Karlsruhe Institute of Technology

Division II – Informatics, Economics, and Society

Institute of Information Security and Dependability (KASTEL)

ANYMOS – Anonymization for Networked Mobility Systems

Mobility Services with Anonymized User Data

Data-driven Mobility

Successful scaling of the public transport in Germany requires a more efficient use of the existing infrastructure. To this end, large data volumes are needed to make detailed prognoses and smart recommendations for users without invading their privacy.

Future mobility solutions will therefore be data-driven and largely based on the needs of users. Personal data will mostly be indispensable, but are subject to data protection regulations.

Anonymous Mobility Techniques

DData are produced by autonomous driving as well as by interconnected infrastructures, such as smart traffic lights or traffic management systems that communicate with each other. Data are also collected by public passenger transport systems, examples being electronic ticket purchasing systems or cameras on trains.

The problem: While a single data source may not allow any conclusions to be drawn about individuals, the situation may change when data from several sources are linked and combined smartly with each other.

To prevent this, ANYMOS is developing ticket systems that charge for the distance covered without revealing the passenger's route. Such cryptographic solutions may help secure anonymity and are aimed at establishing anonymization as a dependable technology in the long term.

Anonymization as Enabling Technology

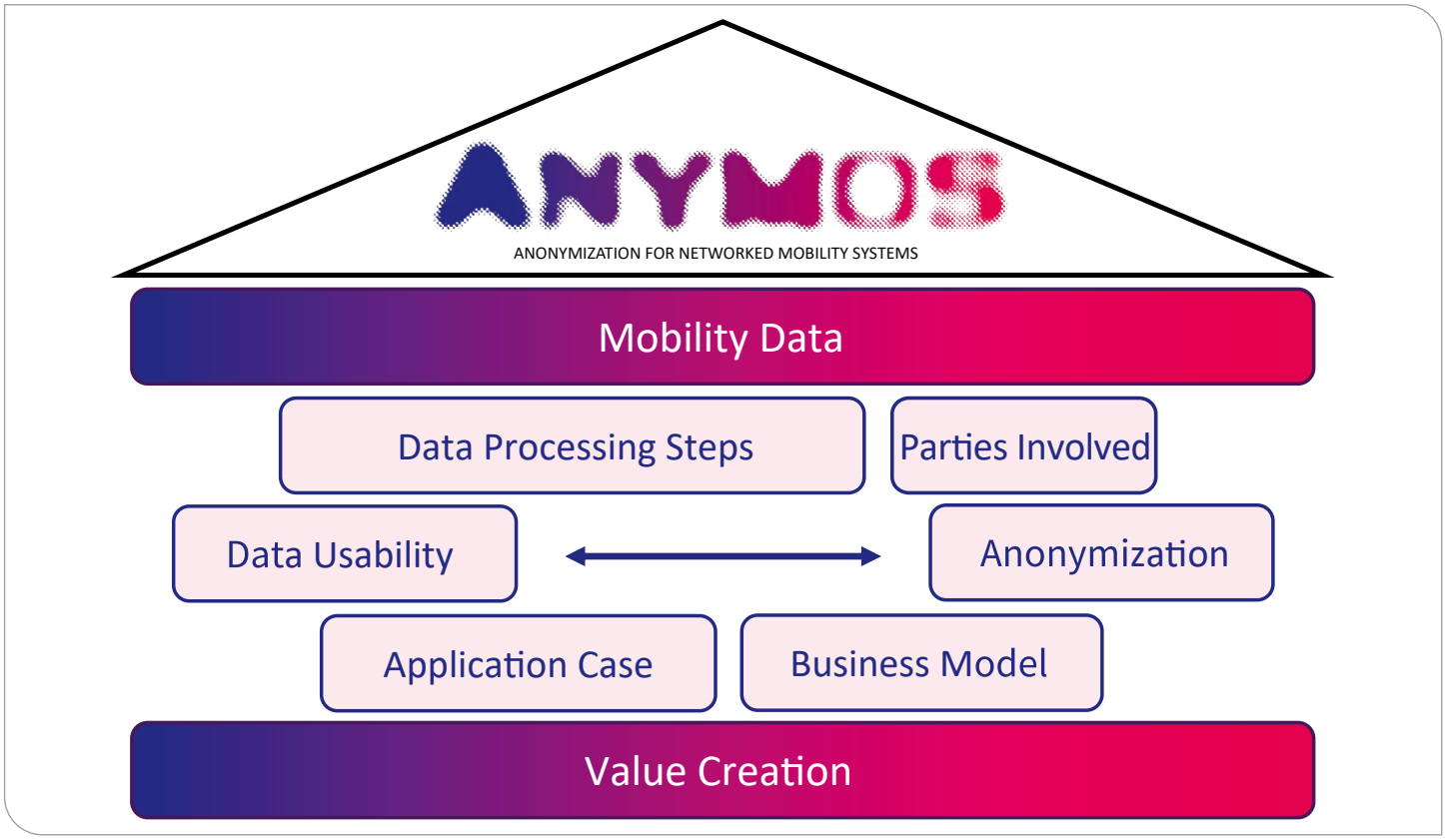
The ANYMOS competence cluster uses concrete applications to study the use of anonymization techniques while maintaining the usefulness of data. The benefit of anonymization in reducing uncertainties about the legally compliant use of personal data must not go at the expense of the usability of data for concrete applications.

Networked public passenger transport systems produce many data. (KIT/Amadeus Bramsiepe)

ANYMOS will establish a model procedure for companies to identify anonymization needs and options, select suitable state-of-the-art methods, use them correctly, and identify and assess systemic re-identification risks.

The exhibit demonstrates the anonymization procedure while maintaining data usability for various mobility applications.

ANYMOS is funded with about EUR 9 million for a duration of three years until late 2025 by the Federal Ministry of Education and Research and the European Union. Members of the ANYMOS consortium coordinated by the FZI Research Center for Information Technology are Karlsruhe Institute of Technology (KIT), Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation (IOSB), and Fraunhofer Institute for Systems and Innovation Research ISI as well as the mobility companies AVL Deutschland GmbH, DResearch Fahrzeugelektronik GmbH, init innovation in traffic systems SE, and Karlsruher Verkehrsverbund GmbH.



Overview of the ANYMOS project. (Graphical representation in German: https://anymos.de)

Karlsruhe Institute of Technology (KIT)
Institute of Information Security and Dependability (KASTEL)

Privatdozent Dr. Robert Heinrich
Am Fasanengarten 5
76131 Karlsruhe, Germany
Phone: +49 721 608-45963
Email: robert.heinrich@kit.edu

Prof. Dr. Jörn Müller-Quade
Am Fasanengarten 5
76131 Karlsruhe, Germany
Phone: +49 721 608-44327
Email: joern.mueller-quade@kit.edu

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Finanziert von der Europäischen Union
NextGenerationEU

Karlsruhe Institute of Technology (KIT) · Professor Dr. Oliver Kraft – Acting President of KIT · Kaiserstraße 12 · 76131 Karlsruhe, Germany