Rechtmässige Datenverarbeitung als Architekturherausforderung für Datenplattformen
Digital Ecosystems

- Industrie 4.0
- Smart Farming
- Smart Energy
- Smart Mobility
- Smart Health
- Smart Rural Areas
- Smart Teams
- Smart X
DATA HUBS / MARKETPLACE PLATFORMS
THE DATA PLATFORM CARUSO
DEVELOPMENT OF CONNECTED VEHICLES IN EUROPE

→ Retrofit suppliers (short-term) & OEM (long-term) become potential data suppliers

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of European cars and light commercial vehicles in millions</th>
<th>Not Connected</th>
<th>Retrofit</th>
<th>OEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>314</td>
<td>285</td>
<td>16</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>91%</td>
<td></td>
<td>21%</td>
<td>69</td>
</tr>
<tr>
<td>2020</td>
<td>325</td>
<td>165</td>
<td>28%</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>51%</td>
<td></td>
<td>40%</td>
<td>137</td>
</tr>
<tr>
<td>2025</td>
<td>344</td>
<td>105</td>
<td>30%</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>31%</td>
<td></td>
<td>31%</td>
<td>105</td>
</tr>
</tbody>
</table>

Retrofit suppliers (short-term) & OEM (long-term) become potential data suppliers.

Source: IHS, LMD, Roland Berger
ECOSYSTEM WITH B2B MARKETPLACE PLATFORM

DATA PROVIDER

DATA CONSUMER

Business

Technical

Legal
ECOSYSTEM WITH B2B MARKETPLACE PLATFORM

Example

Business  Technical  Legal

OEM (BVW)

WORKSHOP (1-2-3-Workshops)

Driver

Car
OUR INITIAL CONNECTED PARTNERS

- ABAX
- BMW (Invented for life)
- BOSCH
- Continental (The Future In Motion)
- OPENMATIC
- TecAlliance
- WERBAS
- Schaeffler
- JimDrive
- ABAX
- Bosch Service
HIGH-LEVEL PLATFORM ARCHITECTURE

CARUSO DATAPLACE

Marketplace

Data needed for brokering

"provider X offers mileage for car with VIN XYZ"

Delivery Engine

Data / Service
brokered via Caruso

"mileage of car with VIN XYZ is 10.382"

Partner System

Partner System
## CARUSO DATA CATALOGUE: HARMONIZED IN-VEHICLE DATA

<table>
<thead>
<tr>
<th>Vehicle Position, Movement &amp; Surroundings (65)</th>
<th>Vehicle Health &amp; Maintenance (43)</th>
<th>Vehicle Non-Powertrain Hardware (76)</th>
<th>Vehicle Powertrain Resources (57)</th>
<th>Vehicle Powertrain Hardware (223)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Movement &amp; Distances (12)</td>
<td>Maintenance (19)</td>
<td>ABS, ESP &amp; Traction Control (5)</td>
<td>Air (8)</td>
<td>Combustion (30)</td>
</tr>
<tr>
<td>Trip Details (16)</td>
<td>Malfunctions – MIL (4)</td>
<td>Brakes (13)</td>
<td>Fuel – Consumption (10)</td>
<td>ECUss (31)</td>
</tr>
<tr>
<td>Vehicle Surroundings Data (10)</td>
<td></td>
<td>External Hardware (3)</td>
<td>Oil (12)</td>
<td>Engine Status (16)</td>
</tr>
<tr>
<td>Vehicle Identification (4)</td>
<td></td>
<td>Heater &amp; AC (9)</td>
<td></td>
<td>Exhaust (39)</td>
</tr>
</tbody>
</table>

**Additional Categories:**
- Vehicle Surroundings Data (10)
- Vehicle Health & Maintenance (43)
- Vehicle Non-Powertrain Hardware (76)
- Vehicle Powertrain Resources (57)
- Vehicle Powertrain Hardware (223)

- ABS, ESP & Traction Control
- Airbags
- Brakes
- Doors, Windows & Locks
- External Hardware
- Heater & AC
- Lights
- Seatbelts
- Tyres, Steering & Suspension
- Wipers

- Air
- Coolant
- Fuel – Consumption
- Fuel – General
- Oil

- Combustion
- Drive Battery
- ECUss
- Electric Vehicle Battery
- Engine Status
- Exhaust
- Ignition
- Particulate Filter
- Transmission
DELIVERY OF PERSONAL DATA

DATA PROVIDER

DATA CONSUMER

Personal Data

Personal Data

B2C

B2B

B2B2C
GDPR
But no legal advice,
and no hard questions please ;)

PERSONAL DATA

Any information relating to an identified or identifiable natural person

GDPR Art. 4 No.1
PERSONAL DATA

Vehicle Identification Number (VIN)?
PERSONAL DATA CAN HARDLY BE PREVENTED

DATA PROVIDER

DATA CONSUMER

VIN, Battery Level
VIN, Mileage
Name, Address

B2C
B2B
B2B2C
ENSURING LAWFULNESS OF DATA PROCESSING
1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
LEGAL OPTIONS COMPARING OVERVIEW

• Consent
  • Higher technical effort
  • Closer to ExVeh standard
  • OEM and Neutral Server can verify consent from user
  • Feels “stronger”
  • Easier to understand
  • Legally sound, all involved parties covered
  • Lower risk of abuse and damage of image

→ More technical effort but possibly more convincing and lower risk for partners

• Legitimate Interest
  • Low technical effort
  • Further from ExVeh standard
  • OEM & Neutral Server give responsibility to service provider
  • Feels “looser”
  • More difficult to understand
  • Legally sound, all involved parties covered
  • Higher risk of abuse and damage of image

→ Less technical effort but possibly less convincing and higher risk for partners
SPECIAL CATEGORIES OF DATA

ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, etc.
LOCATION DATA IS EVIL
REQUIREMENTS FOR CONSENT HANDLING

• The solution approach **must** fulfill the regulations of the GDPR
• The data consumer **must** not be required to interact with all data providers individually
• Involved parties **must** know and be able to store the message that users have been shown and to which they gave consent
• The data provider **should** not be able to identify the data consumer
• The data provider **should** not be able to identify the user / registered keeper
• The data provider **should** not be required to trust a third party unconditionally
• The solution approach **should** be compliant to current ExVe standard ideas
• The solution approach **should** be easily implementable for the data consumer
• The solution approach **should** impede unlawful processing of personal data
• The solution **should** utilize a standard security technology
• The Neutral Server **could** not need to store personal data of the user
• The user **could** be able to manage given consent at a central place
• The user **could** give consent to a whole chain of organizations in a given use case
USE EXISTING SECURITY SOLUTION: OAUTH2

1. provide auth link in app
2. call auth link via app
3. request authorization for Client
4. authorize
5. provide access token & refresh token
6. Get data (access token)
7. Check token and return data
SOLUTION ALTERNATIVES
SOLUTION ALTERNATIVE 1

Data Provider

«Authorization Server»
BVW Authorization Server

Neutral Server

Authorization Server: Data Provider

Neutral Server

Brokering Server

Data Consumer

«Client»
1-2-3-Workshops
Service Backend

Client: Data Consumer
SOLUTION ALTERNATIVE 1

1. authorize
2. provide access token & refresh token
3. request data (access tokens)
4. request data (forwarded access token)
5. return data
6. return data

Data Provider

Neutral Server

Data Consumer

«Authorization Server»
BVW
Authorization Server

«Resource Server»
BVW
Data Server

Neutral Server
Brokering Server

«User Agent»
MyCarData App

«Client»
1-2-3-Workshops
Service Backend

«Resource Owner»
Registered Keeper
Caroline

«User Agent»
MyCarData App

«Client»
1-2-3-Workshops
Service Backend

«Resource Owner»
Registered Keeper
Caroline
SOLUTION ALTERNATIVE 1

1. refresh access tokens (refresh tokens)
2. request data (VINs, access tokens)
3. request data (VINs, forwarded access token)
4. request data (VINs, forwarded access token)

Data Provider

«Resource Server»
Data Provider
Data Server

«Resource Server»
Data Provider
Data Server

«Resource Server»
Data Provider
Data Server

Neutral Server

2. request data (VINs, access tokens)

1. refresh access tokens (refresh tokens)

Data Consumer

«Client»
1-2-3-Workshops
Service Backend

Registered Keeper
Registered Keeper
Registered Keeper
Registered Keeper
SOLUTION ALTERNATIVE 2

Trust :(

1. authorize
2. provide access & refresh token
3. request data (access token)
4. request data
5. return data
6. return data
SOLUTION ALTERNATIVE 3

Data Provider

"Authorization Server" BVW Authorization Server

"Resource Server" BVW Data Server

Neutral Server

Authorization Server: Data Provider

"Client" Neutral Server Brokering Server

Data Consumer

1-2-3-Workshops Service Backend
SOLUTION ALTERNATIVE 3: CONSENT PROVISIONING

Data Provider

«Authorization Server»
BVW Authorization Server

9. check credentials & store consent

Neutral Server

6. call auth link via app

7. request authorization for Neutral Server

8. authorize

10. provide access token & refresh token (state)

Data Consumer

4. return VIN-specific auth link (id in state, data items, purpose in scope)

11. Notify successful authorization

«User Agent»
MyCarData App

1. Start consent process (first time use, new car registered)

5. provide auth link in app (NS callback. NS clientID, id in state, data items, purpose in scope)

«Resource Owner»
Registered Keeper Caroline

No trust required :)  

Platform handles consent :)  Single point of interaction :)

«Resource Server»
BVW Data Server

3. store mapping state id -> VIN, purpose, data items

«Client» Neutral Server

2. request auth link (VIN, purpose, data items)

1-2-3-Workshops Service Backend

11. store mapping VIN, purpose -> tokens

Data consumer remains anonymous :)
OTHER SOLUTION APPROACHES

• Caruso as central consent management hub with custom-built consent mechanism
  • Trust from all parties towards Caruso required
  • Implementation of security technology necessary

• Utilization of Blockchain technology
  • Either identities and provided consent information accessible
  • Or trust toward Caruso required
LAWFULNESS DATA PROCESSING
TECHNICAL REALIZATION
CONSENT: POC – WHAT HAPPENS BEHIND THE SCENES
POC – SETTING

• BVW
  • Has a contract with the registered keeper
  • Has a contract with Caruso
  • Acts as a data provider for „mileage“ and „DTC“

• Insurancia
  • Has a contract with the registered keeper
  • Has a contract with Caruso
  • Acts as a data provider for „address“

• 1-2-3-Workshops
  • Has a contract with the registered keeper that was made via the „MyCarData“ app
  • Has a contract with BVW and Insurancia that was made via the Caruso Marketplace
    • 1-2-3-Workshops decides to remain anonymous towards BVW
  • Has a contract with Caruso
  • Acts as a data consumer for „mileage“, „DTC“, „address“
POC – TECHNOLOGIES IN USE

- **Auth0** (Cloud Service)
  - Authorization Server
  - Simulation of Backend with ExVe
  - Spring Boot Server

- **Auth0** (Cloud Service)
  - Authorization Server
  - Simulation of Backend with ExVe
  - Spring Boot Server

- Simulation of Neutral Server
  - Spring Boot Server

- Simulation of Backend
  - Spring Boot Server

- Simulation of App “MyCar”
  - Angular Web App

- **Organizations**
  - OEM BVW
  - Insurancia
  - Neutral Server Caruso
  - 1-2-3-Workshops
### Insurancia stores given consent:
- Client „Caruso”
- Has the consent to retrieve the data item „address”
- For the car with VIN „3VWD67AJ2GM278385”
- For the purpose of „maintenance”
- Given by „Owner”
- Given at „24.01.2019”

### OEM BVW stores given consent:
- Client „Caruso”
- Has the consent to retrieve the data items „mileage, DTC”
- From the owner of the car with VIN „3VWD67AJ2GM278385”
- For the purpose of „maintenance”
- Given by „Owner”
- Given at „24.01.2019”

### Caruso stores consent request:
- Client „Caruso”
- Has the consent to retrieve the data items „mileage, DTC”
- From the data provider „BVW”
- Has the consent to retrieve the data item „address”
- From the data provider „Insurancia”
- For the car with VIN „3VWD67AJ2GM278385”
- For the purpose of „maintenance”
- Caruso stores state -> VIN, purpose mapping
- Caruso receives and stores OAuth tokens
  - Consent given at „24.01.2019”
  - VIN, purpose -> OAuth token mapping

### 1-2-3-Workshops requests
- Needs the consent to retrieve the data items „mileage, DTC”
- From the data provider „BVW”
- Needs the consent to retrieve the data item „address”
- From the data provider „Insurancia”
- For the car with VIN „3VWD67AJ2GM278385”
- For the purpose of „maintenance”
- 1-2-3-Workshops gets notified about successful consent
  - Consent given at „24.01.2019”

### Owner sees consent:
- Client „Caruso” wants to retrieve data to pass it to 1-2-3-Workshops
- Has the consent to retrieve the data items „mileage, DTC”
- From the Data provider „BVW”
- Has the consent to retrieve the data item „address”
- From the data provider „Insurancia”
- For the car with VIN „3VWD67AJ2GM278385”
- For the purpose of „maintenance”

---

**POC – WHO KNOWS WHAT ABOUT CONSENT?**

Organizations

- **Insurancia**
- **OEM BVW**
- **Neutral Server Caruso**
- **1-2-3-Workshops**

---

**Neutral Server**
INTEGRATION INTO THE PLATFORM

Data Provider

<<Authorization-Server>>
Authorization Server

<<Resource-Server>>
Data Provider Server

Caruso

<<OAuth Client>>
Neutral Server

ConsentHandler

DeliveryService

Data Consumer

Data Consumer Server

MyCarData-App

consent-provisioning
consent-revocation
consent-refresh

fetch access-token

delivery-request with consent

delivery-request with consent

consent-provisioning
consent-revocation

CHALLENGES TO BE SOLVED

• Granularity and naming must match for all parties
  • Mileage as a subcategory of “in-vehicle data”
    • What happens if the data provider cannot offer this data point individually?
  • Odometer ⇔ Mileage
    • Is the user confused by different terminologies on the data provider and data consumer side?

• Processing purpose
  • GDPR compliance without risking the neutrality of the service
Rechtmäßige Datenverarbeitung als Architekturherausforderung für Datenplattformen

https://www.caruso-dataplace.com/
http://architecture.iese.fraunhofer.de/
https://blog.iese.fraunhofer.de/category/architecture/