Privacy in Automated and Connected Vehicles

Panel moderated by Robin Pierce and Florian Stahl with Gergely Biczok, Jean-Loup Dépinay, Juha Röning, and Ian Oliver organized by EU funding project SECREDAS at CPDP Conference 2021

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Moderators

Florian Stahl

- Security & Privacy Expert from Regensburg, Germany
- Team Manager at AVL (Automotive Supplier)
- MSc., CIPT, CISSP, CISM
- Leader of the OWASP Top 10 Privacy Risks Project
- Florian.Stahl@avl.com

Robin L. Pierce, JD, PhD

- Associate Professor at Tilburg Law School
- Specialized in law, regulation, and governance of AI technologies
- She is a lead on the H2020 project on citizen science and GDPR compliance of data trackers and serves on ethics and law advisory boards for several European projects

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Panelists

Gergely Biczok

- Associate Professor at the CrySyS Lab, Budapest Univ. of Technology and Economics, Hungary
- Lab focus: cyber-physical security, privacy enhancing techniques, economics of security and privacy
- biczok@crysys.hu

Jean-Loup Depinay

- Program manager in charge of collaborative R&D projects of IDEMIA
- A 24 projects funded by French or European programs (H2020, FUI, ANR, Eniac...)
- Coordinator IDEASWIFT (ITEA2, Automatic Border Control Gate) Awared in 2018 Excellence for Innovation and Business impact, and SpeechXRays (H2020)
- 6 patents

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Panelists

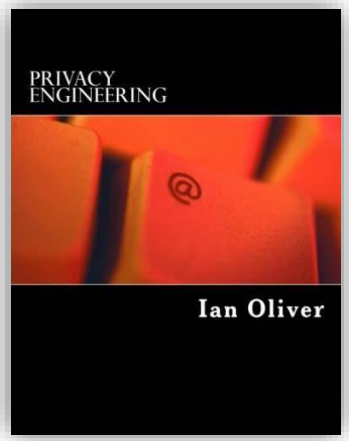
Juha Röning

- Professor on Embedded Systems, University of Oulu, Finland
- Head of Biomimetics and Intelligent Systems Group (BISG)
- Head of University of Oulu Security Program Group (OUSPG)
- Juha.Roning@oulu.fi

OULUN YLIOPISTO

Ian Oliver

- Distinguished Member of Technical Staff at Nokia Bell Labs, Finland
- Trusted Computing
- Author of **"Privacy Engineering"**



SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Introduction

Tesla wins German Big Brother Award

“Tesla receives this award for marketing cars that extensively and perpetually surveil their passengers and car surroundings. The data obtained is constantly analyzed and can be used for any purpose.” *

Surveillance Detection Scout – Your Lookout on Autopilot

- Open Source Software on GitHub uses Tesla’s cameras to identify people following you
- Real-time video analytics with face and license plate detection

* https://bigbrotherawards.de/en/2020/mobility-tesla

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Challenges for Privacy in Automotive

- **Connected vehicles** make it possible to track driver's behavior
- Unclear who owns the data (manufacturer, car owner, driver)?
- Business models consider behavior and location-based ads in cars.
- Often there is no choice to opt-out

- Sensors and cameras in **autonomous cars** record surrounding areas including personal data like pedestrian faces, passengers of other cars and license plates comparable to Google Street View
- Video data leaves the car for analysis purposes and should be protected by:
  - Anonymization (blurring faces and license plates)
  - Access control according to need-to-know
  - Data retention / deletion must be considered
  - Car should be marked with camera symbol

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

How to address these challenges?

- EDPB Guideline on processing personal data in the context of connected vehicles and mobility related applications (01/2020)
- Standards & Regulation (Cybersecurity)
  - ISO/SAE 21434 DIS considers privacy impact
  - UNECE Regulation No. 155 required for vehicle type approval from 2022 demands to cover threats related to privacy like “Unauthorized access to the owner’s privacy information such as personal identity, payment account information, address book information, location information, vehicle’s electronic ID, etc.”
- Privacy Threat Modelling with LINDDUN
- Privacy by Design
- Privacy Enhancing Technologies (PETs)
- (Hope for) Enforcement of the Data Protection Authorities

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Automotive data ecosystem (1)

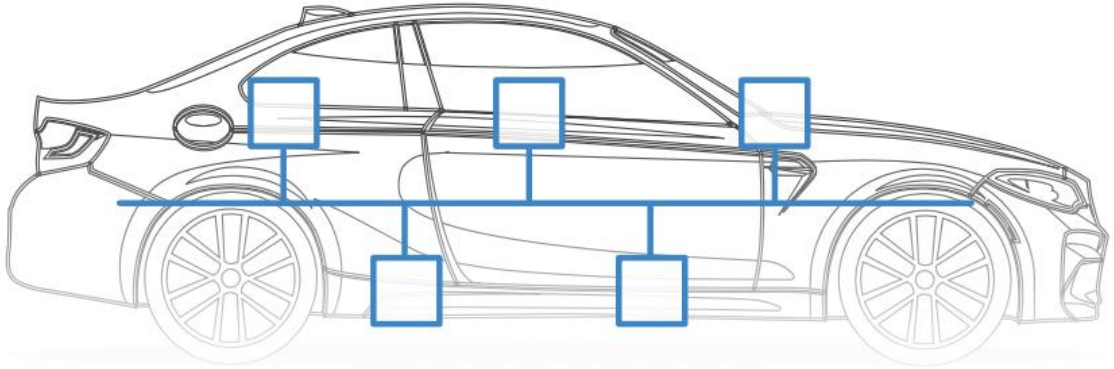
Controller Area Network (CAN): in-vehicle network network connecting ECUs

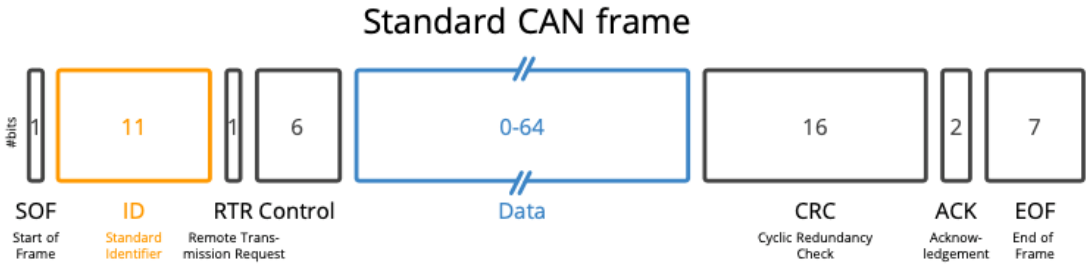
- Low delays – no security
- Designed to be closed – now opened up
- But even if no intrusion…

Manufacturer collects (maintenance) and resells CAN data

- Insurance companies
- location-based services
- fleet management/car sharing)

Why is this a privacy issue?





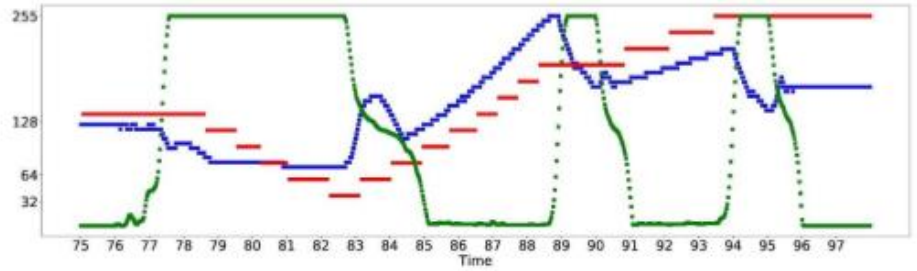
Figures from csselectronics.com

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Driver re-identification (2)

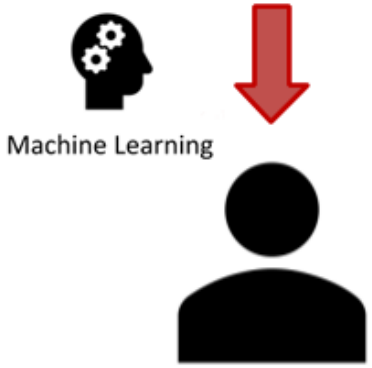
Timestamp	CAN-ID	Req	Len	Data
1481492683.285052	0x0208	000	0x8	0x00 0x00 0x32 0x00 0x0e 0x32 0xfe 0x3c
1481492674.736055	0x02c4	000	0x8	0x82 0xc8 0x00 0x0f 0x03 0x00 0x92 0x3c
1481492674.736055	0x02c4	000	0x8	0x82 0xc9 0x00 0x0f 0x00 0x00 0x92 0x4c
1481492674.736055	0x02c4	000	0x8	0x82 0xcc 0x00 0x0f 0x08 0x00 0x92 0x5a
1497323915.123844	0x018e	000	0x8	0x03 0x03 0x00 0x00 0x00 0x00 0x07 0x3f
1497323915.112910	0x00f1	000	0x6	0x28 0x00 0x00 0x40 0x00 0x00
1481492674.736055	0x02c4	000	0x8	0x82 0xd2 0x00 0x0f 0x0c 0x00 0x92 0x5d
1481492674.736055	0x02c4	000	0x8	0x82 0xa1 0x00 0x0f 0xa1 0x00 0x92 0x4d

Signal extraction



Clutch
Velocity
RPM

Machine Learning



Reverse-engineering is possible

[Lestyan, S., Acs, G., Biczók, G., & Szalay, Z. (2019). Extracting vehicle sensor signals from CAN logs for driver re-identification. In ICISSP 2019.]

Drivers can be re-identified by “brute force ML” on raw CAN messages!

[Remeli, M., Lestyán, S., Acs, G., & Biczók, G. Automatic driver identification from in-vehicle network logs. In IEEE Intelligent Transportation Systems Conference (ITSC), 2019.]

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Tracking (3)

Microtracking: identifying maneuvers from CAN logs (lane change, sudden turn, obstacle avoidance)

- Using velocity and steering wheel angle signals plus basic physics
- [Gazdag, A., Holczer, T., Buttyán, L., & Szalay, Z. (2018, May). Vehicular Can Traffic Based Microtracking for Accident Reconstruction. In Vehicle and Automotive Engineering (pp. 457-465). Springer, Cham.]
- Forensic techniques: a plus for liability (accident reconstruction) and safety (improving ADAS)
- Minus for privacy, reveals driving behavior, enables profiling!

Macrotracking: reconstructing whole routes

- Using CAN signals plus maps and a starting point (home, office, …)
- Pandora's box of location privacy

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

CAN data is private! (4)

Singling out (driver re-identification)

Profiling (driver behavior, microtracking)

Location inference (macrotracking)

No real choice to send back CAN data when purchasing a car!

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Further Privacy Challenges in Automotive

- Complex Stakeholders Management
  - OEM
  - Maintenance Services
  - Entertainment Services
  - Driving Sevices
- Risk: a centralized system to ensure identification
  - Not compatible with Privacy enforcement as soon you request ”strong” authentication
  - How to maintain value chain for all stakeholders
    - How to minimize data (GDPR requirement)

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

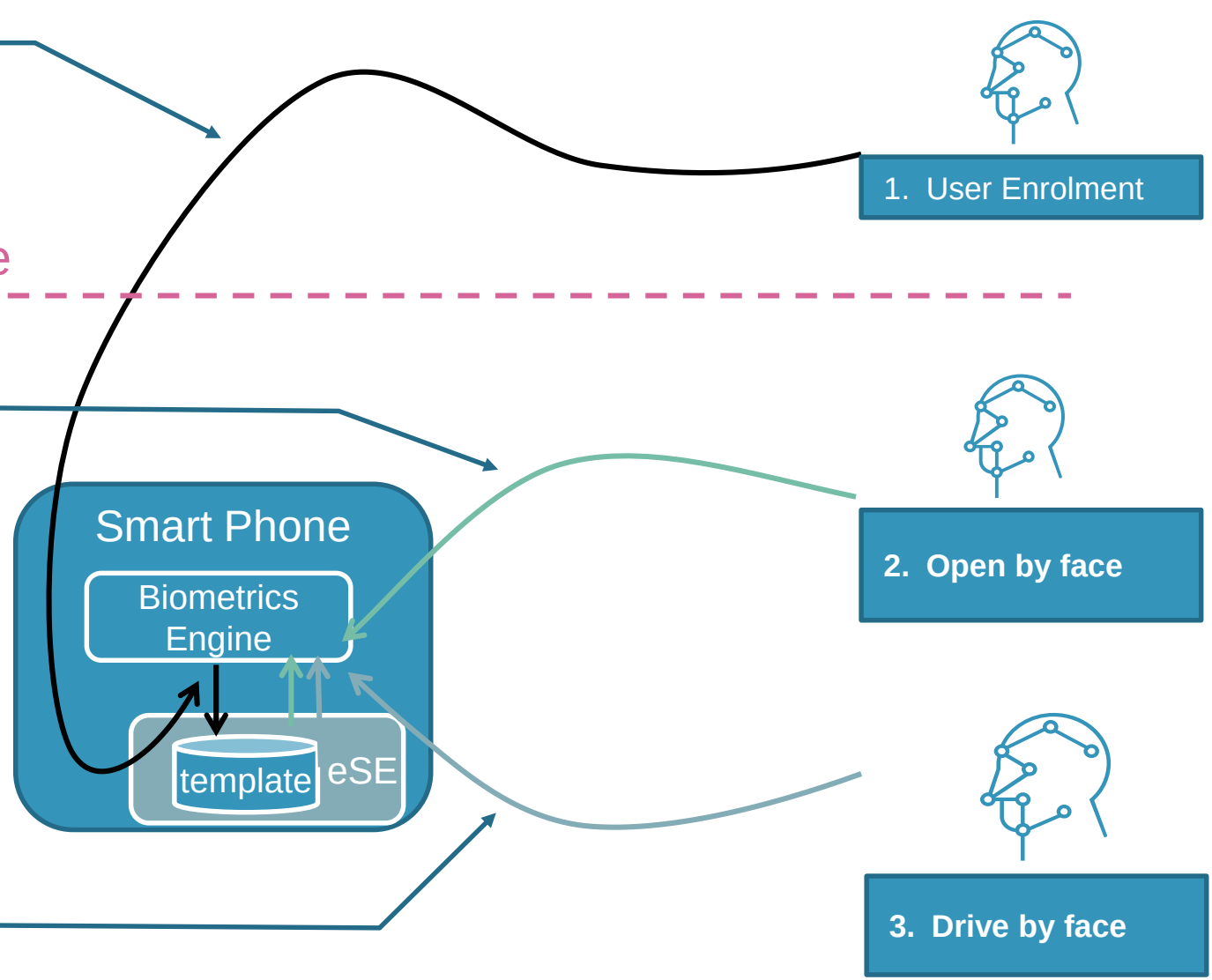
IDEMIA Driver Authentication Demonstrator

1: User enrolment in-car
- Trigger & booting
- Capture user at home
- Extract and store anonymous biometrics template

Enrolment done once

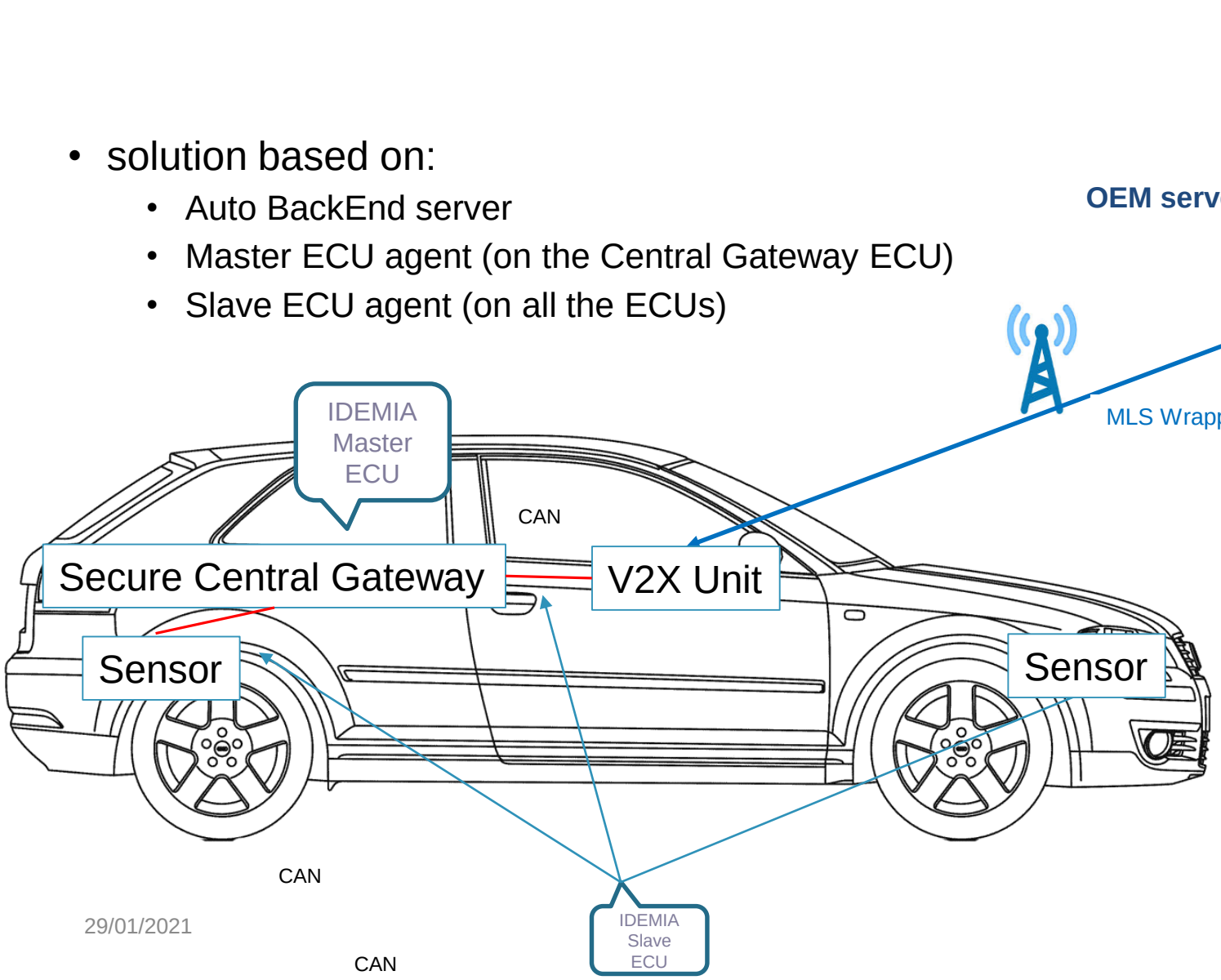
2: Open by face
- Trigger & booting
- Capture user
- Extract template & match with stored template
- Unlock door

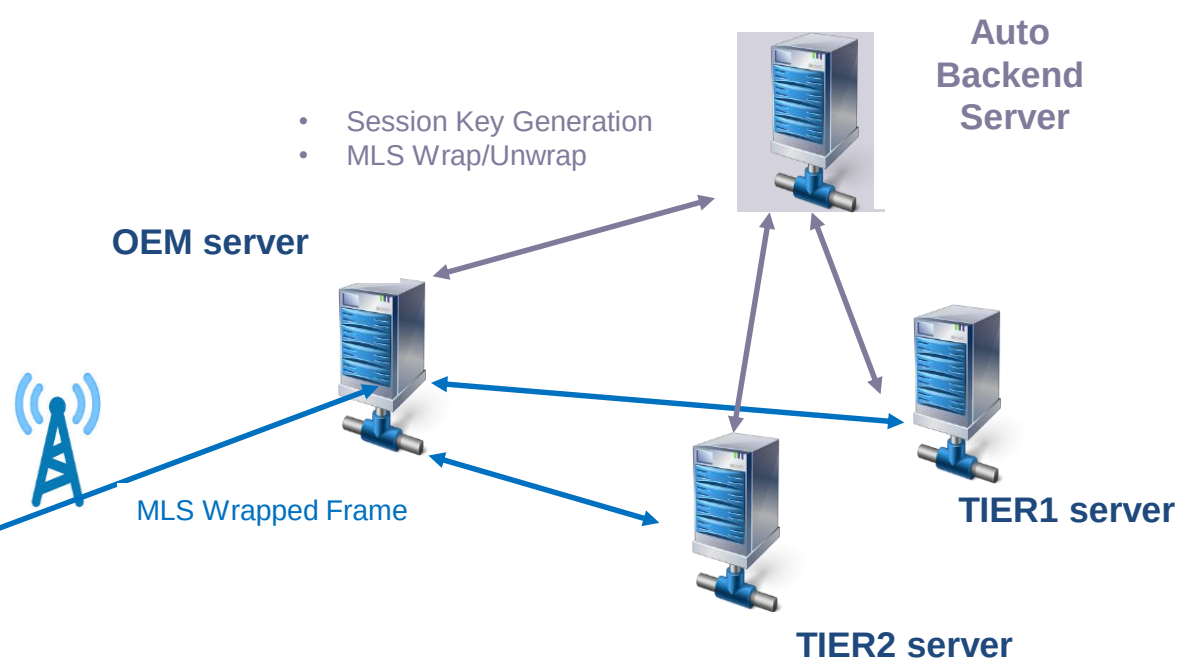
3: Drive by face
- Trigger & booting
- Capture user
- Extract template & match with stored template
- Start engine

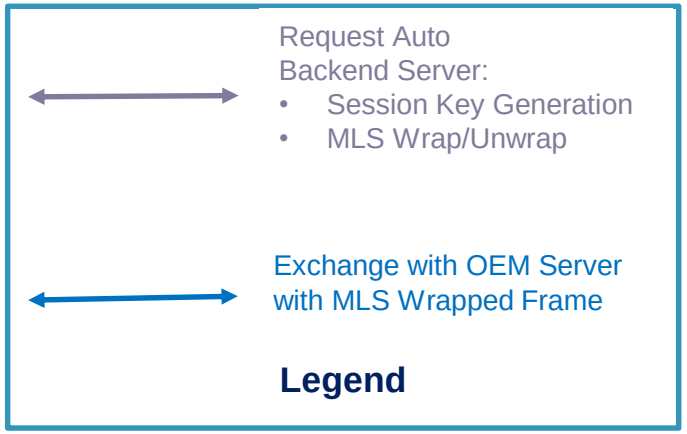


IDEMIA In-Vehicle Secure Network

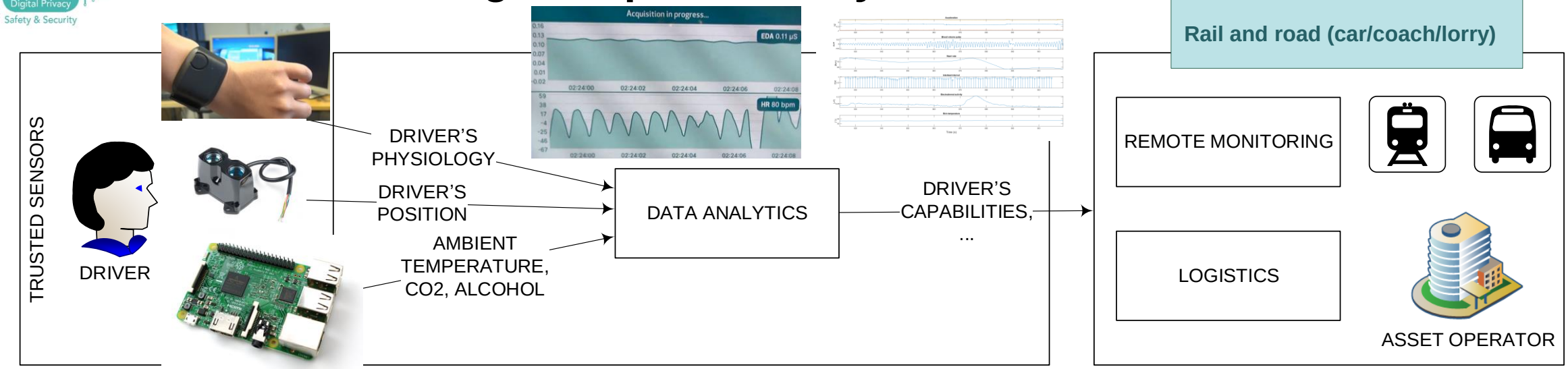
- solution based on:
  - Auto BackEnd server
  - Master ECU agent (on the Central Gateway ECU)
  - Slave ECU agent (on all the ECUs)







Driver monitoring to improve safety



BACKGROUND AND ASSUMPTIONS

- **Sleep quality affects readiness on work period**
- **Heart rate related to attention**
- **Air quality affect driver's readiness**

UNOBTRUSIVE SENSORS

- **Sleep data before driving task**
- **Hearth rate, breath, etc. while driving**
- **Air parameters (temperature, CO2, alcohol)**
- **Driver presence and movement (IR/LIDAR, no camera)**

Machine learning

IN-VEHICLE AND REMOTE EXPLOITATION

- **Assessment of driver aptness**
- **Data visualisation for supervising services**
- **Warnings to driver (stimuli, communication with control centre)**

- Scope: detection of driver capability of driving
- SECREDAS: observe closed eyes (driver's eyelashes by RGB camera); observe breathing (chest movements by laser and IR camera), **driver alertness (hearth rate and other parameters by wearables)**
- Here, unobtrusive sensors selected for **reliability** while considering **user acceptance** and **data minimisation**
  - Wrist-worn PPG instead of chest belt ECG or EEG cap
  - IR sensor or LIDAR instead of camera

IR infrared
PPG photoplethysmography
ECG electrocardiography
EEG electroencephalography
LIDAR light detection and ranging

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Privacy

Communication strongly secured and anonymized

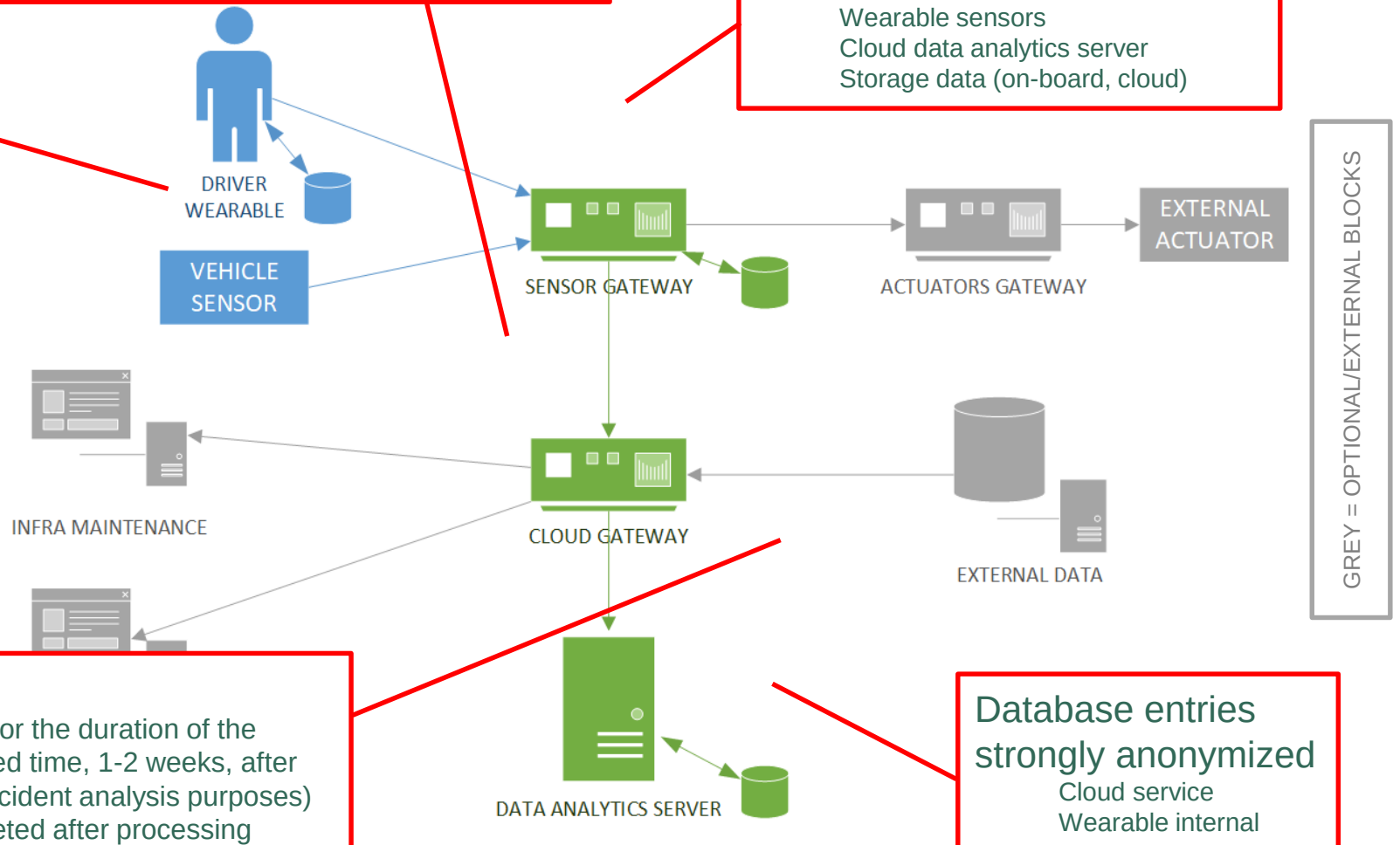
- Between a sensor and its gateway
- Between sensor gateway and cloud gateway
- Between cloud gateway and data analytics server
- Between data analytics server and cloud data storage

Strong access control to data

- Wearable sensors
- Cloud data analytics server
- Storage data (on-board, cloud)

Reject unsecure Bluetooth connection attempts from a device

- With a common default password or
- With security level less than authenticated, encrypted pairing



- GDPR:
- Processing **data concerning health** prohibited in general [art. 9(1)] but allowed for **scientific research** [art. 9(2,j)]
- **Technical** and organisational **measures**, in particular data minimisation, should be in place [art. 89(1)]
- Member states may **derogate** about rights of access by data subject, right to certification, restriction of processing, and to object [art. 89(2)] to facilitate research
- E.g. true in Finland, if data processing is based on a research plan (Data Protection Act 1050/2018, art. 31)

Driver data logs

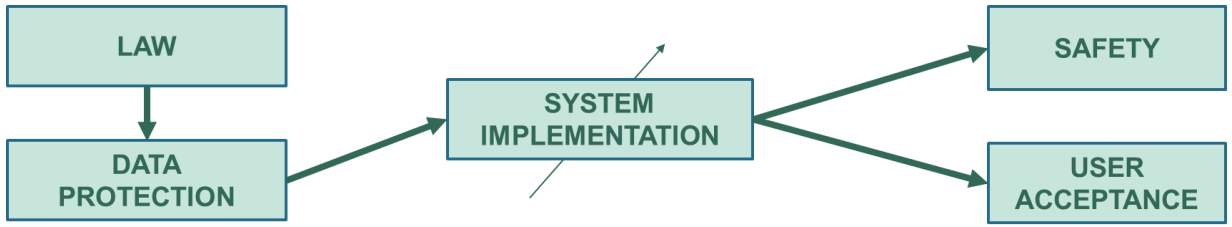
- Securely stored for the duration of the processing (limited time, 1-2 weeks, after car journey for incident analysis purposes)
- Permanently deleted after processing

Database entries strongly anonymized

- Cloud service
- Wearable internal memory

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Trade-off between safety and privacy



- User is central
- Privacy is dictated by law, but
- Data protection compliance also related to user acceptance and thus commercial success
- Recent example, WhatsApp:
  - WhatsApp announced broadened use of personal data (limited in EU, thanks to GDPR)
  - Massive amount of people started leaving WhatsApp for Signal
  - Elon Musk twitted about switching to Signal
  - Impact on stock exchange (although on wrong shares)

- "the **user is the key player**" (ETRMA *)
- "when I use a car, **I want to know** how the car uses my data" (M. Nystrom Agback *)
- "not most, but *all* data in connected vehicles qualify as **personal data** unless anonymized" (FIA, ADAC, ACI, FDM, ÖAMTC *)
- "the user [should] **decide** on the data generated by the connected vehicle" (FIA, ÖAMTC, ACI, ANWB *) "the user shall also be able, with the exception of the wider public interest cases, to **oppose** this processing through the vehicle's HMI (ETRMA *)
- "vehicles and their functionalities must be designed considering all necessary safety measures to ensure that drivers are able to **safely stop the collection of data**" (FIA, ADAC, ACI, ANWB, FDM, ÖAMTC *)

[*] Comments collected by the European Data Protection Board (EDPB) aboute the Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

More challenges...

- Still no good techniques for actually modelling privacy
- Plenty of processes...

- Privacy is just one of the security layers: Security, Privacy, Trust
- Lack of links between the layers
- Eg: much effort is made in securing the EMC, eg: signed firmware, certificates etc.

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Summary & Resource List

- Car manufacturer's have privacy on their list, but often there is no real choice to opt-out
- Some good ideas & concepts for privacy in vehicles are under development, but most technical solutions are not implemented in practice yet
- Conflict of interests: driver vs. other road users vs. manufacturer vs. third parties
- There is hope if regulators start to enforce privacy (by design) for cars
- What are your expectations / outlook?

- EDPB Guideline on processing personal data in the context of connected vehicles
- FPF Consumer Guide Personal Data in your Car
- Auto Alliance Privacy Principles for Vehicle Technologies and Services
- MyCarMyData.eu

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.

Thank you!

Questions?

Privacy in Automated and Connected Vehicles

Panel moderated by Florian Stahl with Gergely Biczok, Jean-Loup Dépinay, Juha Röning, and Ian Oliver
Organized by EU funding project SECREDAS at CPDP Conference 2021

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, the Netherlands, Poland, Romania, Sweden and Tunisia.