DIGITAL SIGNATURES FOR AUTOMOBILES?!

Dr. iur. Lutz Gollan[1]
Prof. Dr. sc. Christoph Meinel

Institute for Telematics
Bahnhofstr. 30-32
54292 Trier
Germany
www.ti.fhg.de

Abstract: Identifying and tracking vehicles is of major importance for today's logistics. The common non-electronic solutions are both easy to forge and difficult to use over distances. Combining the successful technologies of digital signatures and the Global Positioning System allows the secure identification of any car and checking its location. Both types of information can improve the fleet management and offer new fields of applications for both the private and the public sector.

Keywords: Authentication, Position location, Positioning systems, Digital Signatures, Telematics, Security, Mobile Networking, Automobiles.

1. INTRODUCTION

How do you tell which is your car? This question is not only of relevance when a car gets stolen. It is also important when a large number of vehicles has to be managed and their owner needs to know where each car is. - The very fact that in Germany in the year 2000 more than 50 million motor vehicles were in use makes it obvious that identifying a car only by the make, the model and the colour is not sufficient. Relying on the license plates is not advisable either, as they can easily be forged. Therefore more sophisticated methods of identifying an automobile are needed. So far, these methods of identification require firmly attached or engraved unique numbers (chassis and motor numbers). However, these methods are not efficient for today's demanding requirements of fast, reliant and also distant fleet management.

So how can you even tell reliably *across 500 km* which is your car and where it is located? A forwarding agency, a car rental company and especially the military depend on this information. All data mentioned above for identifying a vehicle is rather easy to forge, and, what is even more important, the data can only be read offline. Until today, the identification process requires a person who will look up this data and transmit it to the owner. As explained above, this person cannot be sure about the identification data as it may be forged. Sending *unique* electronic identification data that also includes information about the whereabouts of the vehicle automatically over the air is therefore the answer to the questions formulated above. If this system also reveals whether the data was altered on its way to the recipient, the result is an enormous improvement compared to the antiquated methods used today. Consequently, transferring modern wireless authentication, identification, and locating technology to motor vehicles is an important task.

This paper suggests the usage of *digital signatures* for motor vehicles for authentication and identification purposes within a wireless network. This technology can be complemented by the use of Global Positioning Systems to locate a vehicle. On the basis of this idea a number of highly innovative and practical applications will be explained in this paper. Private, freight and public/military traffic will benefit from this concept. While this paper addresses mostly applications for cars, the idea can be transferred to all other vehicles.

In this article, first the technology for providing the basic features is described. The next chapter shows

[1] E-Mail: Gollan@ti.fhg.de.

what kind of specific applications are possible with this technology. It is followed by remarks on the legal implications regarding the data privacy, and concluded with chapter 5.

2. TECHNOLOGY

The idea discussed here is that a car is supplied with a unique key pair for digitally signing and encrypting (identification) data, which is sent wirelessly to a base station. This base station is run by the car owner or a service provider and is connected to a database storing the details of the vehicles. This technology is called "digital signatures".

2.1 Digital Signatures

Today, digital signatures in connection with high-security components provide adequate means to identify persons, computers and programs in the digital world. They guarantee the authentication and integrity of the signer and the signed data in networks. Digital signatures are based on Public-Key-Encryption systems that are already used in various environments.

Public-Key algorithms make use of two different keys for encryption and decryption: the public key is widely available for any recipient for verifying the signature, and the private key, which is kept secretly and cannot be read out, is used for creating it (c.f. details on the technology Dusemund *et al.,* 2000). In basic, the technology works as follows: Both keys, the private and the public one, are virtually unique and complementary, but cannot be deducted from another. After the signing process where data is encrypted with the private key and thus the signature created, the data is sent to the recipient who can decrypt it only with the public key. If the decryption is successful, the recipient can be sure that only the holder of the private key could have created the signature and encrypted the data. The encryption feature of Public-Key-Infrastructures using a reverse mechanism allows in addition the data privacy.

The infrastructure also requires so called Trust Centers. These Trust Centers act as electronic notaries and guarantee the allocation of a key pair to the respective individual. They identify the individual during the registration phase and assign the key pairs.

So far, digital signatures are primarily used to authenticate persons and programs. But, as demonstrated above, it is similarly important to identify objects, too. The authentication of objects, such as cars, means that a single entity can be unambiguously identified. The additional advantage of digital signatures used in automobiles is founded on the fact that they can be transmitted wirelessly. Therefore, the concept discussed here offers the possibility to transfer data to and from authenticated motor vehicles securely and secretly over long distances.

As the technology would be similar, the usage of digital signatures for motor vehicles could easily use the existing infrastructures that are already in use. In order to prevent unauthorized third persons from getting information about the vehicles, the repository with the publics keys must be accessible only to the owners.

2.2 Implementation

To run this system, some preparatory work has to be done. First, the automobile is registered at the Trust Center and a high-security signature creation device is welded into the car and sealed. Afterwards, a key pair consisting of the public and the private key is generated. The key pair is generated in such a way that it is impossible to deduct one key from the other. In addition, the key length and the generation algorithms must ensure that a high number of different keys is available.

The signature creation device welded into the car holds the private key that can sign data. The signature can only be verified by the complementary public key which is stored in a repository that is connected to the base station and controlled by the car owner. During the registration process the vehicle's specifics and its public key get registered in the repository. Later on in the day-to-day usage, information on the vehicle, like the car's identity, and other data is signed by the signature creation device with the private key of the automobile and sent wirelessly to the base station.

The identification takes place by using a challenge-response system: the base station sends a random data string to the vehicle. This data is signed by the signature creation device using the private key, and is then sent back to the base station. Here the response is relayed to the repository where the data is decrypted by the according public key and then compared with the initial random data string. If the decrypted data and the data sent initially match, the owner can be sure that the right car has answered.

To ensure that no third person can tap the communication between the car and the base station, the data streams should be encrypted and the public key should also be kept secretly (refuting, of course, the original terminology).
Naturally, the vehicle might send identification data without any signature or encryption to the base station. This, however, would only perpetuate today's situation where this data can easily be forged.

3. FIELD OF APPLICATIONS

The possibility to identify and locate a motor vehicle unambiguously by the usage of a digital signature can

be realised in both private and public traffic and transport. The field of applications would allow the improvement

- of the efficiency of fleet management,
- of the car maintenance,
- of comfort,
- and an increase in security.

Some of the potential applications that would deliver these benefits are discussed in the following.

3.1 Automatic Vehicle Location and Fleet Management

Signing a simple random data string may help identify the car, but it does not tell the owner where the car is located. Thus, information on its coordinates must be transmitted, too.

Automatic vehicle location (AVL) is a wireless technology that allows tracking and locating motor vehicles by electronic means. Knowing where you are is not only important to the driver. When a forwarding agency can tell exactly where e.g. a truck carrying valuable goods is located, it can optimise its services for its customers and inform him/her about possible delays. It may also track a car in case of theft or car-knapping as long as the GPS-unit (Global Positioning System, c.f. below) and the signature creation device remain unharmed. Car rental companies can control by AVL whether the car is taken abroad or not etc. In addition, any company using this technology can direct technical or medical help to their vehicles in case of breakdowns or accidents.

Locating the vehicle is accomplished by the usage of the Global Positioning System (GPS). This technology uses satellites as orientation points and can be accessed worldwide. The vehicles carry mobile GPS units that allow their individual locating. GPS was improved not long ago by the United States of America, which runs the 24 satellites used by GPS. On May 1, 2000, the US administration loosened the so-called “selective availability” for non-government usage of the system. Until then it was artificially restricted in its accuracy. The improved availability allows now an accuracy of ca. 20 metres in three dimensions instead of roughly 100 metres for locating a mobile GPS unit. Using *Differential* GPS, where an additional stationary unit as a reference point is used, can narrow the accuracy down to a few metres. As GPS also supports locating in the third dimension, the altitude of the car can be checked, too.

Putting GPS and digital signatures together means knowing unambiguously at any time where a *distinct* car is *located* within a small radius. So far, the available systems transmit the GPS data for AVL not in such a way that the authenticity of the car is guaranteed. This can be accomplished by the use of digital signatures. To inform the owner of the car about its location, the vehicle *signs* its location data calculated from the satellite signals together with the random data string received by the base station and sends it to this station. By decrypting the data the owner can be sure about the identity of the vehicle and can also safely tell its location. However, it must be noted that the GPS signals available for general public use (Standard Positioning Service (SPS)) are not transmitted from the satellites to the mobile units over secure channels or encrypted. Encryption is restricted to the US military usage (Precise Positioning Service (PPS)). A GPS unit may therefore be misled by malicious jamming etc.

AVL in connection with digital signatures is not restricted to the private sector. From a military point of view it is important to know without doubt the location of military vehicles during an operation. This is also true for a fire brigade or any other public service that has to coordinate a certain number of vehicles over a certain distance. In these cases the automatic transmission of digitally signed GPS data would not require that a real person reports the location every now and then via radio to the base station. He or she could rather participate in other emergency actions.

3.2 Payment Systems

So far, payment systems are mostly used to bill a person for services it has acquired and has individually consented to this. For low-priced services it is recommendable to automate this billing and only check it individually in case of unusual incidents like unreasonably high amounts. Hereby, costly manpower can be saved. Automating the billing could take place by agreeing on a basic contract between the vendor and the buyer. The services are subsequently acquired not by the explicit consent of a person, but by the use of a machine, i.e. the vehicle.

By employing digital signatures in combination with motor vehicles, payment systems that are triggered by cars become available. The car itself, with possibly multiple alternating drivers, authenticates itself to the vendor and the owner is bound by a basic contractual agreement. The individual driver does not have to hold a key pair and be registered: the billing for the car-based services is accomplished by identifying the motor vehicle itself. Any such service enables the vendor to bill the owner of the car irrespective of the current driver. This is most interesting for car owners that have numerous drivers using the same vehicles. It allows an efficient cost control, as it is e.g. possible to track the fuelling and cleaning of all cars of a company if the vehicle authenticates itself to the filling station or to the car wash. Any paper-based fiddling with receipts etc. would be superfluous.

3.3 Mobile Tuning and Patching of Systems Software

Another type of services that a car could acquire through authentication is the patching and tuning of its systems software. As car electronics advance and take over many tasks that once were mechanically realised, the systems software for controlling the car will become more complex and important.

The fuel injection for example is highly important for running the car most effectively. If a motor vehicle authenticates itself to a repository via air, patches for the systems software could be installed wirelessly from it. During the authentication the vehicle could also submit relevant data about its technical status, allowing an optimised tuning for the very state the car is in. The car could send relevant information like the mileage, fuel consumption or the exhaust gas value to optimise in return the settings of the vehicle's electronics. The identification of the car would also guarantee that the *right* patch for the car's software would be installed and that the car owner gets billed for it. It could automatically send its make, year of construction, systems software version number etc. to the repository and thus receive the suitable patch.

The update process must, naturally, take place whilst the car is not in use. However, this information about its status could also be sent digitally signed to the base station that would initiate the patching and tuning process. The human involvement could be minimised. As the software could be transmitted to the car via air, too, the patching could be initiated by a mobile breakdown service on the road.

3.4 Application and Entertainment Services

As the car has become more than just a means of transportation, using the car for other purposes such as a mobile office or for entertainment is a highly innovative field for telematics, too. While the tuning or patching of the car's systems software is important for the car itself, application services represent an added value for the passengers.

Already some cars can be equipped with screens and small computers as a standard feature, like Volkswagen's Golf *eGeneration*. As soon as the screens and the input devices allow for a mature office-like environment, the car fleet of a company could be supplied with office applications and add-ons from a vendor wirelessly. Identifying the individual car allows for billing the owner of numerous cars and telling exactly how many and which cars exactly have received the software.

Not only applications, but also entertainment software and other media like street maps for a navigation system could be downloaded over the air after the authentication of the car. The car holder could subscribe to services such as movies that are offered e.g. in connection with a leasing contract for the car.

Customizing certain media to the location of a vehicle is also thinkable (c.f. 3.1). The base station could, for example, send specially selected advertisements to the video screens on certain bus lines with ads that are sponsored by the shops along the route. The use of digital signatures in these cases would guarantee that the right vehicles receive the right kind of information and that they could in return post a receipt if the transmission was successful. This receipt would be the basis for the billing of the advertisement agencies in the latter case.

3.5 Public Prosecution

In the year 2000, the German police registered more than 80,000 car thefts including unauthorized usage of cars (Bundeministerium des Innern, 2001). The number of traffic incidents with motor vehicles involved or the number of felonies and crimes where an automobile was used as a means are even higher. Locating and identifying a vehicle would help the public prosecution authorities in finding out where and when a car was and is at a given point in time. AVL would, for example, help solve questions of the whereabouts of a vehicle in case of an accident or locate it in case it was stolen. The relevant authorities could have access to the repository with the public key of the car and initiate the necessary actions for retrieving it or working out the facts of an accident.

Especially for these purposes a well-considered legal weighing of the rights of the individual and the interest of the public must be accomplished in the first place (c.f. 4). Many situations are conceivable where the authorities might see an advantage in knowing the location of each car. But the privacy of the cars' owners and of the drivers must be respected. Therefore the issue of data privacy must be discussed.

4. DATA PRIVACY

Tracking and locating a car means in most cases also tracking and locating the driver or other passengers inside. If a third person that is not the owner has also access to the information on the whereabouts of a vehicle, the privacy of the owner is affected, too. Thus, all applications suggested in this paper might get into conflict with the data privacy rights of the car's owner and/or the passengers. Knowing the exact location of a motor vehicle at any given point in time equals also that if the car is in use the location of the driver can also be spotted. This, of course, is in contradiction to the data privacy of the person affected if he or she does not consent to the surveillance.

To grasp the full extent of these issues, one must differentiate two situations: While some of the applications discussed here are aimed at the consumers' market, some others address the business

and administration/government market. Both differ in the implications of the data privacy problem.

4.1 Consumer Market

If the motor vehicle is owned by a consumer, he/she must have the possibility to switch the location service off, or he/she has to give consent every time it is used, with the effect that some services will not be accessible when the consent is being denied. This offers the highest level of privacy. If another person is granted access to the car, the owner should inform the other driver about the system and the applications used with it. This, however, is up to the owner's discretion. - If the car gets stolen, the system should allow the remote activation by the owner.

4.2 Business and Administration Market

But what happens if a company or an administrative body decides to use AVL and other services that allow the identification of the car? The owner is interested in the information transmitted by the motor vehicle, but in many countries it will be against the law to monitor the exact movements and location of the employees. However, the employees might not be in a position strong enough to protest against the use of such services that affect their privacy. Therefore it is necessary to carefully check the legal situation, especially in the field of labor law, to avoid any conflicts with the rights of the employees.

5. CONCLUSION

So far, digital signatures were mainly used for persons, computers and computer programs to identify them within a network. This paper suggests authenticating objects of everyday life by this technology, too. By assigning a key pair within in a wireless Public-Key-Infrastructure to a motor vehicle, it can be identified over long distances unambiguously. The identification together with other data unique to the car, like its location, opens new fields of application that are rather easy to put into practice.

The main feature put forward here is the fusion of two already existing technologies to combine their strength for new applications. The examples discussed show that there is a broad field of possible applications for digital signatures in combination with the Global Positioning System used by motor vehicles. GPS technology and Public-Key-Infrastructures are available and prices are dropping constantly, especially for the global positioning software and hardware. Basic PKI functions can be realized by using open source software such as openCA and openSSL, which is free and can be customised.

As demonstrated above, digitally signing location data would allow the unambiguous automatic location of vehicles (AVL), long distance software tuning and patching and the billing of smaller services to the car's owner, irrespective of the drivers. In addition, the public prosecution could benefit from the AVL system discussed here by locating a motor vehicle in case of theft or participation in a criminal offence or accident.

However, in all applications discussed here, the data privacy of the car's driver other passengers and the respective car owner must be respected. Tracing the movements of a person, even if it takes place indirectly, is one of the most sensible dangers to a his/her privacy.

REFERENCES

Bundesministerium des Innern (2001). *Polizeiliche Kriminalstatistik 2000*. Berlin, Germany.

Dusemund, B., Becker, T., Gollan, L., Engel, T., Meinel, C. (2001). *Security in Open Networks: The Functionality of a Public Key Infrastructure*. Institute for Telematics, Trier, Germany.