Datenschutz in IVS

Anna Sinitsyna

Zentrum für Angewandte Rechtswissenschaft (ZAR)
Betreuender Mitarbeiter: Ref. iur. Leonie Sterz

Abstract

Abbildungsverzeichnis

1 Einleitung

Das 21. Jahrhundert bringt mit sich verschiedene Herausforderungen, die wir als Gesellschaft meistern müssen - Klimawandel, steigende Population, Umweltverschmutzung und viel mehr. Um sie zu bewältigen brauchen wir neue Technologien, die uns im Alltag unterstützen und dabei helfen, die individuelle Verantwortungslast zu reduzieren. Darum ist der effiziente und baldige Einsatz Intelligenter Verkehrssysteme ein wichtiger Bestandteil deutscher Verkehrspolitik. Im Mittelpunkt hierbei stehen intelligente Fahrzeuge und andere Straßenanlagen, die durch Kooperation miteinander den Straßenverkehr effizienter, sicherer und umweltfreundlicher gestalten [3].

In näher Zukunft werden nach und nach im Alltag Fahrzeuge eingeführt, die miteinander (Car-to-Car, kurz C2C) und mit der Infrastruktur (Car-to-Infrastructure, kurz C2I) kommunizieren können. Der Oberbegriff zu dieser Art der Kommunikation lautet Car-to-X (C2X). Der Datenaustausch in solchen Kooperativen Intelligenten Transportsystemen (C-ITS) findet statt, um Unfälle auf den Straßen zu vermeiden und damit die Sicherheit im Straßenverkehr zu gewährleisten. Dafür senden Fahrzeuge gegenseitig verkehrsrelevante Daten, wie zum Beispiel Beschleunigung, Geschwindigkeit, Länge und Gewicht des Fahrzeugs. Diese Daten werden verwendet, um ein Verkehrslagebild zu erstellen und zu verteilen, damit teilnehmende Fahrzeuge stets die aktuellsten Informationen besitzen und auf eintretende Verkehrssituationen geeignet reagieren können.

Diese neue Problemstellung bringt einige datenschutzrechtlichen Fragen mit sich, die einen geeigneten Rechtsrahmen benötigen. Es soll sowohl den technischen Schutzzielen der Informationssicherheit nachgekommen werden (Vertraulichkeit und Integrität), als auch den rechtlichen Vorschriften, z.B. der Datenschutz-Grundverordnung (DSGVO). Das Ziel von dieser Seminararbeit ist es, die datenschutzrechtliche Relevanz der C2X-Kommunikation zu untersuchen. Dafür wird zuerst die technische Funktionsweise der C2X-Kommunikation erläutert, mit Schwerpunkt Nachrichtenformate und Public-Key Kryptografie. Außerdem wird die Public-Key Infrastruktur in Europa beschrieben, die den Betrieb der C-ITS praktisch ermöglicht.

Anschließend wird auf die Herstellbarkeit des Personenbezugs eingegangen, da sie entscheidend für die Wirkung der DSGVO ist. Es werden Möglichkeiten diskutiert, wie man aus den grundsätzlich nicht-personenbezogenen Daten, die in einer C-ITS generiert und gesammelt werden, das Fahrzeug und ggf. den Fahrzeughalter identifizieren kann. Im Zusammenhang damit werden technische Möglichkeiten für die Generierung der individuellen Bewegungs- und Verhaltensprofile erläutert. Im Abschluss wird die Vereinbarkeit mit datenschutzrechtlichen Prinzipien diskutiert und es werden Datenschutzmaßnahmen vorgeschlagen, die das Nachkommen der gesetzlichen Pflichten ermöglichen.

2 Hintergrund

Bereits seit etwa Mitte der 2000er existieren einige technischen Lösungen für die Nahbereichskommunikation zwischen Fahrzeugen und ggf. Infrastrukturkomponenten. Zum Beispiel, die IEEE 802.11p ist eine WLAN-Variante, die aktuell in Europa als Funkstandard für Kooperative Intelligente Verkehrssysteme (C-ITS) gilt. Weiterhin existieren mehrere Spezifikationen des ETSI (Europäisches Institut für Telekommunikationsnormen), die unter anderem Nachrichtenformate festlegen [12].

Das Ziel der C-ITS ist es vor allem, den Verkehrsfluss zu verbessern und Unfälle vorzubeugen. Die Autofahrer sollen so früh wie möglich vor Gefahren auf der Fahrstrecke gewarnt werden, selbst wenn diese noch nicht im Sichtbereich sind. So können sie entsprechend reagieren und ihr Fahrverhalten frühzeitig anpassen, um Staus oder sogar zusätzliche Unfälle zu vermeiden. Als ein Beispiel im C-ITS Kontext kann man Sonderfahrzeuge nehmen (z.B. Kranken- oder Feuerwehrwagen) - diese sollten eine sogenannte "Blaulichtnachricht"versenden und somit andere Fahrzeuge darauf hinweisen, dass sie eine Rettungsgasse bilden sollten. Die C2X-Nachrichten auf Basis von 802.11p haben eine Reichweite von bis zu 800 Metern, was herkömmliche Sirenen von z.B. Krankenwagen weit übersteigt, besonders in dicht bewohnten Stadtgebieten.

Die EU hat bereits vor zehn Jahren eine Rechtsgrundlage für intelligente Verkehrssysteme geschaffen. Es handelt sich um die RL 2010/40/EU zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (IVS-RL) [1]. In November 2016 wurde von der Europäischen Kommission

[1] Jochum: Verkehrsdaten für intelligente Verkehrssysteme ZD 2020, 497

eine Strategie für Kooperative Intelligente Verkehrssysteme geschaffen [9], mit der ein praktisches Rahmen für eine Einführung von C-ITS in Europa definiert wurde.

Die Initiativen zur Standardisierung der C2X-Kommunikation liegen jedoch weiter in der Vergangenheit. Bereits in 2002 wurde der Car-2-Car Communication Consortium gegründet (C2C-CC) [4], dem die meisten Fahrzeughersteller und große Zulieferer beigetreten sind. Das Ziel davon ist es, die C2C-Kommunikation zu standardisieren und den Rollout im europäischen Markt voranzutreiben. In 2019 wurde ein wichtiger Meilenstein auf diesem Weg erreicht, da die ersten Fahrzeuge mit kooperativer C2X für den Markt frei verfügbar gemacht wurden. Hier geht es um sogenanntes Day-1 Enrolment, den ersten Schritt auf der Roadmap von C-ITS. Die drei Phasen davon werden in der Tabelle 1 näher beschrieben.

	Day 1	Day 2	Day 3
Fokus	Awareness driving	Sensing driving	Cooperative driving
Beispiele	• Warnung vor langsamen oder stehenden Fahrzeugen • Warnung vor Straßenarbeiten • Warnung vor sich nähernden Einsatzfahrzeugen • Anzeige von Verkehrszeichen im Fahrzeug • Anzeige Missachtung von Verkehrsampeln / Sicherheit auf Kreuzungen	• Überholwarnung • Erweiterte Sicherheit auf Kreuzungen • Kooperative adaptive Geschwindigkeitsregelung • Warnung vor langfristigen Straßenarbeiten • Spezielle Fahrzeugpriorisierung	• Kooperatives Überholen • Kooperativer Spurwechsel • Platooning

Tabelle 1: Phasen der Einführung von C-ITS-Diensten übersetzt nach [4]

Auf Ersuchen der Europäischen Kommission wurde eine Studie durchgeführt, in welcher die Kosten und den Nutzen der durch C-ITS unterstützten Dienste für den Straßenverkehr in den Mitgliedstaaten untersucht wurde [1]. Im Ergebnis wurde erwiesen, dass bei einer europaweiten Einführung von Day 1 C-ITS-Diensten im Zeitraum 2018 bis 2030 das Nutzen-Kosten-Verhältnis bis zu 3:1 betragen wird (falls die Interoperabilität zwischen den Mitgliedsstaaten sichergestellt wird). Dies bedeutet, dass jeder in die für den Day 1 vereinbarten C-ITS-Dienste investierte Euro einen Nutzen von bis zu drei Euro generieren dürfte.

Wie oben erwähnt, wurden die Day 1 Dienste bereits eingesetzt und sind im europäischen Markt verfügbar. Der Einsatz von Day 2 und Day 3 hingegen befindet sich in der Forschungsphase, die ebenfalls von Car-2-Car Communication Consortium (C2C-CC) vorangetrieben wird. Ein von C2C-CC definierter Meilenstein ist eine Marktpenetration von 3%-5%, da ab dann die ersten Vorteile von kooperativem C2X von den Nutzern gespürt werden können [4]. Daher verfolgt C2C-CC folgende Ziele, um diese Entwicklung voranzutreiben:

- Interoperabilität und grenzübergreifende Nutzung von Car-to-Car-Systemen
- Entwicklung der realistischen Strategien und Geschäftsrahmen für die Einführung von C2X
- Kooperation mit der Straßeninfrastruktur zur Entwicklung und Bereitstellung von C2I in der Automobilindustrie
- Zuweisung eines gebührenfreien europaweiten exklusiven 5,9-GHz-ITS-Frequenzbandes für kooperative V2X-Anwendungen
- Weltweite Standardisierung von kooperativen C2X Systemen, insbesondere in Kooperation mit ETSI TC ITS

3 Technische Funktionsweise der C2C-Kommunikation

Im folgenden Abschnitt wird die Funktionsweise der C2C-Kommunikation und die dafür benötigte Infrastruktur näher beschrieben. Zuerst wird in Kapitel 3.1 der Standard WAVE vorgestellt, der die moderne C-ITS Kommunikation definiert, und deren Bausteine werden näher beschrieben. Das Ziel von diesem Standard ist es, eine einheitliche Schnittstelle für die Car-to-Car und Car-to-Infrastructure, bzw. Nahbereichskommunikation zu ermöglichen.

Im Abschnitt 3.2 wird die Public-Key Infrastruktur (PKI) beschreiben, die für den sicheren Nachrichtenaustausch zwischen den Verkehrsteilnehmern essenziell ist. Es wird auf die kryptografischen Prozesse und auf die organisatorische Stellenhierarchie eingegangen, die für die Implementierung einer PKI nötig sind. Abschließend werden einige Besonderheiten der europäischen PKI erwähnt.

Im Abschnitt 3.3 wird auf die Nachrichtenformate der C2C-Kommunikation eingegangen, sowie auf die darin gespeicherten Daten, die möglicherweise zur Identifikation des Fahrzeugs benutzt werden können. Dieses technische Thema bildet eine Grundlage für Herstellbarkeit des Personenbezugs aus den Fahrdaten, deren Möglichkeit in weiteren Kapiteln analysiert wird.

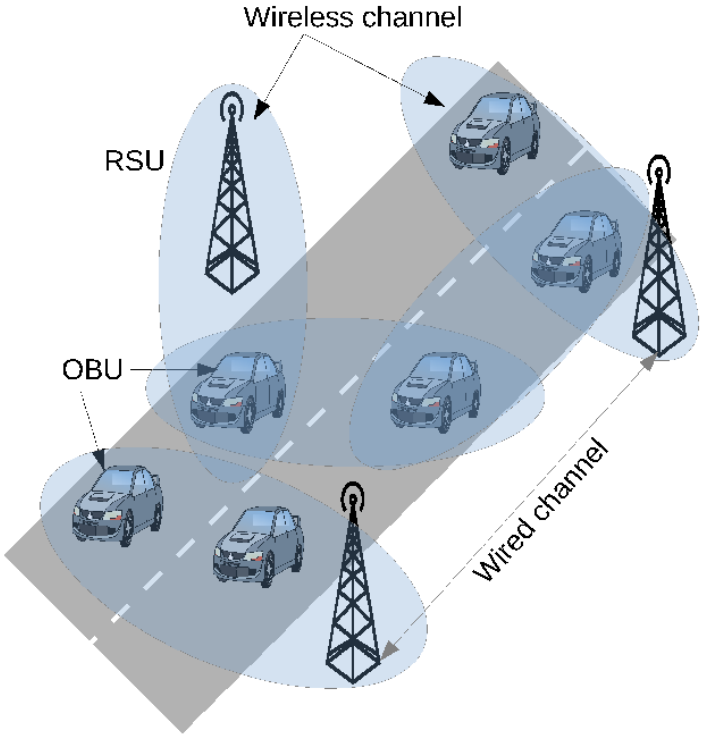

Abbildung 1: Überblick über die WAVE Architektur [11]

3.1 Standard for Wireless Access in Vehicular Environments (WAVE)

Wie vorhin erwähnt, besteht eine C-ITS nicht nur aus Fahrzeugen, die miteinander kommunizieren, sondern auch verschiedenen anderen Infrastrukturkomponenten (z.B. Ampelanlagen und intelligente Verkehrsschilder). Da sowohl Fahrzeuge als auch Infrastrukturkomponenten von verschiedenen Herstellern produziert werden, wird ein gemeinsamer Standard benötigt, um reibungslose Kommunikation und Datenaustausch zu gewährleisten. Daher hat das IEEE Konsortium eine Reihe von Standards geschaffen, die gemeinsam *IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE)* genannt werden [13]. WAVE beschreibt die Architektur, Kommunikationsmodelle, Verwaltungsstrukturen und Sicherheitsmechanismen im Kontext von C-ITS. Der vorher erwähnte WLAN-Funkstandard IEEE 802.11p ist ebenfalls ein Baustein von WAVE und wird hier als ein einheitlicher Standard für Nahbereichskommunikation verwendet.

Die zwei Hauptkomponenten der WAVE Architektur sind *On Board Unit (OBU)* - ein direkt im Fahrzeug installiertes Computer- und Sendegerät, und am Straßenrand installiertes *Road Side Unit (RSU)* - siehe Abbildung 1. Die OBUs tauschen Nachrichten mit anderen Fahrzeugen in der Nähe durch einen direkten Kanal aus, und falls das Zielfahrzeug zu weit weg ist aber sich trotzdem im gleichen Netz befindet, kommunizieren sie durch mehrere Hops [11]. Die Fahrzeuge können sich durch RSUs am Straßenrand mit dem Internet verbinden.

3.2 Public-Key Infrastruktur

Der oben beschriebene Nachrichtenaustausch zwischen Fahrzeugen beruht auf Public-Key Kryptografie, somit werden die Nachrichten mit einer Signatur und einem Zertifikat versehen, die von einer zentralen Stelle ausgegeben werden. Eine kryptographische Signatur ist (analog zu einer Unterschrift) eine Bestätigung, dass die Nachricht tatsächlich von dem Versender stammt und nicht auf dem Weg verändert wurde. Der Empfänger kann dies überprüfen, in dem er die zentrale Stelle kontaktiert und eine Authentizität-Anfrage macht. Die Integrität der Nachricht kann er direkt durch die Signatur verifizieren. Allerdings werden die Nachrichten selbst nicht verschlüsselt und können von allen Verkehrsteilnehmern gelesen werden. Das heißt, dass alle darin enthaltenen Daten ebenfalls von jedem mitgelesen können, was zu datenschutzrechtlichen Problemen führen könnte.

Um den Nachrichtenaustausch zu ermöglichen, braucht man eine entsprechende Public-Key Infrastruktur (PKI), die aus einer oder mehreren Certification Authorities (CAs) besteht. Eine CA ist eine zentrale Stelle die in der Lage ist, digitale Zertifikate zu produzieren, diese Zertifikate den End-Entitäten zu erteilen und später ihre Authentizität zu verifizieren. Als End-Entitäten versteht man ITS-Stationen (u.a. Fahrzeuge), die die erstellten Zertifikate für die Kommunikation untereinander verwenden. Es gibt zwei Arten von Zertifikaten: ein langlebiges Enrolment Credential (EC) und ein kurzzeitgültiges Authorization Ticket (AT). Die Pseudonymität des Datenaustauschs wird durch ständigen Wechsel des ATs gewährleistet, womit die Nachricht signiert wird. Der Enrolment Credential wird hingegen nicht mit der Nachricht übertragen und ist nur den PKI Komponenten bekannt [12].

Die PKI wird aus drei Stufen zusammengesetzt [10]:

- Root-CAs (erstellen Zertifikate für untergeordnete CAs)
- Mindestens zwei Sub-CAs
- End-Entitäten (EEs)

Darüber hinaus gibt es zwei Arten von Sub-CAs: Enrolment Authorities (EA) und Authorization Authorities (AA). Die EAs erstellen langlebige Zertifikate für End-Entitäten, die für die Authentifizierung innerhalb der PKI verwendet werden - Enrolment Credentials (ECs). Die AAs hingegen stellen kurzzeitige Zertifikate zur Verfügung, mit denen die End-Entitäten (z.B. Fahrzeuge) untereinander kommunizieren können ohne die Pseudonymität von einzelnen Entitäten zu verletzen - Authorization Tickets (ATs). Der schematische Aufbau von einer PKI wird in der Abbildung 2 verdeutlicht.

Bevor jegliche Kommunikation stattgefunden hat, muss sich die End-Entität (EE) zunächst bei der zugehörigen Enrolement Authority (EA) registrieren und ein Enrolment Credential (EC) erhalten, das mehrere Jahre gültig ist. Die EA bekommt dabei die Registrierungsinformationen von der EE, zum Beispiel ihre Fahrzeugidentifizierungsnummer und ihren öffentlichen Schlüssel. Diese Information wird verschlüsselt übermittelt und ist nicht öffentlich verfügbar. Die EE signiert den initialen Zertifikatsrequest mit ihrem eingebauten

[2] *Strubbe*, In: DuD 2017, 223

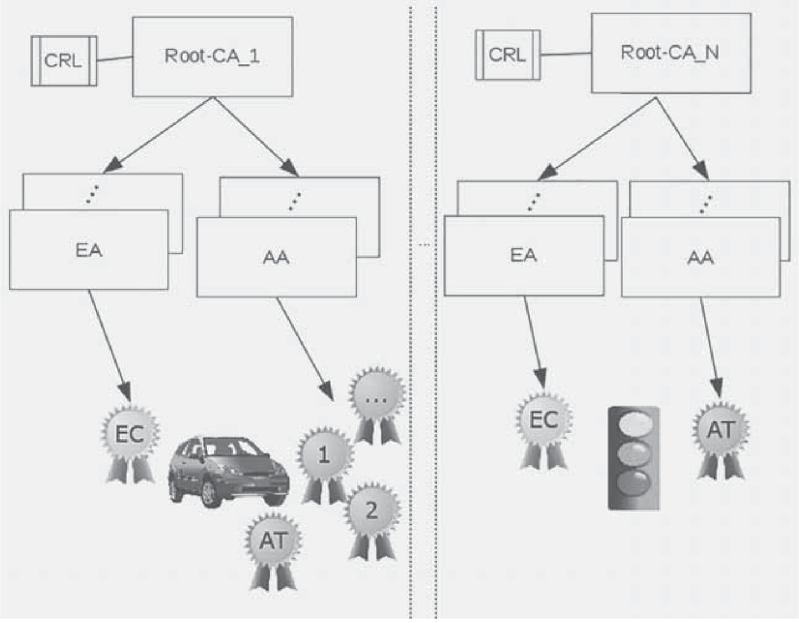

Abbildung 2: Aufbau einer PKI für C2X Kommunikation [2]

privaten Schlüssel und übermittelt ihn an die EA. Falls die Daten übereinstimmen, erhält die EE einen Enrolment Credential.

Mit einem validen EC kann die EE weiterhin kurzzeitgültige Authorization Tickets (AT) bei der Authorization Authority (AA) beantragen. ATs sind wie vorhin beschrieben kurzzeitgültige Zertifikate für C2X Kommunikation, die oft gewechselt werden und somit der Senderpseudonymität dienen. Die Nachrichten sollten keinen eindeutigen Identifikator erhalten, damit kein Personenbezug hergestellt werden kann. Daher werden sie mit ATs signiert und nicht mit den langlebigen ECs, die für ein Fahrzeug über mehrere Jahre gültig ist.

Ein AT wird von einer Entität bei der AA beantragt. Die Anfrage an die AA enthält unter anderem verschlüsselte Daten, die nur von der entsprechenden Enrolment Authority (EA) ausgelesen werden können [6], darunter das langlebige EC von der Entität. Eine AA kann diese Daten nicht auslesen, da sie verschlüsselt sind, also leitet sie diesen Teil der Anfrage an die zugehörige EA. Die EA entschlüsselt die Daten, bestätigt die Authentizität der End-Entität mit dem angehängten EC und schickt eine Statusmeldung an die AA, ohne diese zusätzliche Information preiszugeben. Es ist wichtig, die EA und AA organisatorisch getrennt zu halten, da sonst bei der AT-Anfrage eine Zuordnung zu der End-Entität bzw. ihrem EC möglich wäre.

Nachdem die mit dem AT signierte Nachricht erfolgreich an die empfangende EE übermittelt wurde, nutzt sie den AT um die Nachricht zu verifizieren. Dies erfolgt mittels einer Kettenprüfung durch die AA und die entsprechende Root-CA, wodurch die Authentizität der Nachricht festgestellt wird.

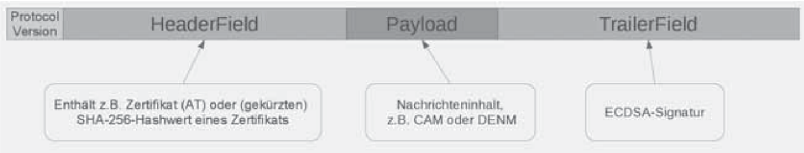

Abbildung 3: Grobaufbau einer verschlüsselten Nachricht [4]

In Europa ist zusätzlich zu der oben beschriebenen PKI eine globale Vertrauensliste vorgesehen, die innerhalb der europäischen Grenzen alle vertrauenswürdige Root-CA-Zertifikate beinhaltet. Diese wird von einem zentralen Trust List Manager erstellt und elektronisch signiert. Somit wird die Interoperabilität von europäischen PKIs über Grenzen sichergestellt, was durch die IVS-RL vorgeschrieben wird[3]. Darüber hinaus ist es wichtig, die nicht mehr vertrauenswürdigen Zertifikate zurückziehen zu können - dies wird durch sogenannte Certificate Revocation Lists sichergestellt. Diese werden allen PKI-Teilnehmern von der jeweiligen Root-CA zur Verfügung gestellt und enthalten die Liste mit allen revozierten Zertifikaten.

3.3 Nachrichtenformate

Die Nachrichtenformate, die für die oben beschriebene PKI nötig sind, wurden von dem Europäischen Institut für Telekommunikationsnormen (ETSI) definiert. Im Weiteren wird auf [6] verwiesen, in dem die Paketstruktur für gesicherte C2X-Nachrichten und deren Zertifikatsformat festgelegt wurde.

Der grobe Aufbau einer gesicherten C2X-Nachricht wird in der Abbildung 3 dargestellt. Sie enthält unter anderem die ECDSA-Signatur ([2]), den Verifikationsschlüssel des Senders und die eigentliche Nachricht, die im Payload gespeichert ist. Für die Car-2-Car Kommunikation sind zurzeit zwei Nachrichtenformate vorgesehen:

- die Cooperative Awareness Message (CAM) und die
- Decentralized Environmental Notification Message (DENM) [14].

CAMs werden von End-Entitäten in regelmäßigen Abständen verschickt, um kooperative Wahrnehmung voneinander zu verschaffen (ab Day 2 Enrolment) . Aktuell in Day 1 können sie etwa für eine Erstellung eines lokalen Verkehrslagebildes benutzt werden. Die DENMs hingegen werden in potentiell gefährlichen Situationen verwendet, um die Teilnehmer über verschiedene Verkehrsereignisse zu informieren - z.B. Staus, Rettungsarbeiten und -fahrzeuge, Straßenbauarbeiten usw.

Im Weiteren wird nur die CAM betrachtet, da die DENM keine personenbezogenen Daten beinhaltet und im datenschutzrechtlichem Sinne kein Problem darstellt [7]. Der Aufbau einer CAM wird in der Abbildung 4 dargestellt. Sie besteht aus vier Elementen: Header, CAM Information, Signature und Certificate. Die tatsächliche Information über das

[3] *Jochum*, In: ZD 2020, 497
[4] *Strubbe*, In: DuD 2017, 223

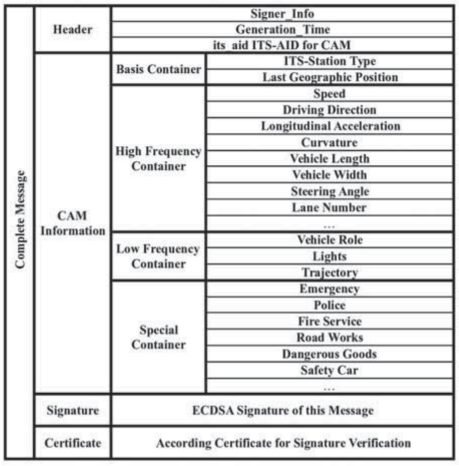

Abbildung 4: Detallierter Aufbau einer CAM [5]

Fahrzeug wird im Block CAM Information gespeichert. Er beinhaltet sowohl dynamische Daten (z.B. Last Geographic Position, Speed) als auch statische Daten über das Fahrzeug, die trotz ständigem Pseudonymwechsel identisch bleiben (z.B. Length, Weights). Eine CAM erhält keinen primären Identifikator, aufgrund dessen eine eindeutige Zuordnung zum Fahrzeug möglich wäre.

4 Anwendbarkeit der DSGVO

Die Datenschutzgrundverordnung (DSGVO) ist eine Verordnung, mit der die Regeln zur Verarbeitung personenbezogener Daten in der Europäischen Union vereinheitlicht werden. Sie ist am 25. Mai 2018 in Kraft getreten und hat zu dem Zeitpunkt geltende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ersetzt.

In diesem Abschnitt wird diskutiert, ob die Erhebung von Fahrdaten in einer PKI ein datenschutzrechtliches Problem darstellt, und geprüft, ob die DSGVO in diesem Fall anwendbar ist. Des Weiteren werden mögliche Angriffe auf die Pseudonymität der Nachrichten aufgeführt, aufgrund deren Bewegungsprofile von Fahrzeugen erstellt werden können. Aktuell ist die Infrastruktur so konstruiert, dass Fahrzeuge Nachrichten und Zertifikate pseudonym versenden, und keine Zuordnung von mehreren über einen längeren Zeitraum versendeten Nachrichten zu einem Fahrzeug technisch möglich ist. Allerdings gibt es andere Methoden, wodurch solch eine Zuordnung ohne Zustimmung des Fahrers realisiert werden kann, diese werden im Abschnitt 4.1 beschrieben. Darüber hinaus wird die Anwendbarkeit der DSGVO auf die in CAMs erhaltenen Fahrdaten diskutiert. Falls diese Daten personenbezogen sind, beziehungsweise für eine eindeutige Identifizierung der Person benutzt werden können, fällt ihre Verarbeitung unter DSGVO. Die Datenschutz-

[5] *Kiometzis*, In: DuD 2017, 227

rechtliche Bedeutung von Bewegungsprofilen wird im Abschnitt 4.2 diskutiert, und die Möglichkeit zur Herstellung des Personenbezugs wird im Abschnitt 4.2 analysiert.

4.1 Datensammlung und -auswertung

Auch wenn CAMs keine primären Identifikationsmerkmale erhalten, existieren es mehrere Möglichkeiten, um mehere CAMs von einem Fahrzeug miteinander zu verbinden und damit ein Bewegungsprofil von diesem Fahrzeug zu erstellen. Dies kann zu diversen Risiken für die Privatsphäre führen, falls der Personenbezug von diesen Fahrdaten hergestellt werden kann, da der gesamte Fahrweg einer Person offengelegt wird. Im folgenden Abschnitt werden einige Angriffsarten auf die Pseudonymität von CAMs näher beschrieben und analysiert.

Als erstes Beispiel sei ein sogenannter 'Big Brother Angreifer' angeführt, der eine Infrastruktur von Empfangseinrichtungen in einer geografischen Region betreibt und in der Lage ist, in dieser Gegend CAMs von Fahrzeugen zu erfassen und auszuwerten. Das wäre möglich, indem der Angreifer zum Beispiel eine Fahrzeug-Flotte aufstellt, die eingehende CAMs an einen zentralen Server übermittelt. Auch wenn vorbeifahrende Fahrzeuge ihr Pseudonym jede zehn Sekunden ändern würden, könnten sie mit solch einer Infrastruktur verfolgt werden [17]. Da diese Art von Überwachung alle Fahrzeugdaten in der Gegend erfassen würde, könnte sie für breitere Verkehrsanalysen genutzt werden.

Darüber hinaus gibt es einige Möglichkeiten, die Bewegungen von einzelnen Fahrzeugen detailliert aufzuzeichnen. Zum Beispiel kann man mithilfe eines sich mit dem Fahrzeug bewegendes Überwachungstools sogenannte CAM-Traces (Bewegungsprofile) erstellen, d.h. die gefahrene Strecke eines Fahrzeugs und alle von ihm auf dieser Strecke erstellten CAMs. Auch wenn das Fahrzeug regelmäßig seinen Signaturschlüssel wechselt, würde es reichen, nur eine CAM aus der CAM-Trace dem Fahrzeug eindeutig zuzuordnen, um die gesamte CAM-Trace diesem Fahrzeug zuzuordnen [7].

Es existiert eine Reihe von Methoden, um diese Zuordnung technisch durchzuführen. In [15] wurde dargelegt, dass sie aufgrund der sog. Secondary Vehicle Identifier erfolgen kann. Diese wird von diversen drahtlosen Schnittstellen im Auto zur Verfügung gestellt (z.B. eine Headunit, die eine öffentliche Bluetooth-Schnittstelle mit einem nutzerfreundlichen Namen besitzt). Die Secondary Vehicle Identifiers sind einfach zu erfassen und können einer eindeutigen Zuordnung der empfangenen CAM-Trace zum Fahrzeug dienen.

4.2 Bewegungsprofile und Verhaltensprofile

Wie vorhin erwähnt, erhalten CAMs keine primären Identifikationsmerkmale, jedoch ist es möglich, mithilfe von einer geeigneten Infrastruktur Bewegungsprofile von Fahrzeugen zu erstellen. Außerdem enthalten CAMs statische Attribute wie zum Beispiel die Fahrzeuglänge und dessen Gewicht, die eine zusätzliche Kennzeichnung von einem Fahrzeug erlauben. So wäre es unter Umständen möglich, ein bestimmtes Modell von einem bestimmten Hersteller nur aus der CAM zu erkennen. In wenig befahrenen Gebieten kann

dies zu einer eindeutigen Identifizierung von dem Fahrzeug und einer Zuordnung zum ganzen CAM-Trace führen. Darüber hinaus kann man mithilfe von Secondary Vehicle Identifiers (z.B. einer öffentlich verfügbaren Bluetooth-Schnittstelle) diese Zuordnung durchführen. Letztens, da die CAM-Daten mit einer hohen Frequenz versendet werden, kann der Fahrweg mit einer hohen Zuverlässigkeit voraus- und zurückberechnet werden.

Somit ist es grundsätzlich möglich, aus einem flächendeckenden Datenbestand aus CAMs über einen längeren Zeitraum Bewegungsprofile zu erstellen, und somit gegebenenfalls auch Verhaltensprofile. In [5] wurde zum Beispiel nachgewiesen, dass anhand der Lenkbewegungen ruhige von nervösen Fahrer unterschieden werden können. Außerdem wäre es durch die Anwendung von künstlicher Intelligenz und maschinellem Lernen durchaus möglich, große Datenbestände von Bewegungsprofilen und somit die zugehörigen Fahrer zu klassifizieren, falls Personenbezug hergestellt werden kann.

4.3 Herstellbarkeit Personenbezug

Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Selbst wenn CAMs direkt keine primären Identifikationsmerkmale enthalten (z.B. die Fahrzeugidentifizierungsnummer), kann deren Personenbezug grundsätzlich mit Zusatzwissen hergestellt werden. Technisch kann das durch eine Auflösung des Pseudonyms bei einer Certification Authority erfolgen [7], aber auch durch andere Wege. Zum Beispiel kann man anhand einer CAM-Trace aufgrund der am meisten gefahrenen Strecken den Wohn- und Arbeitsort einer Person identifizieren. Außerdem wäre es zum Beispiel möglich, durch Datenanalyse die Outliers in der Menge von den aufgezeichneten CAM-Traces identifizieren und versuchen, sie auf Personen mit entsprechendem Tagesablauf zurückzuführen. Besonders in wenig befahrenen Gebieten wäre diese Technik erfolgreich. Letztendlich wäre in vielen Situationen der einfachste Weg, vor Ort das Fahrzeug zu identifizieren (z.B. durch aufgezeichnete Videos oder Zeugenaussagen), und später aus dem Datenbestand die entsprechende CAM-Trace auszusuchen. Alle oben ausgeführten Techniken voraussetzen natürlich eine umfassende Erfassung von Fahrdaten und einen vorhandenen Bestand von Bewegungsprofilen (z.B. den in Kapitel 4.1 beschriebenen Big Brother Angreifer).

Eine besondere Sensibilität allein aus der Art der Daten einer CAM wird nach Art. 9 EU-DSGVO nicht begründet [16]. Allerdings genügt für die datenschutzrechtliche Betrachtung bereits die abstrakte rechtliche Möglichkeit der Informationsverknüpfung. Das heißt: falls es technisch möglich ist, den Fahrzeughalter aus den Daten zu identifizieren, fällt die Erhebung von CAMs unter die DSGVO - unabhängig davon, ob die Voraussetzungen dafür tatsächlich erfüllt sind [6]. Dies könnte sich zukünftig mit der Einsetzung von Shared Mobility-Konzepten ändern, falls man überwiegend nur kurzzeitig ein Fahrzeug anmietet und die Fahrzeugnummer nicht mehr auf natürliche Personen zurückgeführt werden kann.

[6] *Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Aufl., 2019, Rn. 12, 13

5 Vereinbarkeit mit datenschutzrechtlichen Prinzipien

Da die DSGVO auf die in CAMs enthaltenen Daten anwendbar ist, muss sie während der Bearbeitung und ggf. Speicherung der Fahrdaten stets eingehalten werden. Dies ist von großer Wichtigkeit für Betreiber der PKI, Autohersteller und andere an C-ITS beteiligten Unternehmen, da die Nichteinhaltung der DSGVO für sie mit hohen Geldstrafen drohen könnte. In diesem Kapitel werden relevante Grundsätze der DSGVO angefürt und deren Einhaltung geprüft. Für jeden Grundsatz werden die Datenschutzmaßnahmen und offene Fragen beschrieben, die bei der Einführung einer C-ITS beachtet werden müssen.

5.1 Grundsatz der Datenminimierung

Nach Art.5 Abs.1c DSGVO ist der Grundsatz der Datenminimierung folgendermaßen definiert: "Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein". Im Kontext von Intelligenten Verkehrssystemen heißt es, dass eine Erstellung von Bewegungs- und Verhaltensprofilen verhindert werden muss. Nach [7] ergeben sich demzufolge 3 Maßnahmen, die für Datenminimierung in C2C sorgen könnten:

- Transparenzgrundsatz: dem Fahrzeugführer soll transparent angezeigt werden, dass sich das Fahrzeug am Versand von CAMs und DENMs beteiligt.
- C-2-C Deaktivierungsmöglichkeit: der Fahrzeugführer muss selektiv in der Lage sein, den aktiven Versand von CAMs und DENMs zu deaktivieren.
- Vorkonfigurierte C-2-C Standardeinstellung: als Standardkonfiguration wäre es ausreichend, wenn Fahrzeuge CAMs und DENMs empfangen können aber ausschließlich DENMs verschicken

Außerdem sollte man beim Entwurf einer C-ITS darauf achten, dass eine geeignete Pseudonimisierung erfolgen kann. Die grundlegende Anforderung ist hier, dass die Verschlüsselungs-Zertifikate sich regelmäßig ändern müssen, so dass man die CAMs bei der zentralen Sammelstelle nicht auf die gleiche Person zurückführen kann. Wir haben aber bereits gesehen, dass die Zuordnung zur Identität einigermaßen auch mit sich ständig wechselnden Zertifikaten erfolgen kann. Daher stellt sich die Frage, welche Daten in CAMs gespeichert werden müssen, und ob ein Nachrichtenformat für alle Zwecke ausreichend ist.

Aktuell sind CAMs für fast alle Verkehrsszenarien vorgesehen, was aus Sicht der Datenschutz nicht optimal ist. Generell sind aber viele Daten darin für die meisten Anwendungen unnötig, was dem Grundsatz der Datenminimierung widerspricht. Daher wird es in [7] vorgeschlagen, für die häufigsten Anwendungsszenarien einen minimalen Nachrichtentyp zu nutzen, der nur die erforderlichen Daten erhält. Wenn wir uns aber bei Day 3 befinden und echte kooperativen Szenarien in Frage kommen, sollte dafür ein zusätzlicher verbindungsorientierter Kommunikationsstandard genutzt werden. So kann man die Daten auf

eine geeignete Weise voneinander trennen ohne Verlust der Funktionalität, und somit einen datenschutzrechtlichen Kompromiss erreichen.

5.2 Grundsatz der Integrität und Vertraulichkeit

Der Grundsatz der Integrität und Vertraulichkeit (Art.5 Abs.1c DSGVO) sieht vor, dass "personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen". Dies entspricht den Vorgaben des Art. 10 IVS-RL, nach dem die Mitgliedstaaten sicherstellen sollten, dass personenbezogene Daten gegen Missbrauch, d.h. insbesondere unrechtmäßigen Zugriff, Veränderung oder Verlust, geschützt werden. Weiterhin sollen für den Betrieb von C-ITS-Anwendungen und -Diensten soweit wie möglich anonymisierte Daten verwendet werden, um mögliche Schaden zu verringern[7].

Entscheidend ist hier die Anforderung an die Flüchtigkeit der CAMs. Es muss eine Technik für C-ITS entwickelt werden, die eine unbefugte Nutzung der in CAMs enthaltenden Daten unterbinden kann [7], oder nach einer kurzen Zeit den Inhalt davon invalidiert. Das Prinzip davon wäre analog zu anderen Diensten, wo die Verbreitung der Inhalten kontrolliert wird, z.B. Musikanwendungen, die das Abspielen von Dateien nur nach dem Kauf erlauben.

Darüber hinaus besteht nach Art.33 DSGVO unter Umständen eine Pflicht, Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde zu melden. Art.35 DSGVO sieht außerdem vor, dass im Falle von einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen, das durch die Verwendung einer neuen Technologie entsteht, eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchgeführt werden kann. Das ist besonders relevant im Kontext von C-ITS, da mithilfe der neuen AI-Technologien Einsicht in pseudonyme Fahrdaten genommen werden kann, wodurch möglicherweise Personenbezug entstehen könnte[8].

5.3 Grundsatz der Zweckbindung

Nach Art.5 Abs.1b DSGVO gilt der Grundsatz der Zweckbindung, nach dem personenbezogenen Daten nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden müssen. Das heißt: falls personenbezogene Daten erhoben werden, muss der Grund dafür klar definiert und eingehalten werden, durch eine Einwilligung oder auf eine andere Weise (Art.6 Abs.1a DSGVO). Als Ausnahme gelten Archivzwecke, wissenschaftliche oder historische Forschungszwecke und statistische Zwecke - sie gelten nach Art.89 Abs.1 nicht als unvereinbar mit den ursprünglichen Zwecken.

[7] *Jochum*, In: ZD 2020, 497
[8] *Seewald*, In: RAW 2020, 130

Im Kontext von C-ITS heißt es, dass die Zweitnutzung der Fahrdaten nur aufgrund einer Zustimmung erfolgen werden darf. Die Standortdaten allein unterliegen im allgemeinen Datenschutzrecht keinem besonderen Schutz; falls es jedoch möglich ist, Bewegungsprofile aus solchen Daten zu generieren, muss ebenfalls die Zweitnutzung der Daten gesetzlich geregelt werden. Das heißt, jegliche Datenverarbeitung über die ursprüngliche Zwecke hinaus (individualisierte Zweitnutzung) muss explizit eine Einwilligung voraussetzen[9].

Außerdem ist es bei vielen C2X Anwendungen der Fall, dass auch andere Daten zusätzlich zu den Standortdaten regelmäßig versendet werden. Aus dieser Information können mehrere Datenspuren nicht nur zum Aufenthalt des Fahrzeughalters entstehen, was eine Dauerüberwachung verursachen kann[10]. Das ist ein weiterer Grund dafür, die Zweitnutzung jeglicher Fahrdaten nur über eine explizite Einwilligung zu erlauben.

Neben der individualisierten Zweitnutzung von Fahrdaten gibt es andere Möglichkeiten, für die der Grundsatz der Zweckbindung entfallen kann. Im Falle von kollektiver Datennutzung findet die Anonymisierung der Daten vor der Zweckänderung statt, was eine Zweitnutzung ohne Zustimmung von jedem einzelnen Verkehrsteilnehmer erlaubt. Dies setzt aber einen großen Datenbestand voraus, in dem auf keine einzelne Person zurückgeführt werden kann, und aus dem keine Bewegungsprofile generiert werden können. Für anonymisierte Fahrdaten ergeben sich ebenfalls mehrere Nutzungsfälle, z.B. Verkehrslenkung, Gefahrenabwehr, Verkehrsstatistik oder -forschung[11].

5.4 Recht auf Datenübertragbarkeit

Neben den Grundsätzen aus Art.5 Abs.1 DSGVO muss auch der Art.20 DSGVO erwähnt werden, wodurch das Recht auf Datenübertragbarkeit vorgeschrieben wird. Nach dem Artikel hat die betroffene Person das Recht, "die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten". Außerdem ist dem Betroffenen das Recht eingeräumt, seine Daten von einem Anbieter zu einem anderen zu übertragen. Dies entspricht dem Recht auf informationelle Selbstbestimmung nach Art.8 GRCh und ermöglicht es, die Daten ohne Behinderung verschiedenen Interessierten zur Verfügung zu stellen, z.B. Autoherstellern, Vertragshändlern, Versicherungen und Leasinggebern[12].

Hier ist es wichtig zu betonen, dass der Artikel sich auf die Fahrdaten bezieht, die vom Betroffenen bereitgestellt wurden. Diese Bedingung wird erfüllt, wenn die Daten wissentlich und aktiv von betroffenen Personen mitgeteilt wurden[13], aber auch wenn die Daten durch die Nutzung des Dienstes von der Person aufgezeichnet wurden[14]. Im Gegensatz dazu sind die Daten, die durch eine Auswertung der Fahrdaten entstanden

[9] *Weichert*, In: SVR 2016, 361
[10] *Weichert*, In: SVR 2014, 241 f.
[11] *Weichert*, In: SVR 2016, 367
[12] *Klink-Straub/Straub*, In: ZD 2018, 459
[13] *Art. 29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, S. 11
[14] *Strubel*, In: ZD 2017, 355, 357

sind, keine vom Fahrer bereitgestellte Daten[15]. Zum Beispiel sind die Rückschlüsse auf das Fahrverhalten aus den gesammelten Daten ("Person A ist ein vorsichtiger Fahrer") keine bereitgestellten Daten.

Die wichtigste Herausforderung im Kontext von C-ITS besteht zunächst darin, die beim Fahrzeughersteller oder beim Betreiber der PKI gespeicherten Daten im maschinenlesbaren Format betroffenen Personen zugänglich zu machen. Um Art.20 Abs.4 DSGVO gerecht zu werden, müssen die Verantwortlichen dabei die Rechte der Drittbetroffenen beachten, da beim Bereitstellen der Daten möglicherweise die Daten der anderen Verkehrsteilnehmern übermittelt werden könnten[16]. Letztens müssen die Datenschutzmechanismen bei den Empfängern der Daten (z.B. Händler, Werkstätten, Versicherungen) unter die Lupe genommen werden, da sie beim Empfang der Daten nach Art.20 Abs.2 DSGVO selbst zu Verantwortlichen werden.

6 Zusammenfassung und Ausblick

...

Literatur

[1] Nick et al. Asselin-Miller. *Study on the Deployment of C-ITS in Europe: Final Report. Framework Contract on Impact Assessment and Evaluation Studies in the Field of Transport MOVE/A3/119-2013-Lot № 5 Horizontal.* Techn. Ber. MOVE/C.3./№ 2014-794. 2016.

[2] Elaine Barker u. a. „NIST Special Publication 800-56A Revision 2 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography". In: (2013). DOI: 10.6028/NIST.SP.800-56Ar3. URL: https://doi.org/10.6028/NIST.SP.800-56Ar3.

[3] *BMVI - Intelligente Verkehrssysteme im Straßenverkehr.* URL: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/ivs-im-strassenverkehr.htm.

[4] *CAR 2 CAR Communication Consortium.* URL: https://www.car-2-car.org.

[5] Frank Dettki. *Methoden zur objektiven Bewertung des Geradeauslaufs von Personenkraftwagen.* 2005. URL: https://elib.uni-stuttgart.de/handle/11682/4059 (besucht am 24. 11. 2020).

[6] ETSI (European Telecommunications Standards Institute). *TS 102 941 - V1.2.1 - ITS; Security; Trust and Privacy Management.* Techn. Ber. 2018, S. 1–30.

[15] *Art. 29-Datenschutzgruppe*, (o. Fußn. 22)
[16] *Klink-Straub/Straub*, In: ZD 2018, 463

[7] Michael Kiometzis und Markus Ullmann. „Fahrdaten für alle?“ German. In: *Datenschutz und Datensicherheit - DuD* 41.4 (März 2017), S. 227–232. DOI: 10.1007/s11623-017-0763-6.

[8] Klink-Straub/Straub. „Vernetzte Fahrzeuge – portable Daten“. In: *ZD 2018, 459* (2018).

[9] *MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme - ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität.* Techn. Ber. 2016.

[10] *Result of C-ITS Platform Phase II Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) RELEASE 1.* Techn. Ber. 2017. URL: https://ec.europa.eu/transport/sites/transport/files/c-its%7B%5C_%7Dsecurity%7B%5C_%7Dpolicy%7B%5C_%7Drelease%7B%5C_%7D1.pdf.

[11] Mukesh Saini, Abdulhameed Alelaiwi und Abdulmotaleb El Saddik. „How close are we to realizing a pragmatic VANET solution? A meta-survey“. In: *ACM Computing Surveys* 48 (Nov. 2015), S. 1–40. DOI: 10.1145/2817552.

[12] Thomas Strubbe, Nicolas Thenée und Christian Wieschebrink. „IT-Sicherheit in Kooperativen Intelligenten Verkehrssystemen“. German. In: *Datenschutz und Datensicherheit - DuD* 41.4 (März 2017), S. 223–226. DOI: 10.1007/s11623-017-0762-7.

[13] *The ITS Standards Program. Deployment Resources.* URL: https://www.standards.its.dot.gov/factsheets/factsheet/80.

[14] *TS 103 097 - V1.1.1 - Intelligent Transport Systems (ITS); Security; Security header and certificate formats.* Techn. Ber. 2013, S. 1–33.

[15] Markus Ullmann, Thomas Strubbe und Christian Wieschebrink. *Technical Limitations and Privacy Shortcomings of the Vehicle-to-Vehicle Communication.* c. 2016, S. 22–27. ISBN: 9781612085159.

[16] Thilo Weichert. „Car-to-Car-Communication zwischen Datenbegehrlichkeit und digitaler Selbstbestimmung“. In: *Svr* (2016), S. 361.

[17] B. Wiedersheim u. a. „Privacy in inter-vehicular networks: Why simple pseudonym change is not enough“. In: *2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS).* 2010, S. 176–183. DOI: 10.1109/WONS.2010.5437115.