CARUSO dataplace

PERSONAL DATA PROCESSING

DETAILS ON CONSENT HANDLING

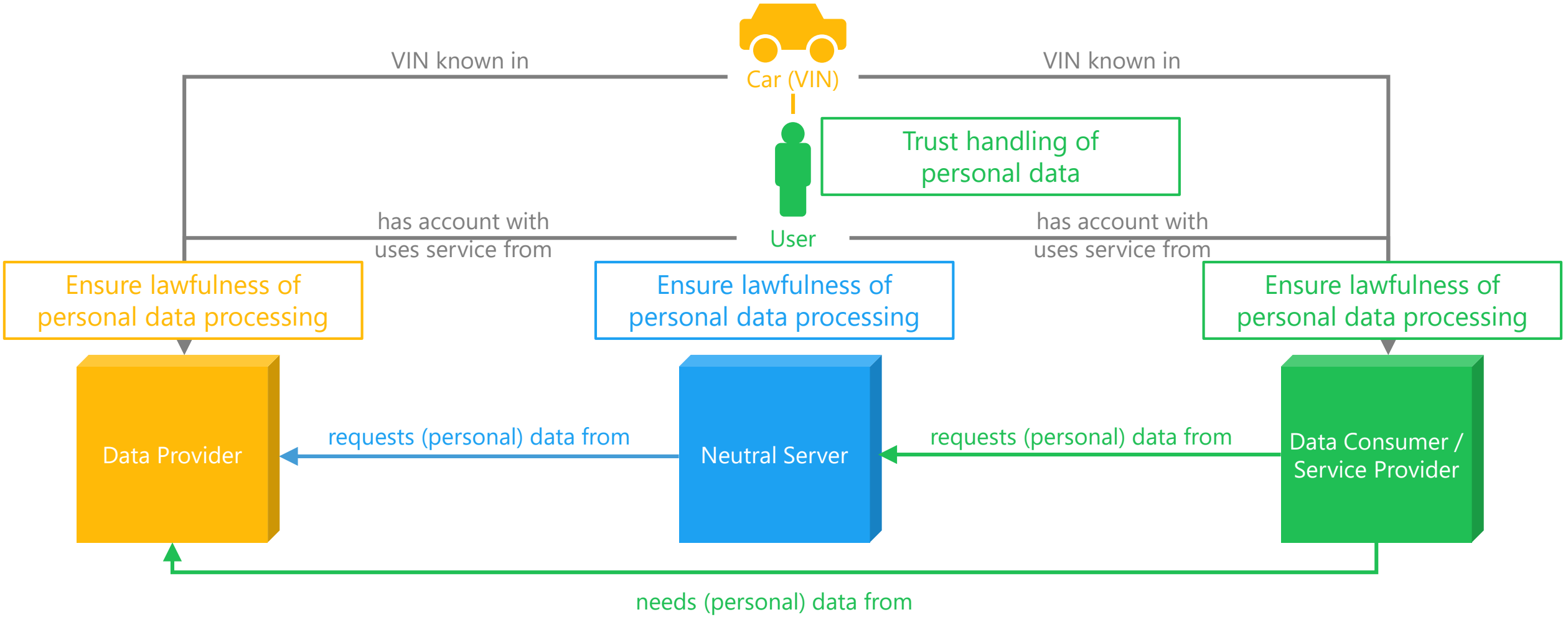
DOMINIK ROST, ULRICH KEIL

W3C, JUNE 14, 2018

KEY MESSAGES

- Groundwork: Analysis of multiple options for lawfulness of data processing via neutral server
- Caruso has a concept for consent handling via a neutral server
  - Neutral server plays a central role in facilitating the consent handling concept
  - The infrastructure concept has to be made public to be of real use
- Caruso / Fraunhofer have shown the viability of the consent handling concept with a PoC
  - Demonstration capabilities with video and very detailed explanation of technical solution
- Key requirements for consent handling the proposal fulfills:
  - Consent handling is compliant with current ideas of ExVe standard
  - Data providers don’t have to interact directly with data consumers / service providers
  - Consent handling is simple for Data consumers (only interaction with Neutral server)
  - Data providers do not have to trust the other parties, they get real consent from the User
  - Using standard security technology: based on OAuth technology
- We are currently assessing further options for lawful data processing (focus consent handling) with advantages and disadvantages

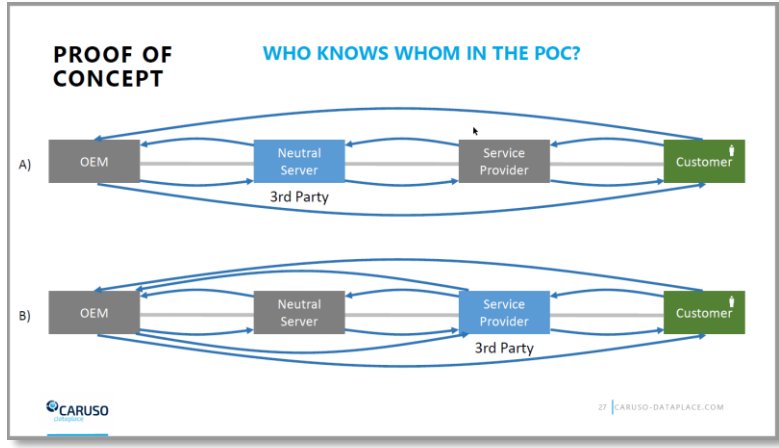
GENERAL SETTING – REQUIRED LAWFULNESS OF PERSONAL DATA PROCESSING

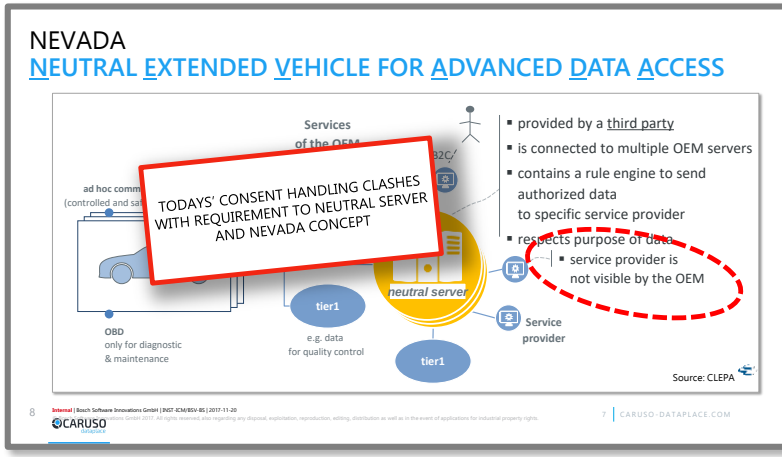


CARUSO dataplace

SHORTCOMINGS OF EXVE FOR PERSONAL DATA PROCESSING

- Neutral Server concept not covered in ExVe
  - Not clear how to realize ExVe with Neutral Server
- Different options shown by Fraunhofer in 03/2017
  - B) Service Provider as "3rd Party"
    - OEM has to know Service Provider
    - Service Provider has to maintain individual relationships with all OEMs
  - A) Neutral Server as "3rd Party"
    - Not clear how it could be realized
    - March 2018: Caruso / Fraunhofer worked on solution concept
    - Which solutions are possible and what are the implications?
    - What is the delta to the ExVe standard?





Data Provider

Neutral Server

Data Consumer / Service Provider

LAWFULNESS OF PERSONAL DATA PROCESSING

Two feasible options for ensuring lawfulness of personal data processing (GDPR)

by Consent

vs.

by Contract / Balancing of Interest (BoI)

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

- Contract/Balancing of 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

LAWFULNESS OF DATA PROCESSING BY CONSENT

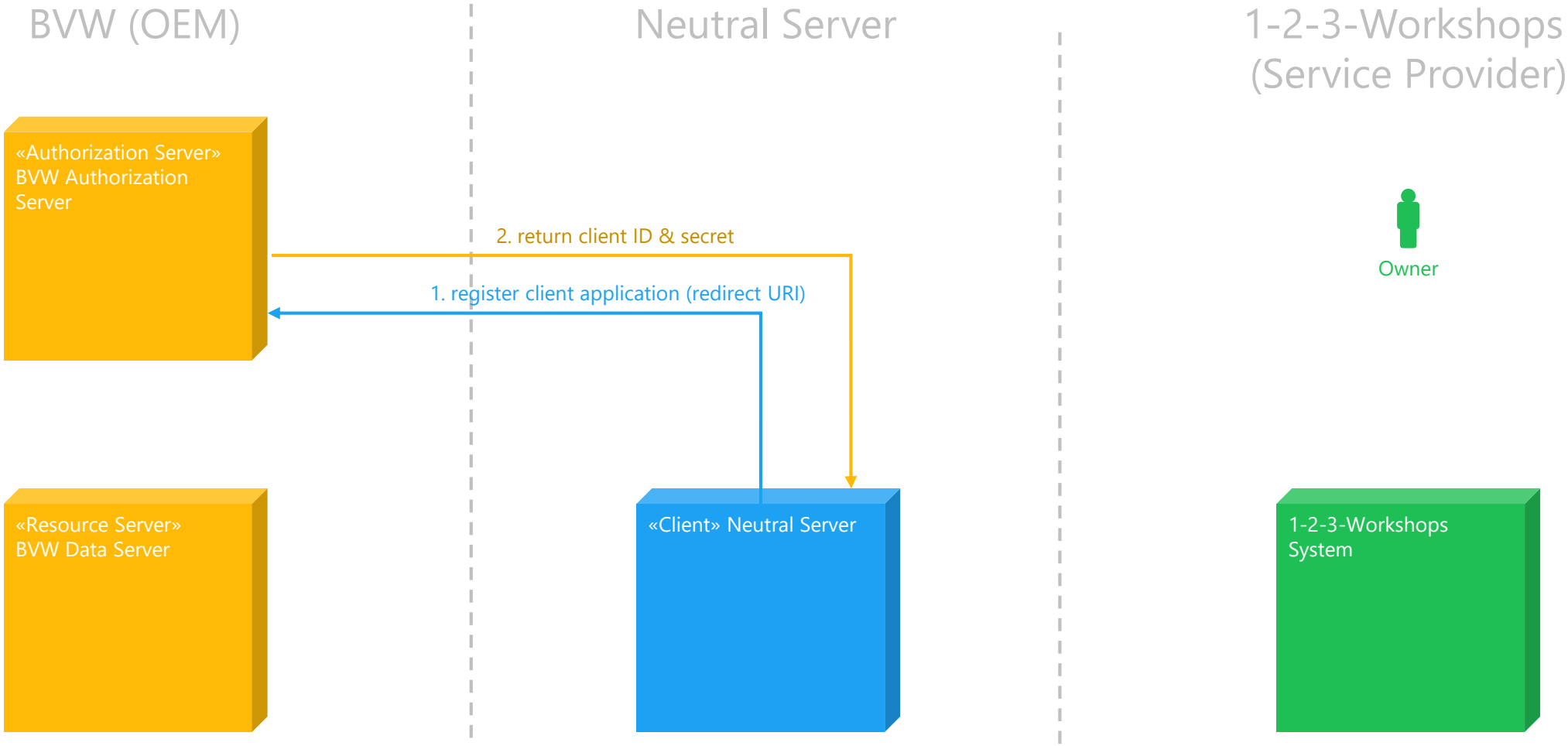
REQUIREMENTS FOR CONSENT HANDLING

- Data provider **must not** see the identity of service providers
- Data consumer **must not** be required to directly interact with all OEMs separately (e.g. for registration or for authorization)
- Car ownership **must** be ensured via identity management before delivering data
- Data provider **should** not have to trust a third party unconditionally
- Building a custom security solution **should** be avoided, if possible
- ExVeh standard **should** be adhered to
- The consent data **could** be stored centrally, not distributed across all OEMs
- Caruso **could** not be visible to end user / driver

SOLUTION APPROACHES OVERVIEW

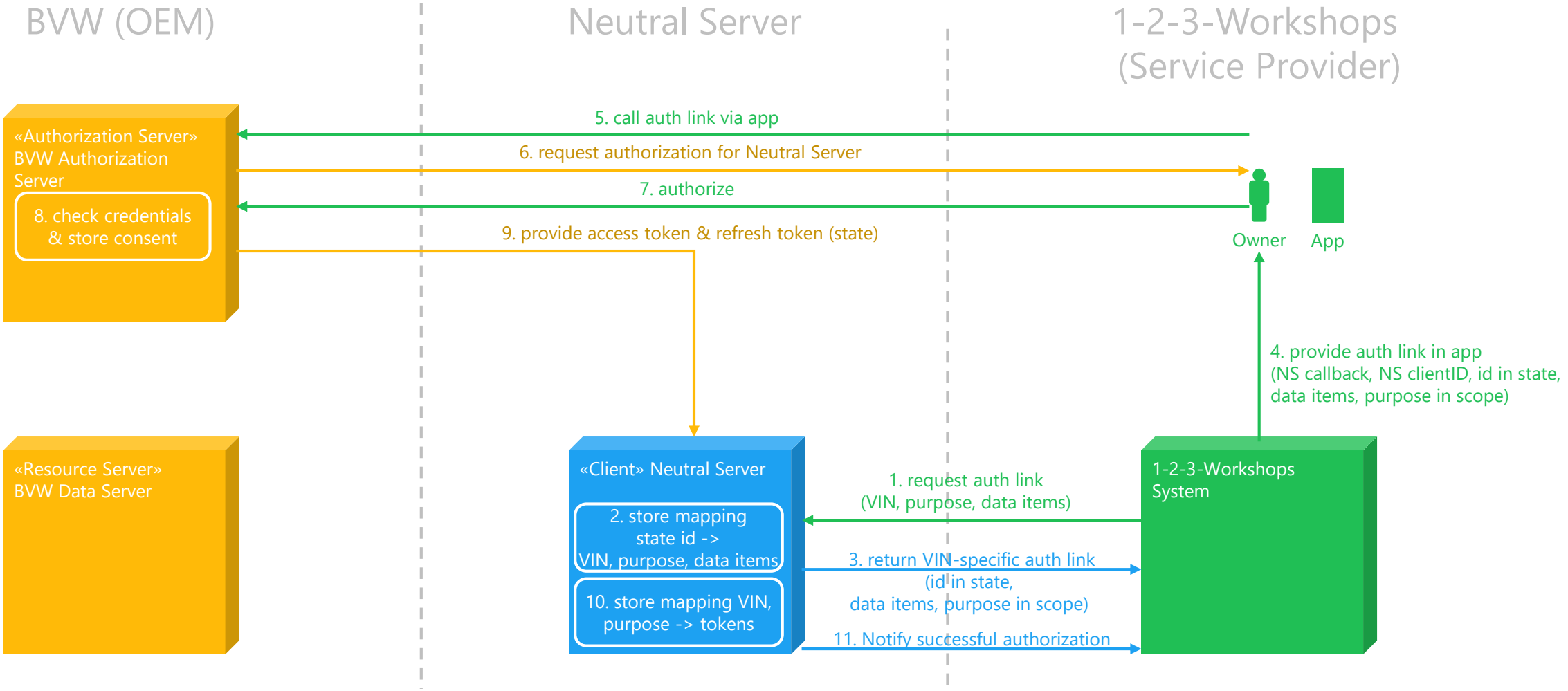
	Data provider must not see the identity of service providers	Data consumer must not be required to directly interact with all OEMs separately	Car ownership must be ensured via identity management before delivering data	Data providers should not have to trust a third party unconditionally	Building a custom security solution should be avoided, if possible	ExVeh standard should be adhered to	The consent data could be stored centrally, not distributed across all OEMs	Caruso could not be visible to end user / driver
SA.I: OAuth – OEM authorization, Service Provider client	✗	✗	✓	✓	✓	✓	✗	✓
SA.II: OAuth – Neutral Server authorization, Service Provider client	✓	✓	✓	✗	✓	✗	✓	✗
SA.III: OAuth – OEM authorization, Neutral Server client	✓	✓	✓	✓	✓	(✓)	✗	✗
SA.IV: Custom – Neutral Server authorization, consent passing	✓	✓	✓	✗	✗	✗	✓	✓

SA.III: OAUTH – OEM AUTHORIZATION, NEUTRAL SERVER CLIENT – CLIENT REGISTRATION



CARUSO dataplace

SA.III: OAUTH – OEM AUTHORIZATION, NEUTRAL SERVER CLIENT – CONSENT PROVISIONING



OEM realizes authorization server, Owner gives consent to OEM
Neutral Server acts as client and handles token management

SA.III: OAUTH – OEM AUTHORIZATION, CLIENT – CONSENT PROVISIONING

Given Consent as stored by OEM:
- Client „Neutral Server“
- Has the consent to retrieve the data items „mileage, …“
- For the car with VIN „1NXBU40E29Z075221“
- For the purpose of „Car Status Information“
- Given by „Owner“
- Given at „01.03.2018“

Neutral Server

Owner sees consent:
- Client „Neutral Server“
- Has the consent to retrieve the data items “mileage, …”
- From the Data provider „BVW“
- For the car with VIN „1NXBU40E29Z075221“
- For the purpose of „Car Status Information“

5. call auth link via app

6. request authorization for Neutral Server

«Authorization Server»
BVW Authorization Server

8. check credentials & store consent

2.: Neutral server stores consent request
- Client „Neutral Server“
- Has the consent to retrieve the data items “mileage, … “
- From the data provider „BVW“
- For the car with VIN „1NXBU40E29Z075221“
- For the purpose of „Car Status Information“

2.: Store state -> VIN, purpose mapping

8.: Receive tokens, store
- Consent given at „01.03.2018“
- VIN, purpose -> access token mapping

Owner sees and provides consent → OK

Owner

Gets consent directly from owner → OK!

4. 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

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

mapping VIN, tokens

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

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

11. Notify successful authorization

1-2-3-Workshops System

Notified about success | Has the contract with the owner → OK!

Notified about success with access token | has full insight into consent → OK

OEM realizes authori… Owner gives consent …
Neutral Server acts as client and handles token manager…

1.: Service Provider requests consent:
- Needs the consent to retrieve the data items “mileage, … “
- (From the data provider „BVW“)
- For the car with VIN „1NXBU40E29Z075221“
- For the purpose of „Car Status Information“

- 10.: Consent given at „01.03.2018“

CARUSO dataplace

CONSENT - POC

CONSENT: POC – BACKGROUND, ORGANIZATIONS, AND SYSTEMS

- BVW has a connectivity solution for the user's car
- BVW acts as a data provider
- BVW provides the in-vehicle data via an ExVe-compliant API
- BVW can provide the in-vehicle data "mileage" and "DTC"

- Caruso acts as neutral server
- Caruso manages partners and their contracts
- Caruso brokers the data between data providers and data consumers

- 1-2-3-Workshops acts as a workshop service provider and offers to its customers the app "MyCar"
- 1-2-3-Workshops is a data consumer and consumes "mileage" and "DTC" data

- The user owns a connected car from the OEM BVW
- The user is customer of 1-2-3-Workshops and uses their app
- The user can view the in-vehicle data "mileage" and "DTC" in the "MyCar" app

Systems

BVW Authorization Server

BVW Backend with ExVe

Caruso Neutral Server Backend

1-2-3-Workshops Backend

1-2-3-Workshops App "MyCar"

Consumed data: DTC, Mileage

Organizations

BVW

OEM BVW

Data Provider

CARUSO dataplace

Neutral Server Caruso

Neutral Server

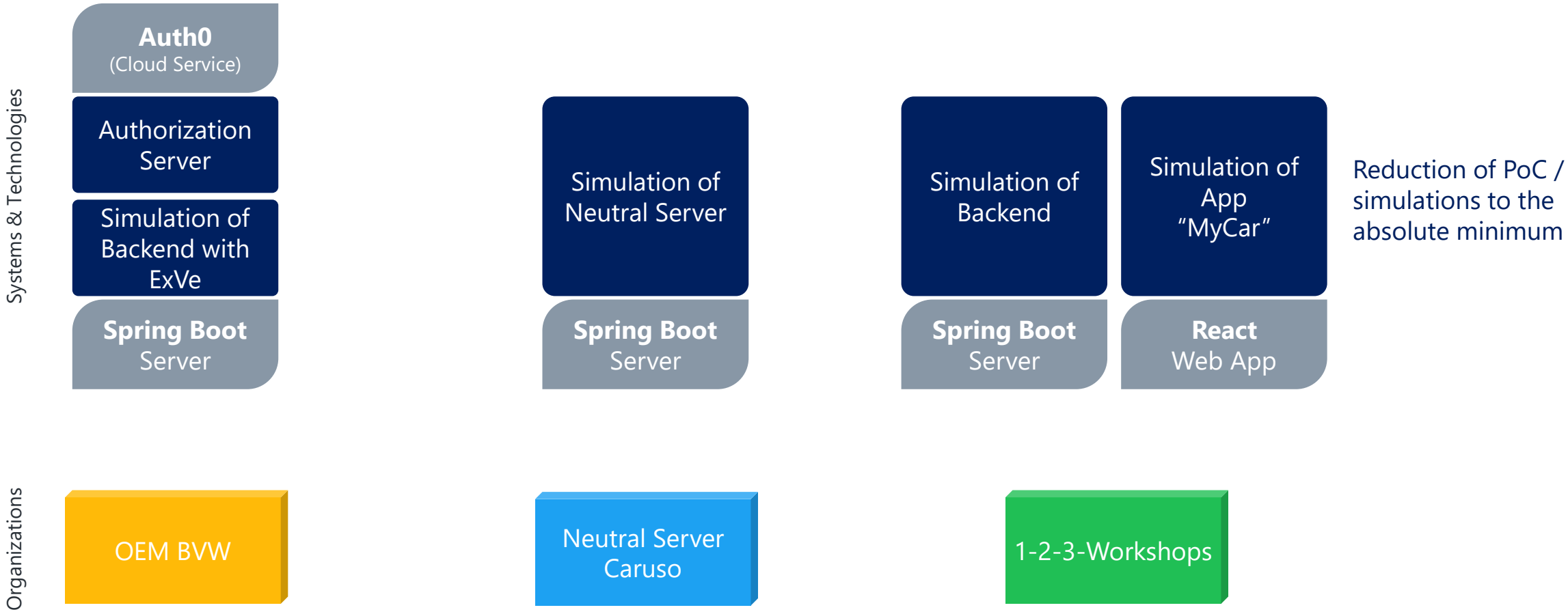
1-2-3-Workshops

1-2-3-Workshops

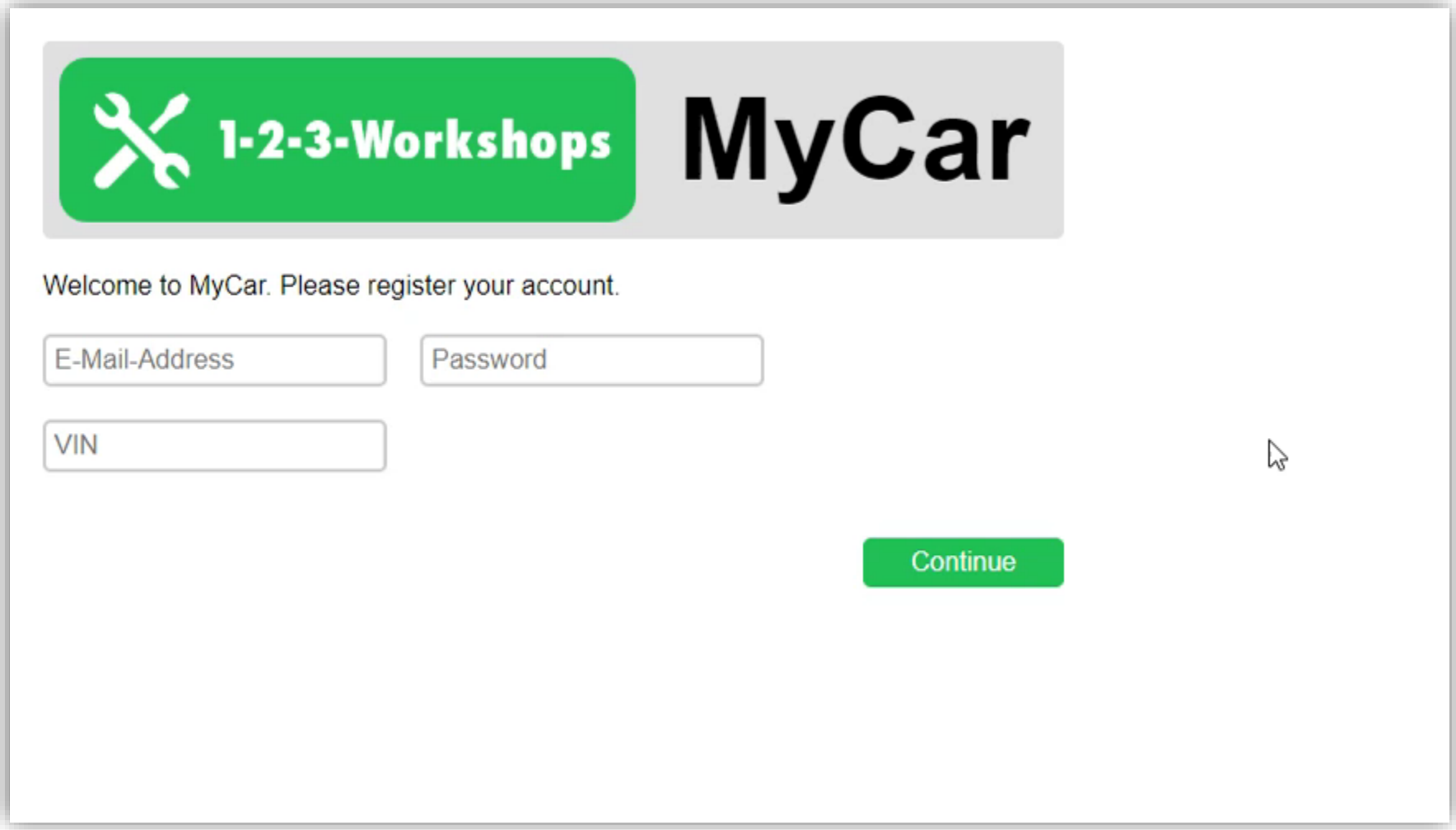
Data Consumer (Service Provider)

User

CONSENT: POC – TECHNOLOGIES IN USE



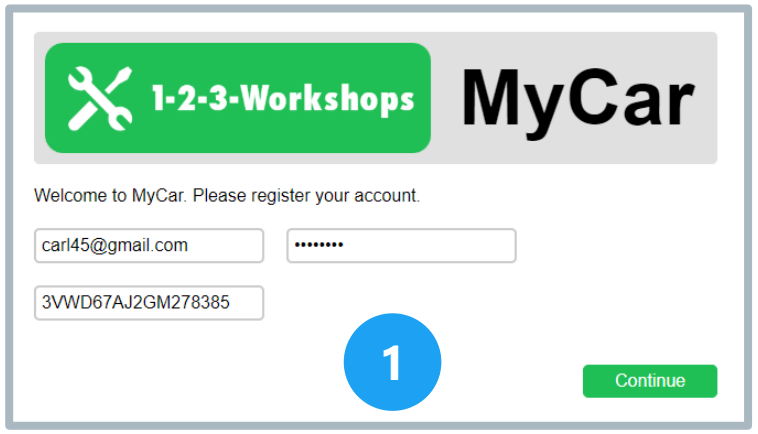
CONSENT: POC – VIDEO OF USER INTERACTION

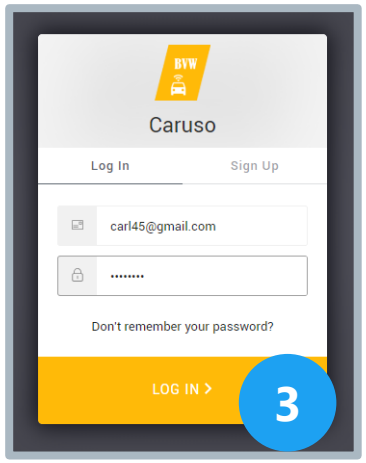


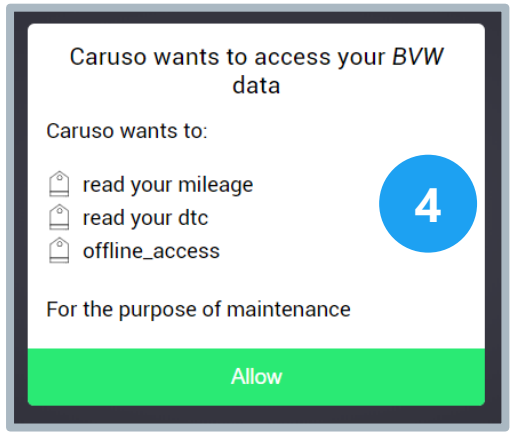
Carl

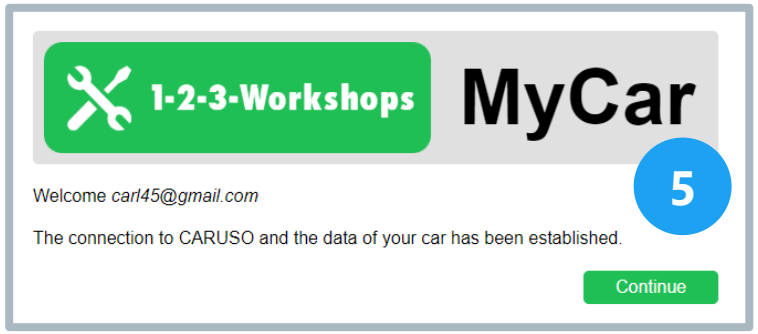
CARUSO dataplace

SCREEN FLOW FROM THE PERSPECTIVE OF THE END USER / CAR OWNER









Carl

CARUSO dataplace

CONSENT: POC – WHO KNOWS WHAT ABOUT CONSENT?

OEM BVW stores given consent:
- Client „Caruso“
- Has the consent to retrieve the data items „mileage, DTC“
- For the car with VIN „3VWD67AJ2GM278385 “
- For the purpose of „Car Status Information“
- Given by „Owner“
- Given at „01.03.2018“

Caruso stores consent request
- Client „Caruso“
- Has the consent to retrieve the data items “mileage, DTC“
- From the data provider „BVW“
- For the car with VIN „3VWD67AJ2GM278385 “
- For the purpose of „Car Status Information“

Caruso stores state -> VIN, purpose mapping
Caruso receives and stores OAuth tokens
- Consent given at „01.03.2018“
- 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“
- For the car with VIN „3VWD67AJ2GM278385 “
- For the purpose of „Car Status Information“

1-2-3-Workshops gets notified about successful consent
- Consent given at „01.03.2018“

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“
- For the car with VIN „3VWD67AJ2GM278385 “
- For the purpose of „Car Status Information“

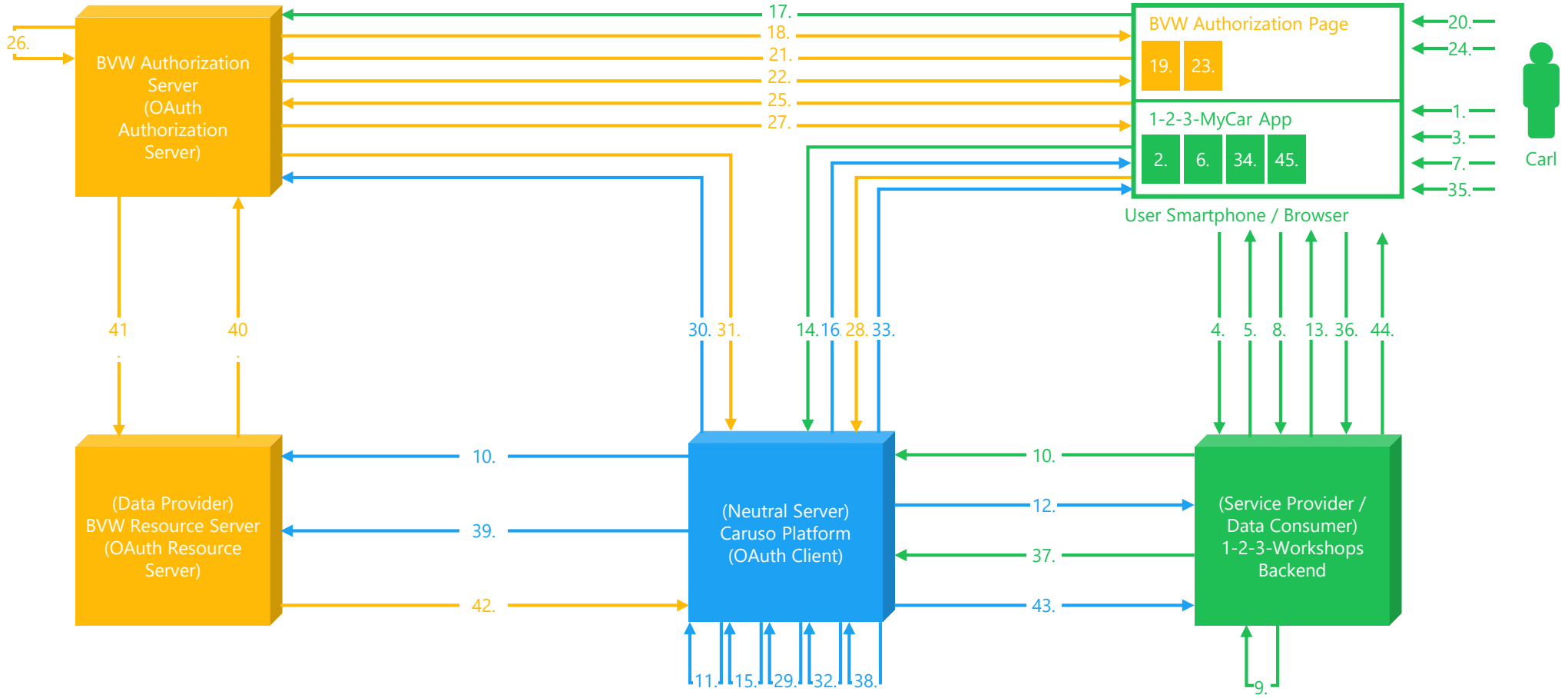
Organizations

OEM BVW

Neutral Server Caruso

1-2-3-Workshops

CONSENT: POC – WHAT HAPPENS BEHIND THE SCENES



CARUSO dataplace

CONSENT: POC – TOPICS COVERED

- **Authentication** of user at OEM and at Data Consumer
- **Authentication** of Data Consumers via Caruso API-Keys
- Realistic example from workshop domain
- **All UI interaction steps** from perspective of user using a service provider app
- **Fine-grained handling of consent**:
  - (data consumer, purpose, data items, data provider)
  - User can **provide** fine-grained consent (to data consumer)
  - User can **view** fine-grained consent information (from Caruso)
  - User can **revoke** fine-grained consent (from Caruso and from Data Provider)
- **Dynamic selection of a Data Provider** based on the VIN → this Data Provider is then addressed for consent handling
- Full **flow over all phases**:
  - registration
  - consent provision & revocation
  - data transfer in operation
- More elaborate example with 2 data providers and 2 data consumers around neutral server Caruso

CONSENT: POC – WHAT WE HAVE SHOWN / KEY MSGS

- Caruso has a concept for consent handling across a neutral server
  - The elaborated **concept for consent handling works as intended**
  - Caruso plays a central role in facilitating the consent handling concept
  - Demonstration capabilities with video and very detailed explanation of technical solution
- The **key requirements** of stakeholders are **fulfilled**
  - Consent handling is compliant with ExVe standard
    - Data Providers do not have to change anything
  - OEMs do not know service providers
  - Consent handling is simple for Data Consumers (only interaction with Neutral server)
  - Data Providers do not have to trust the other parties, they get real consent from the User
  - Car ownership is verified before delivering data
  - Using standard security technology: based on OAuth standard
- Managing consent is **reasonable from the User perspective**

CONSENT: POC – LIMITATIONS & GAPS

- Mutual impacts with other security features and the Caruso platform as a whole are not scope, yet
- Focus was consent handling, not entire GDPR compliance
- Further reviews could uncover more limitations
  - Technical
  - Legal

CONSENT - ROADMAP

DIFFERENT SETTINGS OF PERSONAL DATA PROCESSING

Solution alternatives for personal data processing	**Private car** (registered keeper = driver or driver = person from registered keeper's household)	**Car usage with working contract** (registered keeper has a work contract with driver) (Example: plumber company has 3 cars and 5 employees with work contracts driving the cars)	**Car usage with usage contract** (registered keeper has a contract with driver for car usage) (Example: private person Carla rents a car from Sixt for 2 weeks)
Consent SA.I: OAuth – OEM authorization, Service Provider client	- Provider can see identity of service providers - Consumes have to interact with all providers separately + Provider do not have to trust a 3rd party unconditionally + Fully compliant to ExVe standard - Provider sees identity of registered keeper	…	
Consent SA.II: OAuth – Neutral Server authorization, Service Provider client	+ Provider does not see identity of service providers + Consumer do not have to interact with all providers separately - Providers have to trust a 3rd party unconditionally - Not compliant to ExVe standard + Provider does not see identity of registered keeper		
Consent SA.III: OAuth – OEM authorization, Neutral Server client	+ Provider does not see identity of service providers + Consumers do not have to interact with all OEMs separately + Providers do not have to trust a 3rd party unconditionally + Fully compliant to ExVe standard - Provider sees identity of registered keeper		
Consent SA.IV: Custom – Neutral Server authorization, consent passing	+ Provider does not see identity of service providers + Consumer do not have to interact with all OEMs separately - Providers have to trust a 3rd party unconditionally - Not compliant to ExVe standard + Provider does not see identity of registered keeper		
Contract / BoI	…	…	…

Details so far were mainly focusing on the **"Private car"** case.

We are currently working on the assessment of all constellations (elaboration of advantages and disadvantages).

Maybe, further requirements or also solution alternatives might arise.

THANK YOU.

CARUSO
dataplace