# Sicherheit in Car2Car – Kommunikation

Safety 1: Autorisierung

TECHNISCHE UNIVERSITÄT DARMSTADT

# Ausarbeitung zum Seminar

Die vorliegende schriftliche Ausarbeitung entstand im Rahmen des Seminars

**Sicherheit in Car2Car-Kommunikation –**
**Safety 1: Autorisierung**

Wintersemester 2007/08
Technische Universität Darmstadt

Verantwortlicher Dozent:
Lars Fischer
Fachgebiet Sicherheit in der Informationstechnik
Fachbereich Informatik, TU Darmstadt

Verfasst von:

**Andreas Schwarzkopf**
1201387 | Dipl.-Informatik | 9. Semester

Tag der Abgabe: 19. Februar 2008

# Safety 1: Autorisierung

## Inhaltsverzeichnis

**Förmliche Erklärung**

Ich versichere hiermit gegenüber dem veranstaltenden Institut der Technischen Universität Darmstadt, dass die vorliegende schriftliche Ausarbeitung selbstständig und nur unter Zuhilfenahme der im Literatur- und Abbildungsverzeichnis genannten Quellen angefertigt wurde.
Zitate und übernommene Ausführungen innerhalb der Ausarbeitung sind als solche deutlich kenntlich gemacht.

Darmstadt, den _____

_____
Andreas Schwarzkopf

**Abstract**

Fahrzeugkommunikation wird, direkt oder indirekt, das Fahrverhalten beeinflussen. Die erste Prämisse der Sicherheitsbestrebungen muss es also sein, das Einspielen von unerwünschten Nachrichten zu unterbinden.

## Einleitung

Die vorliegende Ausarbeitung behandelt Aspekte authentischer, integerer vehicular ad-hoc network (VANET) Kommunikation.
Da Fahrzeugkommunikation drahtlos – vermutlich auf einem IEEE 802.11 Standard basierend – stattfinden wird, ist natürlich das physikalische „Einspielen unerwünschter Nachrichten" schlichtweg jederzeit möglich. Schutz bietet nur eine Autorisationslogik die verhindert, dass fehlerhafte Nachrichten beliebiger Kommunikationspartner Schaden anrichten können. Im folgenden sollen die Begriffe „*Autorisation*" und „*Authentifikation*" abgegrenzt werden.
Daran anknüpfend soll ein konkretes Leightweight-Authentifikationsprotokoll – das *TESLA* Protokoll – vorgestellt werden, da es interessante Aspekte der Authentifikation in VANET Szenarien verdeutlicht. Abschließend soll ein Überblick gegeben werden, welche Bedeutung der Authentifikation und der Autorisation in aktuellen Beiträgen und wissenschaftlichen Papieren zur Zeit zukommt und vorallem wie das Verständnis dieser Sicherheitbegriffe in den jeweiligen Arbeiten ausfällt.

## Security in VANETs

Ein visionäres Gebilde eng verzahnter Hard- und Softwarekomponenten zeichnet sich vor den Entwicklungsbestrebungen unterschiedlicher nationaler und internationaler, privater und staatlicher Interessenverbände ab.
Im Fall der VANETs spielen nicht nur das Vertrauen des Marktes, das Image der Hersteller und das enorme Risiko potentieller Schäden eine Rolle, sondern auch die technische Seite ist hochkomplex und bedingt die Entwicklung von Sicherheitstechniken von Anfang an. Die oft zitierten „lessons learned" in Bezug auf Sicherheitsaspekte anderer Kommunikations-netzwerke und deren Protokolle sowie die Komplexität des Anwendungsgebietes verbieten es technisch machbare Lösungen vorschnell auf Kosten fehlender oder zu schwacher Sicherheitsmechanismen zu entwickeln.

Die Eintwicklung eines einheitlichen Basissystems, sowohl was die technischen als auch die softwareseitigen Layer eines VANET Schichtenmodells angeht, gestaltet sich jedoch schwierig, da die Security Requirements auf den ersten Blick unvereinbare Ziele haben und starke zeitliche und räumliche Randbedingungen erfüllen müssen – und das im Hinblick auf die bis zu 75 Anwendungsszenarien, die in [VS05] bereits skizziert wurden.

Darüber hinaus ist Security Engineering in VANETS keinesfalls lediglich eine Adaption bestehender, altbewährter informationstheoretischer Konzepte an ein neues Umfeld. Einfache kryptographische Primitive, deren Anwendung und Implementation in statischen Netzen „Studentenübungen" darstellen, sind hier wieder Gegenstand der Forschung.

Es muss bei bestehenden Lösungen geprüft werden, welche Annahmen bei deren Adaption in einem VANET überhaupt noch gelten.

„*In der Informatik ist die Hauptfragestellung nach der Authentizität von Informationen durch digitale Signaturen gelöst worden*.“ [WKAT]

“*The Security of VANETs: Is public key kryptography fit?*” [RH05]

Die on board unit (OBU) eines Fahrzeuges wird Sensordaten und empfangene Nachrichten auswerten und verarbeiten, gegebenenfalls Handlungen initiieren und selbst Nachrichten verschicken. Fahrzeugkommunikation muss also in jedem Fall geschützt ablaufen und insbesondere die Information selbst muss autorisiert werden, bevor auf ihr aufbauend Annahmen getroffen und Modelle über Zustand und Entwicklung der Umwelt gebildet werden.

Doch was genau bedeutet „*Autorisation*“ von Informationen in VANETs?
Die inhärente Dynamik von Netzwerken und vereinfachte Privacyüberlegungen legen vielleicht nahe, wann immer es geht vom Sender abstrahieren zu wollen, doch das grundsätzliche Problem bleibt: Es müssen unter Umständen Safety-Messages von einem einzelnen Peer entgegengenommen werden, deren korrekte Verarbeitung innerhalb weniger Millisekunden im Extremfall über Leben und Tod entscheiden kann.

Man kann hier bereits folgendes Ergebnis festhalten: Die Verarbeitung von Informationen aus Nachrichten ist korrekt formuliert an „autorisierte Sender“ gekoppelt, was direkt zur Frage nach deren „*Authentizität*“ führt.

## Autorisation und Authentifikation

Im Folgenden sollen die Begrifflichkeiten Autorisation und Authentifikation definiert und in Bezug zueinander gesetzt werden, danach folgt eine kurze Diskussion über deren Bedeutung im Kontext mobiler ad-hoc Netzwerke.

Die in der IT-Sicherheit genutzten Begriffe *Autorisation* und *Authentifikation* sind nicht nur sachlogisch miteinander verwand, sondern werden bisweilen in einigen Szenarien synom eingesetzt, da sie sich in der Regel gegenseitig bedingen und ergänzen.
Diese Vereinfachung und Gleichsetzung ist jedoch nicht korrekt: *Authentifikation* ist immer an eine *Entität* – oft sogar an eine spezielle *Identität* – geknüpft, während *Autorisation* Rechte und Befugnisse zum Ausdruck bringt.

Von [MDNF] stammen folgende Definitionen:

„*Authentifizierung besteht im Erlangen von Informationen zur Identifizierung von einem Benutzer und im Überprüfen dieser Informationen. Wenn die Informationen gültig sind, wird die Entität […] als authentifizierte Identität betrachtet. […] Der Zweck der Autorisierung ist zu bestimmen, ob einer Identität die angeforderte Zugriffsart auf eine angegebene Ressource gewährt werden soll.*“

Diese Beschreibung impliziert eine chronologische Abhängigkeit dieser beiden Vorgänge: Autorisation erfordert offensichtlich eine vorherige Authentifikation; Authentifikation geht der Autorisation voraus!

Ein gutes Beispiel für Systeme, die diese beiden Vorgänge voneinander trennen, sind RBAC – (role based access control-, dt. „Rollenbasierte Zugriffskontroll“) Systeme.
Hier werden *Benutzer*, *Rollen* und Rechte unterschieden:

Jeder Benutzer wird, nachdem seine Identität festgestellt wurde – das ist die Authentifikation –, einer oder mehreren *Rollen* zugeordnet. Je nach Rolle dürfen nun gewisse Aktionen ausgeführt oder Ressourcen genutzt werden – das ist die *Autorisation* –, also *Rechte* wahrgenommen werden.
Die Unterscheidung in Authentifikation und Autorisation macht aber auch vor einem zeitlichen, dynamischen Hintergrund Sinn: Nicht jede authentifizierte Entität behält ihre Autorisation in Bezug auf bestimmte Aktionen über einen beliebig langen Zeitraum. Die eigentliche Authentifikation ist bei geschlossenen Sitzungen nur zu Beginn der Kommunikation notwendig, die Autorisation muss wegen ihrer zeitlichen Begrenztheit aber vor jeder Aktion bzw. jedem Resourcenzugriff geprüft werden.

So könnte zum Beispiel ein Mitarbeiter nach dessen Authentifikation die Autorisation erhalten auf geschäftskritische Projektdaten zuzugreifen, andererseits kann ein solcher Mitarbeiter auch korrekt authentifiziert werden wenn das Projekt für ihn abgeschlossen ist und die Autorisation für den Zugriff nicht mehr erteilt wird.
Noch kurzfristiger muss in einem so hochdynamischen Anwendungsfeld wie dem VANET gedacht werden, indem statische Autorisierung in der Regel nicht ausreicht um die notwendige Sicherheit zu gewährleisten, was zum Thema "`Isolation"' von fehlverhaltenden Knoten führt.
In VANET Anwendungen, die größtenteils auf zustandslosen Kommunikationsprotokollen basieren, wird die zeitliche Trennung von Autorisation und Authentifikation im Sinne von „Sitzungen“ nicht so scharf ausfallen, dafür jedoch der Aspekt des Objektes der Authentifikation in den Vordergrund treten, also „was“ authentifiziert wird:
Man spricht von *Message Authentication* oder *Sender Authentication*. Beides sind Entitäten, von deren Echtheit man sich überzeugen kann.

[TK05] schreibt hier in Bezug auf Car2Car Networks:

*“It is extremely important to ensure message integrity - a risky driving manoeuver based on a false message information might be fatal - while sender authentication is not needed in many cases*”

Inwiefern diese Aussage an sich haltbar ist steht sicher aus, da integere (aber semantisch falsche) Nachrichten mutwillig auch von nicht authentifizierten Dritten eingespielt werden könnten. Allerdings ist davon auszugehen, dass der Autor „Authentifikation“ hier auf eine konkrete Identität bezieht und in Car2Car Szenarien unter Umständen schwächere Randbedingungen als die „Authentifikation der Identität“ gefordert werden könnten.

Dennoch wird hier die  gedankliche Trennung der „Message-“ und „Sender-Authentication"' deutlich.

Eine „*Nachricht zu* authentifizieren“ bedeutet kryptographisch:

- Sicherzustellen, dass der Inhalt unverändert ist (Integrität gewährleisten).
- Sicherzustellen, dass sie wirklich von der Entität kommt, von der sie augenscheinlich ist. Der Ursprung ist also validiert, eine Zuordnung zum Sender möglich.

Einen „*Sender zu authentifizieren“* stellt dagegen folgendes sicher:

- Die sendende Entität kann sich gegenüber dem Empfänger ausweisen.
  Die Identität (oder eine Eigenschaft der Identität) ist validierbar.
- Außerdem kann zusammen mit einer eindeutigen Identität und einer fixierten Zeit, zum Beispiel einem Timestamp in der authentifizierten Nachricht (Integer und Senderbezogen), die Zurechenbarkeit (non-repudiation) gewährleistet werden.

Ein Begriff der auch hier einzuordnen ist, ist die „*Property authentication*“ und beschreibt eine Form der „*Sender–Authentication*“', bei der nicht die gesamte Identität offenliegt sondern nur gewisse Eigenschaften nachgewiesen werden, zum Beispiel die „*location authentication*“ (vgl. [FK06]).

Als Zusammenfassung lässt sich hier bereits festhalten:
Die Grundlage sinnvoller Autorisation ist die vorausgegangene Authentifikation. Die Autorisation muss immer neu geprüft werden und ist je nach Szenario ein hochgradig dynamisches Element. Bei zustandslosen VANET Anwendungen muss unter Umständen jedes einzelne Datenpaket Authentifikationsmerkmale aufweisen, um die Autorisation zu ermöglichen.

Die Authentifikation *kann*, *muss aber nicht* an eine Identität gekoppelt sein. Vielmehr reicht es in VANET Szenarien oftmals aus, dass sich eine Entität, lediglich soweit authentifiziert, dass die Echtheit gewisser Eigenschaften nachgewiesen wird, ohne die Identität preiszugeben: Die sogenannte *Property Authentication*.

## Babylonische Sprachverwirrung in der IT-Sicherheit

Der in der Praxis häufig anzutreffende synonyme Gebrauch der Begriffe *Authentifikation* und *Autorisation* ist nicht sonderlich verwundert. Doch selbst einschlägige Literatur, die sich dediziert der Thematik IT Sicherheit verschrieben hat, liefert oft keine umfassenden, richtigen Definitionen der Begrifflichkeiten (siehe [CE04], [JB04]), die so weit vom konkreten Kontext abstrahieren, dass sie auch auf die hier untersuchten VANET Szenarien passen.
Aus diesem Grund liefere ich nun eine eigene Abgrenzung der Begriffe, die sich im wesentlichen an den Kerngedanke in [WKAU] anlehnt.

**Authentisierung**: Ist der Nachweis der eigenen Authentizität.

**Authentifizierung**: Ist die Verifikation einer behaupteten Authentizität.

**Authentizität:** Bezeichnet die „Glaubwürdigkeit“ einer Aussage bzw. die „Echtheit“ einer Sache. (adj. *authentisch*, gr. *authentikos* = „Urheber“)

„Authentifizierung“ und „Authentisierung“ sind *Vorgänge* (dynamischer Charakter), „Authentizität“ ein *Attribut* (statischer Charakter).

Authentifikationsmerkmale sind Merkmale, die zur Authentisierung genutzt werden und die Authentifizierung ermöglichen; sie lassen sich in die Bereiche „Wissen“, „Besitz“ / „Biometrie“ einordnen.

**N.B.**: In der deutschen Sprache wird in das Begriffspaar „Authentisierung“ und „Authentifizierung“ unterschieden, im Englischen gibt es lediglich den Begriff „authentication“. Im Deutschen wird also der Tatsache Rechnung getragen, dass bei der Authentizitätsprüfung immer zwei Parteien involviert sind, es eine passive (vorlegende) und aktive (prüfende) Seite gibt!

**Identifizierung**: Ist der Vorgang des Identifizierens; das eindeutige Erkennen einer Person oder eines Objektes, also das exakte *Feststellen der Identitä*}. Technisch wird eine Identität durch einen „Charakterisierungsvektor“ beschrieben, der eine Entität („abgrenzbaren Wesenseinheit“) eindeutig beschreibt.

Folgendes sollte hier als Ergebnis festgehalten werden:
Erstens impliziert „Authentifizierung“ nicht gleich „Identifizierung“ und zweitens ermöglicht „Authentifikation“ Zugriffskontrolle (also „Autorisation“), ohne dass gleich eine eindeutige Identifizierung notwendig ist. Einfache Authentifikation ist im Sinne der Identifizierung notwendig, aber nicht hinreichend.

Ausserdem gilt es oft folgendes zu bedenken: Wahrgenommene Rechte (Frage der Autorisation bzw. Authentifikation) sind nicht immer kongruent zur Verantwortung (z.B. die Bank PIN wird an Ehegatten gegeben).
Die Identifizierung fixiert in der Regel eine Identität, die sich verantworten muss. Diese Sachverhalt ist sehr gut mit einem Beispiel in [WKAU] erläutert, die Kernaussage lautet: „Nur eine sehr starke Authentifizierung kann auch zur Identitätsfeststellung herangezogen werden“.

## Authentifikation in VANETs

Authentifikation bedeutet sich der Authentizität, der Echtheit, einer Person oder eines Objektes, allgemein einer Entität, zu vergewissern, diese also zu verifizieren. Johannes Buchman geht in seinem bekannten Werk „Einführung in die Kryptographie“ sogar soweit, Aspekte der Identität an die Authentizität zu knüpfen:

„*Kryptographische Techniken geben Aufschluss über die Identität des Absenders elektronischer Nachrichten und garantieren damit ihre Authentizität.*“ [JB04]

Zu bemerken ist hier allerdings, dass „Aufschluss über die Identität“ nicht mit „Identität“ gleichzusetzen ist. Durchaus kann lediglich eine Eigenschaft des Senders authentifiziert werden (z.B. „location authentication“). Die Identifizierung als das eindeutige Verifizieren einer bestimmten Identität ist also ein deutlich einschränkenderer Vorgang als die reine Authentifikation.

Im Anwendungsfeld „VANET“ kommt als Authentifikationsmerkmal offensichtlich ausschließlich Wissen (bzw. Information) in Frage, das innerhalb eines definierten Kommunikationsprotokolls ausgetauscht wird.

Das Wissen, das in Kryptosystemen als mathematischer Schlüssel vorliegt, kann beiden bzw. allen Kommunikationspartnern bekannt sein (symmetrische Kryptosysteme) oder es kommt ein asymmetrisches Kryptosystem zum Einsatz. In jedem Fall erfolgt die Authentifizierung technisch dadurch, dass die Partner an der Kommunikation teilnehmen können, also den Schlüssel kennen bzw. zumindest den Schlüssel auf einen Fingerprint der Nachricht (typischerweise ein kryptographischer Hash-Wert) anwenden können.

Symmetrische Verfahren mit globalem Schlüssel können für das Anwendungsfeld VANETs ausgeschlossen werden. Wohl wären hohe Performanz und Privatheit gewährleistet, jedoch nicht die ausreichende Robustheit bzw. das nötige Recoveryvermögen gegenüber Kompromittierung. Weitere Informationen hierzu finden sich in [„4.5.3 Global Symmetric Keys“, VH05].
Es bleibt de facto nur die Möglichkeit asymmetrische Kryptographiesysteme einzusetzen; also „public key cryptography“ und die damit realisierten „digitalen Signaturen“ zur Authentifikation heran zu ziehen. Die Authentizität der öffentlichen Schlüssel, die zur Erzeugung der Signatur verwendet werden, kann über „Web of trust–„, P2P oder PKI Systeme realisieret werden. (vgl. [„Public Kry Cryptography”, WPKI])

Da unter Umständen die Information einer einzigen signierte Nachricht innerhalb kürzester Zeit autorisiert werden muss und natürlich die Verantwortung für eine solche Information im Nachhinein feststehen muss, stützen sich fast alle vorliegenden Arbeiten zum Thema Security in VANETs auf Public Key Infrastrukturen (PKIs).

Fazit: Die Frage nach der Authentizität einer VANET Nachricht lässt sich darauf reduzieren, dass eine bestimmte OBU die Nachricht digital signiert hat und eine Struktur (z.B. PKI) dann den notwendigen „Anchor of Trust“ für die Authentizität der OBU liefert..

## Public Key Kryptographie in VANETs

Digitale Signaturen und die Verwendung einer PKI stossen im wesentlichen auf das Problem der *Privatheit* und den Vorwurf, dass sie enormen *zusätzlichen Aufwand* hervorrufen.
Allerdings lösen sie neben der Authentizität und Integrität auch gleich ein anderes Sicherheitsziel: Die Zurechenbarkeit [JB04] (non-repudiation). Gerade bei Safety Messages, die z.B. nach einem Unfall von einer Black Box gesichert werden, sollte sichergestellt sein, dass auch im Nachhinein eine Zuordnung zum Sender möglich ist, ohne dass dieser sie abstreiten kann.

Der Overhead digitaler Signaturen, kommt insbesondere bei der Übermittlung kurzer Beacon Nachrichten zu tragen. So liegen DSA [DS00] und IEEE 1609.2 konforme ECDSA [ITSS] Signaturen laut [HL06] bei 40 bzw. 64 Bytes, was für kurze Nachrichten von unter 20 Bytes Nutzlast (vgl. [ER01]) einen erheblichen Mehraufwand bedeutet.

Allerdings sollte man sich auch die absoluten Zahlen vor Augen halten, die ein Public Key Verfahren im VANET charakterisieren: Anwendungen, die auf der Dedicated Short Range Communications (*DSRC*) Funktechnologie basieren (vgl. [„5.9 GHz Band“, VS05]), nehmen für sicherheitsrelevante Szenarien eine 100ms Latenzzeit in Kauf. [RH05] geben für die Verifikation einer ECDSA Signatur 7.617 ms, für eine NTRU Signatur sogar nur 1,488 ms an. Da die Verifikation von Nachrichten parallel und in Hardware erfolgen kann, ist eine ausreichende Geschwindigkeit gewährleistet. [RH05] sehen in den Knoten des VANETs rechenstarke, energie- und ressourcenreiche Einheiten: Ein Vorteil, der asymmetrische Kryptographie trotz der relativ hohen Kosten ermöglicht.

Fazit: Selbst digitale Signaturen mit relativ hohem Overhead sind für VANET Anwendungen annehmbar. Für periodisch verschickte Nachrichten oder gar „streaming content“ existieren Methoden diesen asymmetrischen Authentifikationsoverhead drastisch zu senken, indem hybride Verfahren genutzt und Folgepakete symmetrisch authentifiziert werden.
In VANET Szenarien mit vielen denkbaren sicherheitskritischen Broadcast-Anwendungen (vgl. Anwendungsliste in [VS05]) spielt das Thema der „Lightweight-Authentifikation“ eine besondere Rolle, weshalb im folgenden ein Protokoll speziell vorgestellt werden soll.

## Authentifikation: Unicast vs. Broadcast

Es gibt allgemein zwei Ausprägungen der kryptographischen Primitive „Authentifikation“: *One-to-one* und *one-to-many*.
Die in den meisten klassischen Anwendungen implementierten Authentifikationsprotokolle sind typischerweise für Unicast Szenarien realisiert, also für Punkt–zu–Punkt Kommunikationsprozesse, da den interkonnektierenden Knoten keine Partizipation am Inhalt sondern lediglich an der technischen Übertragung und eventuell ein Fehlverhalten („malicious nodes“) im Kommunikationsmodell zugesprochen wird.
Aus Performanzgründen werden in Unicast Szenarien in der Regel in einer eventuell asymmetrischen Verhandlungsphase symmetrische Schlüssel ausgetauscht. All diese Protokolle realisieren die Authentifikation – abstrahiert man von der exakten Vorgehensweise und den jeweils genutzten Termini – durch Anhängen eines message authentication codes (MAC) an die Nachricht und nutzen somit den herkömmlichen Ansatz symmetrischer Kryptographie.

Diese Art der Authentifikation ist nicht auf Broadcast Szenarien übertragbar:
„In unicast authentication, it is sufficient to prove that the message must have come from either the sender or the receiver. Because the receiver knows that it did not originate the message, it can ascertain that the sender sent it“. [HL06]
In Broadcast Szenarien können Sender offensichtlich nicht aus dem Wissen um die Empfänger abgeleitet werden.
Neben der Nutzung von *MACs* bleibt als Alternative lediglich die Verwendung asymmetrischer Verfahren für alle Datenpakte der Kommunikation zu nutzen – so könnte also auch die digitalen Signatur bei der Broadcastauthentifikation Anwendung finden.

„*Indeed, signing each data packet provides secure broadcast authentication; ...*” [TP02]

Die Überlegung, dass in Broadcast Szenarien der Sender nur authentifiziert werden kann, indem er über mehr Wissen als die übrigen Kommunikationsteilnehmer verfügt und andererseits MAC basierte Unicastlösungen bedeutend weniger Overhead erzeugen, führte zu Entwicklung von TESLA.

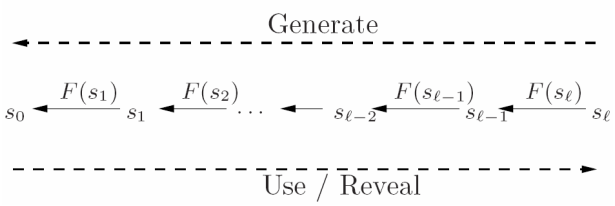
## TESLA

TESLA steht für „*Timed Efficient Stream Loss-tolerant Authentication*"" und bietet die Möglichkeit MAC basierte Unicast Protokolle in Broadcast Protokolle umzuformen.
Die wesentliche Idee hinter TESLA ist es, die Zeit als Ursprung asymmetrischen Wissens zu verwenden. Neben den symmetrischen kryptographischen Funktionen wird es so um eine assymmetrische Eigenschaften erweitert. An die versandten Nachrichten wird auch bei TESLA ein MAC angehängt, der aus einem Schlüssel k abgeleitet ist, der nur dem Sender bekannt ist. Die Empfänger puffern die Nachricht für einen kurzen Moment, den der Sender verstreichen lässt, bis er den Schlüssel k veröffentlicht. Mit dem veröffentlichten Schlüssel können alle Empfänger die soeben empfangene Nachricht authentifizieren.
Nachrichten, die zeitlich nach der Veröffentlichung des Schlüssels empfangen wurden, müssen verworfen werden. Authentifikation ist hier an die Zeit gekoppelt, aus der Umschreibung wird jedoch schon eine der Besonderheiten der Requirements deutlich:

- TESLA benötigt keine global synchronisierte Zeit. Eine einfache Zeitsynchronisation ermöglicht die obere Abschätzung der aktuellen Lokalzeit des Senders.
- TESLA beruht auf einer Hashfunktion, die eine effiziente und schnelle Berechnung von Hashketten (den Schlüsseln), auf Empfängerseite zulässt.

### One-Way Key Chain

Zur Erzeugung einer one-way chain wird eine kryptographische Hashfunktion F(x) benötigt.
Der Sender erzeugt eine Kette der Länge l indem er ein $s_l$ vorgibt und darauf l mal wiederholt die Funktion F anwendet.

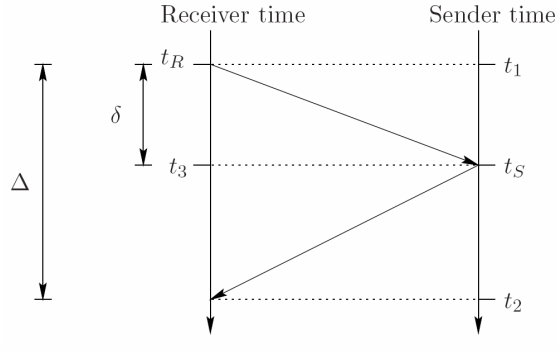



Die Indizes werden absteigend bis zur 0 vergeben, $s_0$ ist also das Endprodukt l maliger Anwendung von F auf $s_1$. $F^l(s_1) = s_0$
Man kann mit Element $s_i$ der Kette prüfen ob $s_j$ auch Teil der Kette ist, indem man für $i < j$ das Element $s_j$ auf $s_i$ überführt: $F^{j-i}(s_j) = s_i$
Da Elemente der Kette einfach erzeugt werden können, ist nicht nur der Platzbedarf gering, sondern auch die Robustheit der Authentifikation von Folgepaketen nach etwaigem Datenverlust möglich. Im Sinne von TESLA spricht man – die Ergebnisse der Hashfunktion H(x) als Schlüssel aufgefasst – von One-Way Key Chains.

### Time Synchronization

Unter der Annahme, dass kurzzeitiger Zeitdrift zwischen den zu synchronisierenden Uhren vernachlässigbar ist und auf lange Sicht Resynchronisationen möglich sind, kann ein einfaches Synchronisationsprotokoll wie folgt implementiert werden:

1. Der Empfänger initiiert einen Time-Sync Request zum Zeitpunkt $t_R$
2. Der Sender antwortet auf den Request zu seiner Lokalzeit $t_S$
3. Der Empfänger kann zum Zeitpunkt $t_r$ die obere Zeitgrenze $t_s$ auf der Senderseite nun abschätzen: $t_s \leq t_r - t_R + t_S$




Da der Empfänger jedoch nicht weiss, wie hoch das propagation delay des Sync-Paketes war, andererseits jedoch nur eine obere Schranke benötigt wird, kann der Synchronisations Error mit der gesamten Round Trip Time ΔRTT abgeschätzt werden.

Die Autoren selbst machen hier auf verschiedene Probleme aufmerksam:

- Die Validierung des Time Sync Packets erfordert eine Digitale Signatur.
- Die Synchronisation mit vielen Broadcast Partnern kann die gleichen Muster wie DDoS Attacken (z.B. „SMURF“) haben.

### Bewertung

Sind die Requirements erst einmal erfüllt, bietet nach [TP02] das TESLA Verfahren die folgenden Vorteile:

- Geringer Berechnungs - Overhead (Generieren / Verifizieren des Hashes)
- Geringer Kommunikations - Overhead (Größe des Hashes)
- Zeitnahe Authentifikation für jedes einzelne Paket ist gewährleistet
- Das Protokoll ist robust gegenüber verlorenen Paketen
- Das System skaliert gut für eine große Anzahl an Empfängern

Die Bandbreitenersparnis ist ein Vorteil, der in VANET Anwendungen, zum Beispiel bei Heartbeat Messages, stark zum Tragen kommt. In [HL06] nehmen Hu und Laberteaux an, dass eine 200 bit Heartbeat Message mit 512 bit PKI Signatur durch Anwendung des TESLA Verfahrens auf 200 bit zuzüglich 80 bit TESLA Signatur plus ein weiteres 80 bit Paket, der TESLA Key Veröffentlichung, verkleinert werden kann. Das macht hier eine Ersparnis von 352 bit pro 200 bit Nutzlast. Im Falle von vielen kleinen Nachrichten wäre dieser Effekt sogar noch stärker, da TESLA Pakete, die im selben Zeitslot versand werden, nur ein weiteres Veröffentlichungspaket des Schlüssels benötigen.

Allerdings ist das Protokoll stark auf Streaming Szenarien ausgelegt. Hier kann es seine Stärke voll ausspielen, da das „aufwändige“ Verankern des Trust nur einmal geschehen muss. In VANET Szenarien zeichnet sich für viele Anwendungen jedoch der Trend zu kurzen, zustandslosen, aus nur einem Datenpaket bestehenden Nachrichten ab. Safetymessages werden zum Beispiel nur aus einem Typecode und einigen physikalischen Vektoren bestehen (vgl. [ER01]).

Im Bereich „Safetymessages“ wird auch das zweite Problem deutlich: Authentifikation über TESLA liefert zunächst keine „Zurechenbarkeit“ (*non-repudiation*).

Jeder kann authentische TESLA Pakete nach Ablauf der non-disclosure time mit den nunmehr bekannten Schlüsseln generieren. Ein Sender von TESLA Paketen kann sich auf diese Tatsache berufen und das Senden der Pakete abstreiten.

### Fazit

Für VANET Szenarien ist das TESLA Protokoll, wie viele der anderen Lösungsansätze im Bereich mobiler ad-hoc Netzwerke auch, nur die Lösung für eine spezielle Anwendungsklasse. TESLA kann beständige Streamauthentifikation zu niedrigen Kosten auf eine einmalige Authentifikation zu Beginn der Kommunikation zurückführen.

Dennoch bleibt es ein Bootstrap, eine „Root of Trust“ bildet sich doch wieder nur durch herkömmliche Signaturen. [HL06] spricht in der Analyse des Protokolls zutreffend von einem „Break-Even Point“, was klar die Ambivalenz des Nutzens herausstellt:

Für kurze Protokolle, wie sie für viele VANET Anwendungen typisch sind, überwiegen die Nachteile. Auf der anderen Seite ist jedoch auch abzusehen, dass eine ganze Reihe von VANET Anwendungen kleine Nachrichten als kontinuierliche Datenströme verschicken werden (z.B. Heartbeats u.a.). Kombiniert mit der Fehlertoleranz bei verlorenen Datenpaketen hat TESLA hier vielversprechendes Potential für die Zukunft.

## Autorisierung und Authentifizierung in den Arbeiten

Es folgt eine Querschnitt über das Verständnis der Autorisation bzw. den Authentifikationsbegriff in verschiedenen Arbeiten. Im Sinne der vorgestellten Abgrenzungsmöglichkeiten in Abschnitt 2.1 wird hier nun herausgearbeitet auf welche Aspekte die jeweiligen Autoren ihren Schwerpunkt legen. Dazu wird ein kurzer Überblick über die Arbeiten geliefert und dann der Bezug zum Thema Autorisation bzw. Authentifikation hergestellt.

### Architecture for Secure and Private Vehicular Communications

In [PA07] geht es um die Bereitstellung einer Sicherheitsarchitektur, welche die Themen „Management von Identitäten und Kryptographischen Schlüsseln“, Kommunikations-sicherheit und die Integration von Mechanismen zur Privatheit aufgreift. Es wird hervorgehoben, dass die Sicherung von VANET Kommunikation ein herausforderndes Problem darstellt und zusätzlich zu den anspruchsvollen technischen Aspekten soziale, rechtliche und ökonomische Überlegungen eine Rolle spielen. Grundlage der vorgestellten Lösung ist eine Adaption Digitaler Signaturen und eine auf internationaler Ebene cross – zertifizierende PKI als „Anchor of Trust“.

„*Entity authentication is rather straightforward to achive in our context”* [PA07]

Das von einer CA ausgestellte Zertifikat eines Fahrzeuges oder einer RSU ist definiert als $Cert_{CA}\{V, K_V, A_V, T\}$, wobei V die Identität, $K_V$ die zugehörigen Schlüssel (public and private), $A_V$ ein Attributsvektor des Teilnehmers und T die Zertifikatsgültigkeitsdauer darstellt.
Traut man der CA, erhält man über den Vektor $A_V$ gleich auch die Grundlage für eine generelle Autorisationslogik.

Problematisch ist in diesem Ansatz, dass aus Sicht der Autorisation nicht unbedingt die Identität V offenliegen muss, V also anderweitig fixiert werden müsste.

Fazit: Autorisation ist in diesem Szenario das Ergebnis von zertifikatsgestützter Authentifikation, es handelt sich hier um die Sichtweise der „Sender Authentication“, wie sie in Abschnitt 2.1 dieser Arbeit vorgestellt wurde.

### VSC Project WAVE/DSRC Architecture

Das vom US Department of Transportation getragene Vehicle Safety Communications (VSC) Project veröffentlichte im April 2006 den „Final Report”, dessen Appendix H sich mit WAVE/DSRC Security befasst. Wireless Access in Vehicular Environments (WAVE) oder Dedicated Short Range Communication (DSRC) setzt auf der für 2009 geplanten IEEE 802.11 Erweiterung 802.11p auf. [VS05]

Im Appendix H werden zunächst die Security Services *Message Integrity / Origin Authentication* (*MI/OA*), *Correctness*, *Privacy*, *Robustness* und *Fail-Safety* definiert und Communication Security über eine „Strawman Security Architecture“ umrissen, die mit einem globalen symmetrischen Schlüssel arbeitet.

In Bezug zu dieser einfachen Architktur werden Vor- und Nachteile anderer Ansätze („Simple Public Keys“, „Anonymous Certificates“, „Anonymous Self-Enforcing Certificates“, „Dynamic Combinatorics“) erörtert ohne zunächst eine eindeutige Alternative zu wählen. Die Autoren vertreten den Standpunkt, dass digitale Signaturen der einzig gangbare Weg sind.
Schlussendlich wird das VSP (VSC Security Protocol) vorgestellt, das eine Variante anonymer Zertifikate darstellt. Das VSC Projekt verfolgt für OBUs und RSUs/PSOBUs (Public Safety OBUs) das gleiche Konzept: Es soll jeweils eine „klassische“ PKI zum Einsatz kommen („Duale Authentication Structure“). Autorisation ist also im Endeffekt das Ergebnis einer PKI gestützten Authentifikation.

Fazit: Das Verständnis von „Authentifikation” ist hier von „Identifizieren” weit entfernt, im VSC Projekt stellt Authentifikation (für OBUs) eher eine *Property Authentifikation* in Verbindung mit dem Security Service “Correctness” dar:
“*The purpose of MI/OA is to allow a receiving unit to determine whether messages that it receives were generated by valid VSC units and have not been tampered during transit.”* [VS05]

Die Identität liegt nicht direkt offen, da anonyme Zertifikate genutzt werden.
Allerdings ist das grundsätzliche Problem möglichen Missbrauchs dadurch nicht gelöst. Noch immer liegt die Kontrolle bei einer einzigen CA, und mit genug Rechenkraft können einzelne IVCs (Inter Vehicle Communication Keys, aus einem Hauptschlüssel abgeleitete Kommunikationsschlüssel) verlinkt werden.

*„[…] OBU revocation will happen relatively rarely and therefore need not be inexpensive […] Thus, w should be chosen so that it is […] impractical to do so on a mass basis.}“* [5.6.1, VS05]

Im Paper „SRAAC“ wird unter anderem dieses „weak cryptography“ Problem aufgegriffen, was es prädestiniert auch dort die Aspekte „Autorisation und Authentifikation“ näher zu beleuchten.

### Secure Revocable Anonymous Authenticated Inter-Vehicle Communication

In [FA06] gehen Fischer, Aijaz, Eckert und Vogt auf die kritischen Aspekte im Konzept der IEEE WAVE Group ein. Kerngedanke ist die spezielle Zielsetzung keine einzelne Instanz mehr zu etablieren, welche die Zertifikate zentral ausstellt und die Möglichkeit hat Zertifikate und Identitäten zu verknüpfen.

Die IVC Zertifikate sind relativ kurzlebig, nicht abstreitbar und nur verlinkbar, wenn mindestens eine gewisse Anzahl („t–out–of–n–scheme“) der Server der Revokation zustimmen.
Bei der Beschreibung des zugrundeliegenden Szenarios wird deutlich und korrekt hervorgehoben, dass jede Safety Message zumindest authentifiziert werden muss; der Aspekt der Autorisation wird umschrieben als „*Trust in the correctness of messages is rooted in trust in the manufactures...“* [FA06].

Korrekterweise wird hier jedoch nicht die Offenlegung der Identität gefordert – schließlich behandelt das Paper den Aspekt der Privatheit und nutzt die Begrifflichkeiten dementsprechend feiner granuliert.

„*In summary anonymity [...] is provided by separation of owner identity and vehicle/OBU identity. The linkability of the messages of a vehicle is prevented by frequently changing the IVC certificates used for authentication“* [FA06]

Im direkten Vergleich mit dem Paper „Architecture for Secure and Private Vehicular Communications“ von Papadimistratos et al. fällt auf – wir betrachten jetzt nur den Aspekt der Autorisierung und Authentifikation –, dass das SRAAC Paper als einen entscheidenden Vorteil den korrekten Umgang mit der notwendigen Information über den Sender aufweist:
Lediglich die Authentizität (durch die hinreichend schnell verfallenden IVC Zertifikate) ist gewährleistet, die Identität ist nicht pauschal offengelegt, dennoch kann im begründeten Fall die zugrundeliegende Identität ermittelt werden.
Im Sinne der hier durchgeführten Analyse des Authentifikationsbegriffes der Autoren, beschreibt das „SRAAC“ Paper eine „Sender Authentication“, bei der gewisse Properties/Eigenschaften durchaus mit einfließen können, die Identität selbst jedoch durch die anonymen Zertifikate nicht offengelegt wird.

## Zusammenfassung

Die vorliegende Ausarbeitung beschäftigte sich mit dem Themenkomplex „Autorisation und Authentifikation“ in VANETs und stellte insebesondere einen Querschnitt über die Authentifikationsbegriffe verschiedener Autoren und Werke im Forschungsfeld VANET dar.

Dazu wurde im Grundlagenteil auf die Probleme bei der Abgrenzung der Begriffe eingegangen, diese in Bezug zueinander gesetzt und schließlich definiert. Die kryptographische Primitive „Authentifikation“ wurde erläutert und dabei besondere Aufmerksamkeit auf Aspekte in VANET Szenarien gelegt.

Exemplarisch wurde die one-to-many Authentifikation erläutert und dabei am Beispiel von TESLA ein konkretes Authentifizierungsprotokoll bzw. ein Vorgehen zur Adaption bestehender Techniken an die Randbedingungen eines neuen technischen Umfeldes aufgezeigt. Es wurde beschrieben inwiefern public key Kryptographie eine Antwort auf die Authentifikationsbedürfnisse mobiler ad-hoc Anwendungen darstellt und welche Ansätze von diversen Autoren für sinnvoll erachtett werden.

Es wurde deutlich, dass es einen gewisses Kontinuum, einen Spielraum in der „Stärke“ der Authentifikation und im Verständnis des Begriffes gibt: Von der Sichtweise auf die Nachricht an sich (geht im wesentlichen mit Integrität bestenfalls mit Kohärenz zum aktuellen Umweltmodell der OBU einher), über „Property Authentication“ bis hin zu Authentifikationsprotokollen, welche Aufschluss über die Identität geben. Nicht–Abstreitbarkeit erfordert Mechanismen zur Offenlegung der Identität, während Privatheit konträre Anforderungen stellt. Die Autorisationslogik vieler Anwendungen jedoch benötigt meist nur die Sicherheit über gewisse Eigenschaften (z.B. Art und Lokation) des Senders.

Generell ist in vielen der ohnehin überschaubaren Publikationen zum Thema VANETs das Thema „*Sicherheit*“ ausgeklammert bzw. auf spätere Entwicklungen verschoben. Obwohl viele Autoren die Relevanz der einhergehenden Fragestellungen nicht abstreiten, tendieren auch viele Stimmen dazu, dass Security–Aspekte in späteren Entwicklungsphasen Berücksichtigung und Eingang finden werden. Autoren die sich mit der Entwicklung einer allgemeinen Basisarchitektur beschäftigen, gehen erwartungsgemäß eher auf sicherheitsrelevante Fragestellungen ein.

Angesichts der Bedeutung und Komplexität einer sicheren Basisarchitektur für die Fülle angedachter Anwendungen ist eine allzu einfache, isolierte Betrachtungsweise nicht gerade empfehlenswert. Dabei sind Autorisation bzw. Authentifikation noch vergleichsweise einfache Designziele, die Entwicklung konkreter Implementationen wirft Fragen der *Repudiation*, *Isolation* und *Linkability* auf, welche die Adaption bestehender Systeme an VANET Szenarien weiter erschwert und als Herausforderung die Entwicklung von neuen Verfahren und Protokollen mit sich bringt.

## Literaturverzeichnis


[BR07] Der Brockhaus: In 15 Bänden Leipzig, Mannheim: F.A. Brockhaus
2002-2007 Bib. Inst. F.A. Brockhaus AG, Mannheim

[CE04] Prof. Dr. Claudia Eckert:
„IT-Sicherheit: Konzepte-Verfahren-Protokolle“
München: Oldenbourg W.Verlag GmbH, 2004, 3. Auflage, Kapitel 4.9

[DS00] “Digital Signature Standard”
National Institute of Standards and Technology, FIPS Pub 186-2, 2000

[ER01] André Ebner, Hermann Rohling:
„A Self-Organized Radio Network For Automotive Applications”
8th World Congress on ITS, ITS 2001, Sydney, Australia, October 2001

[FA06] Lars Fischer, Amer Aijaz, Claudia Eckert, David Vogt:
“Secure Revocable Anonymous Authenticated Inter-Vehicle Communication (SRAAC)”
13-15 November 2006, In ESCAR 2006 - Embedded Security in Cars

[FK06] Frank Kargl, Zhendong Ma, Elmar Schoch: “Security Engineering for VANETS”
4th Workshop on Embedded Security in Cars, Berlin, 2006

[HL06] Yih-Chun Hu and Kenneth P. Laberteaux
“Strong VANET Security on a Budget”
Proceedings of the 4th ACESC (escar 2006). is-its, Berlin, Germany, November 2006

[ITSS] “ITS Standards Program"} Stand: 22.12.2007, 20:02 Uhr
http://www.standards.its.dot.gov/StdsSummary.asp

[JB04] Johannes Buchmann: „Einführung in die Kryptographie“
Berlin: Springer Verlag, 2004, 3. erw. Auflage

[MDNF] Microsoft Developer Network .NET Framework} Stand: 13.12.07, 19:50 Uhr
http://msdn.microsoft.com/library/deu/default.asp?
1. url=/library/DEU/cpguide/html/cpconASPNETAuthentication.asp
2. url=/library/DEU/cpguide/html/cpconaspnetauthorization.asp

[PA07] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, and M. Raya,
“Architecture for Secure and Private Vehicular Communications",
In Proceedings of the 7th International Conference on ITS Telecommunications,
Sophia Antipolis, France, June 2007

[RH05] Maxim Raya, Jean--Pierre Hubaux
“The Security of Vehicular Ad Hoc Networks”
Proceedings of the 3rd ACM workshop on Security of ad hoc and
sensor networks (SASN'05), pp. 11-21, 2005

[TK05] Timo Kosch “Technical Concept and Prerequisites of Car-to-Car Communication”
5th European Congress and Exhibition on ITS, Hannover, 2005

[TP02] Adrian Perrig, Ran Canetti, J.D. Tygar, Dawn Song
“The TESLA Broadcast Authentication Protocol”
In RSA Cryptobytes, Summer 2002.

[WKAT] Wikipedia (DE), „Authentisch“, „Authentizität von G./I.“, „Inf.“
Stand: 16.12.2007, 05:13 Uhr http://de.wikipedia.org/wiki/Authentisch

[WKAU] Wikipedia (DE), „Authentifikation“ Stand: 21.12.2007, 22:22 Uhr
http://de.wikipedia.org/wiki/Authentifikation

[WPKI] Wikipedia (EN), “Public Key Cryptography” Stand 18.12.2007, 08:25
http://en.wikipedia.org/wiki/Public-key_cryptography

[VS05] “Vehicle Safety Communications Projekt Task 3 Final Report”
U.S. Department of Transportation, nhtsa
National Technical Information Service, Springfield, Virginia, 2005

[VH05] “Appendix H: WAVE/DSRC Security” zu [VS05]