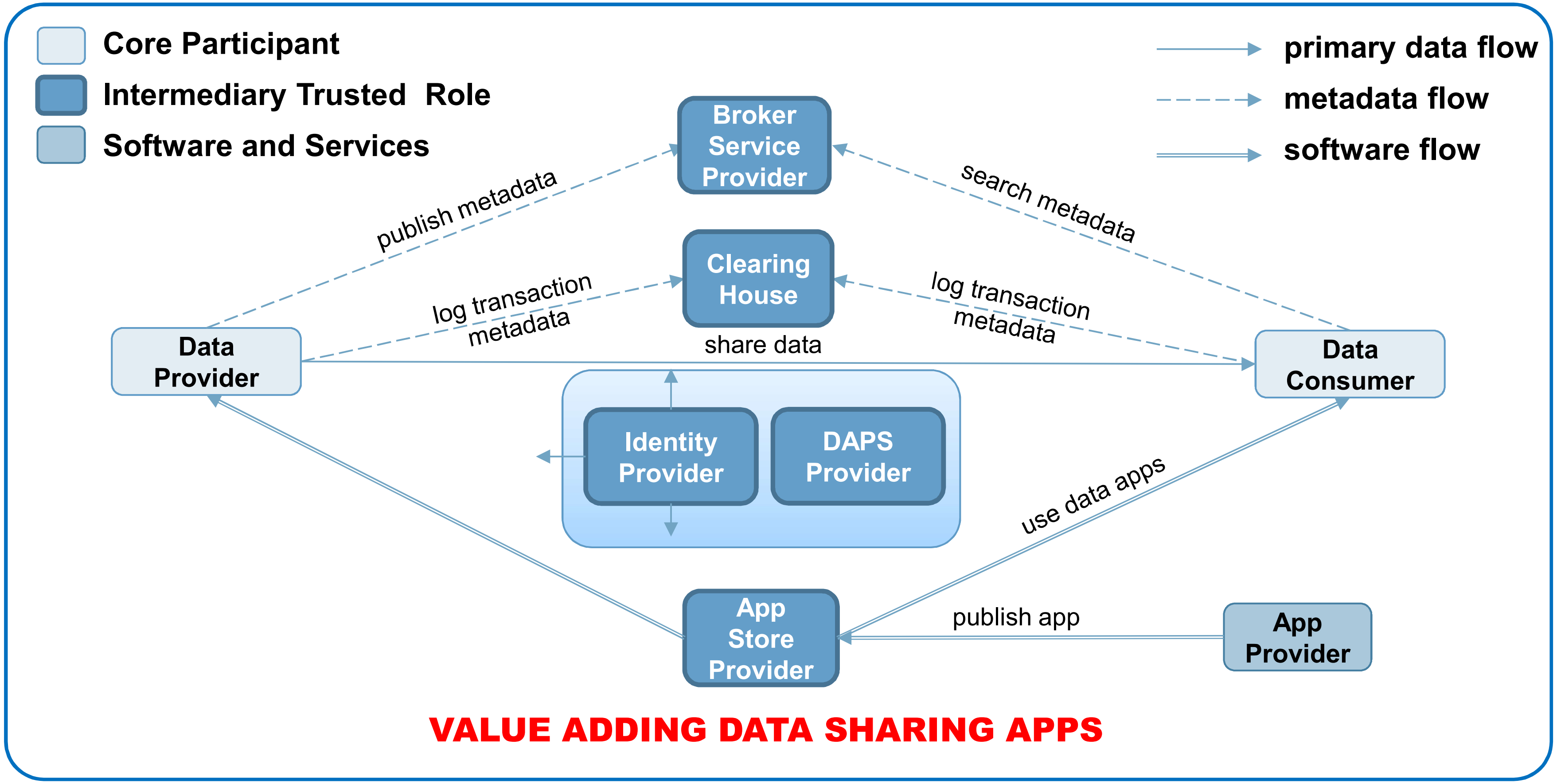
IDS – A REFERENCE ARCHITECTURE

OPEN NETWORK MODEL OF TRUSTED INTERMEDIARY ROLES



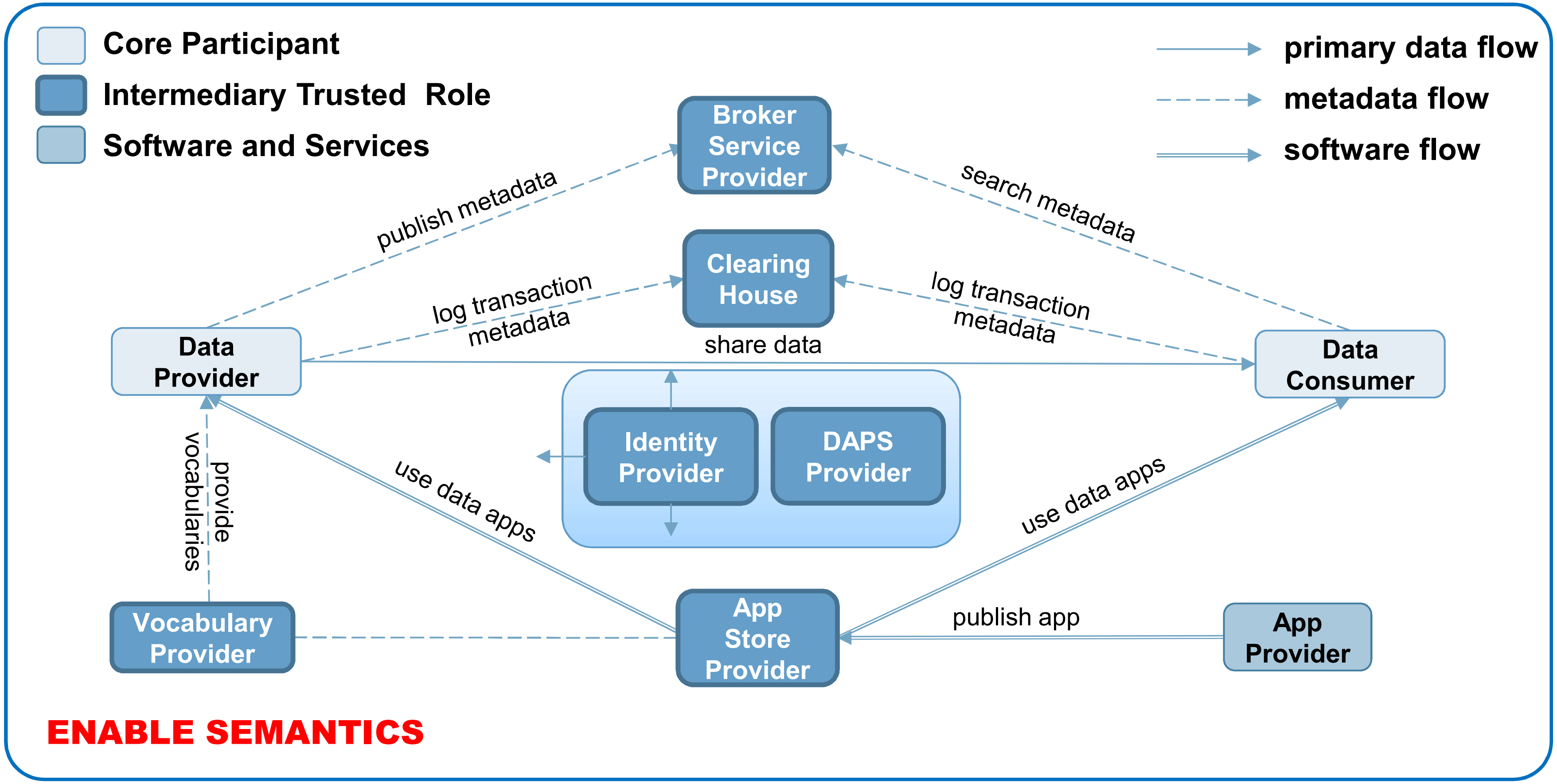
IDS – A REFERENCE ARCHITECTURE

OPEN NETWORK MODEL OF TRUSTED INTERMEDIARY ROLES



IDS – A REFERENCE ARCHITECTURE

OPEN NETWORK MODEL OF TRUSTED INTERMEDIARY ROLES

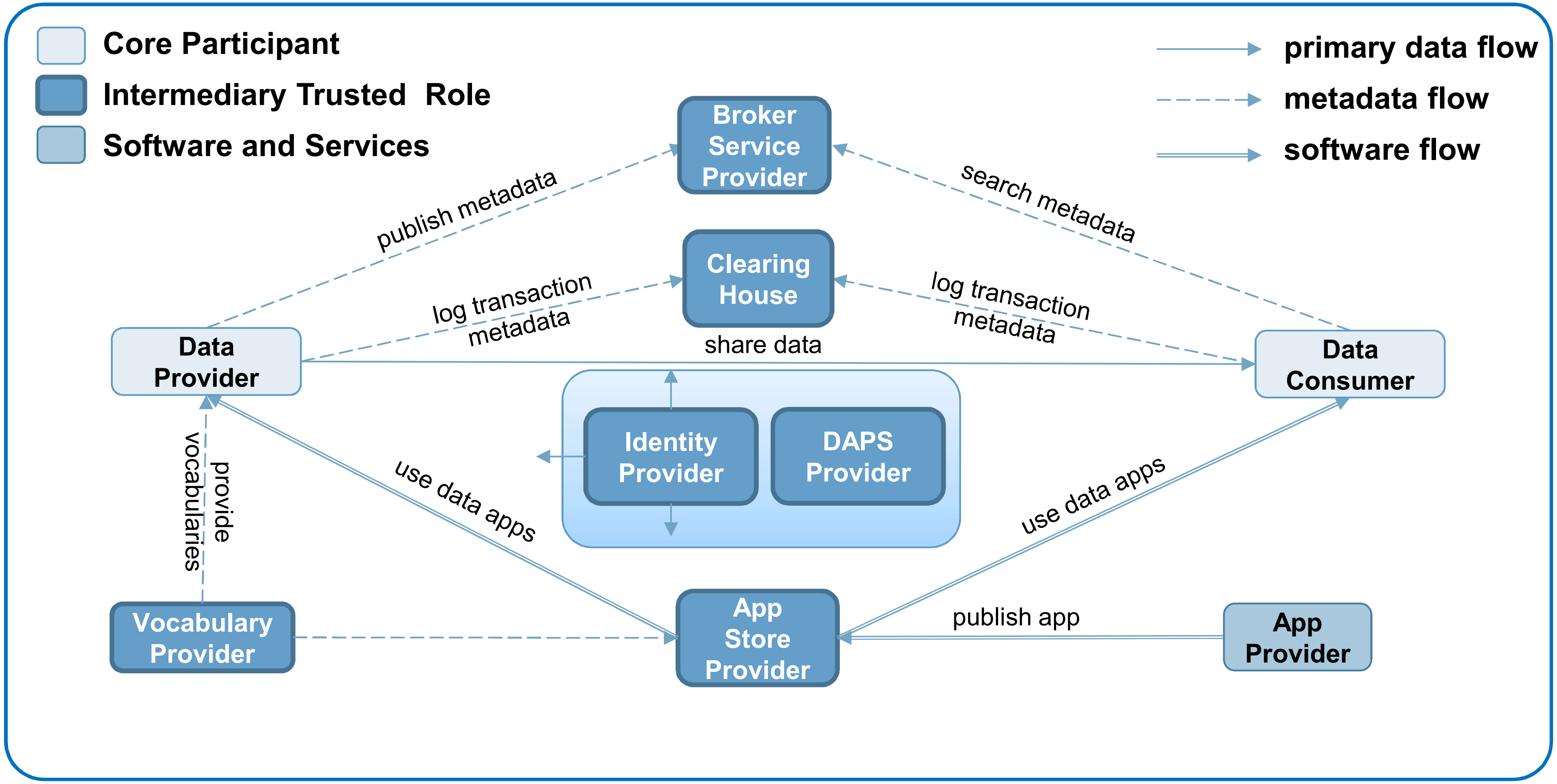


ENABLE SEMANTICS

IDS – A REFERENCE ARCHITECTURE

OPEN NETWORK MODEL OF TRUSTED INTERMEDIARY ROLES

TNO innovation for life



DISCUSSION

Implementation of the new world requires that shippers, LSP’s, transporters and other service providers in the logistic value chain share (potentially sensitive) business and operations data. As such, they give rise to new challenges:

- *Compliance to internal business policies for trusted data sharing:* to reap the indicated benefits of exchanging data, operational data which may be valuable and business-sensitive has to be shared with stakeholders that could potentially be competitors. A trustworthy infrastructure based on solid agreements and contracts and a technical secure data sharing infrastructure are a prerequisite for convincing stakeholders to exchange such data, i.e. an interoperable, multi-lateral, trusted data sharing infrastructure.
- *Compliance to external regulatory policies:* to share data, different regulations are introduced by European law makers. Notwithstanding the inherent complex role of data and algorithms, an increased understanding is needed about how data regulation should be applied in case of data platforms.

Logistics Data DL4LD Data Logistics

THANK YOU FOR YOUR ATTENTION

Take a look:

- WWW.DL4LD.NET
- TIME.TNO.NL

TNO innovation for life

S. (Simon) Dalmolen, MSc

Tel: +31 6 153 26114

Simon.Dalmolen@TNO.NL

TKI DINALOG Dutch Institute for Advanced Logistics
NWO Netherlands Organisation for Scientific Research
Commit 2 Data connecting business and science
THALES
BiZZdesign
ciena
evofenedex
AIRFRANCE KLM
TRANSFIDES
ORACLE
Gemeente Amsterdam
Universiteit van Amsterdam
TNO innovation for life

IDS - ORGANIZATION

IDS ASSOCIATION: REGIONAL HUBS

VTT

Technical Research Centre of Finland
-Espoo, Finland

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Czech Technical University in Prague
-Prague, Czech Republic

innovalia ASSOCIATION

Technological Centre
-Bilbao, Spain

Institut Mines-Télécom

Higher Education and Research Institution
-Paris, France

Cefriel

Digital Innovation Centre
-Milan, Italy

TNO

Organization for Applied Scientific Research
-The Hague, Netherlands

IDS - DATA SOVEREIGNTY

RELATION TO ALICE INFORMATION SYSTEM RESEARCH AND INNOVATION ROADMAP

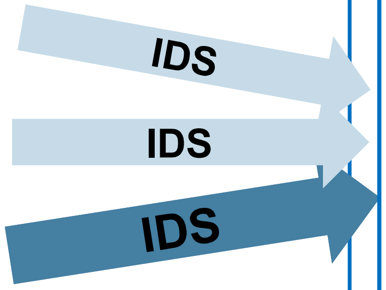
TNO innovation for life

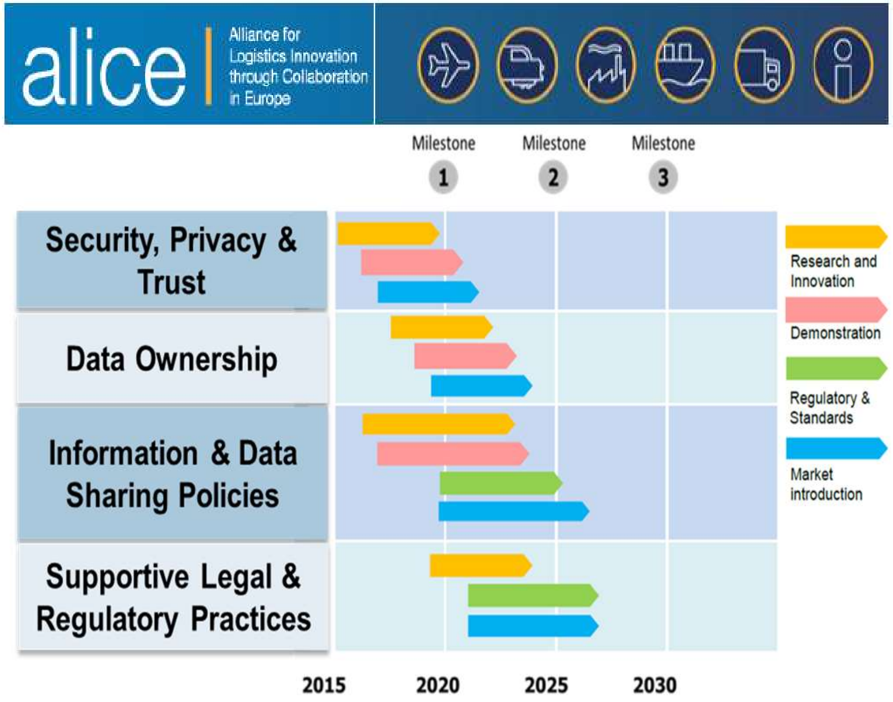
IDS MAY FILL-IN (PART OF) THE ALICE DATA GOVERNANCE ROADMAP

ALICE THEMES

Themes addressed in the ALICE 'Information Systems for Interconnected Logistics' Research and Innovation Roadmap:

- ICT Innovation
- New Business Models
- **Data Governance**



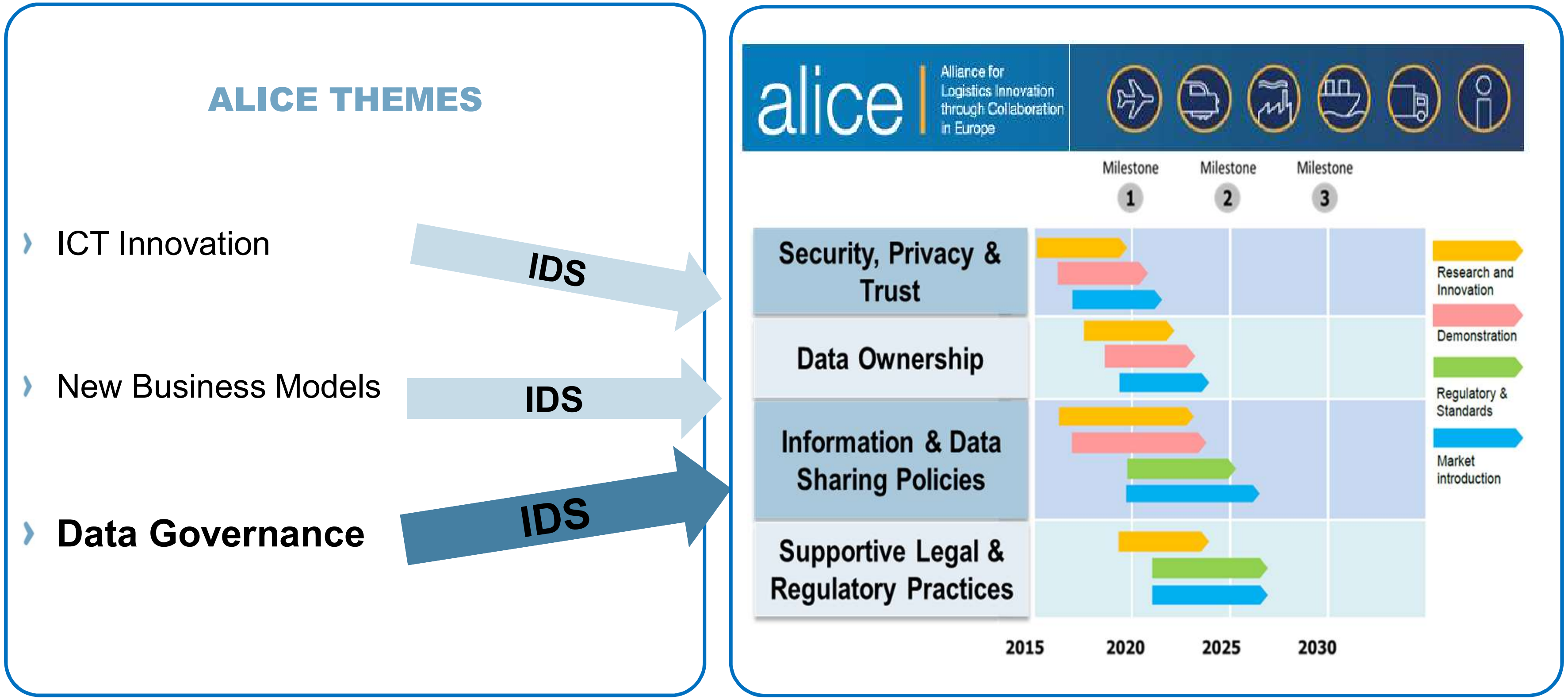


Source: http://www.etp-logistics.eu/wp-content/uploads/2015/08/W36mayo-kopie.pdf

IDS - DATA SOVEREIGNTY

RELATION TO ALICE INFORMATION SYSTEM RESEARCH AND INNOVATION ROADMAP

IDS MAY FILL-IN (PART OF) THE ALICE DATA GOVERNANCE ROADMAP



ALICE THEMES

- ICT Innovation
- New Business Models
- **Data Governance**

IDS

IDS

IDS

alice
Alliance for Logistics Innovation through Collaboration in Europe
Milestone 1
Milestone 2
Milestone 3
Security, Privacy & Trust
Data Ownership
Information & Data Sharing Policies
Supportive Legal & Regulatory Practices
Research and Innovation
Demonstration
Regulatory & Standards
Market introduction
2015
2020
2025
2030

Source: http://www.etp-logistics.eu/wp-content/uploads/2015/08/W36mayo-kopie.pdf

IDS – REFERENCE ARCHITECTURE

IDS: WHAT IT IS & WHAT IT IS NOT

WHAT IT IS

- Fundamental approach to the basic issue of data sovereignty across sectors and organizations
  - Interoperability, Standardization, Governance
  - Based on open network model
- Infrastructural layer to build value adding services and solutions upon

WHAT IT IS NOT

- Solution to all challenges in logistics
  - Supply chain collaboration
    - However: combined IDS and blockchain solution are considered
  - Semantic interoperability
    - Doesn’t prescribe semantic standards
    - However, provides the ‘hooks’ for semantic conversion app’s