A NEUTRAL AND SECURE APPROACH FOR ACCESSING IN-VEHICLE DATA FOR 3RD PARTY SERVICES.

SEBASTIAN ZIMMERMANN, PETER ZOLLER
AGENDA.

1 Motivation: Sharing In-Vehicle Data.
2 Possible Alternatives for Accessing In-Vehicle Data.
3 VDA NEVADA – Share & Secure.
4 First solution following the extended vehicle approach: BMW CarData.
MOTIVATION: SHARING IN-VEHICLE DATA.
VEHICLE GENERATED DATA ARE ENABLING NEW DIGITAL SERVICES IMPROVING SAFETY, EFFICIENCY AND COMFORT.

- More safety and more efficiency on the road.
  - For connected foresight sensor data is essential.
  - Training data from vehicle sensors are the basis of machine learning for autonomous driving.

- More reliable travel and better planning of garage visits.
  - Vehicle data signals service requirements at an early stage.

- Recognize and fulfill individual needs.
  - Data as a basis for personalized functions.

_DATA SECURITY AND PRIVACY ARE TOP PRIORITY_
THERE ARE MANY REASONS FOR SHARING DATA.

- Improving Driver Assistance Systems
- Repair and Maintenance Services
- General Digital Services
OEMs and 1st tier suppliers within VDA (Verband der Deutschen Automobilindustrie) as well as within ACEA (European Automotive Manufacturers Association) and CLEPA (European Association of Automotive Suppliers) worked together on a concept meeting these basic principles.

Basic principles:
- Customer choice
- Privacy and data protection
- Fair competition
- Safety, security and liability
- Interoperability
- Return on investment
AUTOMOTIVE SECURITY IS ORGANIZED IN PROTECTIONS LAYERS WHICH EXTEND FROM THE VEHICLE VIA THE IT-BACKEND TO EXTERNAL PARTNERS.
2

POSSIBLE ALTERNATIVES FOR ACCESSING IN-VEHICLE DATA.
POSSIBLE ALTERNATIVES FOR ACCESSING IN-VEHICLE DATA.

OVERVIEW.

Scenario 1: OEM Backend (Extended Vehicle)
Scenario 2: 3rd-Party Backend
Scenario 3: OBD Device
Scenario 4: CE-Device
Scenario 5: In-Vehicle Gateway
EVALUATION OF THE DIFFERENT SCENARIOS. SAFETY AND SECURITY.

Scenario 1: OEM Backend (Extended Vehicle)
- End-2-end security concept
- Maximum firewall protection
- Offboard Security Shield

Scenario 2: 3rd-Party Backends
- Bypass to vehicle security zones

Scenario 3: OBD Device
- Bypass to vehicle security zones
- Insufficient security of most devices
- Designed for stationary use

Scenario 4: CE-Device
- Bypass to vehicle security zones

Scenario 5: In-Vehicle Gateway
- Bypass to vehicle security zones

OEM
EVALUATION OF THE DIFFERENT SCENARIOS.
RESPONSIBILITY AND LIABILITY.

Scenario 1: OEM Backend (Extended Vehicle) + clear

Scenario 2: 3rd Party Backends - unclear

Scenario 3: OBD Device - unclear

Scenario 4: CE-Device - unclear

Scenario 5: In-Vehicle Gateway - unclear
EVALUATION OF THE DIFFERENT SCENARIOS.
EASE OF ACCESS AND NON-DISCRIMINATION.

Scenario 1: OEM Backend (Extended Vehicle)
- Unlimited 3rd parties
- No automotive know-how
- No hardware
  - No anonymity
- Anonymity via Neutral Server

Scenario 2: 3rd Party Backends
- Detailed automotive know-how
- Vehicle variety

Scenario 3: OBD Device
- Only one 3rd party

Scenario 4: CE-Device
- Specific vehicle option
- Specific customer device

Scenario 5: In-Vehicle Gateway
- Limited 3rd parties

A Neutral and Secure Approach for Accessing In-vehicle Data for 3rd Party Services | BMW Group | April 18th, 2018
3

VDA NEVADA – SHARE & SECURE.
ACCESS TO IN-VEHICLE DATA. 
CORE ELEMENTS OF THE VDA NEVADA – SHARE & SECURE CONCEPT.

1. Safe, Secure, and Fair Access to In-Vehicle Data
2. Use Case Categories
3. Demonstration of Operational Capability through Proof-of-Concepts

NEVADA: Neutral Extended Vehicle for Advanced Data Access
NEVADA – SHARE & SECURE COMBINES THE EXTENDED VEHICLE WITH NEUTRAL SERVERS TO GUARANTEE FAIR COMPETITION AND NON-DISCRIMINATION.
## USE CASE CATEGORIES.

<table>
<thead>
<tr>
<th>Category 1</th>
<th>Category 2</th>
<th>Category 3a</th>
<th>Category 3b</th>
<th>Category 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data for improved traffic safety</strong>&lt;br&gt;Traffic safety relevant data</td>
<td><strong>Data for cross brand services</strong>&lt;br&gt;None differentiating vehicle data</td>
<td><strong>Data for brand specific services</strong>&lt;br&gt;Vehicle data differentiating and IP relevant for OEM</td>
<td><strong>Data for component analysis and product improvement</strong>&lt;br&gt;Vehicle data differentiating and IP relevant for OEM and supplier</td>
<td><strong>Personal data</strong>&lt;br&gt;“Right of access” granted only to the parties authorized to process data by law, contract or consent</td>
</tr>
</tbody>
</table>

| Fire Department, Police, 911, … | Product | Dealer, Subsidies | Product | Customer |

### B2B Agreement between OEM and 3rd Party

#### Customer Consent

- **Category 1**: Personal data
  - “Right of access” granted only to the parties authorized to process data by law, contract or consent

- **Category 2**: Data for cross brand services
  - None differentiating vehicle data

- **Category 3a**: Data for brand specific services
  - Vehicle data differentiating and IP relevant for OEM

- **Category 3b**: Data for component analysis and product improvement
  - Vehicle data differentiating and IP relevant for OEM and supplier

- **Category 4**: Product
  - Fire Department, Police, 911, …

- **Product**: Available to 3rd parties
- **Dealer, Subsidies**: Limited availability to 3rd parties
- **Customer**: Available to 3rd parties
PROOF-OF-CONCEPTS OF THE NEUTRAL SERVER CONCEPT.

- Proof-of-Concept implementations of Neutral Servers by independent parties.
- Different Use Cases to demonstrate overall concept and customer consent process.
- Open for large number of Neutral Servers to promote competition and diversity.
4

FIRST SOLUTION FOLLOWING THE EXTENDED VEHICLE APPROACH: BMW CARDATA.
UseCase #1:
Transparent access for car owner to vehicle generated data that has been transmitted over the air to BMW data center, all free of charge.

UseCase #2:
Having consent of the car owner (✅), transmitted data is accessible by corporate third parties.
A Neutral and Secure Approach for Accessing In-vehicle Data for 3rd Party Services | BMW Group | April 18th, 2018
BMW CARDATA.
NON-DISCRIMINATORY ACCESS FOR THIRD PARTIES.

1. Register.
BMW Group Aftersales Online Services Portal

2. Create Data Container.

3. Request Customer Consent.
BMW CarData API

BMW ConnectedDrive Customer Portal

5. Transfer Data.
BMW CarData API

Benchmark: 24 hours
BMW CARDATA.
NEXT STEPS.

Rollout EU
Rollout USA
MINI CarData
Additional Features

- Updates while driving
- High-frequency data
- Additional data

A Neutral and Secure Approach for Accessing In-vehicle Data for 3rd Party Services | BMW Group | April 18th, 2018
No hardware expenses, no integration costs.

Integrated end-to-end security concept from vehicle to backend.

No cooperation with BMW required (100% self registration process).

Non-discriminating:
- Available for all European companies, no restrictions regarding industrial sector or use case.
- Data of a given vehicle is available to an unlimited number of 3rd parties (in contrast to dongle solutions).
- Access via standard web-interfaces, no automotive know-how required.
THANK YOU FOR YOUR ATTENTION.

We are hiring: https://www.bmwgroup.com/de/karriere.html
Specialists (m/f) Data Management and Data Governance

A Neutral and Secure Approach for Accessing In-vehicle Data for 3rd Party Services | BMW Group | April 18th, 2018