Automotive Privacy

MOB1 Guest Lecture at Goethe University Frankfurt

Sarah Syed-Winkler | Dec. 13th, 2022

Security & Privacy Specialist

Sarah Syed-Winkler

Security & Privacy Specialist

2016-10-01

Education

- Master of Applied IT-Security (2022)
- Bachelor of Engineering (2016)

Roles

- S&P Manager, Researcher, Trainer, Analyst

Highlights

- Developed first IDS (Intrusion Detection System) in brake ECU for Asian OEM (2017)
- TechTalk at ITCS Online Conference (2020)
- Publication on TLS Security (2021)
- Paper on Data Protection-Oriented System Model (2022)
- Talk on Automotive Privacy at VDI Conference and Automotive Cybersecurity Europe (2022)

Continental Group

Our Structure

Group	Continental
Group Sector	**Automotive**	**Tires**	**ContiTech**
			
Business Area	› Safety and Motion › Autonomous Mobility › User Experience › Smart Mobility › Architecture and Networking › **Software and Central Technologies**	› Original Equipment › Replacement APAC › Replacement EMEA › Replacement the Americas › Specialty Tires	› Advanced Dynamics Solutions (AD) › Conveying Solutions (CS) › Industrial Fluid Solutions (IFS) › Mobile Fluid Systems (MFS) › Power Transmission Group (PTG) › Surface Solutions (SSL)

Agenda

1	Motivation
2	Challenges & Opportunities
3	Automotive Privacy at Continental
4	Q&A

Agenda

European General Data Protection Regulation

EU GDPR

1995 – › **EU Data Protection Directive**

2012 – **Notion of "Privacy by Design"**

2013 – Edward Snowden

2015 – › "Democracy" (documentary)

2016 – › **European General Data Protection Regulation** Published

2018 – › "The Simpsons" S30E05

2020 – › Tesla Data Protection Study

2021

The Privacy Principles ISO/IEC 29100 (2011)

Update Process

Trialogue

Application

› **General Data Protection Regulation** Draft passed the EU Parliament

› **EU GDPR Enforced**

Privacy Information Management ISO/IEC 27701 (2019)

› **Expert Study** "GDPR application in the context of car connectivity "

Motivation

Automotive Privacy Case Studies

MCU HACK

DATA PROTECTION REPORT

Fines and Penalties

GDPR Enforcement Tracker

- 200.000€
- OR 4% of the annual turnover

(whichever amount is higher)

ETid	Country	Date of Decision	Fine [€]	Controller/Processor
ETid-778	LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.
ETid-820	IRELAND	2021-09-02	225,000,000	WhatsApp Ireland Ltd.
ETid-978	FRANCE	2021-12-31	90,000,000	Google LLC
ETid-980	FRANCE	2021-12-31	60,000,000	Facebook Ireland Ltd.
ETid-23	FRANCE	2019-01-21	50,000,000	Google LLC
ETid-405	GERMANY	2020-10-01	35,258,708	H&M Hennes & Mauritz Online Shop A.B. & Co. KG

Source: https://www.enforcementtracker.com

Fines and Penalties

Volkswagen Penalty for Test Vehicles

› Art. 13: **Information to be provided where personal data are collected from the data subject**

For example, magnetic signs with camera symbols on vehicles illustrating video recording

› Art. 28: **Processor**

Missing processing agreement with the contractor for test drives

› Art. 35: **Data protection impact assessment**

Missing DPIA prior to data processing

VIOLATIONS OF GDPR

1,100,000.00 €

Source: German state data protection commission fines Volkswagen for GDPR violation (iapp.org), 26.07.2022

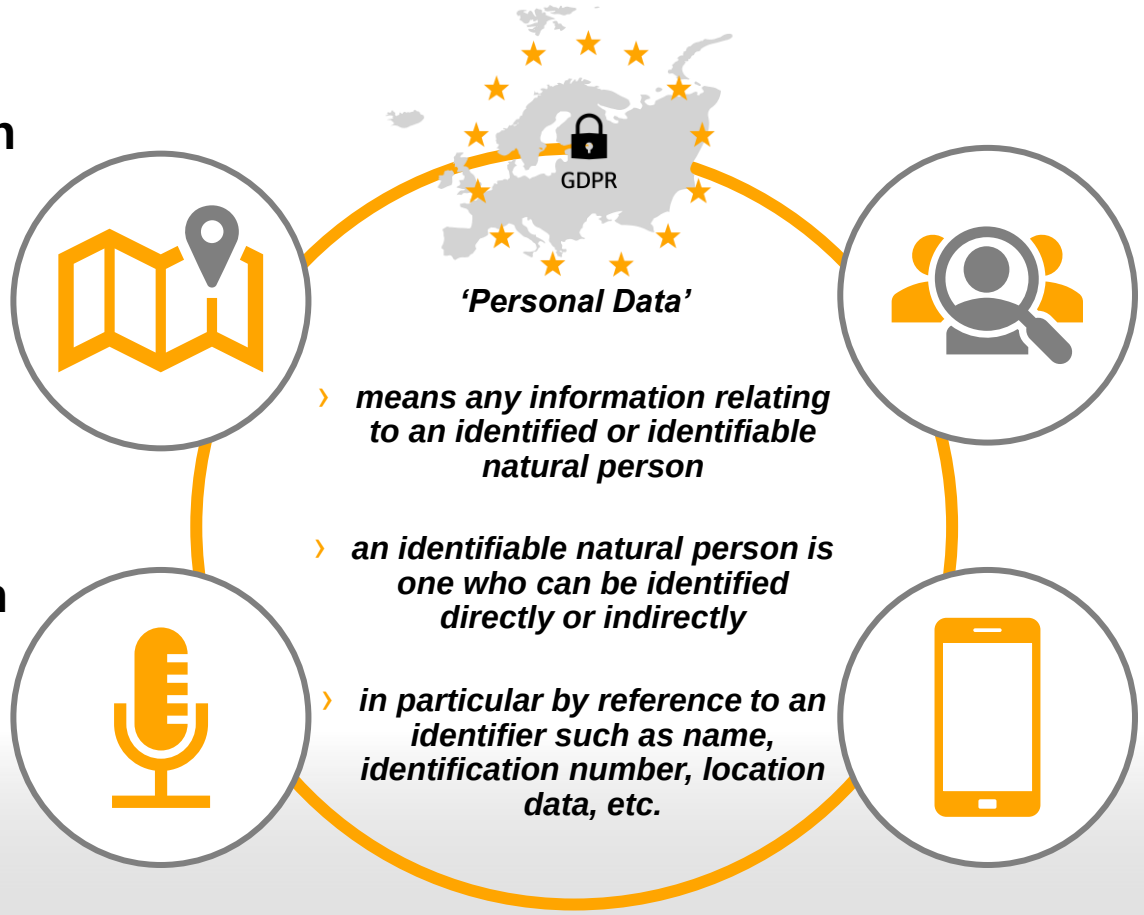
Agenda

Data Collection in Smart Vehicles

Examples

- **Location Information**
  - Starting position
  - Destination
  - Route
  - Time
  - Speed

- **In-Cabin Information**
  - Microphone
  - Camera
  - Infotainment
  - Vehicle Occupants



- **User Recognition**
  - Physical/ Biometrics
  - Fingerprint
  - Face
  - Eye movement
  - Seat Configuration

- **Applications**
  - Contacts
  - Call logs & Messages
  - Payment
  - Subscriptions

Source: PERSONAL DATA IN YOUR CAR, National Automobile Dealers Association and the Future of Privacy Forum, https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf

7 Principles of Privacy by Design

Dr. Ann Cavoukian

1. Proactive not Reactive

2. Privacy as the Default Setting

3. Privacy Embedded into Design

4. Full Functionality

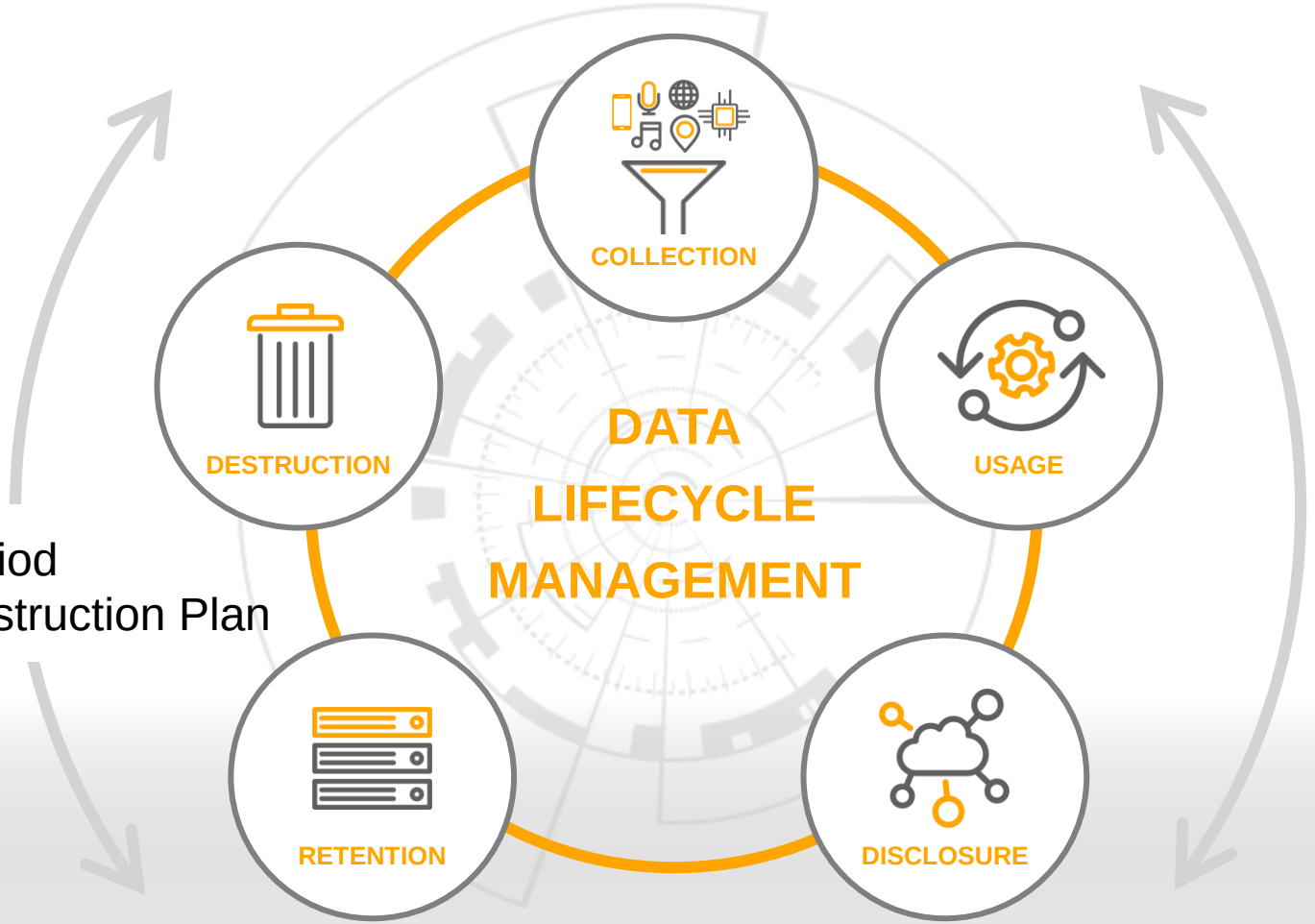
5. End-to-End Security

6. Visibility and Transparency

7. Respect for User Privacy

Source: THE 7 FOUNDATIONAL PRINCIPLES, Cr. Ann Cavoukian, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

Data Lifecycle Management
Data Protection Measures



- User Consent Management
- Privacy Notice (ext)
- Privacy Policies (int)

- Data Minimization
- Purpose Limitation

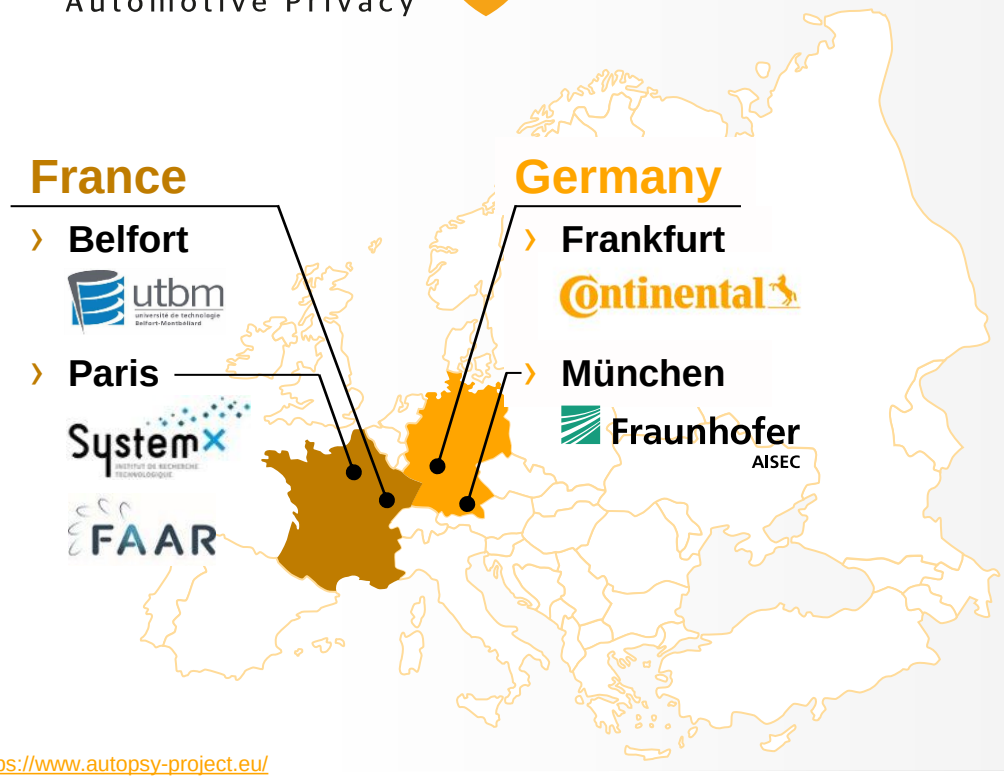
- Deidentification
- Identity and Access Management

- Retention Period
- Automatic Destruction Plan

Agenda

AUTOPSY
Research Project on Automotive Privacy

AUTOPSY
Automotive Privacy



https://www.autopsy-project.eu/

1st July 2021 – 30th June 2024

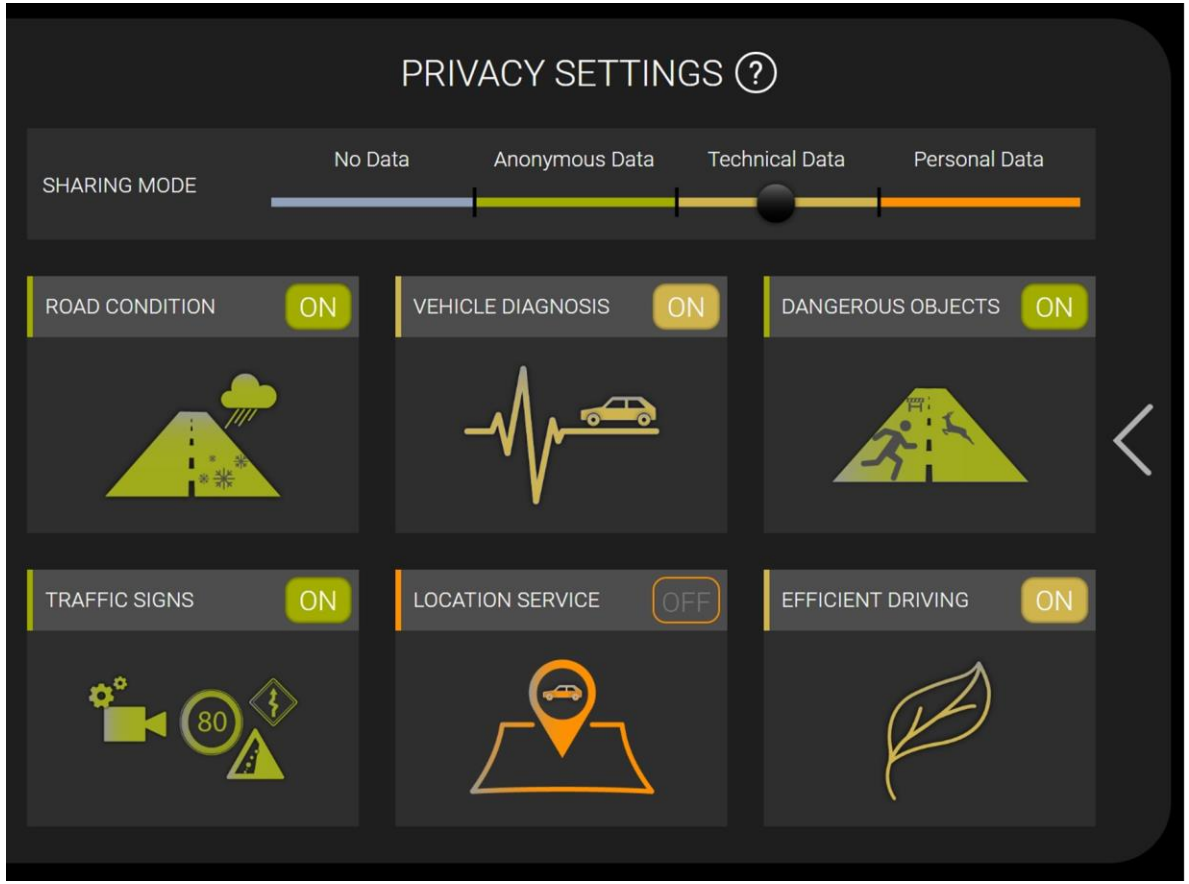
Research Project partly funded by BMBF and ANR

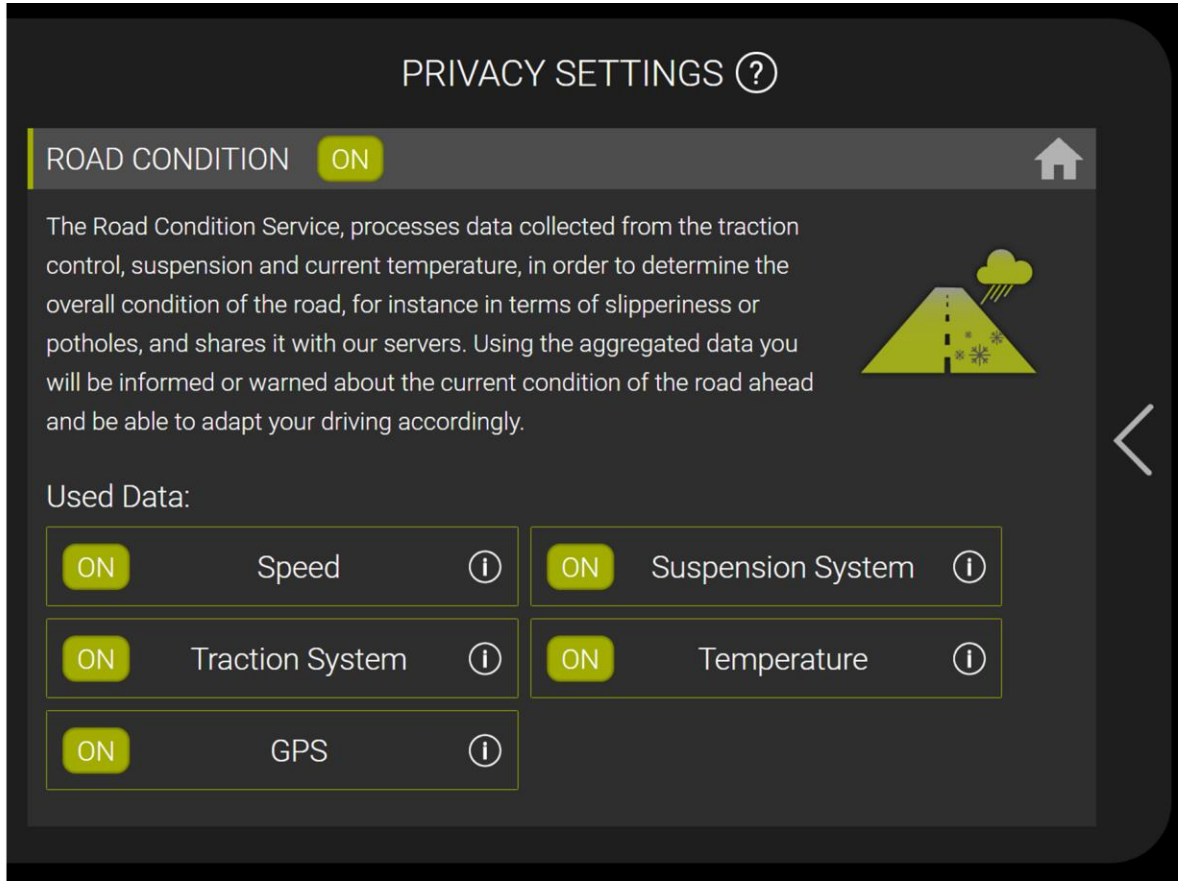
To create better understanding of **Data flows** in **Automotive environments**

To create **Privacy-Aware System Model** for an **Automotive Use-Case** in specific **technical design**

User Consent Management

Privacy HMI





Source: Continental, Cybersecurity Lab. 2021. Privacy Human Machine Interface. Internal Document.

AUTOPSY
Research Paper Publication

› Published at ACM-CSCS 2022, 8th Dec

A Data Protection-Oriented System Model Enforcing Purpose Limitation for Connected Mobility

Sarah Syed-Winkler
Sebastian Pape*
Ahmad Sabouri
sarah.syed-winkler@continental.com
sebastian.pape@continental.com
ahmad.sabouri@continental.com
Continental Automotive Technologies GmbH, Software and Central Technologies
Frankfurt, Hesse, Germany

ABSTRACT

Cars are getting rapidly connected with their environment allowing all kind of mobility services based on the data from various sensors in the car. Data privacy is in many cases only ensured by legislation, i. e., the European General Data Protection Regulation (GDPR), but not technically enforced. Therefore, we present a system model for enforcing purpose limitation based on data tagging and attribute-based encryption. By encrypting sensitive data in a way only services for a certain purpose can decrypt the data, we ensure access control based on the purpose of a service. In this paper, we present and discuss our system model with the aim to improve technical enforcement of GDPR principles.

CCS CONCEPTS

• **Security and privacy** → *Human and societal aspects of security and privacy*; **Privacy protections**; **Usability in security and privacy**; • **Computer systems organization** → *Special purpose systems.*

KEYWORDS

privacy model, data protection implementation, automotive, data tagging, attribute-based encryption

ACM Reference Format:

Sarah Syed-Winkler, Sebastian Pape, and Ahmad Sabouri. 2022. A Data Protection-Oriented System Model Enforcing Purpose Limitation for Connected Mobility. In *Computer Science in Cars Symposium (CSCS '22), December 8, 2022, Ingolstadt, Germany.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3568160.3570231

1 INTRODUCTION

With the increasing connectivity of (autonomous) vehicles, the automotive industry is facing major changes. The current trend [21] of connecting vehicles with local infrastructures and cloud backends opens great potential for data-driven applications, improved user experiences, and new business models. Like mobile phones, cars may hold massive information about their drivers such as where they are driving, what speed they are driving at, and even whether they are tired. As a result, the vehicle changes from being a private space to being a part of the internet. Drivers' mobile lives are recorded and made available to various (3rd) parties. However, one major challenge is still to respect the users' privacy when providing data-driven applications. The problem is being addressed through several legislative initiatives from a legal perspective such as the European General Data Protection Regulation (GDPR) [29] or the upcoming ePrivacy Regulation [10]. In many cases key aspects such as transparency or purpose limitation are not technically enforced. If at all, many of them are only implemented within the processes of the data handler. However, this approach has several drawbacks. On the one hand, the realization is not enforced but rather implemented manually which may cause problems in terms of transparency, and consistency of the implemented guidelines. On the other hand, with an increasing number of 3rd parties and a rapidly changing environment around the Internet of Things (IoT) this approach is also error-prone and labour-intensive. This paper presents a data protection-oriented system model for connected mobility with the aim of technically enforcing privacy regulations. Since the GDPR is quite extensive, this paper cannot cover all aspects. While there are privacy principles in the GDPR, e. g., integrity and confidentiality of certain data that are technically feasible with state-of-the-art technologies, other principles are not as straightforward to realize, e. g., storage limitation. This paper has a specific focus on the technical implementation of "Purpose limitation" (Article 5(1)(b) GDPR) as well as "Data protection by design and by default" (Article 25 GDPR) with state-of-the-art privacy-preserving technologies. The contribution of this paper is a system model for connected mobility where the technical enforcement of purpose limitation is incorporated into the system design in an early design phase. To the best of our knowledge, there is no academic or industrial solution for the technical assurance of data-protection goals in vehicles, yet. Related applications of data tainting in the internet of things are focused on data flow analysis and enforcement, but not on purpose limitation (cf. Sect. 2). The remainder of this paper is structured as follows: Section 2 presents background and related work. Sections 3 and 4 describe the methodology and the underlying use case. The main Section 5 presents the proposed system model which is discussed and evaluated in Section 6. Section 7 concludes the paper.

CSCS '22, December 8, 2022, Ingolstadt, Germany

ACM ISBN 978-1-4503-9786-5/22/12…$15.00
https://doi.org/10.1145/3568160.3570231

RESEARCH-ARTICLE FREE ACCESS

A Data Protection-Oriented System Model Enforcing Purpose Limitation for Connected Mobility

Authors: Sarah Syed-Winkler, Sebastian Pape, Ahmad Sabouri Authors Info & Claims

CSCS '22: Proceedings of the 6th ACM Computer Science in Cars Symposium • December 2022 • Article No.: 10 • Pages 1–11 • https://doi.org/10.1145/3568160.3570231

Published: 08 December 2022 Publication History

CSCS '22: Proceedings of the 6th ACM...
A Data Protection-Oriented System Mod...
Pages 1–11
← Previous Next →
ABSTRACT
References
Index Terms
Comments

ABSTRACT

Cars are getting rapidly connected with their environment allowing all kind of mobility services based on the data from various sensors in the car. Data privacy is in many cases only ensured by legislation, i. e., the European General Data Protection Regulation (GDPR), but not technically enforced. Therefore, we present a system model for enforcing purpose limitation based on data tagging and attribute-based encryption. By encrypting sensitive data in a way only services for a certain purpose can decrypt the data, we ensure access control based on the purpose of a service. In this paper, we present and discuss our system model with the aim to improve technical enforcement of GDPR principles.

System Model
Motivation

I

Art. 25 GDPR

DATA PROTECTION BY DESIGN AND BY DEFAULT

- Controllability of the user over his personal data
- Privacy-friendly default settings
- Privacy preferences by user are reflected within system

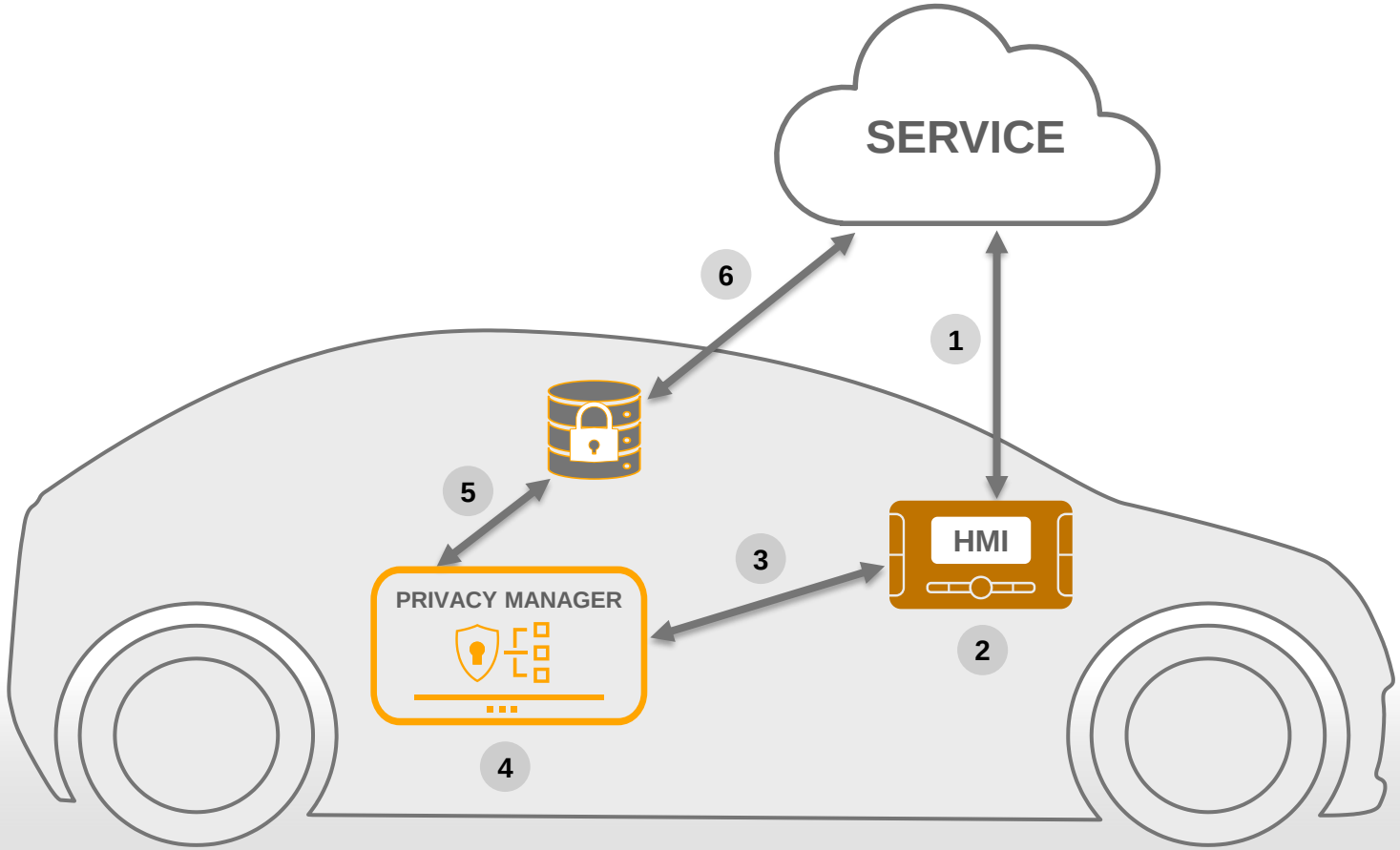
II

Art. 5(1)(b) GDPR

PURPOSE LIMITATION

- Personal data shall only be collected for specified, explicit, and legitimate purposes
- Collected data shall not be processed in a different or incompatible manner than for the initial purpose

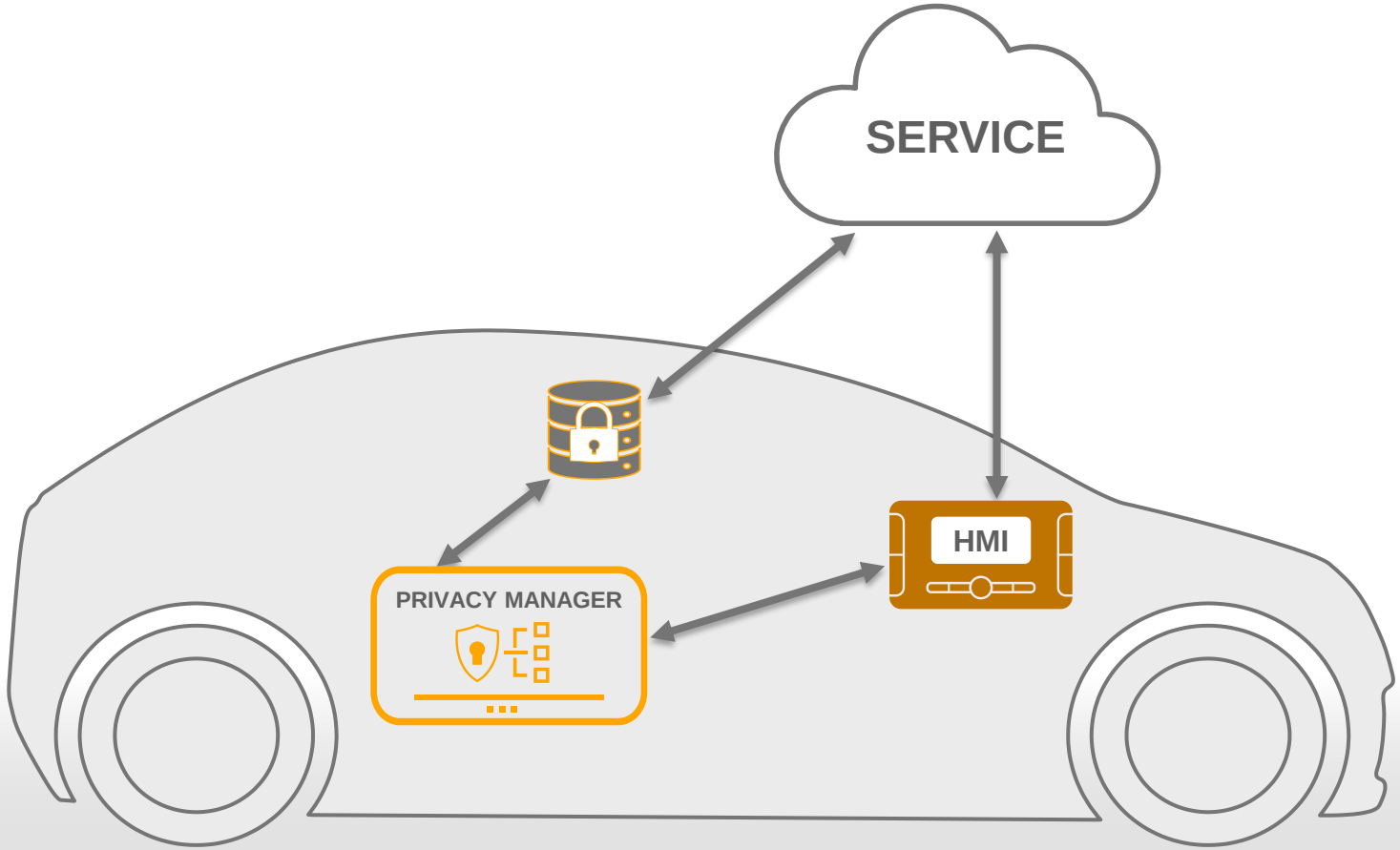
System Model
Use Case



LEGEND:

1. Service requests access to personal data
2. User sets privacy preferences
3. Update privacy policy
4. Apply PETs to data
5. Store priv. protected data in data storage
6. Access to data enabled or declined

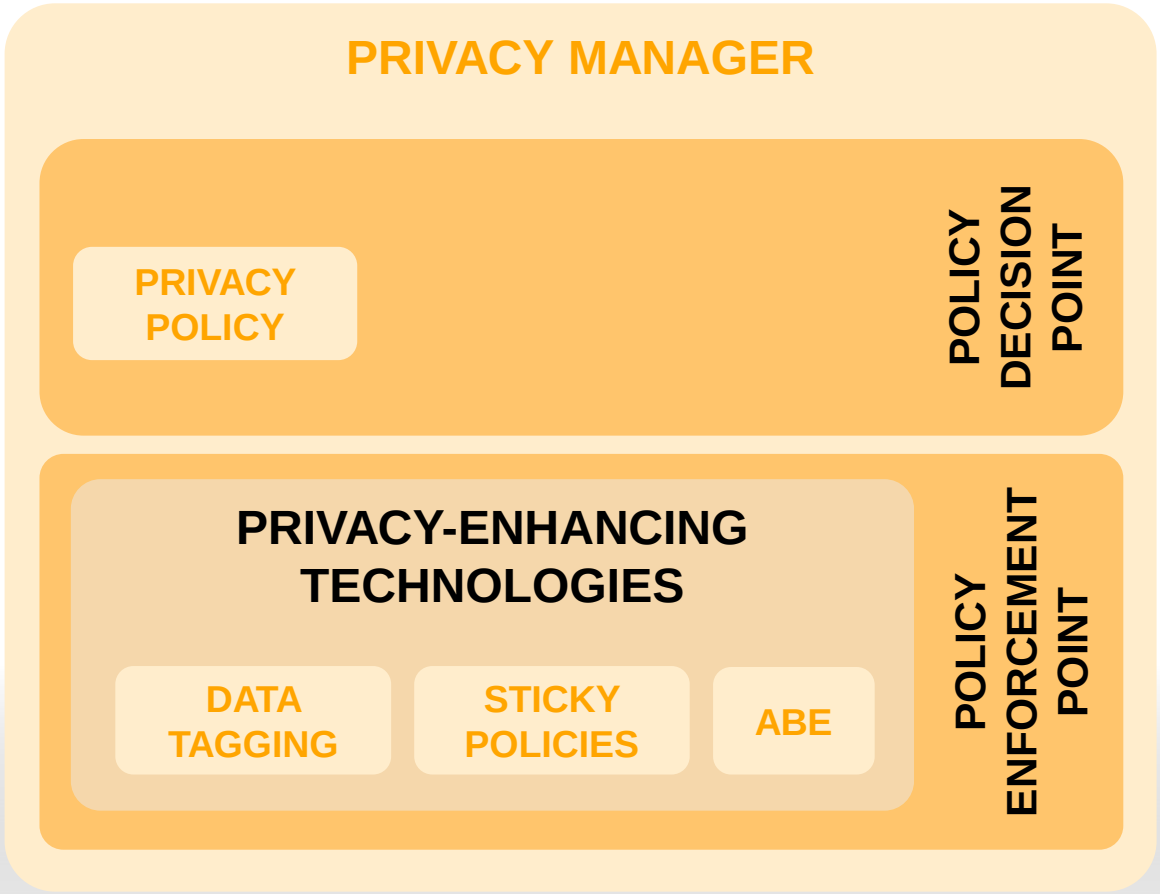
System Model
Use Case



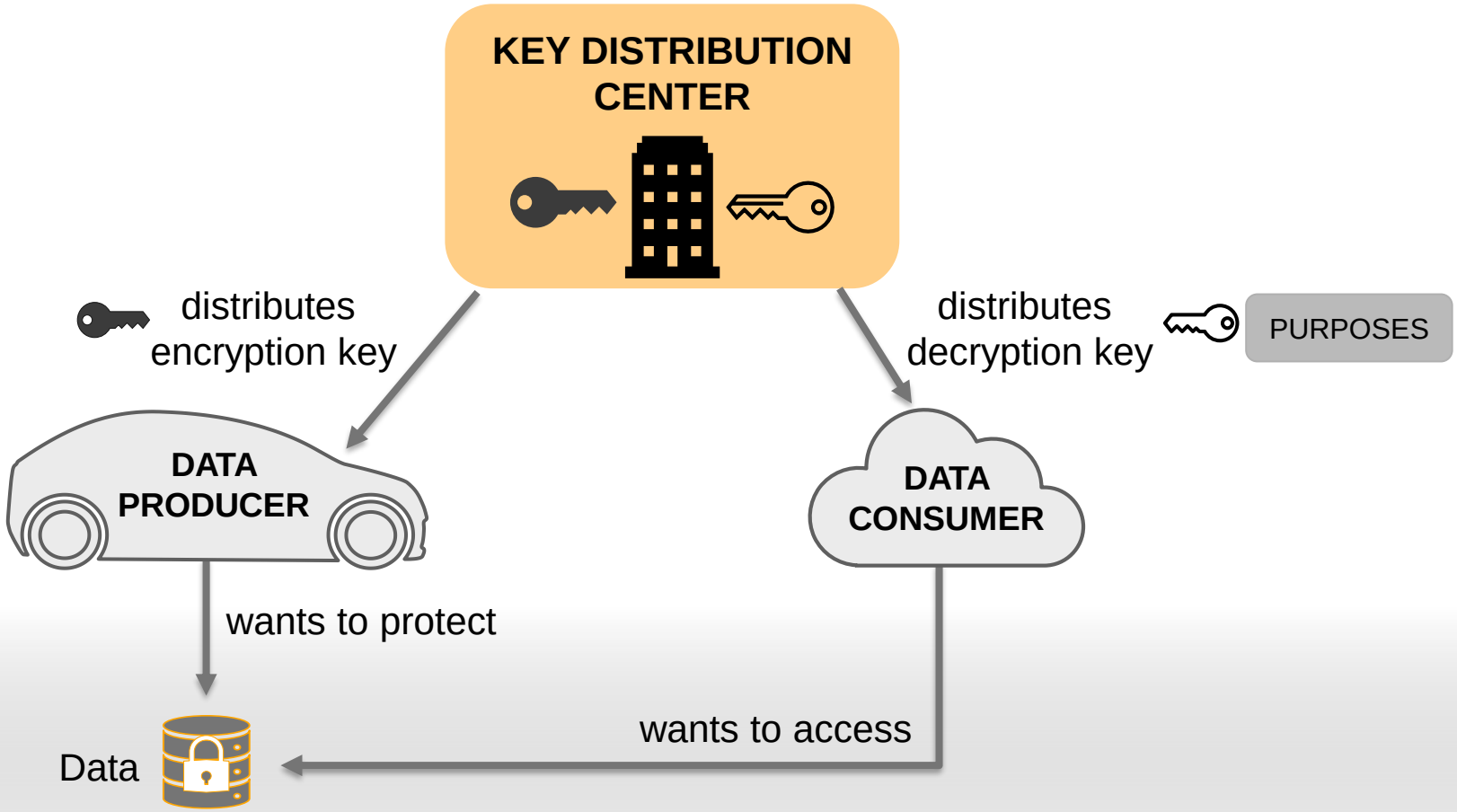
ASSUMPTIONS

- Application is running in state-of-the-art secure environment
- Data classification performed beforehand
- Mobility services are following privacy by default

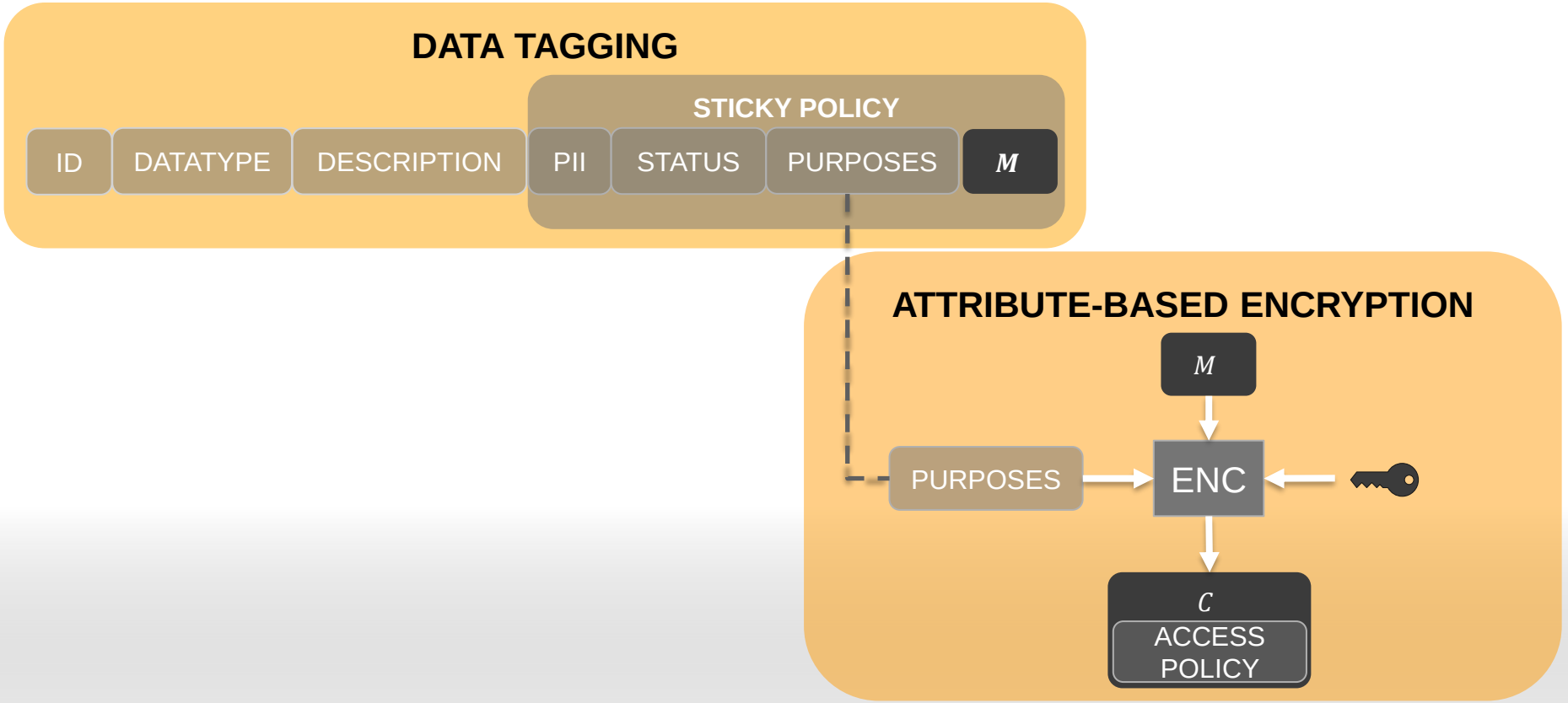
System Model
Privacy Manager



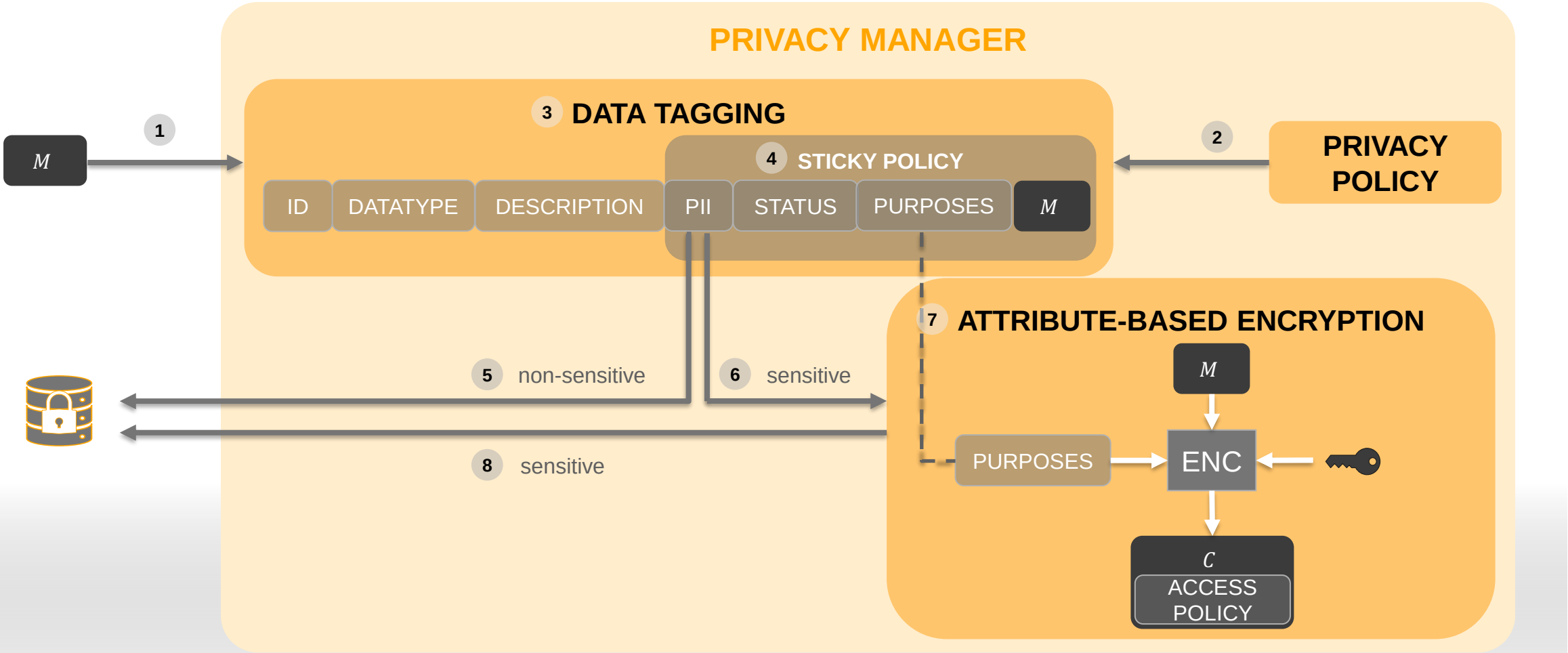
Privacy Manager
Attribute-Based Encryption



Privacy Manager
Purpose Limitation



Privacy Manager
Data Processing



Conclusion & Future Work

Purpose limitation accomplished through sticky policies and attribute-based encryption

Data protection by default and by design accomplished with the help of privacy policies and data tagging.

Future work to build **simulation** and provide proof of concept

Performance evaluation in vehicle environment

Agenda

1	Motivation
2	Challenges & Opportunities
3	Automotive Privacy at Continental
4	**Q&A**

Key Messages

(Almost) **all data in vehicles** is likely to be **personal** data, even if it does not seem that way at first glance

All Automotive Products and Mobility Services need to meet Data Protection Regulations (since 2018)

Privacy Enhancing Technologies **are enablers** for future personalized Mobility Services and Automotive Products

Privacy Enhancing Technologies open **new business opportunities**

Further investigation and collaboration with stakeholders is sought

Thanks for Listening

Any Questions?

Security & Privacy Specialist

Sarah Syed-Winkler

Continental Automotive Technologies GmbH
Product Cybersecurity & Privacy Office
Guerickestraße 7
60488 Frankfurt am Main, Germany

Phone: **+49 151 18871572**

E-Mail: **sarah.syed-winkler@continental.com**