A Secure and Privacy-Preserving Electronic License Plate

Marko Wolf

escrypt GmbH, Munich, Germany

<marko.wolf@escrypt.com>

Abstract

The paper in hand describes a general, holistic approach for designing, securing, implementing, and applying an electronic license plate (ELP) for various existing and upcoming vehicular application scenarios. It contains a discussion about the manifold benefits of ELPs against conventional, pure physical license plates. The paper describes a possible ELP hardware architecture and the corresponding software architecture. It further describes the security mechanisms and protocols that enable a cryptography-based logical fixture between ELP and vehicle as well as an approach for effective ELP information access control based on at least four different access categories. The paper closes with a comprehensive set of possible ELP applications as well as a short discussion about the privacy aspects for a potential ELP application.

Keywords: automotive, security, e-plate, electronic license tag, electronic registration plate, RFID, IEEE 802.11p, hardware security module

1 Motivation

Companies or municipalities securely controlling access of vehicles to their premises or to (low emission) city zones, vehicles safely crossing bridges with height or weight limits, public authorities efficiently checking vehicle registration approvals – there exist already today many practical applications for vehicles communicating with their environment. While most vehicle-to-vehicle (V2V) communications solutions still lack a lucrative entry application to enable their practical implementation, vehicle-to-infrastructure (V2I) "communication" solutions have been being successfully applied for about 100 years – of course – mainly based on the visibility of the vehicle's license plate or special vehicular badges, labels, or stickers (e.g., toll stickers). Nonetheless, traditional pure physical license plates and most vehicle sticker approaches have a number of constraints that limit their application within existing and future applications. Some of them are indicated in the following listing.

Easy to remove or counterfeit. Even though it usually yields to severe legal consequences, unauthorized removal or counterfeiting license plates or vehicular stickers are still cheap and easy [6].

Limited amount of communicable information. The amount of information imprinted on license plates and vehicular stickers is limited due to the limited (physical) capabilities of humans (and the normally, similarly limited capabilities of automatic recognition systems) for reading information from a (fast moving) vehicle especially in the case of an improper perspective or under heavy weather conditions (e.g., night, rain) only via an optical channel.

Error-Prone Reading. For the same reason as stated above, the optical readout of information from a (moving) vehicle is very prone to errors especially under bad physical conditions.

Inflexible, costly, and disturbing. Adding, renewing, or removing especially stickers, tags, or badges from a vehicle (windshield) is annoying and costly. Moreover, having dozens of different stickers on the vehicular windshield increasingly perturbs the sight and the aesthetic sense of most drivers.

Can be security-critical and privacy-invasive. Having attached a sign that is visible for anybody that a vehicle, for instance, is a rental car, belongs to a certain company, or regularly pays toll fees for a certain road can be security-critical and privacy-invasive.

A new approach based on electronic license plate (ELP) that is able to communicate with its environment in a wireless manner would be a great opportunity to overcome most of the mentioned constraints. But instead of adding another new proprietary, expensive V2X box into every vehicle (e.g., as the German Toll Collect system [19]), this work proposes a simple but secure and privacy-preserving electronic license plate based on a small security microcontroller equipped with a wireless short-range communication transponder together with some well-adapted access control and privacy protection schemes. Thus, the electronic license plate is able to realize effective access control on restricted ELP information and hence is able to enforce driver's privacy in a dependable manner. The proposed approach, moreover, provides an effective approach for a logical fixture between ELP and vehicle (cf. Section 4.1) and is able to enforce intervisibility for certain information to prevent automated and easily scalable vehicle surveillance (cf. Section 4.2). Concretely, an ELP approach would/should provide at least the following benefits.

Difficult to remove and to counterfeit. Unauthorized removals and counterfeiting can be thwarted by a strong integration through the application of some physical tamper-protection measures together with strong cryptographic measures.

Enhanced communication bandwidth. The communication bandwidth of (wireless) electronic communication channels is much larger than the bandwidth of pure optical-based communication (under the previously described conditions).

Integrity-preserved reading. Underlying digital integrity-verification algorithms enables integrity-preserving reading and hence efficiently reduces the error rate on reading. Moreover, wireless electronic communication is almost independent from weather conditions and relative vehicle position.

Efficient, flexible, and non-disturbing. The application of electronic radio communication enables a very efficient and flexible adaption for new ELP information or different access restrictions and is virtually invisible for the driver.

Effective information access control and privacy protection. An underlying cryptography-based information access control scheme enforces restricted and authenticated access to all non-public information based for instance on the identity of the (wireless) reader or by enforcing vehicle intervisibility.

This work, hence, will provide a proposal for realizing such a secure and privacy-preserving electronic license plate as follows. Hereafter, it directly gives a first short overview about related work in the area of ELPs (cf. Section 2) followed by Section 3 describing a possible ELP hardware architecture and the corresponding software architecture. The paper then describes in Section 4 the effective security protocols that provide a cryptography-based logical fixture between ELP and vehicle as well as a possible approach for an effective ELP information access control based on at least four different access categories. The paper closes with a manifold set of ELP application scenarios (cf. Section 5) together with a short discussion about some important privacy aspects for potential ELP applications (cf. Section 6).

2 Related Work

Integrating electronic reading capabilities into license plates, of course, is not completely new. There are, for example, already some first RFID-based implementations continuously broadcasting a small data set (e.g., plate number and vehicle owner) in plain. However, the *e-plate* realization [8] does not implement any security or privacy protection mechanism and fully relies on the physical fixture to the vehicle (i.e., has no logical connection). The security and privacy protection measures of another ELP approach named *il-tag* [20] remains completely inexplicit (i.e., are not publicly available), but in any case does not provide any higher-level, more sophisticated protection measures such as enforcing intervisibility or logical plate fixture. Other existing electronic license plates proposals focus, for instance, on upgrading the license plate into an electronic display [4] without any further ITS (intelligent transportation system) functionality. The approaches proposed in this paper are in particular completely different (and independent) from electronic solutions for optical license plate recognition (LPR) systems.

3 System Architecture

As shown in the overview in Figure 1, the proposed secure electronic license plate (ELP) is based on a conventional physical license plate (1) enhanced by an RFID-chip or any similar dedicated short-range radio communication (DSRC) device (2) together with a small but hardware-cryptography-enabled microcontroller (i.e., a microprocessor together with a tamper-protected [17] hardware security module) (3). The electronic license plate, furthermore, should have a (wireless) in-vehicle network interface (4) to realize a strong logical connection between vehicle and license plate (cf. Section 4.1). Since the electrical power requirements of the ELP will be rather low, the ELP could be easily connected to the already available license plate illumination (vehicle on-board) power supply. If automotive manufacturers could consider ELPs already at the beginning of their vehicle (electronics) developments, the ELP components except (1) could ideally become safely integrated into and realized as a standardized, in-vehicle electronic control unit (ECU) directly connected with the in-vehicle communication networks.

For external infrastructures (or vehicles) interacting with the ELP a wireless digital reader device is required (6) and – depending on the individually effective information access restrictions (cf. Section 4.2) – direct intervisibility to the physical license plate (1).

3.1 Hardware Architecture

Figure 2 depicts the underlying ELP hardware architecture as described in the following. The microcontroller is assumed to be a single integrated chip including a small CPU (e.g., class of *ARM Cortex-M* family or similar) and all elementary periphery (e.g., clock, timers, I/O ports, and some small amount of RAM, ROM, and non-volatile flash memory). The microcontroller is assumed to be able to securely execute at least symmetric cryptography (e.g., AES) and is able to generate random numbers in an efficient manner. To protect the cryptographic artifacts (e.g., secret keys, random number generator states) and corresponding cryptographic

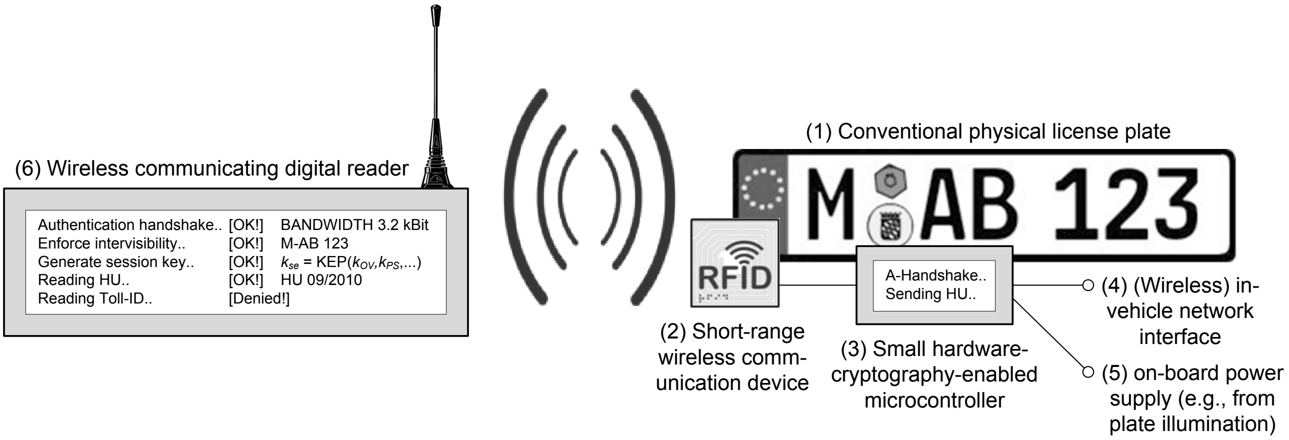
(6) Wireless communicating digital reader
Authentication handshake.. [OK!] BANDWIDTH 3.2 kBit
Enforce intervisibility.. [OK!] M-AB 123
Generate session key.. [OK!] k_{se} = KEP(k_{OV},k_{PS},...)
Reading HU.. [OK!] HU 09/2010
Reading Toll-ID.. [Denied!]
(1) Conventional physical license plate
M AB 123
RFID
A-Handshake..
Sending HU..
(2) Short-range wireless communication device
(3) Small hardware-cryptography-enabled microcontroller
(4) (Wireless) in-vehicle network interface
(5) on-board power supply (e.g., from plate illumination)

Figure 1: ELP architecture overview.

operations (e.g., random number generation (RNG), encryption, decryption) against unauthorized read-out or tampering this work proposes the application of an automotive-capable security microcontroller (e.g., *Atmel's ATA5795* [1]) or a microcontroller connected to an automotive-capable hardware security module (HSM) as specified for instance by the HIS consortium [11] or as currently developed by the EVITA research project [9]. The dedicated short-range radio communication (DSRC) system connected to (or integrated into the microcontroller) is assumed to communicate at least 64 Bytes (at all), up to 100 meters, up to a relative vehicle speed of 200 km/h. This in turn can be achieved for instance by applying automotive-capable transponders based on the (extended) RFID standard [14] or based on the IEEE 802.11p standard [15].

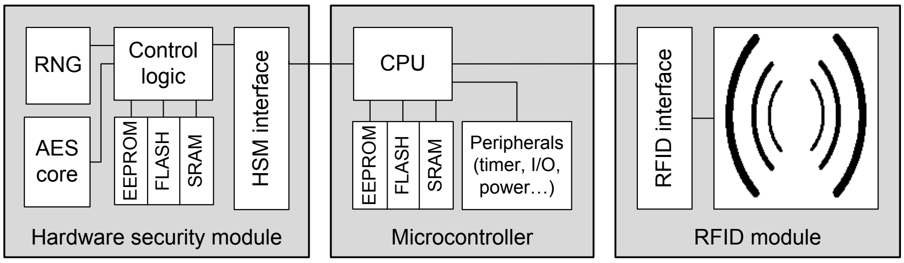

Figure 2: Exemplary ELP hardware architecture.

3.2 Software Architecture

The ELP software architecture as depicted in Figure 3 consists of the underlying hardware layer as described in Section 3.1, the resource management layer, the software security layer above, and the ELP application layer on top that executes possible ELP applications (cf. Section 5).

The resource management layer provides typical operating-system-like services such as (strong) runtime process isolation, management of I/O ports, memory, and further microcontroller periphery. It especially provides the software drivers to access the hardware security module and the RFID or DSRC communication device. The software security layer in turn implements elementary security services built on a hardware security module acting as tamper-protected security anchor. The secure storage service, for instance, enables applications to persistently store their individual states while preserving authenticity, integrity, confidentiality, and freshness of the managed data. The secure communication service in turn enables applications to securely communicate with external parties while preserving authenticity, integrity, confidentiality, and freshness of the communicated data by providing necessary communication security protocols and algorithms. The last exemplary mentioned basic security service is a pseudonym services that enables applications to retrieve appropriate pseudonyms to anonymize (external) authentications while preserving driver's privacy (cf. Section 4.2). However, possible realizations and implementations of such basic security services are not an integral part of this article but can be found amongst others in [5, 7, 18, 21].

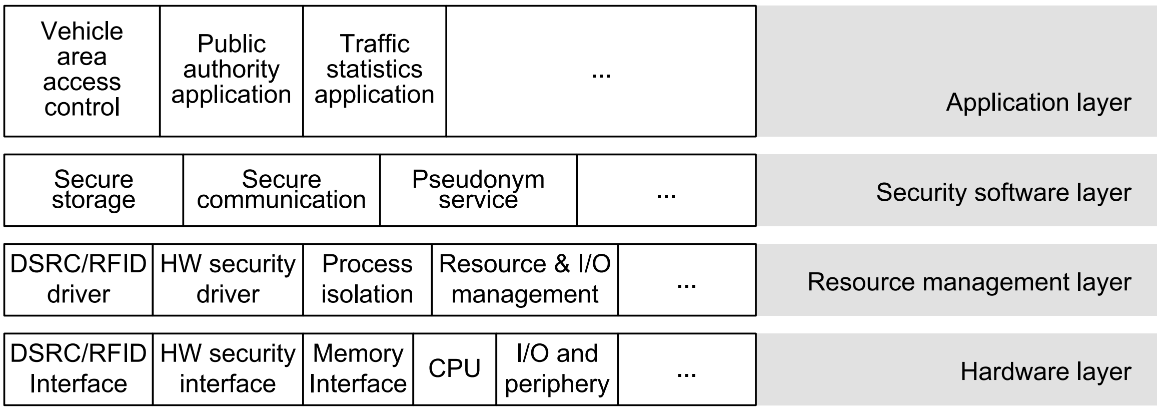

Figure 3: Exemplary ELP software architecture.

4 Security Protocols

This section describes effective security protocols that provide a cryptography-based logical fixture between ELP and vehicle as well as a possible approach for an ELP information access control based on at least four different access categories. Table 1 below gives a short overview about some important symbols frequently used thereafter.

Symbol	*Description*
k_{ID}	Globally unique identification key for each license plate
k_{OV}	Vehicle individual only optical visible information for each license plate
k_{PS}	Pre-shared symmetric key brought in a trusted environment
HSM_P	ELP hardware security module with tamper-protection (e.g., for k_{ID}, k_{PS})
HSM_V	In-vehicle hardware security module (ideally also with tamper-protection)

Table 1: Symbol descriptions frequently used in ELP security protocols.

4.1 Logical Plate Fixture

In order to prevent unauthorized removals, thefts, or counterfeiting, the license plate has to be attached securely to the corresponding vehicle. On the other hand, authorized removals must be possible in a fast and simple manner. Hence, solely relying on the physical capabilities of the plates' fixture usually is both insufficient and inflexible. However, having a cryptography-enabled microcontroller and a wireless communication device integrated within the electronic license plate, enables efficient, reliable, and flexible approaches for a strong logical connection between the license plate and the vehicle based on cryptographic authentication protocols. Thus, for instance, the solution presented by Weimerskirch et al. [12] – originally designed to protect in-vehicle components only – can be easily extended to include also the external electronic license plate. Therefore, the license plate and the vehicle have to establish a shared secret, that means, a symmetric key k_{ID} known only to the in-vehicle hardware security module HSM_V and to the license plate hardware security module HSM_P. Assuming each license plate has a globally unique and fixed identification key k_{ID}, the vehicle owner will securely connect HSM_P to HSM_V by manually entering k_{ID}, which can be found for instance in the plate's corresponding documentation at HSM_V. From now, k_{ID} is (i) used for mutual authentication using a simple mutual challenge-response protocol (e.g., mutually requesting encryption of self-generated nonces) and (ii) used for repeatedly generating symmetric session keys to secure all communications between HSM_P and HSM_V. Without a successful authentication of HSM_V (e.g., executed on every vehicle start) the electronic license plate would not provide any further functionality, while the connection of an electronic license plate to a new vehicle would delete all vehicle-individual data stored at the plate. Doing so, an unauthorized removal, theft or (physical) counterfeit would be worthless, as the stolen or counterfeit plate could not become connected to another vehicle without the knowledge of k_{ID}. Even vehicle owners could be prevented from mounting their electronic license plate to another vehicle without proper authorization, for instance, from a public authority. For doing so, connecting a license plate to another vehicle would always require that HSM_V first verifies a digital certificate $c = f(k_{ID}, HSM_V)$ from HSM_P issued only by the respective public authority at the official registration of the corresponding vehicle (plate).

Lastly, in case a thief would simply add a stolen plate to a non-electronic-license-plate-enabled vehicle, the license plate could always provide some wirelessly visible information (cf. Section 4.2) describing some clearly containing but still privacy-preserving vehicle information such as the color or the type of the original vehicle that usually would yield to an obvious contradiction.

4.2 Information Access Control

Instead of providing all information (optically and electronically) available at the ELP wirelessly to every reader device in plain, this work proposes to limit and protect ELP information access at least as classified in the four general access categories (AC). As shown in Table 2 each of the ACs has its individual effective access restrictions and information access procedures as described in the following paragraphs.

	Optical channel	**Wireless channel**	**Authentication & Authorization**
AC1: Optically visible	■	□	□
AC2: Wirelessly visible	□	■	□
AC3: Wirelessly restricted visible	□	■	■
AC4: Wirelessly restricted visible and intervisibility	■	■	■/□

Table 2: ELP information access categories and their individually effective requirements (■).

Optically Visible Information (AC1). ELP information classified with AC1 (e.g., the unique license number or similar) should remain optically visible, easy to read by humans, and physically robust on every vehicle without the need for any additional technical device. Such AC1 information would enable humans, for instance, to quickly identify their own vehicle at a huge parking lot or would enable humans to clearly identify another vehicle in case of an accident. However, note that optically visible AC1 information is not (and should not) automatically wirelessly visible as well.

Wirelessly Visible Information (AC2). ELP information classified with AC2, which is visible in plain for all wireless reader devices and without affecting the privacy of the driver and passengers, could be for instance (i) vehicle pseudonyms for counting available parking lots, (ii) intelligent traffic management solutions based on automatic, anonymized traffic surveys, or (iii) any anonymized, general vehicle information (depending on driver or effective legacy requirements) such as engine emission class (for accessing environmental zones), fuel type (to prevent wrong fueling), or number of passengers (i.e., for special lanes).

Wirelessly Restricted Visible Information (AC3). ELP information classified with AC3 is only visible for certain entities (e.g., police, public authorities, service providers, OEM) if they have been successfully authenticated and if they have the necessary access rights. Such information, hence, is communicated only in an authenticated, integrity and confidentiality-preserving manner. For mutual authentication between ELP and the external reader it would be possible to apply a simple challenge-response authentication protocol based on a pre-shared symmetric key k_{PS} that could be brought into the ELP (HSM_P) within a protected environment, for instance, during vehicle registration. If the successfully authenticated external reader has necessary access authorizations (i.e., is authorized to access the requested information), ELP will encrypt all subsequently communicated information with a session key derived from the corresponding k_{PS} (and previously exchanged random nonces to prevent replay attacks) using, for instance, the Advanced Encryption Standard (AES) block cipher [10] in Galois/Counter mode of operation to enforce confidentiality and authenticity. In case pre-shared keys are considered inappropriate for certain applications (e.g., to prevent attacks on widespread secret keys), the ELP could implement (e.g., at the microcontroller security software layer) also an efficient public key scheme such as RSA or ECC [13] that would allow mutual authentication and subsequent session encryption based on digital signatures (e.g., DSA or ECDSA) and key establishment protocols (e.g., Diffie-Hellman key exchange) without requiring pre-shared secret key(s) within ELP.

Wirelessly Restricted Visible Information Requiring Intervisibility (AC4). Although access on critical ELP information can be restricted to certain authenticated and authorized entities, a fully automated readout of potentially privacy-critical information could endanger the privacy of the vehicle driver or passengers. This remains true even if the single ELP information itself does not yet inherently reveal any privacy-critical information, but could be repeatedly read-out (from many connected readers on many different locations). These messages could then be collected and stored in a huge *data warehouse* that in turn could enable potentially privacy-critical data mining or data aggregation procedures.

In order to keep a fair balance between the driver's privacy requirements and the necessary interests of the police and public authorities this work proposes, *in addition* to the information access control schemes as described above, a secondary cryptographic mechanism enforcing vehicle intervisibility for readout of AC4 classified ELP information that could yield to privacy-invasive automated vehicle surveillance. The proposed security protocol is – similar to the key-agreement mechanism(s) for machine readable travel documents [3] – based on the availability of a vehicle individual information k_{OV} that can be obtained only over the optical channel, that means, a vehicle individual information that is only optically visible at the vehicle and that cannot be retrieved in a fast, cheap, and easily scalable manner, for instance, using the wireless interface. In practice, k_{OV} could be the individual license plate number but also some information neither always (e.g., only at certain time periods, certain locations, or certain occasions) nor that easily visible (e.g., not retrievable by standard surveillance camera systems). In order to access AC4 classified ELP information both the ELP and the external reader derive the vehicle individual keys for mutual authentication k_{auth} and session encryption k_{enc} using a key establishment protocol (KEP) based at least on k_{OV}, the corresponding pre-shared key for access authorization k_{PS} (if set), and previously exchanged random nonces n_R to prevent replay attacks. Thus, $k_{AC4} = KEP(k_{OV}, k_{PS}, n_R, ...)$ whereas $k_{auth} = KEP(k_{AC4}, ...)$ and $k_{enc} = KEP(k_{AC4}, ...)$. Thus, only entities that have direct intervisibility and the corresponding authorization are able to access such potentially privacy-critical information. A capable KEP could be the Password Authenticated Connection Establishment (PACE) protocol as proposed by the BSI [3]. A successful security analysis of the PACE protocol by Bender et al. [2] showed that the proposed key establishment can be secure even if it applies passwords (i.e., k_{OV}) with low entropy. A German license plate [16], for instance, currently consists of 383 different region identifiers together with two (ideally) random letters and up to four random numbers. This yields to an entropy of ≈ 31 bits ($383 \times 26^2 \times 10^4$ possible combinations). Hence, brute-forcing k_{OV} should be sufficiently costly (e.g., in contrast to an effective LPR system).

5 Applications

An electronic license plate, as proposed in this work, would enable manifold interactive vehicular application scenarios. Thus, the following list will give only a first (and certainly incomplete) collection of potential ELP applications based on a secure, mutually authenticated, and privacy-preserving information exchange.

- **Enhanced road safety** by checking effective limitations (e.g., height/weight, freight).
- **Automated area access control for vehicles**, for instance, for environmental zones, city zones, special lanes (e.g., lanes only for fully occupied vehicles), or for restricted private areas or premises.
- **Public authority vehicle inspection**, for instance, regarding necessary vehicle insurances, vehicle taxes, inspection or registration validity periods, special access authorizations (e.g., for special parking lots for women or handicapped).
- **Enhanced anonymous traffic and traffic infrastructure management** solutions based on anonymized statistics, for instance, about vehicle quantities, vehicle types, their respective emissions, destinations, or occupations.
- **Efficient (anonymous) infrastructure services**, for instance, for anonymous e-tolling or congestion charging; or for vehicle individual notifications, for instance, regarding driver language, vehicle type, or individual relevance, wrong fueling alarm.
- **Stolen vehicle tracking**, for instance, by publishing a distinctive "stolen vehicle" identifying k_{PS} that then would enable easy wireless readout (e.g., without the need for k_{OV}) of explicit vehicle identity information to quickly locate the stolen vehicle.
- **Automated vehicle arrival (leaving) mechanisms**, for instance, automated garage door opener, automated duplex parking space positioning, or automated location lightning.
- **Advanced parking services**, for instance, by registering the vehicle with an appropriate ELP pseudonym at the respective parking location that can then be queried later on with a cellular; or the driver can be automatically informed in case of an unauthorized vehicle leave.

6 Discussion on Privacy Aspects

This last section shortly discusses some important privacy aspects with regard to potential ELP applications.

Driving a vehicle was never fully anonymous. License plates have been in use for almost as long as automobiles exist, that means, for about 100 years already. Initially, license plates were introduced to constrain hit-and-run accidents or to prove proper vehicle taxes payment. Over the decades, people have accepted that driving a car will make them identifiable to a certain extend. Hence, vehicles could always be identified that they have been on certain location or even tracked (of course, only with huge imprecision and/or great efforts). Thus, the society agreed on a fair balance between the driver's privacy requirements and the necessary interests of the police and other public authorities.

The proposed ELP, hence, will not and should not lower nor increase automatically the status quo privacy situation for vehicle driving. Every vehicle still should have visible license plates that can be read easily by humans without the need for any additional technical device, for instance, to clearly identify vehicles at huge parking lots, for being able to (indirectly) contact a vehicle owner, or to constrain hit-and-run accidents. On the other hand, it is not necessary that vehicles show their emission parameters (e.g., via emission class stickers), the driver's recent travel destinations (e.g., via national vignettes), the driver's home or business location (e.g., via resident parking permit), or their last technical inspections (e.g., via vehicle inspection sticker) constantly to everyone in the public. Here, the ELP could help to restrict access to such information only to entities which require a particular information and which, moreover, are explicitly authorized for accessing it. Further, by strictly applying an information access enforcement as proposed, the creation of movement profiles during the application of ELPs is not more or less difficult as today (e.g., by directly spotting or directly pursuing a vehicle). Hence, the application of ELPs has clear manifold valuable benefits for vehicle safety, driving comfort, and mobile business without endangering the existing privacy level.

7 Summary and Outlook

This work has described a holistic approach for designing, implementing, and applying a secure and privacy-preserving electronic license plate (ELP). It has provided a comprehensive treatment about the manifold benefits of ELPs as well as various existing and upcoming vehicular application scenarios. Furthermore, it has provided exemplary proposals for the underlying cost-efficient hardware and software architecture together with some capable security protocols for enabling a cryptography-based logical fixture between ELP and vehicle and an effective ELP access control enforcement.

As already mentioned in the privacy discussion in the end, the authors believes that ELPs have manifold valuable benefits for vehicle safety, driving comfort, and mobile business without endangering the existing privacy level (in fact, partly quite the contrary).

Acknowledgments

The author would particularly like to thank my colleagues Timo Gendrullis, Ellen Gerhardt, and Christian Schleiffer for their valuable comments and helpful contributions to this work.

References

[1] Atmel Corporation. ATA5795 Embedded AVR Automotive Security Microcontroller. `www.atmel.com/dyn/products/product_card.asp?part_id=4754`, 2010.

[2] J. Bender, M. Fischlin, and D. Kügler. Security analysis of the pace key-agreement protocol. In *ISC '09: Proceedings of the 12th International Conference on Information Security*, 2009.

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI). Advanced Security Mechanisms for Machine Readable Travel Documents. Technical Report TR-03110, Version 2.02, 2009.

[4] Bundesdruckerei GmbH. Blick in die Zukunft bei der Bundesdruckerei: Elektronische Kfz-Nummernschilder und hauchdünne Displays. `www.bundesdruckerei.de/de/presse/presse_meldungen/pm_2009_03_02.html`, 2009.

[5] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy. Efficient and Robust Pseudonymous Authentication in VANET. In *Proceedings of the 4th ACM International Workshop on Vehicular Ad-hoc Networks*, 2007.

[6] CBS Broadcasting. Congestion Pricing Flaw: Cloned License Plates. `http://wcbstv.com/topstories/congestion.pricing.london.2.597052.html`, 2007.

[7] F. Dotzer. Privacy Issues in Vehicular Ad-hoc Networks. *Lecture Notes in Computer Science*, 3856:197–209, 2006.

[8] e-Plate Ltd. RFID enabled licence plates. `www.e-plate.com`, 2001.

[9] EVITA: E-safety vehicle intrusion protected applications. `www.evita-project.org`, 2008.

[10] FIPS-197. *Advanced Encryption Standard (AES)*. National Institute of Standards and Technology, 2001.

[11] Herstellerinitiative Software (HIS). Secure Hardware Extension (SHE) Version 1.1. `www.automotive-his.de`, 2009.

[12] K. Höper, C. Paar, A. Weimerskirch, and M. Wolf. Cryptographic Component Identification: Enabler for Secure Vehicles. In *62nd IEEE Semiannual Vehicular Technology Conference, VTC 2005 Fall, Dallas, Texas, USA, September 25 – 28*, 2005.

[13] IEEE P1363-2000. *Standard Specifications for Public-Key Cryptography*. IEEE, 2000.

[14] ISO/IEC 18000. *Information technology – Radio frequency identification for item management*, 2008.

[15] D. Jiang and L. Delgrossi. IEEE 802.11p: Towards an international standard for wireless access in vehicular environments. In *Proc. of IEEE Vehicular Technology Conference (VTC) Spring*, 2008.

[16] Kraftfahrt-Bundesamt (KBA). Kraftfahrzeug-Kennzeichen für Deutschland. `www.kba.de/cln_007/nn_124384/DE/Service/Kennzeichen/Functions/kennzeichen.html`, 2009.

[17] K. Lemke. Physical Protection against Tampering Attacks. In *Embedded Security in Cars: Securing Current and Future Automotive IT Applications*. Springer-Verlag, 2006.

[18] M. Scheibel, C. Stüble, and M. Wolf. An Interoperable Security Architecture for Vehicular Software Protection. In *International Workshop on Interoperable Vehicles, IOV 2008, ETH Zürich, Switzerland, March 26*, 2008.

[19] Toll Collect GmbH. `www.toll-collect.de`, 2010.

[20] UTSCH AG. iltag – High Security Intelligent License Tag. `www.iltag.com`, 2003.

[21] B. Weyl, M. Wolf, F. Zweers, T. Gendrullis, M. Idrees, Y. Roudier, H. Schweppe, H. Platzdasch, R. E. Khayari, O. Henniger, D. Scheuermann, L. A. A. Fuchs, G. Pedroza, H. Seudié, J. Shokrollahi, and A. Keil. Secure On-Board Architecture Specification, EVITA Deliverable D3.2. `www.evita-project.org`, 2010.