# Implementation eines anonymen Mobility Pricing auf Basis eines Gruppensignaturschemas

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Dr. Eric Dubuis
Experte: Dr. Igor Metz (Glue Software Engineering AG)



**Mobility Pricing beschäftigt sich mit der Frage, ob Fahrgäste, die unsere Mobilitätsinfrastruktur zu den Spitzenuhrzeiten belasten, einen höheren Preis bezahlen könnten als Fahrgäste, die zu anderen Uhrzeiten unterwegs sind. Unser Projekt hat analysiert, wie in diesem Zusammenhang die Mobilitätsdaten der Kunden besser geschützt werden können.**

## Einleitung

In der Schweiz gibt es im Jahr 2017 kein Mobility Pricing. Es sind aber bereits Mobilapplikationen wie lezzgo von der BLS AG im Einsatz, die Mobility-Pricing erlauben würden. Statt vor der Fahrt ein Billett zu kaufen, muss der Kunde während der Fahrt seine Mobilapplikation aktivieren. Die Applikation generiert während der Fahrt in regelmässigen Abständen Zeit- und Ortsdaten. Diese lädt sie anschliessend zum Leistungserbringer hoch. Durch die Analyse dieser Daten kann der Leistungserbringer dem Kunden nachgelagert die Rechnung für die bezogene Leistung stellen. Die laufende Applikation gilt als gültiges Ticket.

Das Problem, das wir in unserer Arbeit analysiert haben ist, dass in diesem Modell der Leistungserbringer zwingend die Bewegungsprofile seiner Kunden kennt. Auf Basis eines Papers der Universität von Luxembourg haben wir ein anonymes Mobility Pricing System mit Vorbild der lezzgo-Applikation entwickelt. Dieses System erlaubt es, die Anonymität der Bewegungsprofile mittels eines kryptografischen Ansatzes zu schützen.

## Idee

Auf Basis des kryptografischen Schutzes besteht unser Prototyp aus der folgenden Idee:

- Es gibt eine Staatsstelle, welche ein Kryptosystem verwaltet und die Identitäten der Kunden kennt.
- Die Kunden laden ihre Zeit- und Ortsdaten anonym, aber im Kryptosystem signiert, zum Leistungserbringer hoch. Der Leistungserbringer verfügt also über alle Zeit- und Ortsdaten.

Somit hat weder die Staatsstelle noch der Leistungserbringer alle nötigen Informationen um die Anonymität der Bewegungsprofile zu brechen. Die Staatstelle hat keine Zeit- und Ortsdaten und der Leistungserbringer kennt die dazugehörigen Identitäten nicht.

## Projekt

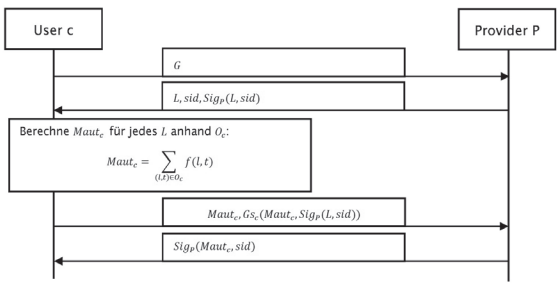
Neben der Implementation des Prototyps und den technischen Herausforderungen haben wir uns Gedanken zu den Auswirkungen dieser Idee auf das Schweizer ÖV-System gemacht. In diesem System bezahlt man nicht für die Tatsache von A nach B zu fahren, sondern man bezahlt in regelmässigen Abständen für die Tatsache, zur Zeit X am Ort Y gewesen zu sein. Wir haben Lösungsvorschläge zu den praktischen Problemen, die dieser Ansatz birgt, erarbeitet.

## Vision

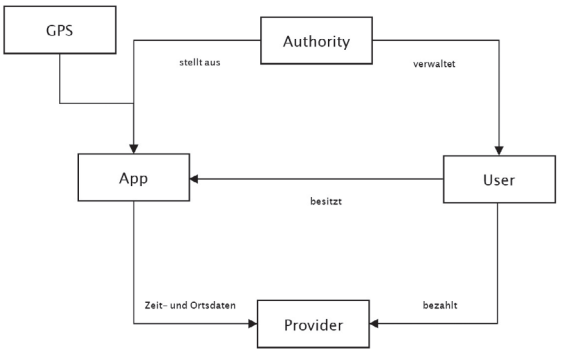
Unsere Vision ist, dass es mit einer einzigen App möglich wird, anonym Mobilitätsleistungen bei den Dienstleistern zu beziehen. Unserer Meinung nach ist es durchaus möglich, Anonymität in die bestehenden Systeme zu integrieren.

Pascal Ammon

Gabriel Simon Wyss




Das Toll Calculation Protokoll




Die Teilnehmer des Systems