Designing a Distributed System for Mobility-as-a-Service

Markus Raiber [1]

Abstract: Mobility-as-a-Service (MaaS) integrates various modes of transportation into a single accessible platform to enable seamless travel. Current mobility-as-a-service solutions are built around a single operator controlling the system (for example Deutsche Bahn). This can lead to discriminatory practices, such as prioritizing services from preferred companies, charging higher fees from non-preferred companies, or limiting access to analytical data, resulting in poorer network optimization. Furthermore, the operator of the MaaS platform usually gains detailed knowledge of the usage of all partnered mobility services.

We are building an inherently decentralized MaaS system with strong security. This allows the system to operate in a nondiscriminatory way, as all participating companies have an equal stake in the operation of the system. This not only ensures discrimination-free operation of the MaaS platform, but also protects the trade secrets of all participating companies.

The decentralized nature of our system allows for reliable and fault-tolerant operation, even against misbehaving participants.

Keywords: Mobility-as-a-Service, Distributed System, Secure Multiparty Computation (MPC)
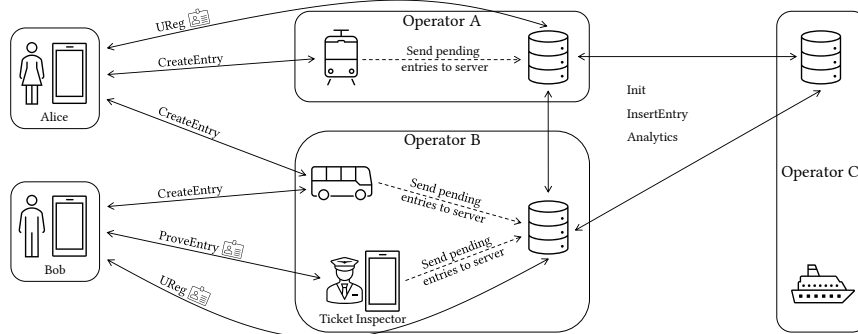
Fig. 1: Overview of our MaaS platform.

In a Mobility-as-a-Service (MaaS) platform, a variety of different modes of transportation and their operators are integrated to allow a seamless user experience. This includes planning, booking and payment processing across diverse transportation modes, such as trains, busses, rental bikes and many more. By enhancing user convenience and promoting multimodal travel, MaaS aims to reduce dependency on private vehicles, thereby alleviating urban congestion and contributing to sustainable mobility solutions. An example of such a MaaS platform is the "DB Navigator". However, since its operation is controlled by a single

---
[1] Karlsruhe Institute of Technology (KIT), KASTEL SRL, Karlsruhe, Germany, markus.raiber@kit.edu, https://orcid.org/0000-0001-6449-9494

centralized entity, it is susceptible to monopolistic misuse.[2] We provide a decentralized system that handles the booking and payment of trips across multiple mobility providers in a unified way. Additionally, our solution allows for detailed usage analytics in a privacy-friendly way, without revealing sensitive usage data, which often times is considered a trade secret, to other mobility providers.

We follow a pay-as-you-go approach, where users tap in and out of vehicles as they use them. For each such interaction, a certified entry is created, which guarantees to the operator of the vehicle that the user is allowed to participate in the MaaS system and which is used for fare calculation and usage analytics. In addition, the user can use it during spot checks to prove the presence of a valid ticket. This process is handled entirely locally between the user device (typically a smartphone) and the vehicle device, e.g., a turnstile before entering a train station or an NFC reader when entering the vehicle.

The core of our system is then the decentralized backend, where these entries are securely aggregated. For this, we employ secure multiparty computation as a way to both protect usage data, ensure correct fare calculation and distribution, and guarantee high availability even in the face of malicious (Byzantine) mobility providers.

Our system started out with a strong focus on user privacy but without any availability guarantees. This talk will be about our (still ongoing) journey from a decentralized system that provides security with abort (i.e. guarantees correctness and privacy under Byzantine faults, but not availability) to one that can also guarantee liveness.

---

[2] Deutsche Bahn has been repeatedly admonished by the Federal Cartel Office, see e.g. https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2022/20_04_2022_Bahn.html