Rechtmässige Datenverarbeitung als Architekturherausforderung für Datenplattformen

Dominik Rost (Fraunhofer IESE)
Matthias Naab (Fraunhofer IESE)
Joshua Vécsei (Caruso)

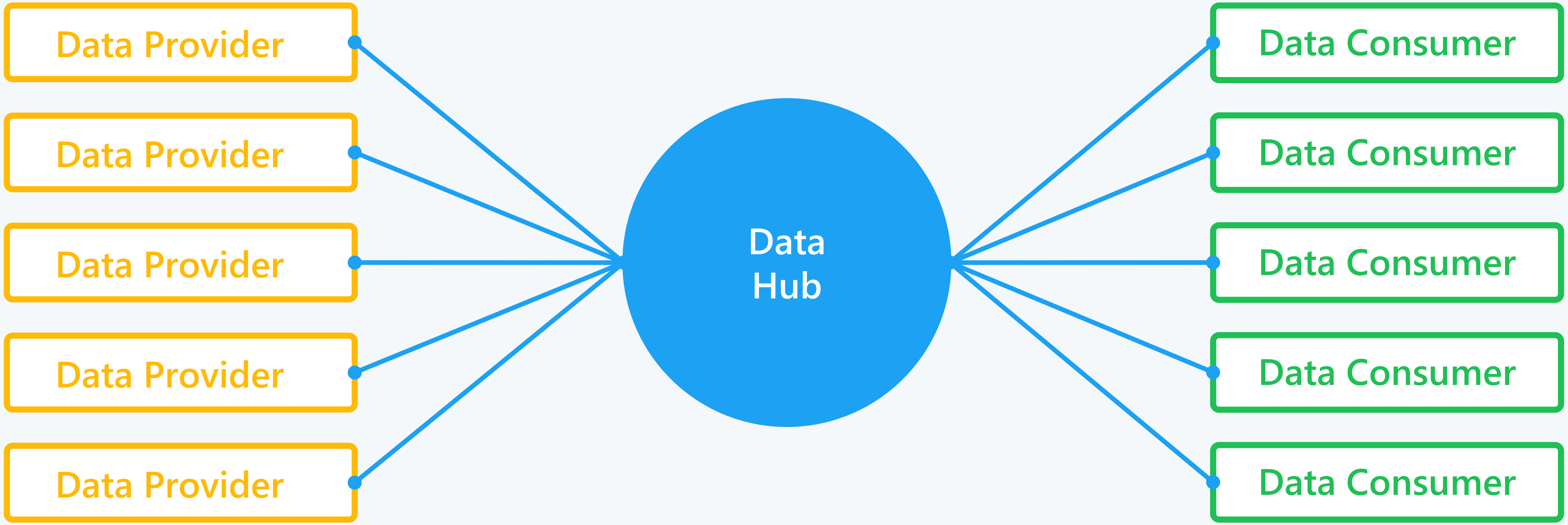
OOP 2019
München

Digital Ecosystems

Industrie 4.0
Smart Farming
Smart Energy
Smart Mobility
Smart Health
Smart Rural Areas
Smart Teams

Smart X

DATA HUBS / MARKETPLACE PLATFORMS

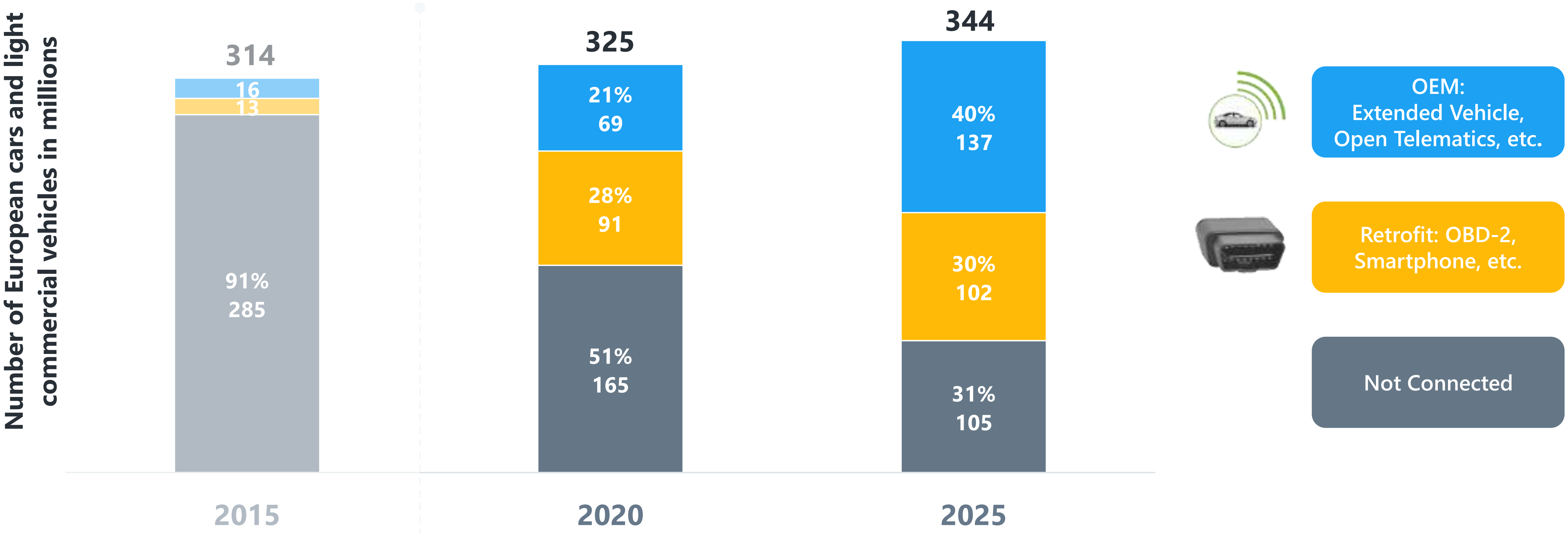


THE DATA PLATFORM CARUSO

CARUSO dataplace

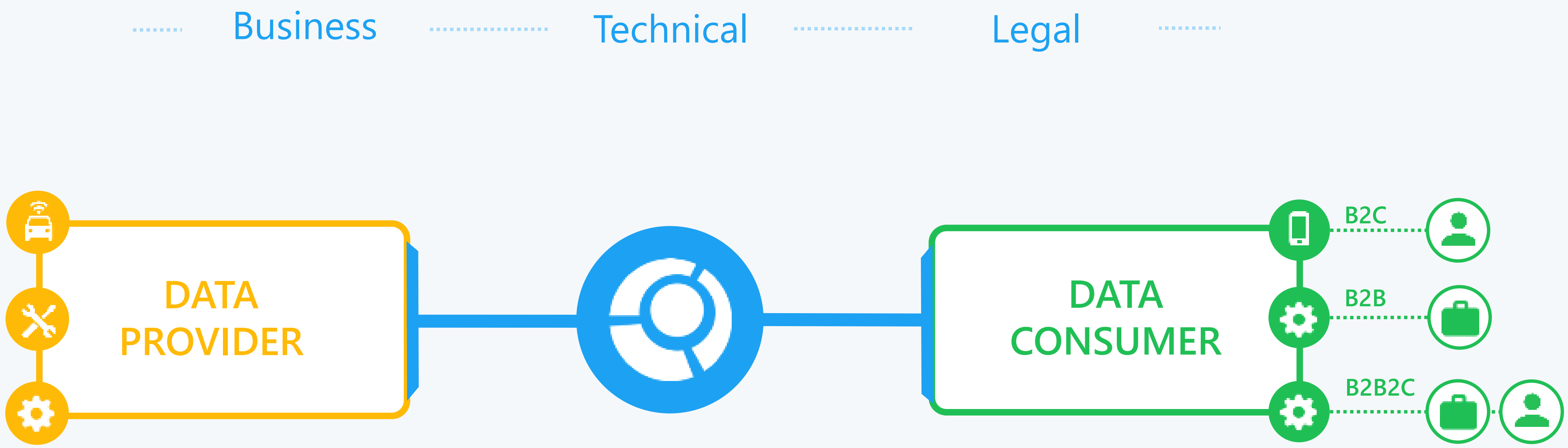
DEVELOPMENT OF CONNECTED VEHICLES IN EUROPE

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



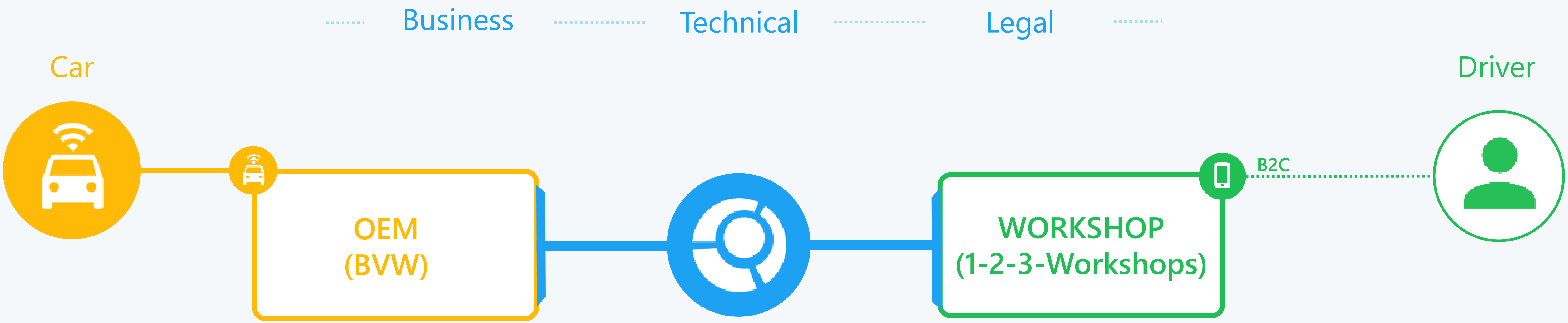
Source: IHS, LMD, Roland Berger

ECOSYSTEM WITH B2B MARKETPLACE PLATFORM



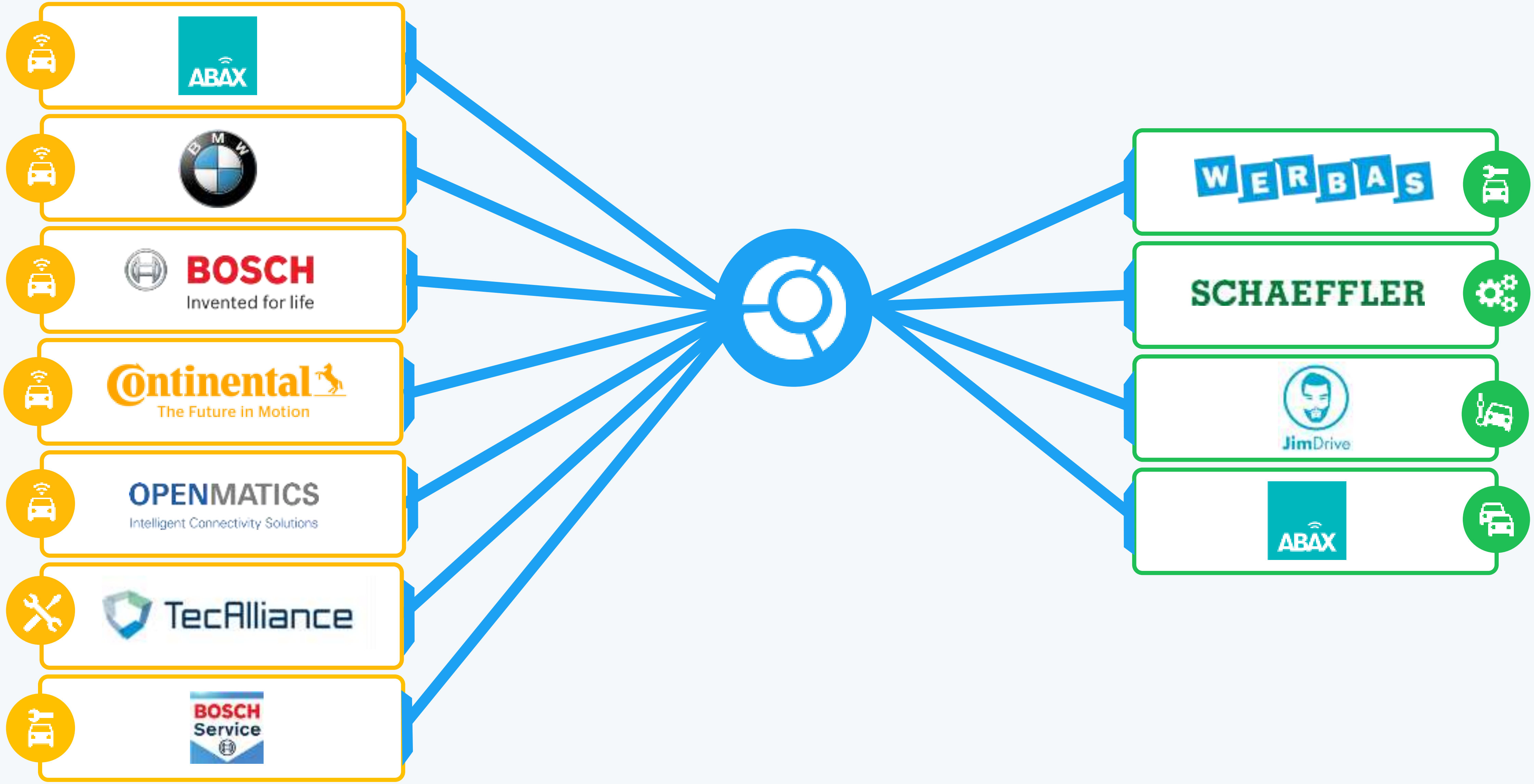
ECOSYSTEM WITH B2B MARKETPLACE PLATFORM

Example



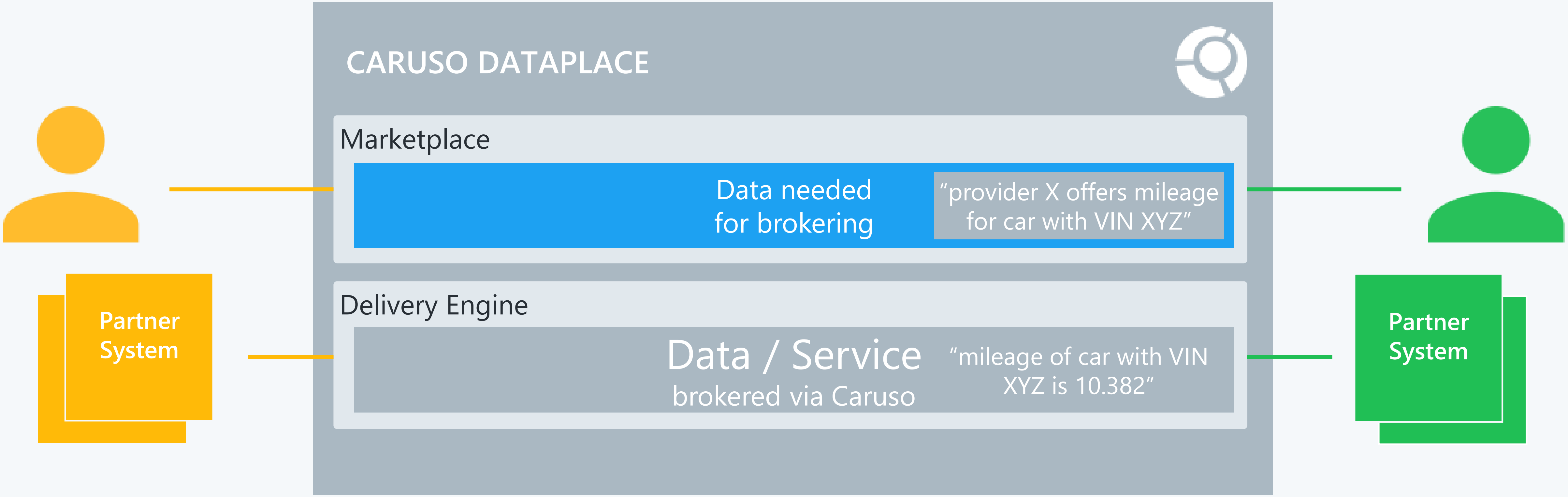
OUR INITIAL CONNECTED PARTNERS

DATA PROVIDER



DATA CONSUMER

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

Vehicle Position, Movement & Surroundings (65)

- Movement & Distances (12)
- Time, Position & Orientation (13)
- Trip Details (16)
- Driving Assist Data (10)
- Vehicle Surroundings Data (10)
- Vehicle Identification (4)

Vehicle Health & Maintenance (43)

- Maintenance (19)
- Malfunctions – DTC (11)
- Malfunctions – MIL (4)
- Malfunctions – Occurrence (9)

Vehicle Non-Powertrain Hardware (76)

- ABS, ESP & Traction Control (5)
- Airbags (4)
- Brakes (13)
- Doors, Windows & Locks (21)
- External Hardware (3)
- Heater & AC (9)
- Lights (5)
- Seatbelts (3)
- Tyres, Steering & Suspension (10)
- Wipers (3)

Vehicle Powertrain Resources (57)

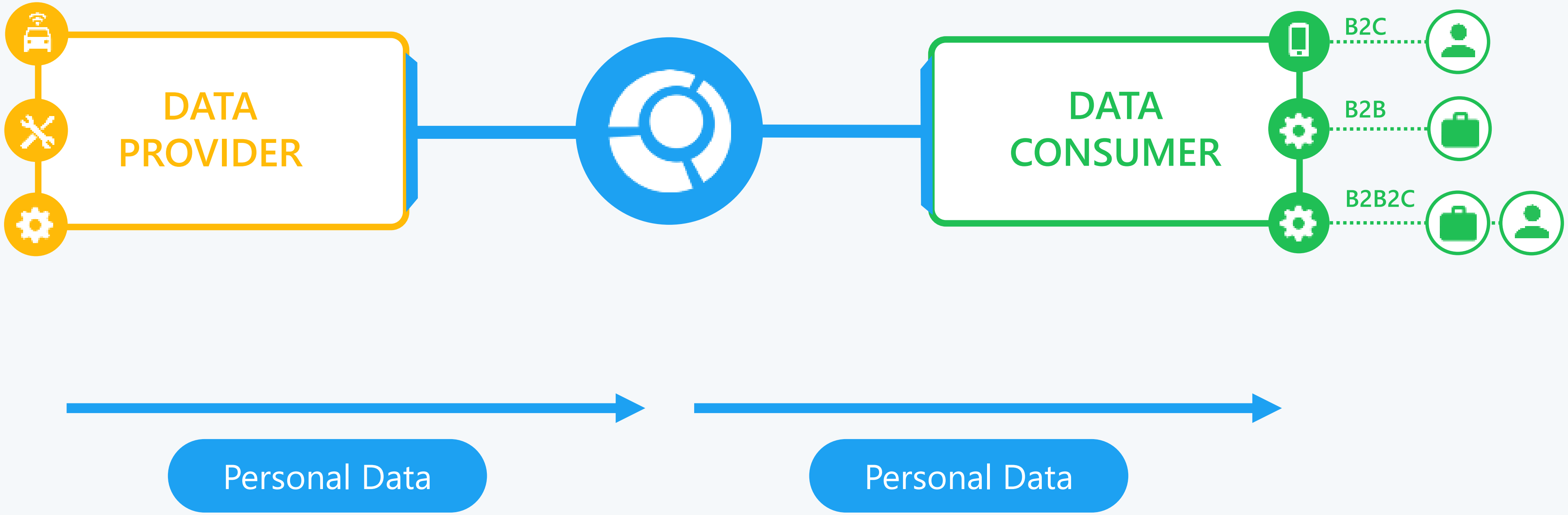
- Air (8)
- Coolant (8)
- Fuel – Consumption (10)
- Fuel – General (19)
- Oil (12)

Vehicle Powertrain Hardware (223)

- Combustion (30)
- Drive Battery (11)
- ECUs (31)
- Electric Vehicle Battery (30)
- Engine Status (16)
- Exhaust (39)
- Ignition (30)
- Particulate Filter (17)
- Transmission (19)

CARUSO dataplace Fraunhofer IESE

DELIVERY OF PERSONAL DATA



LAWFULNESS OF DATA PROCESSING

CARUSO'S REQUIREMENTS AND SOLUTION APPROACH

GDPR

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

PERSONAL DATA

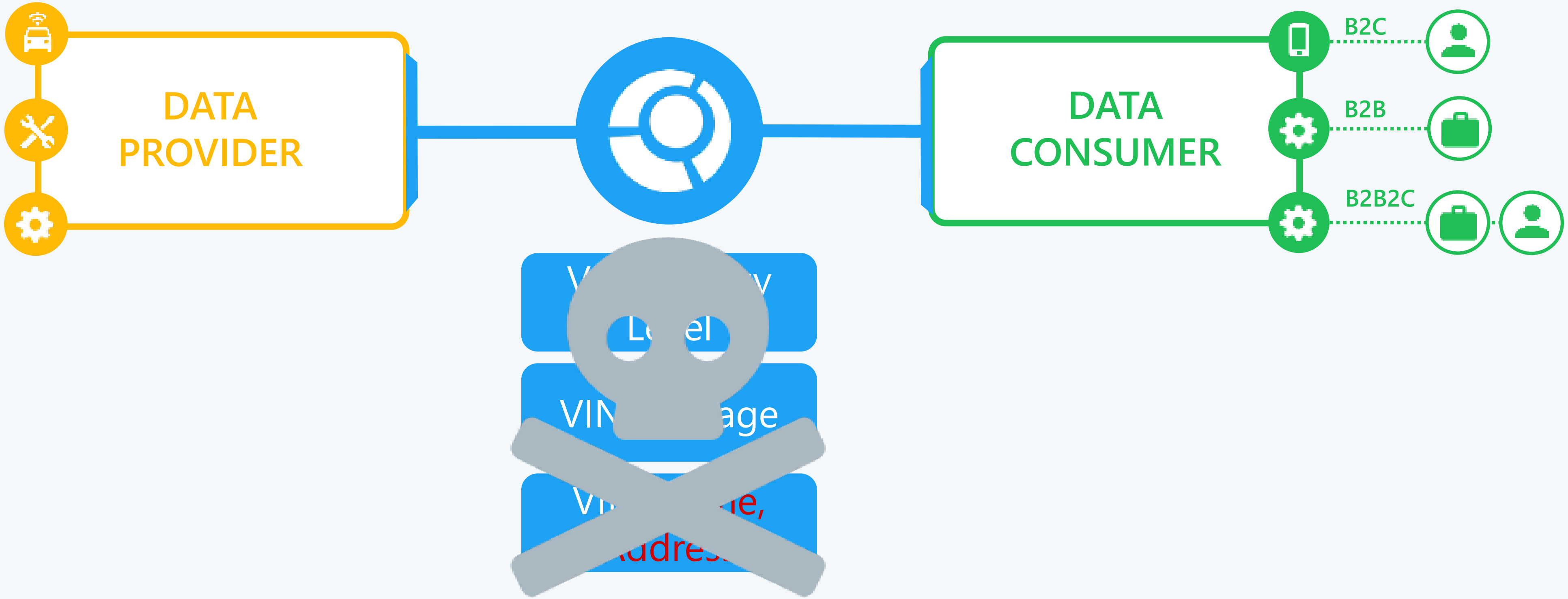
Any information relating to
an identified or identifiable natural person

GDPR Art. 4 No.1

PERSONAL DATA

Vehicle Identification Number (VIN)?

PERSONAL DATA CAN HARDLY BE PREVENTED



ENSURING LAWFULNESS OF DATA PROCESSING

CARUSO dataplace

LAWFULNESS OF PROCESSING

GDPR Art.6

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;

Consent

(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;

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.

Legitimate Interest

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

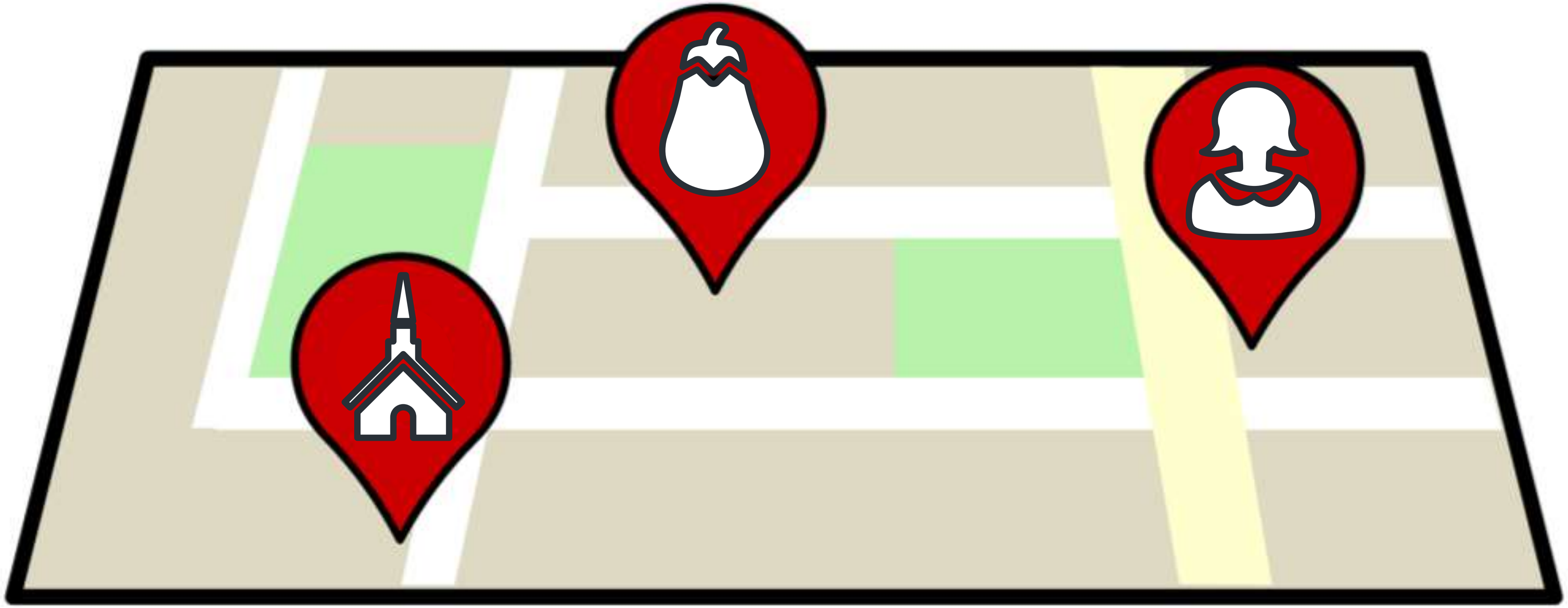
- Legitimate Interest
  - Low technical effort
  - Further from ExVeh standard
  - OEM & Neutral Server give responsibility to service provider
  - Feels “looser”
  - More difficult to understand
  - Legally sound, all involved parties covered
  - Higher risk of abuse and damage of image

→ 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.

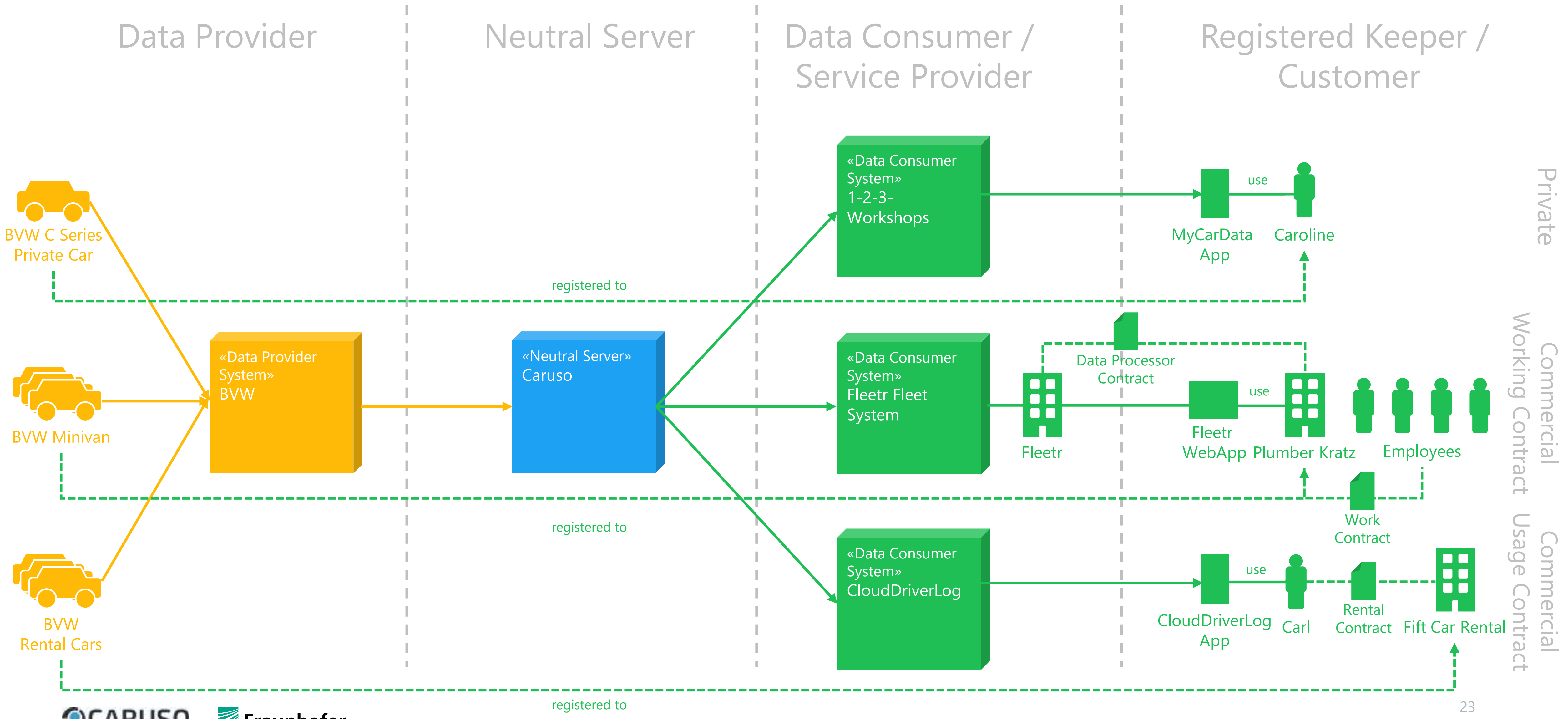
LOCATION DATA IS EVIL



CONSENT HANDLING

CARUSO dataplace

SETTINGS



Data Provider

Neutral Server

Data Consumer / Service Provider

Registered Keeper / Customer

BVW C Series Private Car

BVW Minivan

BVW Rental Cars

«Data Provider System» BVW

«Neutral Server» Caruso

«Data Consumer System» 1-2-3-Workshops

«Data Consumer System» Fleetr Fleet System

«Data Consumer System» CloudDriverLog

MyCarData App

use

Caroline

registered to

Fleetr

Data Processor Contract

Fleetr WebApp

use

Plumber Kratz

Employees

Work Contract

registered to

CloudDriverLog App

use

Carl

Rental Contract

Fift Car Rental

registered to

Private

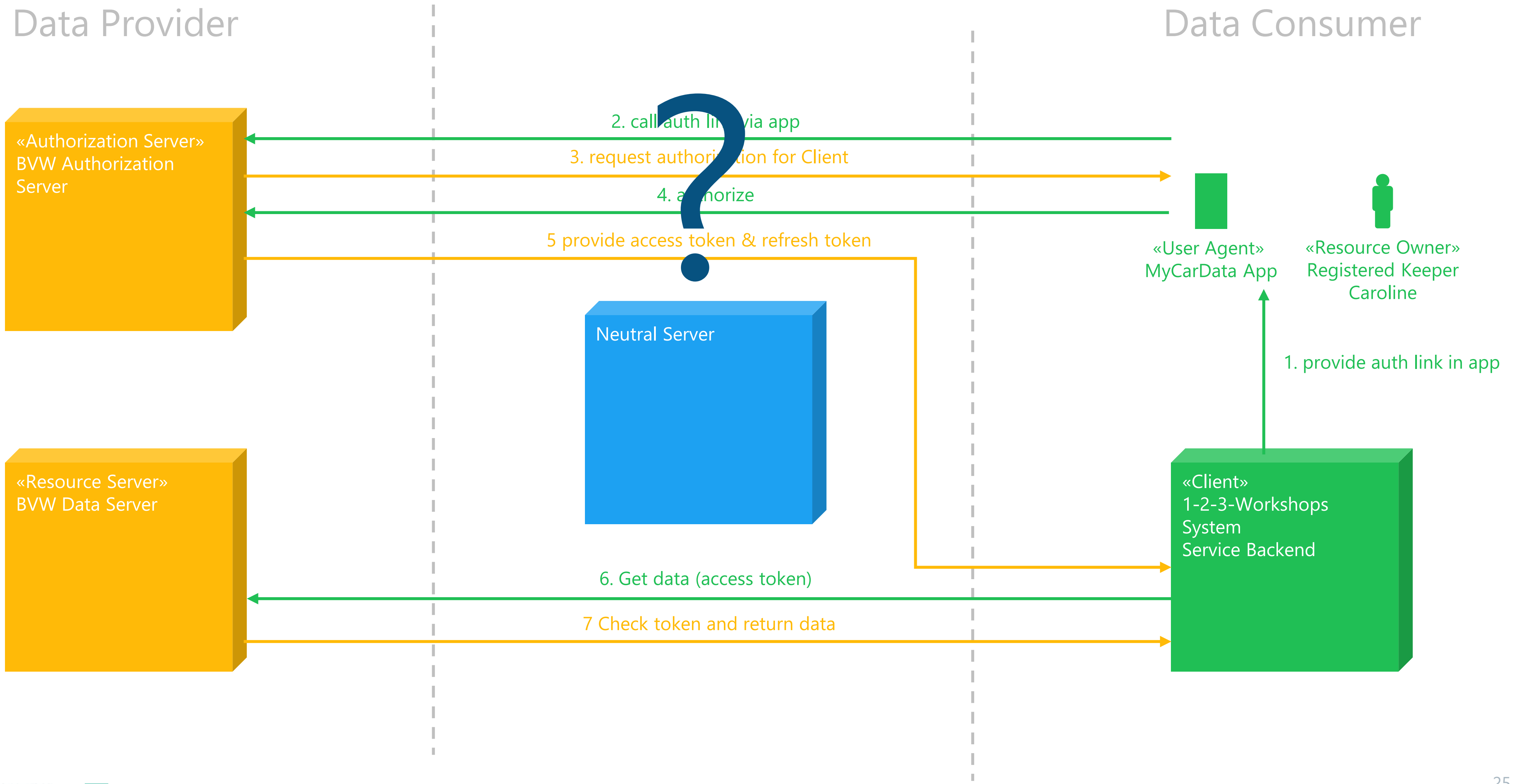
Commercial Working Contract

Commercial Usage Contract

REQUIREMENTS FOR CONSENT HANDLING

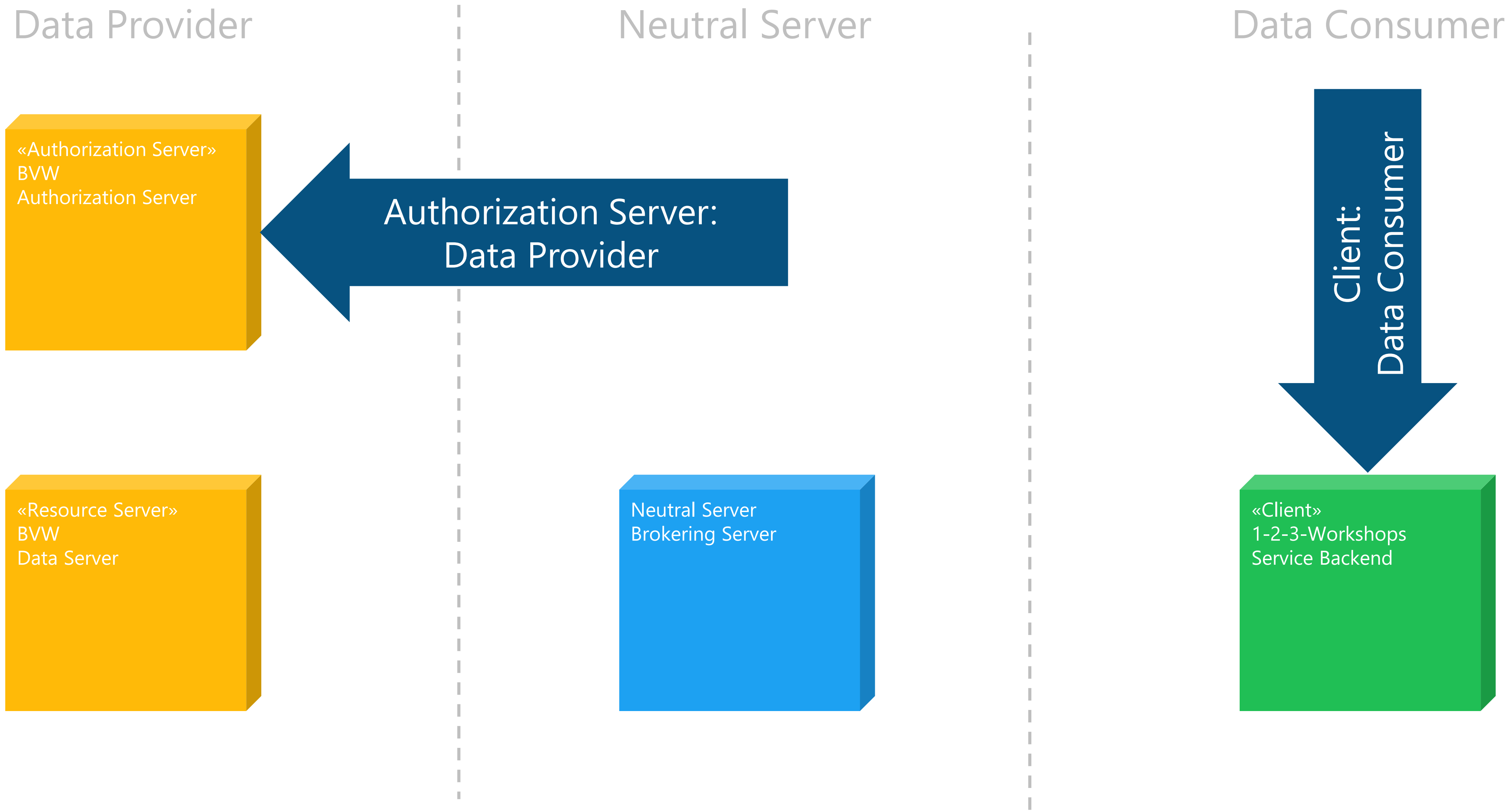
- The solution approach **must** fulfill the regulations of the GDPR
- The data consumer **must** not be required to interact with all data providers individually
- Involved parties **must** know and be able to store the message that users have been shown and to which they gave consent
- The data provider **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

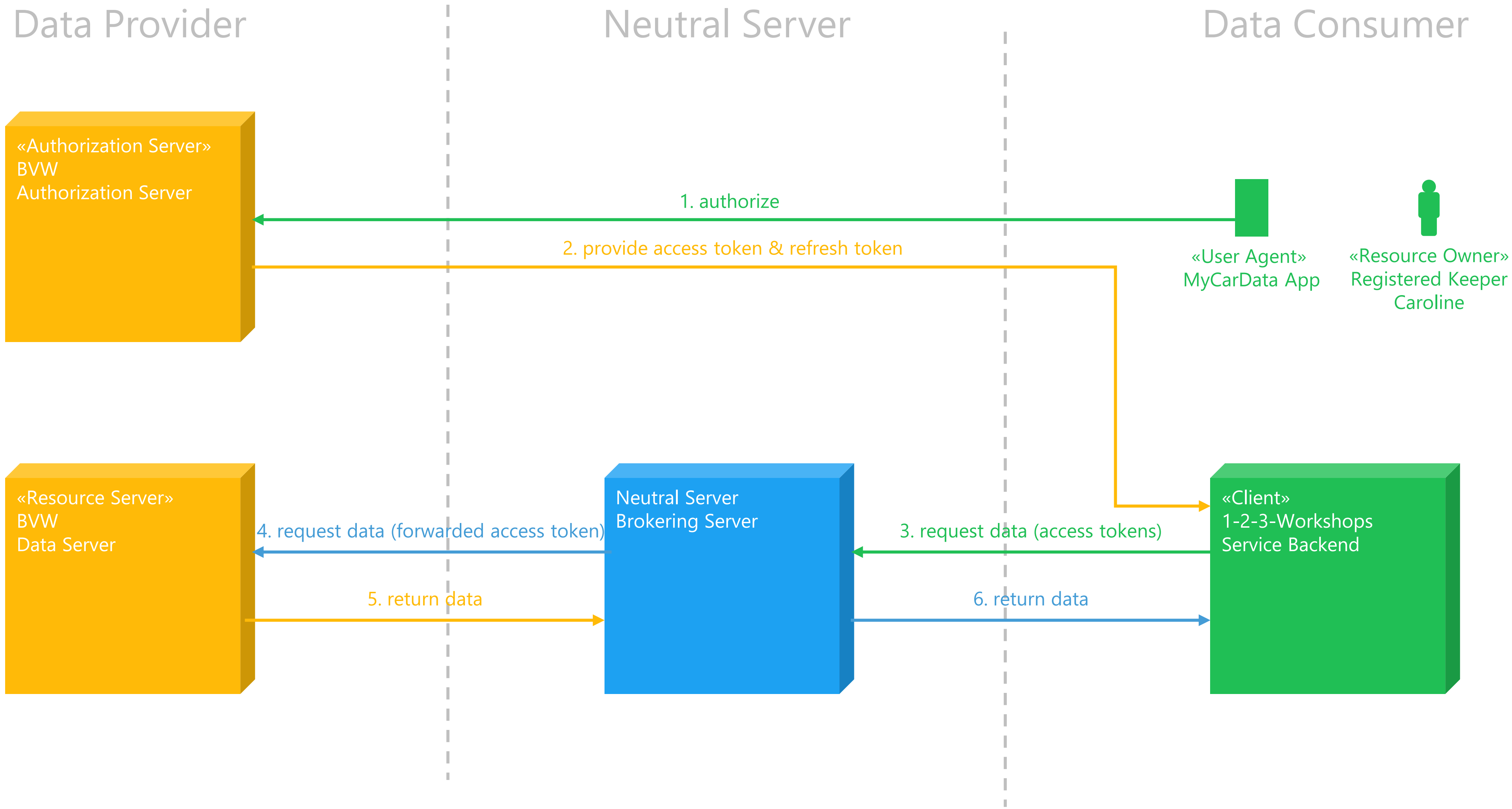


SOLUTION ALTERNATIVES

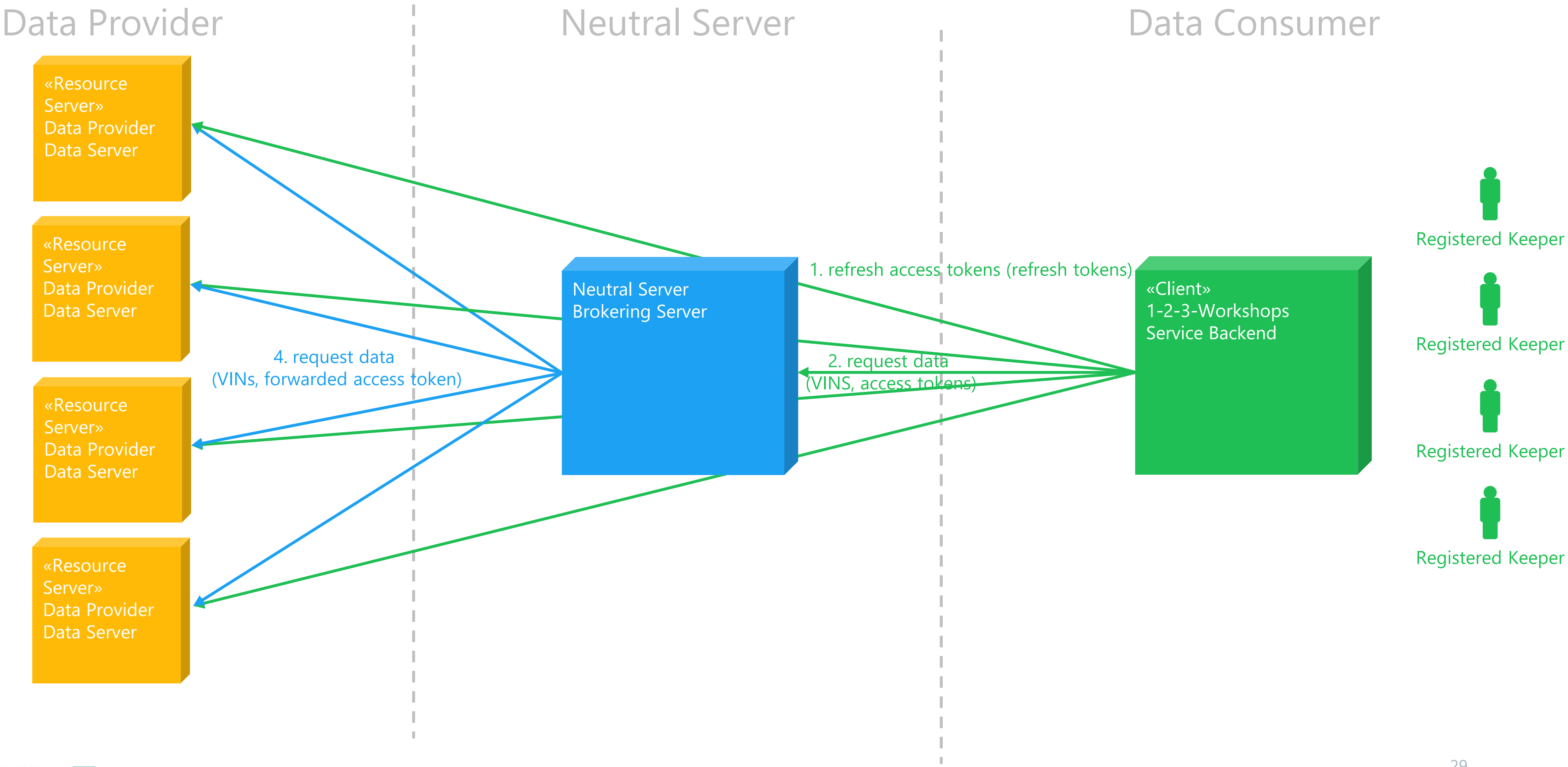
SOLUTION ALTERNATIVE 1



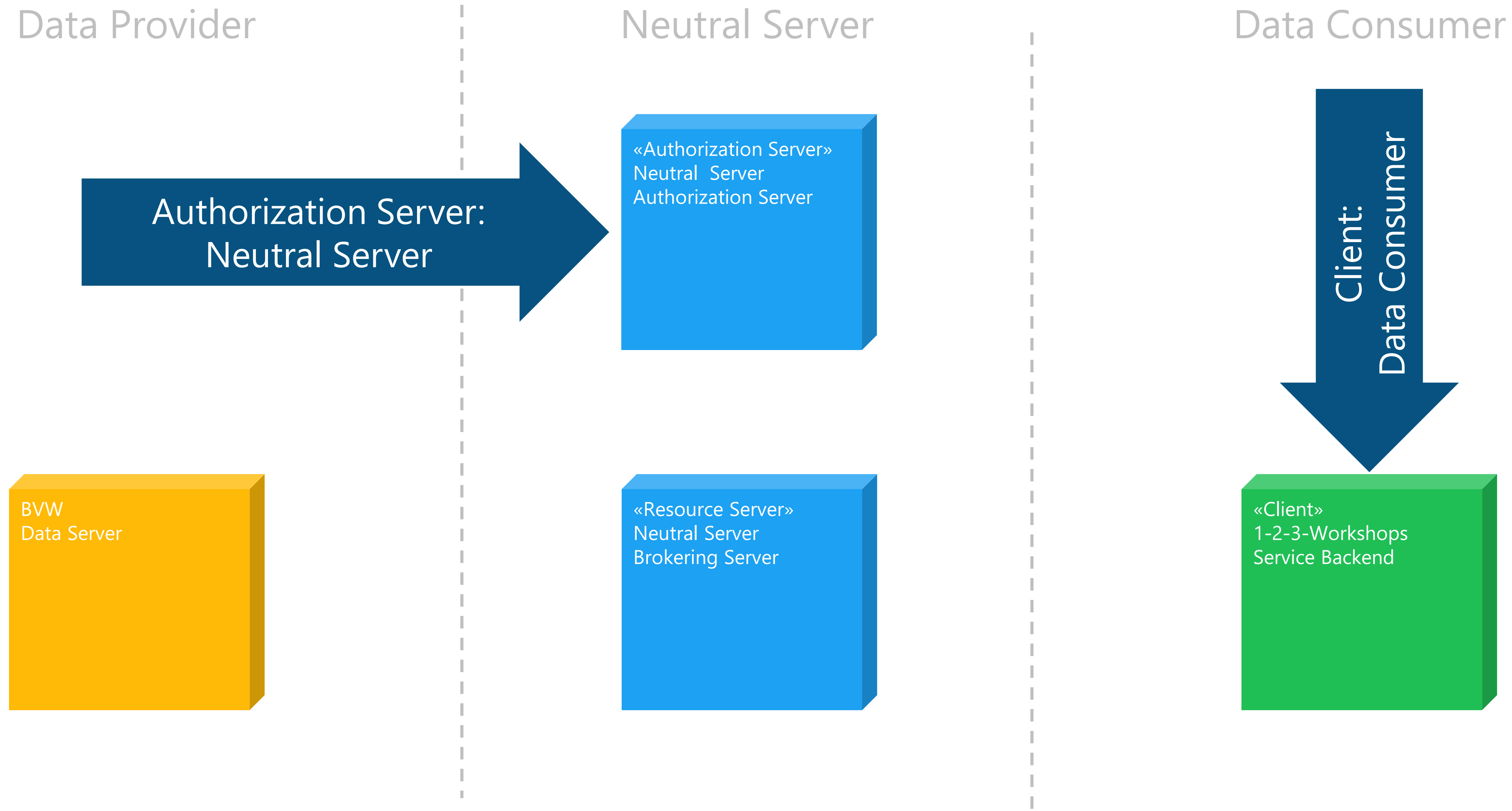
SOLUTION ALTERNATIVE 1



SOLUTION ALTERNATIVE 1


Data Provider
Neutral Server
Data Consumer
«Resource Server» Data Provider Data Server
«Resource Server» Data Provider Data Server
«Resource Server» Data Provider Data Server
«Resource Server» Data Provider Data Server
Neutral Server Brokering Server
«Client» 1-2-3-Workshops Service Backend
Registered Keeper
Registered Keeper
Registered Keeper
Registered Keeper
1. refresh access tokens (refresh tokens)
2. request data (VINS, access tokens)
4. request data (VINs, forwarded access token)

SOLUTION ALTERNATIVE 2



Data Provider

Neutral Server

Data Consumer

Authorization Server:
Neutral Server

«Authorization Server»
Neutral Server
Authorization Server

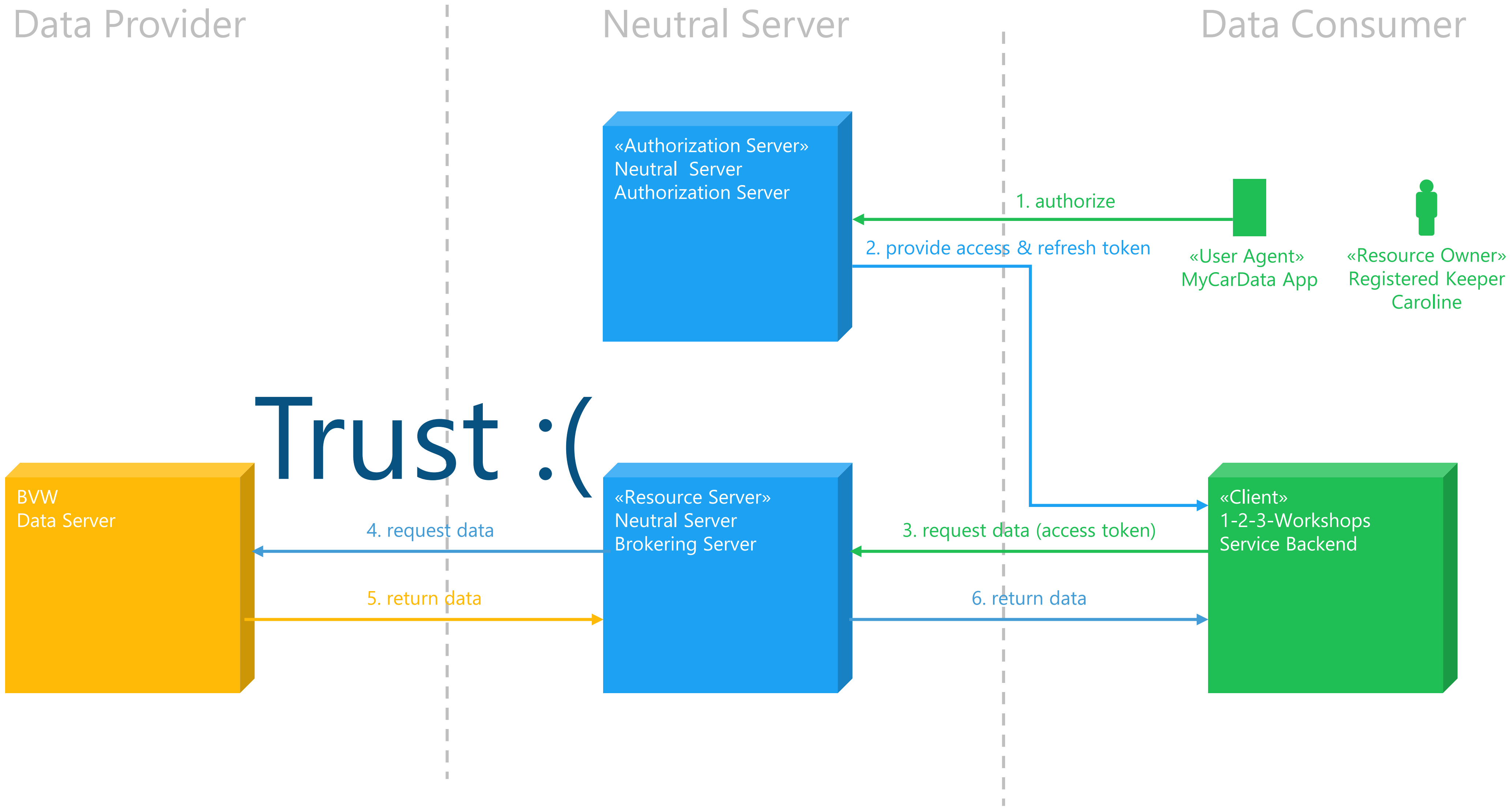
Client:
Data Consumer

BVW
Data Server

«Resource Server»
Neutral Server
Brokering Server

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

SOLUTION ALTERNATIVE 2



Data Provider

Neutral Server

Data Consumer

«Authorization Server»
Neutral Server
Authorization Server

1. authorize

2. provide access & refresh token

«User Agent»
MyCarData App

«Resource Owner»
Registered Keeper
Caroline

Trust :(

BVW
Data Server

4. request data

5. return data

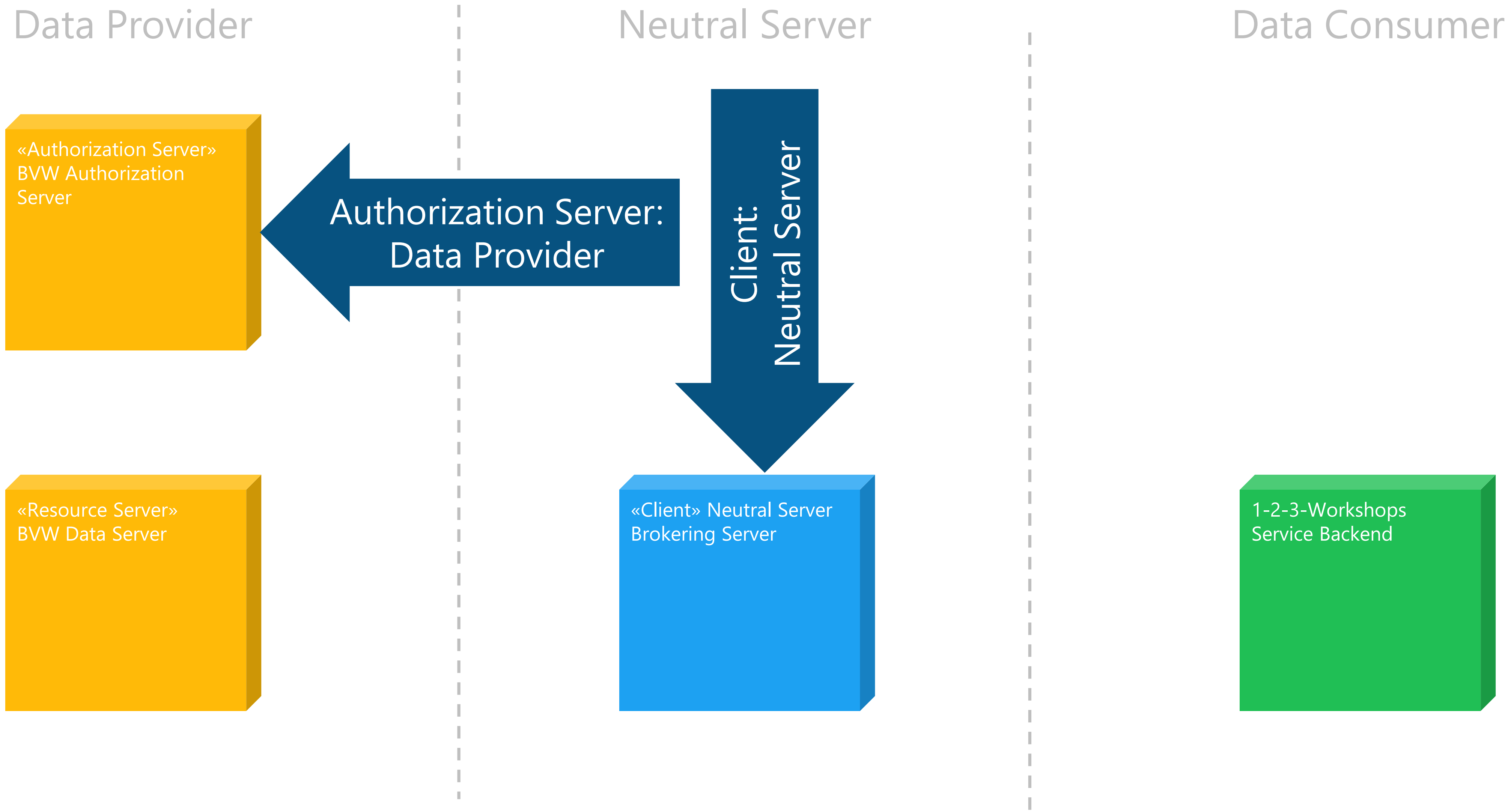
«Resource Server»
Neutral Server
Brokering Server

3. request data (access token)

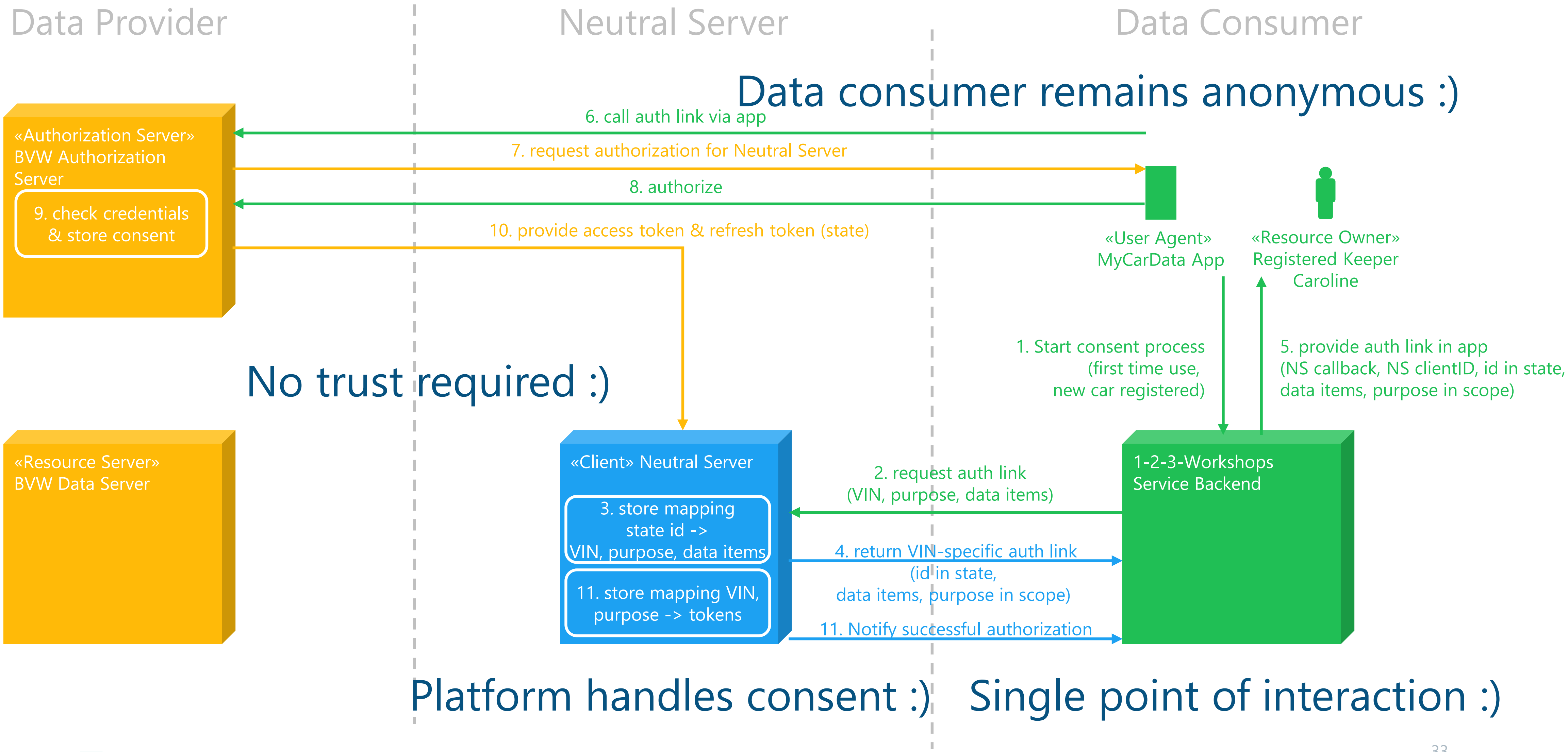
6. return data

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

SOLUTION ALTERNATIVE 3


Data Provider
Neutral Server
Data Consumer
«Authorization Server» BVW Authorization Server
Authorization Server: Data Provider
Client: Neutral Server
«Resource Server» BVW Data Server
«Client» Neutral Server Brokering Server
1-2-3-Workshops Service Backend

SOLUTION ALTERNATIVE 3: CONSENT PROVISIONING


Data Provider
Neutral Server
Data Consumer
6. call auth link via app
7. request authorization for Neutral Server
8. authorize
10. provide access token & refresh token (state)
«Authorization Server» BVW Authorization Server
9. check credentials & store consent
«User Agent» MyCarData App
«Resource Owner» Registered Keeper Caroline
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 Server» BVW Data Server
«Client» Neutral Server
3. store mapping state id -> VIN, purpose, data items
11. store mapping VIN, purpose -> tokens
2. request auth link (VIN, purpose, data items)
4. return VIN-specific auth link (id in state, data items, purpose in scope)
11. Notify successful authorization
1-2-3-Workshops Service Backend

Data consumer remains anonymous :)

No trust required :)

Platform handles consent :)

Single point of interaction :)

OTHER SOLUTION APPROACHES

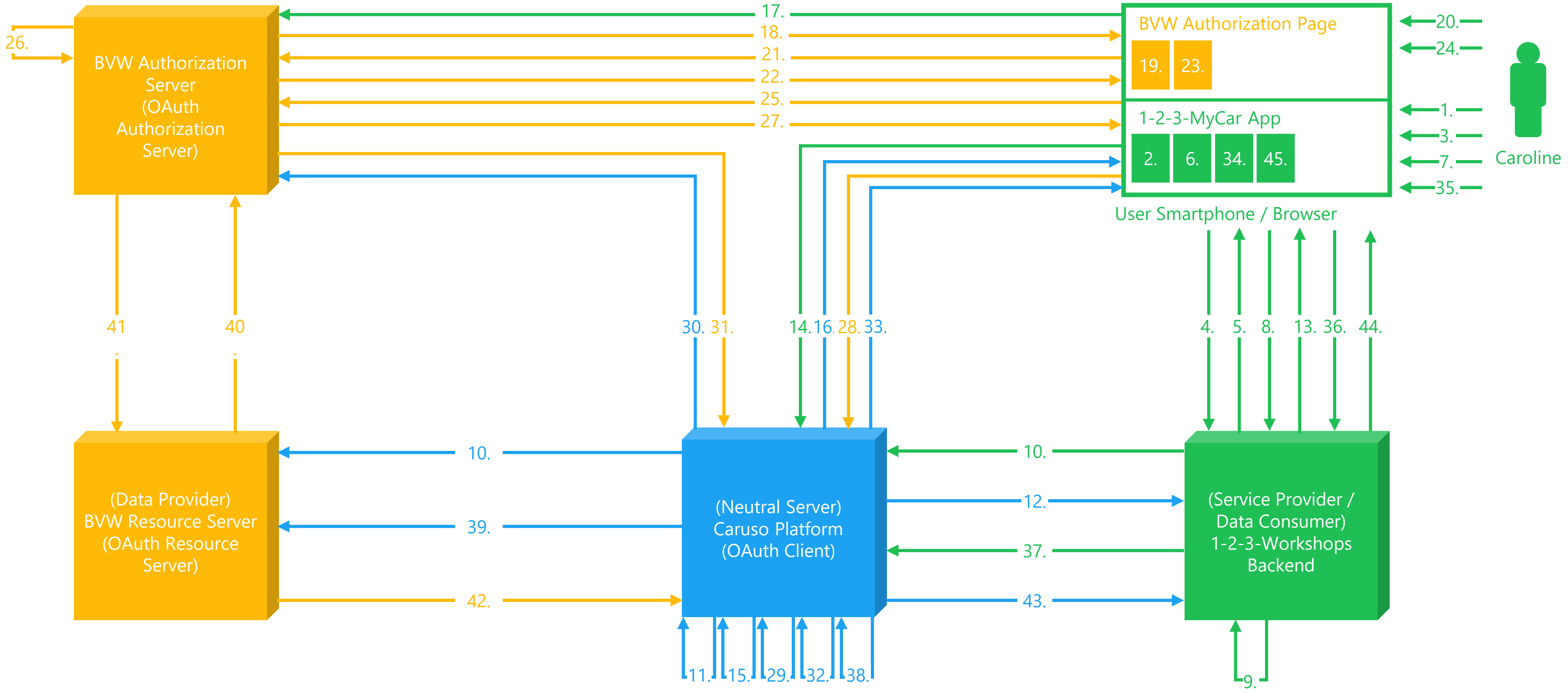
- Caruso as central consent management hub with custom-built consent mechanism
  - Trust from all parties towards Caruso required
  - Implementation of security technology necessary
- Utilization of Blockchain technology
  - Either identities and provided consent information accessible
  - Or trust toward Caruso required

LAWFULNESS DATA PROCESSING

TECHNICAL REALIZATION

CARUSO dataplace

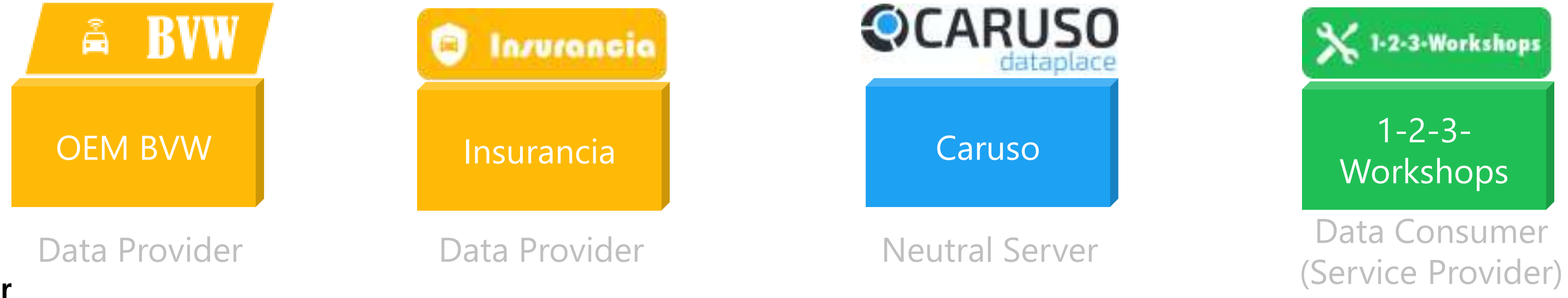
CONSENT: POC – WHAT HAPPENS BEHIND THE SCENES



BVW Authorization Server (OAuth Authorization Server)
26.
17.
18.
21.
22.
25.
27.
BVW Authorization Page
19.
23.
1-2-3-MyCar App
2.
6.
34.
45.
User Smartphone / Browser
20.
24.
1.
3.
7.
35.
Caroline
41
40
30.
31.
14.
16.
28.
33.
4.
5.
8.
13.
36.
44.
(Data Provider) BVW Resource Server (OAuth Resource Server)
10.
39.
42.
(Neutral Server) Caruso Platform (OAuth Client)
10.
12.
37.
43.
(Service Provider / Data Consumer) 1-2-3-Workshops Backend
11.
15.
29.
32.
38.
9.

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“



OEM BVW

Data Provider

Insurancia

Data Provider

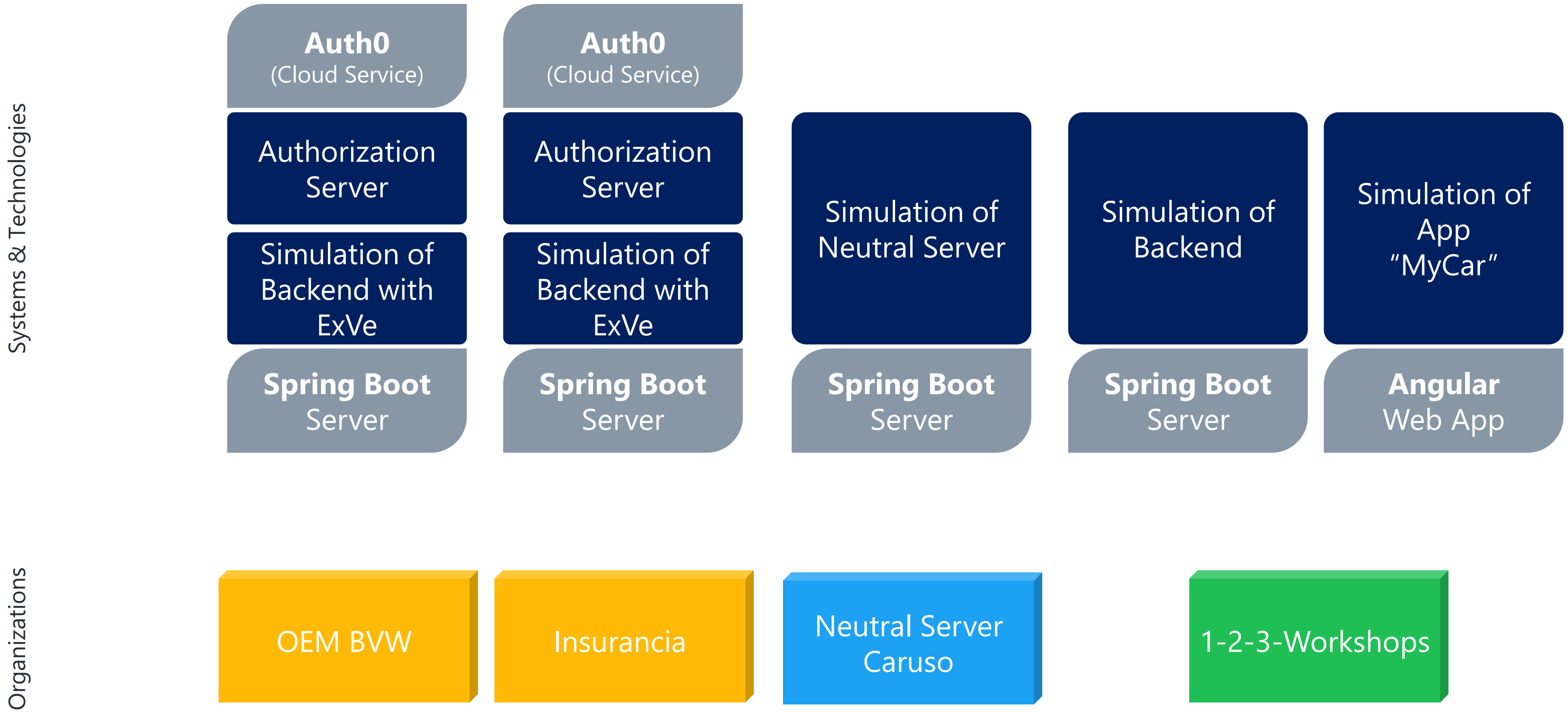
Caruso

Neutral Server

1-2-3-Workshops

Data Consumer (Service Provider)

POC – TECHNOLOGIES IN USE



Systems & Technologies

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

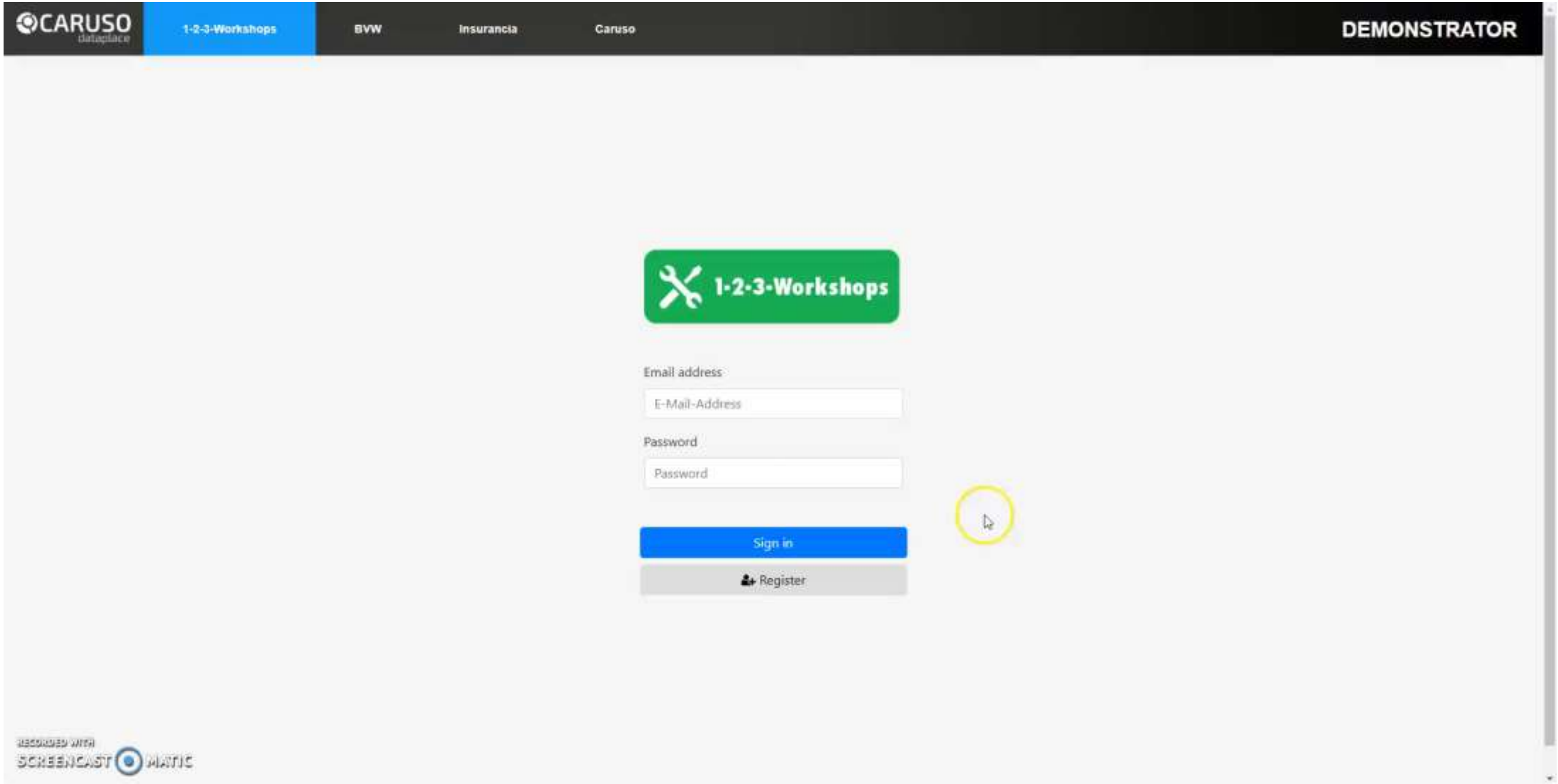
Neutral Server Caruso

1-2-3-Workshops

CARUSO dataplace

Fraunhofer IESE

POC – SCREENCAST



Email address

E-Mail-Address

Password

Password

POC – WHO KNOWS WHAT ABOUT CONSENT?

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 consent:
- 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“

Organizations

Insurancia

OEM BVW

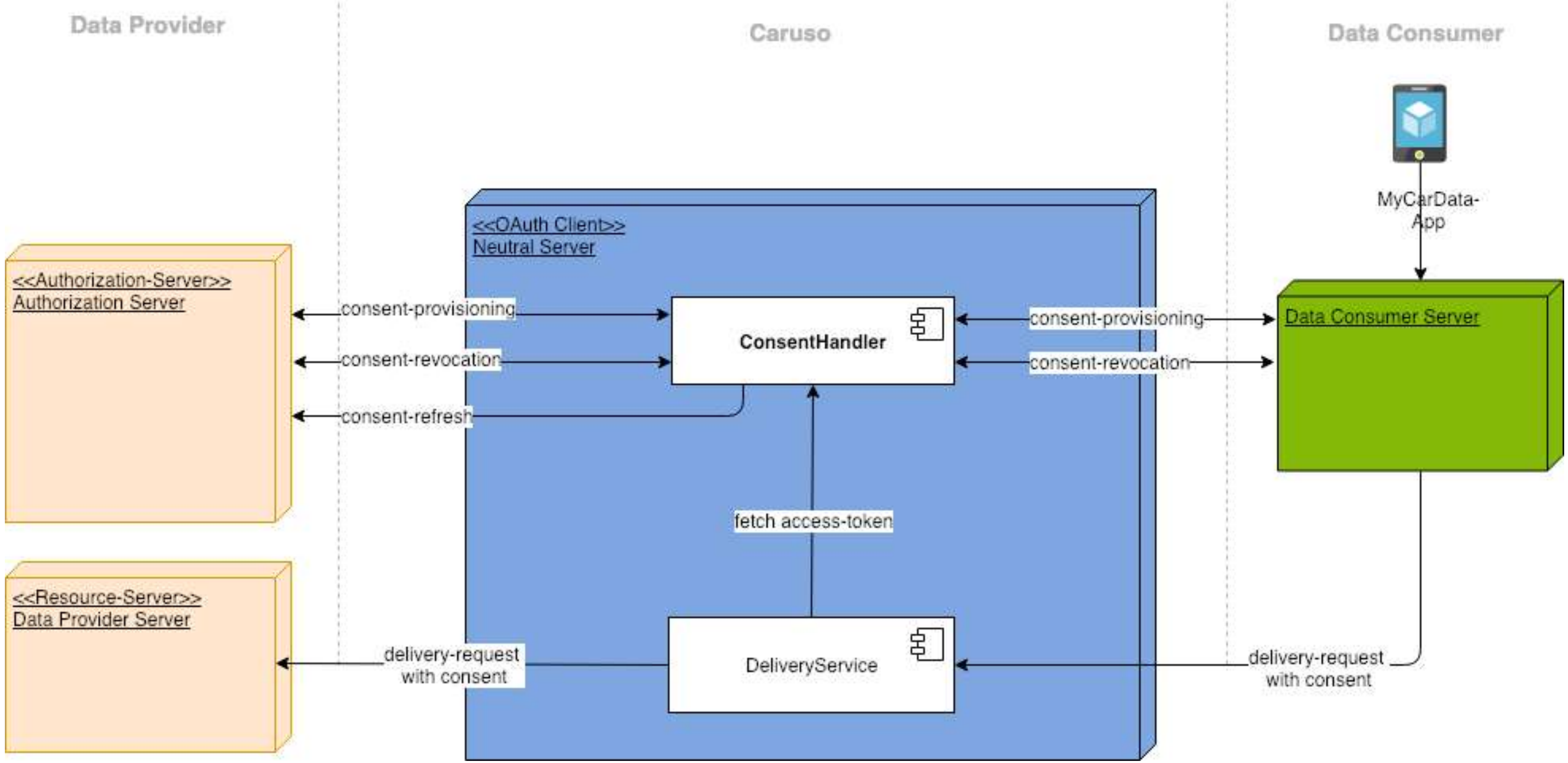
Neutral Server Caruso

1-2-3-Workshops

CARUSO dataplace

Fraunhofer IESE

INTEGRATION INTO THE PLATFORM



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/