

---

## - Masterthesis -

### Entwicklung eines Konzeptes zum Schutz vor unerlaubter Nutzung von Pseudonymen in der Car-to-X Kommunikation

---

#### Motivation

Seit einigen Jahren werden in der Fahrzeug-Fahrzeug und Fahrzeug-Infrastruktur Kommunikation (Car-to-X oder C2X) drahtlose Ad-hoc Netzwerke mit dem WLAN Standard eingesetzt, die es erlauben Informationen auszutauschen um unter anderem die Verkehrssicherheit zu erhöhen. Bis zum großflächigen Einsatz dieser Netze sind jedoch viele offene Fragestellungen der IT-Sicherheit zu klären. Zum Beispiel sind durch die Abwesenheit zentraler Kontrollinstanzen und den drahtlosen Schnittstellen Angriffe auf die Ad-hoc Kommunikation möglich und schwierig zu erkennen. Eine mögliche Lösung stellt die dezentrale kryptografische Absicherung der Datenübertragung mit asynchronen Schlüsseln dar, bei der alle Nachrichten beim Absenden signiert und beim Empfang verifiziert werden können. Zum Schutz der Privatsphäre bietet diese Lösung die Möglichkeit, dass jedes Fahrzeug mehrere Pseudonym-Zertifikate besitzt, die regelmäßig gewechselt werden, um eine automatisierte Rückverfolgung dessen Aktivitäten zu erschweren.

Dieser Lösungsansatz verwendet klassische Zertifikate, die jedoch nur bedingt den IT-Sicherheitsanforderungen im C2X-Kontext genügen, da ein Angreifer zum Beispiel die Möglichkeit hat mehrere Pseudonyme eines Fahrzeuges unkontrolliert gleichzeitig zu benutzen. Ein alternativer und vielversprechender Ansatz zur Einschränkung der unerlaubten Nutzung der Pseudonym-Zertifikate stellen moderne Anonymous Credential Systems (ACS) dar.

#### Ziel der Arbeit

Ziel dieser Arbeit ist es, zunächst verschiedene ACS Ansätze bzgl. ihrer Potentiale zur Nutzungseinschränkung der Pseudonyme in C2X-Kommunikation zusammenzustellen und auszuwerten. Aufbauen auf der Analyse soll ein existierendes ACS Schema, das die zuvor beschriebenen Probleme lösen kann, angepasst, prototypisch implementiert und evaluiert werden.

#### Voraussetzungen

- Gute analytische Fähigkeiten, Selbstständiges Arbeiten, Kenntnisse in IT-Sicherheit, Sicherer Umgang mit englischsprachiger Fachliteratur und Programmiererfahrung in Java sowie anderen Programmiersprachen.
- Kenntnisse in Ad-hoc Netzwerken, Übertragungstechnik und Netzwerkprotokollen sind von Vorteil

#### Kontakt

Bei Interesse kontaktieren Sie bitte Norbert Bißmeyer oder Hervais Simo  
Fhom  
Fraunhofer SIT  
Rheinstraße 75, Raum 110  
E-Mail: [norbert.bissmeyer@sit.fraunhofer.de](mailto:norbert.bissmeyer@sit.fraunhofer.de)  
[hervais.simo@sit.fraunhofer.de](mailto:hervais.simo@sit.fraunhofer.de)

Tel: +49 6151 869 324 oder 6151 869 60041