



**Institut für Telematik** unter Betreuung der  
**Fraunhofer Gesellschaft**



 **Preprint 02-04**

## **Digitale Signaturen für Kraftfahrzeuge**

Lutz Gollan

Christoph Meinel

Author	Lutz Gollan Dr. iur. Christoph Meinel Univ.-Prof. Dr. sc. nat.
Copyright	© 2002 Institut für Telematik e.V., Trier
Trademarks	All terms that are mentioned in this paper that are known to be trademarks or service marks have been appropriately capitalised. Use of a term in this paper should not be regarded as affecting the validity of any trademark and service mark. The product or brand names are trademarks of their respective owners.
Printing	08/02
Document status	Version 0.3 (08.2002) Printed in Germany All rights reserved The documentation was accomplished through the Institut für Telematik. The information contained in this document represents the current view of the authors on the issues discussed as of the date of publication. Because the present methodology must respond to changing research conditions, the results of this paper should not be interpreted to be a commitment on the part of the authors. Any information presented after the date of publication are subject to change. The right to copy this documentation is limited by copyright law. Making unauthorised copies, adaptations or compilation works without permission of the authors or institutions mentioned above is prohibited and constitutes a punishable violation of the law.

## Inhaltsverzeichnis

1. Zusammenfassung .....	4
2. Einleitung .....	4
3. Technologievorschlag.....	5
4. Anwendungsgebiete .....	8
4.1. Zweifelsfreie automatische Lokalisation von Fahrzeugen.....	8
4.2. Sichere Bezahl- und Abrechnungsvorgänge .....	10
4.3. Fahrzeug-Softwareupdates aus der Ferne .....	11
4.4. Mobile Versorgung mit digitalen Gütern .....	11
4.5. Personalisierung digitaler Güter.....	12
4.6. Aufklärung bzw. Verhinderung von Straftaten .....	12
5. Datenschutz.....	13
6. Zusammenfassung .....	14
Literatur .....	15

## 1. Zusammenfassung

Das Identifizieren und Lokalisieren von Fahrzeugen ist für die Flottenlogistik von herausragender Bedeutung. Die bestehenden, nicht automatisierten Verfahren sind leicht zu täuschen oder aufwändig über Entfernungen hinweg durchzuführen. Das Kombinieren der erfolgreichen Technologie der digitalen Signatur mit dem Global Positioning System oder anderen Lokalisationstechnologien bei Nutzung drahtloser Übertragungswege macht hingegen die sichere Identifikation und Authentifikation von Fahrzeugen und die eindeutige Bestimmung ihres Standorts möglich. Dies kann genutzt werden, um das Flottenmanagement zu verbessern und neue Anwendungsbereiche für den privaten, geschäftlichen und öffentlichen Sektor zu erschließen.

## 2. Einleitung

Wie kann ein Auto identifiziert werden? Diese Frage ist nicht erst dann von Bedeutung, wenn das Fahrzeug gestohlen wurde. Sie ist schon dann wichtig, wenn man eine größere Zahl von Kraftfahrzeugen verwalten will und als Eigentümer stets wissen muss, wo diese sich momentan befinden. – Die Tatsache, dass allein in Deutschland im Jahr 2001 mehr als 50 Millionen Kraftfahrzeuge in Betrieb waren, macht offensichtlich, dass die Identifizierung allein anhand von Marke, Modell und Farbe nicht ausreicht. Sich auf die Nummernschilder zu verlassen, ist angesichts der relativen Einfachheit von Fälschungen ebenfalls nicht empfehlenswert.

Es empfehlen sich daher komplexere Methoden. Bislang griff man auf fest angebrachte oder eingravierte Seriennummern an Chassis, Fenster oder Motor zurück. Den Anforderungen an ein modernes, effizientes und verlässliches Flottenmanagement auch über große Entfernungen hinweg kann diese Technik jedoch nicht gerecht werden. Denn wie kann mit dieser Methode ein 500 km entferntes Auto identifiziert werden? Und wie kann eindeutig dessen Position bestimmt werden? Speditionsunternehmen, Firmenfuhrparks, Autovermietungen, Rettungsdienste, besonders aber auch das Militär sind jedoch auf diese Informationen verstärkt angewiesen. Die genannten Methoden kranken zunächst an ihrer örtlichen Gebundenheit, d.h. an die Anwesenheit des Fahrzeugs zur Identifizierung. Außerdem können die genannten Daten leicht gefälscht werden. Bis heute muss zur Identifizierung eines Kraftfahrzeugs eine Person die genannten Daten am Fahrzeug nachschauen und mit einem

Papierdokument oder einer Datenbank über einen Sprechfunk-Kontakt vergleichen. Dabei besteht regelmäßig die erhebliche Gefahr der Fälschung der Daten.

Werden jedoch einmalige, praktisch nicht zu fälschende Daten zusammen mit einer eindeutigen Positionsangabe automatisiert versendet, so erhält man schnell eine zufriedenstellende Antwort auf die oben formulierten Fragen. Wenn das System dabei Gewähr dafür trägt, dass eine Veränderung der Daten während der Übermittlung einfach bemerkt werden kann, so ist das Ergebnis ein unvergleichlicher Fortschritt zur heutigen Lage. Die Übertragung entsprechender moderner Technologien auf diesen Bereich der Identifizierung und Lokalisation von Fahrzeugen stellt folglich eine bedeutende Aufgabe dar.

Dieser Aufsatz schlägt als Lösung für den genannten Problemkreis den Einsatz digitaler Signaturen zur Identifizierung von Kraftfahrzeugen über drahtlose Netze vor (vgl. auch [1]). Diese Technologie kann durch die Verwendung des Global Positioning Systems oder von Zellen- und Standortdaten aus dem GSM-Mobilfunknetz ergänzt werden, um die Lokalisation der Fahrzeuge zu ermöglichen. Auf Grundlage dieser Idee wird eine Reihe von hoch innovativen und praktischen Einsatzmöglichkeiten vorgestellt. Der Privat-, Geschäfts- und Güterverkehr sowie der öffentliche und militärische Bereich werden aus diesem Konzept erheblichen Nutzen ziehen können. Auch wenn dieser Aufsatz sich vorrangig auf den Einsatz der entsprechenden Technologien bei Automobilen bezieht, kann das Prinzip auch auf andere Fahrzeuge übertragen werden.

Zunächst wird die einzusetzende Technologie vorgestellt. Das darauf folgende Kapitel zeigt verschiedene Einsatzgebiete im Detail auf. Anschließend erfolgen Ausführungen zum Datenschutz. Abgeschlossen wird die Arbeit durch eine Zusammenfassung.

### **3. Technologievorschlag**

Der hier vertretene Ansatz geht davon aus, dass ein Fahrzeug mit einem kryptografischen Schlüsselpaar ausgestattet wird. Dieses kann zum Signieren und Verschlüsseln von Daten verwendet werden, die anschließend drahtlos an eine Basisstation und eine Datenbank gesendet werden. Die Basisstation bzw. die Datenbank werden im Auftrag des Fahrzeugeigentümers oder von ihm selbst betrieben und sind mit einer Datenbank verbunden, die Informationen über das Fahrzeug enthält.

Das einzusetzende Verfahren stützt sich auf digitale Signaturen. Heute und auch auf längere Sicht hin stellen diese in Verbindung mit hochsicheren technischen Komponenten ein

adäquates Mittel zur Identifizierung von Personen, Computern und Programmen dar. Sie garantieren die digitale Authentifikation des Unterzeichners und der Daten in Netzwerken. Digitale Signaturen beruhen auf einem sogenannten Zwei-Schlüssel-Verschlüsselungsverfahren (asymmetrische Kryptografie), die vielerorts Anwendung finden.

Zwei-Schlüssel-Verschlüsselungsverfahren verwenden anders als die herkömmlichen symmetrischen Systeme zwei verschiedene Schlüssel zum Ver- und Entschlüsseln: Der öffentliche Schlüssel ist für die mutmaßlichen Empfänger frei abrufbar und dient der Überprüfung einer mit dem privaten Schlüssel, der ausschließlich in der Verfügungsmacht des Unterzeichners steht, signierten Nachricht. Hierbei ist erforderlich, dass der private Schlüssel sicher verwahrt wird und Dritte darauf keinen Zugriff haben [2]. Grundsätzlich funktioniert das Verfahren folgendermaßen: Beide Schlüssel sind praktisch einmalig, ergänzen sich jedoch zu einem Paar. Gleichwohl können sie nicht von einander hergeleitet werden. Beim Signieren wird eine ebenfalls praktisch einmalige Kurzform der zu signierenden Nachricht mit dem privaten Schlüssel codiert. Anschließend erhält der Empfänger Nachricht und die codierte Kurzform, die eigentliche Signatur. Diese kann nur mit dem öffentlichen Schlüssel decodiert werden. Die Nachricht, die gegebenenfalls noch selbst zusätzlich verschlüsselt war, wird nun vom Empfänger in die gleiche Kurzform gebracht und mit der entschlüsselten Signatur überprüft. Stimmen beide überein, so kann der Empfänger sicher sein, dass der Unterzeichner die Datei signiert hat, denn nur er hatte den korrespondierenden privaten Schlüssel. Sollte die Kurzform nicht übereinstimmen, so passen entweder die Schlüssel nicht zueinander, oder die Nachricht, die der Empfänger erhalten hat, stimmt nicht mit der überein, die der Unterzeichner signiert hatte.

Dieses Verfahren setzt in seiner sichersten Variante den Einsatz sogenannter Trust Center voraus. Diese fungieren als "elektronische Notare" und bestätigen – ebenfalls durch eine digitale Signatur in einem elektronischen Zertifikat –, dass ein bestimmtes Schlüsselpaar einer bestimmten Person oder einem bestimmten Computer zugeordnet ist.

Bislang werden digitale Signaturen nur zur Authentifizierung von Personen, Programmen und Computern verwendet. Es ist jedoch, wie eingangs dargelegt, in vielen Fällen von ebenso großer Bedeutung, Gegenstände zu authentifizieren. Dies bedeutet, dass die Identität eines Objekts, wie z.B. eines Autos, eindeutig sichergestellt werden kann. Ein weiterer Vorteil der Verwendung von elektronischen Verfahren liegt darin, dass diese ohne weiteres drahtlose Übertragungswege nutzen können. Der hier beschriebene Ansatz diskutiert da-

her das Konzept der drahtlosen Datenübertragung von Kraftfahrzeugen zur sicheren Identifikation über längere Strecken.

Da die einzusetzende Technologie grundsätzlich vorhanden ist, können die bestehenden Komponenten und Infrastrukturen zum größten Teil genutzt werden. Das Verzeichnis mit den Zertifikaten und den Identifikationsdaten der Fahrzeuge darf jedoch anders als bei den bestehenden Public-Key-Infrastrukturen, die das Rückgrat der digitalen Signaturen bilden, nicht unbeschränkt einsehbar sein. Durch eine intelligente Rechteverwaltung muss sichergestellt werden, dass nur der Eigentümer und Fahrzeugführer, in besonderen Fällen auch Dritte, zu Abfragen berechtigt sind. Soll dies auf wenige Male beschränkt werden, bieten sich Transaktionsnummern zur Autorisierung an.

Um das beschriebene System auch tatsächlich zu betreiben, sind jedoch noch spezifische weitere Vorarbeiten zu leisten. Zuerst müssen die jeweiligen Fahrzeuge registriert und mit einer Signatureinheit ausgestattet werden. Diese sollte mit dem Fahrzeug fest verschweißt und versiegelt werden. Außerdem muss das Schlüsselpaar sicher erzeugt und dem Fahrzeug zugeteilt werden. Hierbei müssen Schlüssellänge und die Erzeugungsalgorithmen eine ausreichend hohe Sicherheit und Anzahl verschiedener Schlüssel sicherstellen.

Die mit dem Fahrzeug verschweißte Signaturerstellungseinheit beinhaltet den privaten Schlüssel, der nur durch einen Berechtigten, in der Regel den Fahrer und den Eigentümer, zum Signieren eingesetzt werden kann. Die Signatur wiederum kann nur mit dem im Zertifikat enthaltenen öffentlichen Schlüssel, der sich in der Fahrzeug-Datenbank befindet, überprüft werden. Beim eigentlichen Gebrauch werden Informationen wie die Fahrzeug-Identifikationsnummer und andere Daten von der Einheit signiert und zur Basisstation gesendet.

Die Identifizierung kann dabei auch durch ein Challenge-Response-System erfolgen. Die Basisstation schickt einen Zufallscode an das Fahrzeug, dieses signiert ihn und schickt ihn zurück. Dieses Verfahren könnte sogar automatisiert werden. In der Basisstation wird die Signatur mit dem öffentlichen Schlüssel überprüft. Stimmt die Signatur bzw. die entschlüsselte Kurzform des Zufallscodes mit dem ursprünglich gesendeten überein, so steht fest, dass das Fahrzeug mit dem dazugehörigen privaten Schlüssel geantwortet hat. Um sicher zu stellen, dass kein Dritter die Kommunikation abhört, kann diese selbst über verschlüsselte Kanäle (z.B. SSL oder WTLS [3]) erfolgen.

## 4. Anwendungsgebiete

Die Möglichkeit, ein Fahrzeug über digitale Signaturen zu identifizieren, kann sowohl im privaten bzw. geschäftlichen wie auch im öffentlichen bzw. staatlichen Bereich genutzt werden. Folgende Anwendungsbereiche könnten profitieren:

- Flottenmanagement
- Autowartung
- Mehrwertdienste
- Sicherheit.

Einige der möglichen Einsatzbereiche, die einen unmittelbaren Nutzen aus der geschilderten Technologie ziehen können, werden im Folgenden besprochen.

### 4.1. *Zweifelsfreie automatische Lokalisation von Fahrzeugen*

Das Signieren von Zufallscodes oder IDs genügt zwar, ein Fahrzeug zu identifizieren, über dessen Aufenthaltsort ist damit jedoch nichts gesagt. Zur Lokalisation des Kraftfahrzeugs müssen daher weitere Daten bereitgestellt werden.

Die Automatische Fahrzeug Lokalisation ("Automatic vehicle location", AVL) nutzt drahtlose Übertragungstechnologien zur Ortsbestimmung von Fahrzeugen mit Hilfe digitaler Informationen. Zu wissen, wo sich ein Fahrzeug befindet, ist nicht nur für den Fahrer interessant. Wenn eine Spedition genau bestimmen kann, wo sich ein bestimmter Lastkraftwagen mit einer bestimmten Ladung momentan befindet, kann diese ihre Dienste optimieren und z.B. den Kunden über etwaige Verspätungen automatisch benachrichtigen. Außerdem kann das Fahrzeug bei Diebstahl oder Carnapping verfolgt werden. Autovermietungen können über AVL überprüfen, ob das Fahrzeug möglicherweise unberechtigt die Landesgrenze übertritt etc.. Schließlich können Firmen, die diese Technologie einsetzen, technische oder medizinische Hilfe direkt an den Aufenthaltsort vermitteln.

Die Ortsbestimmung kann zum einen über das Global Positioning System (GPS), zum anderen über Zelleninformationen des GSM-Mobilfunknetzes erfolgen. Die GPS-Technologie nutzt Orbitalsatelliten, die weltweit ansteuerbar sind. Die entsprechenden Fahrzeuge würden neben der Signaturerstellungseinheit über einen GPS-Empfänger verfügen, der die Ortsbestimmung anhand des Koordinatensystems der Erde ermöglicht. GPS wurde vor zwei Jahren von den USA, die als Betreiber 24 Satelliten für das aus dem militärischen Bereich

stammende System bereitstellen, erheblich verbessert. Am 01.05.2000 wurde von den USA die "selective availability" für die nicht-behördliche Nutzung aufgehoben. Bis dahin war das System in seiner Genauigkeit künstlich beschränkt. Die Genauigkeit der Messung beträgt nun wenige Meter im dreidimensionalen Raum, während es zuvor noch ca. 100 Meter waren. Verwendet man zusätzlich das *Differential* GPS, bei dem neben den Satelliten feste Sender auf der Erde als Referenzpunkte genutzt werden, so kann die Positionsbestimmung auf wenige Zentimeter optimiert werden. Da GPS auch die Z-Koordinaten übermittelt, kann sogar die Höhe des Empfängers, allerdings nicht so genau wie die Position in der Fläche, ermittelt werden.

GPS und digitale Signaturen zu verbinden bedeutet, dass eindeutig und jederzeit die Position eines bestimmten Fahrzeugs erkannt werden kann. Bisher können die GPS-Daten, die ein Fahrzeug weitergeben kann, nicht mit Sicherheit auf das bestimmte Fahrzeug rückverfolgt werden kann. Dies kann jedoch mit Hilfe der digitalen Signaturen geschehen. Um den Eigentümer über den Aufenthaltsort zu informieren, signiert das Fahrzeug die von den GPS-Satelliten erhaltenen Koordinaten, gegebenenfalls zusammen mit einem von der Basisstation des Eigentümers erhaltenen Zufallscode, und leitet diese drahtlos an die Basisstation weiter. Schon anhand der Entschlüsselungsmöglichkeit, aber auch unterstützt durch den ebenfalls signierten Zufallscode kann der Eigentümer sich sowohl über die Identität des Fahrzeugs, als auch über dessen Aufenthaltsort sicher informieren. Nicht vergessen werden darf jedoch die Tatsache, dass das frei verfügbare GPS-System („Standard Positioning Service“ - SPS) keine verschlüsselten Kanäle nutzt. Diese sind dem US-Militärgebrauch vorbehalten („Precise Positioning Service“ - PPS). Ein GPS-Empfänger kann daher theoretisch mit Fehlinformationen versorgt oder ganz gestört werden.

Alternativ oder ergänzend zum GPS-System können auch Zelleninfos aus dem GSM-Mobilfunknetz verwendet werden. Diese sind nicht so genau, dafür besteht jedoch gerade in mit Hochhäusern dichter bebauten Stadtgebieten unter Umständen eine bessere Empfangseigenschaft als beim GPS-System, das einen freien Blick zu den Satelliten erfordert. Auf dem Land ist jedoch wegen weniger Mobilfunk-Zellen mit großem Durchmesser (bis 35 km) das GPS-System vorzuziehen. Ein weiterer Vorteil z.B. des GSM-Systems ist das Vorhandensein eines Rückkanals bzw. eines Kanals zum Eigentümer und dessen Datenbank, die über ein GSM-Gateway erreicht werden kann.

Der Einsatz von AVL in Verbindung mit digitalen Signaturen ist nicht auf den privaten bzw. geschäftlichen Bereich beschränkt. Das Militär könnte z.B. bei Nutzung der verschlüsselten GPS-Kanäle zweifelsfrei Einsatzfahrzeuge orten. Gleiches gilt für einen Notfalleinsatz der Feuerwehr oder von sonstigen Rettungsmannschaften oder der Polizei. Bei diesen Szenarien können die Daten von den Fahrzeugen automatisch signiert werden, die Fahrzeugbesatzung müsste dann nicht regelmäßig Positionsangaben per Funk, womöglich noch unverschlüsselt, übertragen.

#### **4.2. Sichere Bezahl- und Abrechnungsvorgänge**

Bislang basieren Bezahlmechanismen auf der Berechnung gegenüber Einzelpersonen, die einen Dienst oder eine Leistung in Anspruch nehmen und hierzu ihr Einverständnis erklärt haben. Im Bereich der Minimal-Beträge bietet es sich an, die Berechnung zu automatisieren und lediglich zu überprüfen, ob unverhältnismäßig hohe Summen entstehen. Hierdurch könnten erhebliche Personalressourcen eingespart werden. Die Abrechnung könnte auf Grundlage eines Rahmenvertrags erfolgen. Die diesen ausfüllenden Einzelverträge könnten unabhängig von dem Einverständnis einer bestimmten Person erfolgen – die Bestätigung des Fahrzeugs könnte ausreichen. Etwas Vergleichbares ist für das automatisierte Autobahn-Maut-System in Deutschland vorgesehen.

Bei der Verwendung von digitalen Signaturen durch Fahrzeuge könnten von diesen ausgelöste Abrechnungsvorgänge auf eine technisch sichere Basis gestellt werden. Das Kraftfahrzeug, mit möglicherweise verschiedenen Fahrern könnte sich gegenüber dem Dienstleister authentifizieren und seinen Eigentümer über den Rahmenvertrag rechtlich binden. In diesem Modell braucht nicht jeder einzelne Fahrer registriert und mit einer Signaturerstellungseinheit ausgerüstet sein – das Fahrzeug allein wäre ausreichend. Hierdurch kann der Dienstleister stets gegenüber dem Fahrzeug-Eigentümer, unabhängig vom jeweiligen Fahrer, abrechnen. Dies eignet sich insbesondere für die Fälle, in denen verschiedene Fahrer niedrig bepreiste Dienste wie Parkhäuser, Waschstraßen und Tankstellen nutzen. Aufwändige papierbasierte Abrechnungen mit Kleinstbeträgen würden dadurch hinfällig.

### **4.3. Fahrzeug-Softwareupdates aus der Ferne**

Ein weiterer Typus von tauglichen Diensten, die ein Fahrzeug erwerben könnte, wäre das Aktualisieren und Reparieren der Kraftfahrzeugelektronik. Diese wird heutzutage, genau wie mittlerweile auch viele Bereiche der Mechanik (z.B. der Motor), zunehmend durch Software gesteuert. Der Benzinfluss kann z.B. in vielen Fahrzeugen elektronisch geregelt und durch eine Abgas- und Leistungskontrolle optimiert werden. Bei einer Identifizierung des Fahrzeugs könnten Patches oder neue Versionen der Bord-Software – z.B. über GSM, GPRS oder UTMS - eingespielt werden. Wenn dabei detaillierte Informationen über das Fahrzeug und seinen Zustand mit übertragen werden, so können für dieses spezifische Einstellungen mit berücksichtigt werden. Die Authentifizierung und Identifizierung des Fahrzeugs würde neben der Sicherheit hinsichtlich der Abrechnung auch garantieren, dass die richtige Software eingespielt wird.

Der Update-Prozess dürfte selbstverständlich nicht während der Fahrt erfolgen. Die Information, ob und wie lange das Fahrzeug schon steht – und wo – kann jedoch jederzeit ebenfalls signiert und versendet werden. Außerdem ist es möglich, durch die Erforderlichkeit einer weiteren Signatur, z.B. die einer autorisierten Kraftfahrzeugwerkstatt, die Sicherheit des Verfahrens auch in dieser Hinsicht zu gewährleisten. Die erforderliche Mitarbeit von Personen wäre minimiert. – Da die Software drahtlos übertragen werden kann, wäre darüber hinaus auch eine Reparatur bzw. Unterstützung einer solchen bei einer Autopanne außerhalb einer Werkstatt möglich.

### **4.4. Mobile Versorgung mit digitalen Gütern**

Da ein Auto heute für viele Bevölkerungsschichten nicht mehr nur ein bloßes Fortbewegungsmittel ist, sondern vielmehr auch von den Nutzern als Büro, Kommunikationsort und Unterhaltungsraum verwendet wird, stellt es für die Telematik einen interessanten Entwicklungsbereich dar. Während das Tunen und Reparieren der Kraftfahrzeugelektronik für das Auto als solches von Bedeutung ist, können verschiedene andere softwarebasierte Dienste einen Mehrwert für die Passagiere darstellen.

Schon heute sind einige Fahrzeuge mit Kleinst-PCs und Multimedia-Geräten ausgestattet, wie z.B. der VW Golf *eGeneration*. Sobald Bildschirme und Eingabegeräte in Autos eine büroähnliche Umgebung bilden, kann der Fuhrpark eines Unternehmens über die hier geschilderte Technologie die Fahrzeuge spezifisch mit Office-Software, Kommunikationslö-

sungen und auch Unterhaltungsdienste ausstatten - über einen entsprechenden Dienstleister oder Application Service Provider. Die jeweiligen Fahrer oder Insassen zu identifizieren, ist oft nicht erforderlich. Bei den niedrig bepreisten Anwendungen steht für die Flotten-Inhaber allein schon wegen der zu vereinfachenden Abrechnung die Identifizierung des Fahrzeugs im Vordergrund.

Nicht nur Anwendungen, auch Inhalte, wie z.B. Landkarten für Navigationssysteme oder Spielfilme könnten drahtlos an das Fahrzeug übermittelt und direkt in die Anwendungen integriert werden. Der Fahrzeuginhaber, unter Umständen ist dies ein Busunternehmer, könnte diese Inhalte abonnieren, möglicherweise im Zusammenhang mit einem Leasingvertrag.

#### **4.5. *Personalisierung digitaler Güter***

Das Anpassen spezieller digitaler Inhalte für bestimmte Fahrzeuge ist ebenfalls vorstellbar. Die Basisstation könnte speziell auf eine Bus- oder Bahnlinie abgestimmte Werbung für an der Route liegende Geschäfte auf Bildschirme in die Wagen übertragen, abhängig von deren momentanem Aufenthaltsort während der Fahrt. Die Verwendung von digitalen Signaturen und Lokalisationsdaten zur Authentifizierung und Ortung der einzelnen Fahrzeuge würde zum einen sicherstellen, dass die richtigen Fahrzeuge „getriggert“ würden, zum anderen wäre eine nach Fahrzeug, Route und Werbekunde aufgegliederte Abrechnung möglich. Hierzu würde sich das Versenden von digitalen Quittungen durch die Fahrzeuge als weiteres Sicherheitsmerkmal anbieten.

#### **4.6. *Aufklärung bzw. Verhinderung von Straftaten***

Im Jahr 2001 gab es in Deutschland mehr als 75.000 [4] polizeilich registrierte Autodiebstähle, einschließlich der unbefugten Gebrauchsnutzung. Die Zahlen der Verkehrsunfälle mit Kraftfahrzeugen oder von Straftaten, bei denen Automobile zur Tatausübung genutzt wurden, sind noch höher. Das Lokalisieren und Identifizieren von Fahrzeugen würde den Strafverfolgungsbehörden das Auffinden und das Bestimmen des Aufenthaltsortes eines Fahrzeugs zu einem bestimmten Zeitpunkt erheblich erleichtern. Die entsprechenden Behörden könnten, auf richterliche Anordnung hin, Zugang zu den Datenbanken der Basisstationen haben und auch die Sicherstellung der Fahrzeuge an ihrem aktuellen Standort einleiten.

Insbesondere für diese Fälle ist jedoch ein Abwägen von Individualrechten und dem öffentlichen Interesse unerlässlich. In vielen Fällen wird man zu dem Ergebnis kommen, dass ein staatlicher Zugriff auf die Daten nicht zulässig ist. Aus diesem Grund darf der Aspekt des Datenschutzes nicht vernachlässigt werden.

## 5. Datenschutz

Das Verfolgen und Lokalisieren eines Fahrzeugs durch den Eigentümer bedeutet in den meisten Fällen, dass auch der Fahrer und die anderen Insassen aufgespürt und kontrolliert werden können. Falls ein Dritter, der nicht der Eigentümer des Fahrzeugs ist, Zugriff auf die Datenbanken bekommt, so sind die Datenschutzrechte bzw. andere Rechte aus seinem Gewerbebetrieb ebenfalls gefährdet. Daher können alle hier geschilderten Anwendungsbeispiele, die AVL nutzen, in Konflikt mit dem Datenschutz und privaten Rechten geraten. Hier können Einwilligungen der Beteiligten entgegenwirken.

Um den Gesamtbereich der Auswirkungen auf den Datenschutz zu betrachten, sollten zwei Situationen unterschieden werden. Während einige der hier diskutierten Anwendungen auf Verbraucher gerichtet sind, eignen sich andere mehr für den Geschäfts- oder öffentlichen Bereich. Beide unterscheiden sich hinsichtlich ihrer datenschutzrechtlichen Relevanz.

In den Fällen, in denen ein entsprechend ausgerüstetes Fahrzeug einer Privatperson gehört und nur von dieser genutzt wird, muss diese die Möglichkeit haben, die Dienste, insbesondere die AVL, abzuschalten (Erlaubnis mit Verbotsvorbehalt). Alternativ kann jede Nutzung von einer konkreten Zustimmung abhängig gemacht werden (Verbot mit Erlaubnisvorbehalt). Letzteres sichert den größtmöglichen Schutz personenbezogener Daten. Wird einem Dritten die Nutzung des Fahrzeugs gestattet oder fahren Dritte als weitere Insassen mit, so muss der Eigentümer diese über die installierte Technik und die darauf aufbauenden Anwendungen informieren. - Für den Fall des Diebstahls des Fahrzeugs sollte unabhängig davon die Möglichkeit der Fernaktivierung der AVL existieren.

Die Situation ist eine andere, wo die mit AVL ausgestatteten Fahrzeuge einem Unternehmen oder einer Behörde gehören. In diesen Fällen sind auch arbeits- bzw. beamtenrechtliche Einschränkungen zu beachten. Der Inhaber oder Vorgesetzte wird vielfach ein erhebliches Interesse an der Nachverfolgung und Lokalisation der Fahrzeuge haben. Die Mitarbeiter, die die Fahrzeuge nutzen, werden möglicherweise jedoch nicht in der Position sein, ih-

re unveräußerlichen Rechte hinsichtlich ihrer Privatsphäre durchzusetzen. Aus diesem Grund muss bei der Einführung und Regelung entsprechender Anwendungen ein besonderes Augenmerk nicht nur auf das Datenschutz-, sondern auch auf das Arbeitsrecht gelegt werden.

## 6. Zusammenfassung

Bislang werden digitale Signaturen ausschließlich zum Authentifizieren von Personen, Programmen und Rechnern verwendet. Dieser Aufsatz beschreibt die Ausdehnung des Verfahrens auch für den Bereich der Authentifizierung von anderen Gegenständen, konkret von Kraftfahrzeugen. Durch die Zuordnung eines kryptografischen Schlüsselpaares innerhalb einer Public-Key-Infrastruktur kann ein Fahrzeug bei Nutzung drahtloser Übertragungswege über eine Distanz hinweg eindeutig erkannt werden. Die Identifizierung zusammen mit der Verwendung weiterer Daten, wie z.B. den Standort-Koordinaten, eröffnen neue Einsatzbereiche für moderne Software-Anwendungen, die leicht zu implementieren sind.

Zentraler Bestandteil dieser Abhandlung ist die Beschreibung der neuartigen Idee, zwei schon bestehende technische Systeme zusammenzuführen, um ihre Vorteile für neue Einsatzbereiche zu kombinieren. Die hier vorgestellten Beispiele führen die Nutzung von digitalen Signaturen mit automatischen Lokalisationstechniken zusammen. Sowohl die Technologie der digitalen Signaturen unter Nutzung der schon bestehenden Public-Key-Infrastrukturen als auch die Global Positioning System-Technik oder die Mobilfunk-Alternative fallen kontinuierlich im Preis. Basis-PKI-Funktionalitäten können sogar mit kostenloser Software genutzt und angepasst werden.

Wie in diesem Aufsatz dargelegt, erlaubt das digitale Signieren von eindeutigen Positionsdaten bei Nutzung drahtloser Übertragungswege auch über große Entfernungen hinweg das Aktualisieren und Reparieren von Fahrzeugen über Softwareanpassungen. Ferner können moderne Abrechnungsverfahren für Anwendungen und digitale Inhalte gegenüber dem Fahrzeughalter eingeführt werden, unabhängig vom jeweiligen Fahrer. Darüber hinaus können Inhaber von Autofloten deren Management verbessern. Schließlich können Strafverfolgungsbehörden durch den Zugriff auf die Datenbanken mit den Standort-Daten die entsprechenden Fahrzeuge leicht lokalisieren und verfolgen.

Bei all diesen Anwendungen darf jedoch nicht übersehen werden, dass sehr leicht datenschutzrelevante Informationen über die jeweiligen Fahrer und weitere Insassen gewonnen

werden können. Die Beachtung des Datenschutzes, aber auch des Arbeitsrechts und der Rechte des Fahrzeughalters darf daher bei der Einführung entsprechender Systeme nicht vernachlässigt werden. Bei Berücksichtigung der hier dargestellten Grundsätze werden jedoch leicht und kostengünstig neue Anwendungen zur Erhöhung der Fahrzeugsicherheit, der Steigerung der Effizienz von Fahrzeugflotten und des Komforts der Passagiere und Fahrer implementierbar.

## Literatur

- [1] L. Gollan, Ch. Meinel, *Digital Signatures for Automobiles ?!* (Proc. SCI 2002, Orlando, Florida, USA, 2002, pp. 225-230).
- [2] B. Dusemund, T. Becker, L. Gollan, T. Engel, C. Meinel, *Security in Open Networks: The Functionality of a Public Key Infrastructure* (Institut für Telematik, Trier, 2001).
- [3] L. Gollan, A. Mabrouk, T. Engel, Ch. Meinel, *Mobile Commerce* (Institut für Telematik, Trier, 2000).
- [4] Bundeskriminalamt, *Polizeiliche Kriminalstatistik 2001* (BKA, Wiesbaden, 2001).