A COLLABORATIVE LEGAL FRAMEWORK FOR CERTIFIED ENFORCEMENT WITH ITSIbus ALPR

Jorge Silva[1], Arnaldo Abrantes[1], A. Luís Osório[2], Bruno Basílio[3], J. Sales Gomes[3]
[1]ISEL, Instituto Superior de Engenharia de Lisboa, M2A research group, PORTUGAL
{jgs, aja}@.isel.ipl.pt
[2]ISEL, Instituto Superior de Engenharia de Lisboa, GIATSI research group, PORTUGAL
aosorio@deetc.isel.ipl.pt
[3]BRISA, Auto-estradas de Portugal, DIT Innovation and Technology Department, PORTUGAL
{Jorge.Gomes, Bruno.Basilio}@brisa.pt

This paper discusses a collaborative framework for the legal certification of toll enforcement on motorways operated by Brisa Auto-Estradas de Portugal, based on the Advanced License Plate Recognition (ALPR) system/service. The developed ALPR service produces a composite JPEG picture documenting an irregular situation. An enforcement transaction is generated at Brisa's toll infrastructure and later delivered to the toll clearing company Via Verde Portugal (VVP). This company processes the generated composite picture, matching it with the client data base and, if necessary, pursuing legal action. The enforcement picture might also be delivered to other organizations, such as the official entity for car registration management, in Portugal the General Direction of Traffic (DGV). Certification is based on Public Key Infrastructure (PKI) and legal digital certificates. Its purpose is to guarantee the validation of an ALPR generated picture as genuine, at a court of law; any change will be detected by a validation service. The paper discusses the adopted strategy, considering not only technical but also organizational issues, since the trust required for the management of enforcement pictures along the involved networked organizations requires a set of procedures to be followed in order to ensure the required legal confidence (trust).

1. INTRODUCTION

Enforcement is an essential component of an automated toll system, and presents organizational as well as technological challenges. The success of an enforcement solution depends not only on its effectiveness but also on the trust that networked participants and actors involved in the enforcement process place in the solution. A key step in cementing such trust consists in the preemption of falsification claims regarding the evidence documenting any irregularity. This need is particularly acute when such evidence exists in electronic form and might have to be presented at a court of law. Furthermore, the number of involved networked organizations and

Please use the following format when citing this chapter:

Silva, J., Abrantes, A., Osório, A. L., Basílio, B., Gomes, J. S., 2006, in IFIP International Federation for Information Processing, Volume 224, Network-Centric Collaboration and Supporting Fireworks, eds. Camarinha-Matos, L., Afsarmanesh, H., Ollus, M., (Boston: Springer), pp. 635–642.

clients of the toll infrastructure configure a trusted collaborative network (Camarinha-Matos, 2004), where enforcement information is exchanged following the established legal framework.

This paper describes both a certification strategy and a collaborative model for the involved organizations, designed to address the above issue in the specific case of motorway toll enforcement for the Via Verde Portugal (VVP) toll clearing company, at motorways operated by Brisa Auto-Estradas de Portugal.

In regular conditions, electronic toll collection in the Via Verde is performed through Dedicated Short Range Communication (DSRC) at microwave frequencies (5.8 GHz) between an antenna in the toll plaza and an identifier device, also called an On-Board Unit (OBU), inside the vehicle. The identifier contains information about the owner's identity and the vehicle class, the latter being confirmed by the Automatic Vehicle Detection and Classification (AVDC) system.

Enforcement is based on the Advanced License Plate Recognition (ALPR) system/service, developed by Brisa and integrated in the ITSIbus architecture (Gomes, 2003), (Osório, 2004). In an irregular situation, such as a vehicle without an OBU, or when any other problem prevents the toll infrastructure from registering a valid transaction, the ALPR system generates a composite picture in Joint Photographic Experts Group (JPEG) format, showing a rear view of the vehicle, as well as sub-images of the front and rear license plates obtained from two separate IR cameras. Additionally, meta-information is appended so that other services may subsequently extract the license plate.

The certification technology is based on Public Key Infrastructure (PKI) (Schneier, 1996) and legal digital certificates. However, it is necessary to certify other processes beyond the service/system that appends the digital signature to the original picture. As an example, management of the private key, used to generate the digital signature associated with a certificate generated by a certification authority, needs to be maintained under rigorous collaborative guidelines. The overall certification strategy has been designed to comply with requirements expressed in national legislation for electronic documents to be used as evidence, while ensuring protection of the motorway users' privacy. The structure of this paper is the following: the logical and physical architecture of the enforcement data collection and transmission system, including the ALPR, integrated in the context of the overall toll management system, are described; next, the proposed security, collaborative framework and related organizational as well as legal issues are discussed, followed by concluding remarks.

2. ARCHITECTURE OF THE ENFORCEMENT SYSTEM

There are four levels in toll management, as illustrated in Figure 1, ranging from individual Via Verde lanes to the toll plaza and finally up to the central Toll Coordination System (TCS).

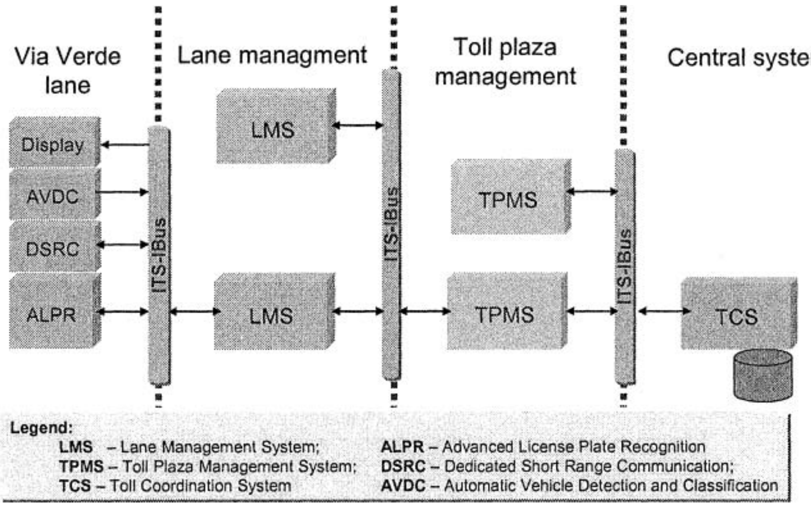
Via Verde lane
Lane managment
Toll plaza management
Central system
Display
AVDC
DSRC
ALPR
ITS-IBus
LMS
LMS
ITS-IBus
TPMS
TPMS
ITS-IBus
TCS
Legend:
LMS – Lane Management System;
TPMS – Toll Plaza Management System;
TCS – Toll Coordination System
ALPR – Advanced License Plate Recognition
DSRC – Dedicated Short Range Communication;
AVDC – Automatic Vehicle Detection and Classification

Figure 1 – Toll management levels.

Communication takes place between each level and the ones adjacent to it, using a service-based communication bus, the ITSIbus. The ITSIbus defines a set of basic services, such as security, configuration and administration, as well as "*plug-and-play*" mechanisms. Besides the basic services, an additional set of services is defined as standard for each class of systems, to be implemented by all developers.

The lane management level, implemented by LMS systems, controls the passage of vehicles and the generation of transactions according to each specific situation. Among the possible scenarios to be handled by an LMS, emphasis is given to the following: passage of a vehicle without an OBU; OBU with a low battery; mismatch between the automatically detected vehicle class and the class associated with the OBU.

In case such an irregularity occurs, the ALPR generates a proof of passage of the vehicle involved, at the request of the LMS. This proof of passage consists of a composite picture of the vehicle. The picture is forwarded by the LMS to the corresponding TPMS, where it is stored for later transmission to the TCS. Thus, pictures are generated by the ALPR system in response to events originating in lane-level equipment and systems like the DSRC and AVDC, resulting in a flow of information across the private and secure network infrastructure of the motorway operator, from the lane to the central TCS. The internal ITSIbus collaborative service infrastructure has no direct access from outside the organization, which removes the vulnerability from Internet-based attacks.

Under an enforcement scenario, should the authenticity of the picture need to be verified in court, a validation application (itself certified) can perform the necessary check, by confronting the digital signature in the JPEG header with the remaining data. A collaborative process models and manages the necessary information exchange, in this case between the motorway operator and the road authority and if necessary a court. The overall flow of information is illustrated in Figure 2.

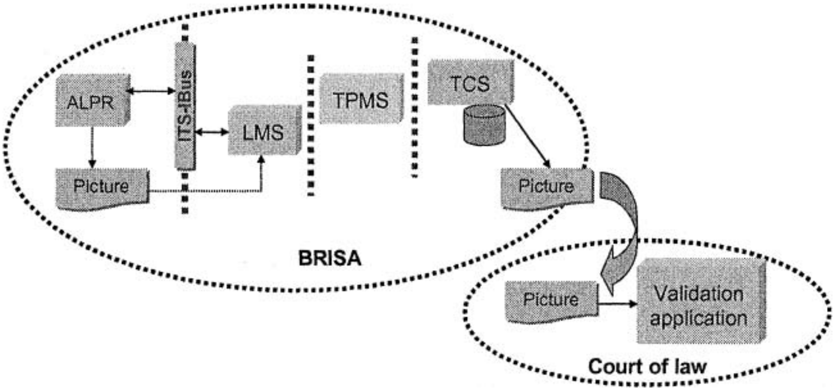

Figure 2 – Flow of an ALPR-generated picture across all involved systems.

The legal value of the ALPR-generated picture depends on other factors beyond the ALPR itself. In fact, the collaborative processes and procedures regarding physical equipment accessibility, as well as other involved systems, contribute towards maintaining the required information integrity and trust among the involved partners.

3. DESCRIPTION OF THE ALPR

The ALPR is one of the roadside systems on a Via Verde lane. Its purpose is to provide an electronic document (picture plus meta-information) allowing the identification of the vehicle, the place and date/time of passage, whenever the LMS, in response to a vehicle passage event, requires such a document. An example picture is depicted in Figure 3.

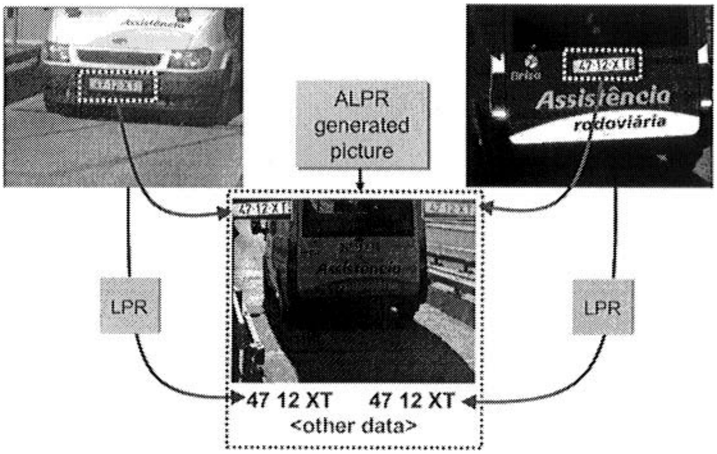

Figure 3 – Example of an ALPR picture.

The primary requirements of the ALPR are as follows:

- Acquisition of a panoramic rear view of the vehicle, allowing visual inspection
- Automatic recognition of the front and rear license plates
- Generation of a JPEG composite picture, with the cropped front and rear plate sub-images overlaid on the rear panoramic view
- Independence of the image quality on weather conditions, time of day, condition of the plate and other variables
- Regarding acquisition of the front image, only the license plate must be extracted and appended to the composite picture, while the remainder of the image must never even be written to disk

Figure 4 illustrates the logical architecture of the ALPR, including the optional *certification module*, which generates a digital signature included in the meta-information appended to the enforcement picture. The remaining meta-information includes a timestamp and also the vehicle class, as detected by the AVDC.

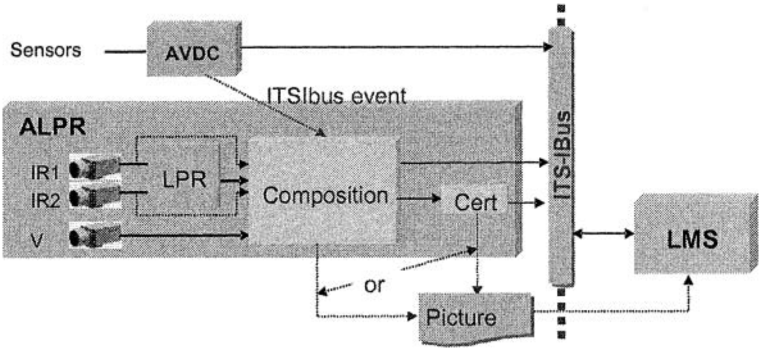

Figure 4 – Logical architecture of the ALPR system, including the optional certification module (Cert).

The ALPR was developed using artificial vision and Optical Character Recognition (OCR) technology (Rahman, 2003), (Duc Duan, 2005). The license plate recognition process has been decoupled from the visual inspection process by using different images, in different wavelengths: infra-red (IR) images for license plate recognition; visible images, in color, for human inspection.

One of the reasons for this decoupling is the fact that the recognition process benefits from high contrast images where the license plate is highlighted, unlike the visual inspection image, which should clearly show the vehicle and its surroundings. Also, the use of IR images for recognition is a common procedure for making the recognition process as independent from lighting conditions as possible.

The physical architecture of the ALPR can be seen in Figure 5. The system consists of two modules, one in front and another in the rear of a passing vehicle. The front module contains an IR camera and an IR illuminator, and it is connected to the rear module, which contains another IR camera and illuminator, together with a visible spectrum color camera and a computer equipped with a multi-channel frame grabber. The computer is connected to the LMS and the motorway operator's network.

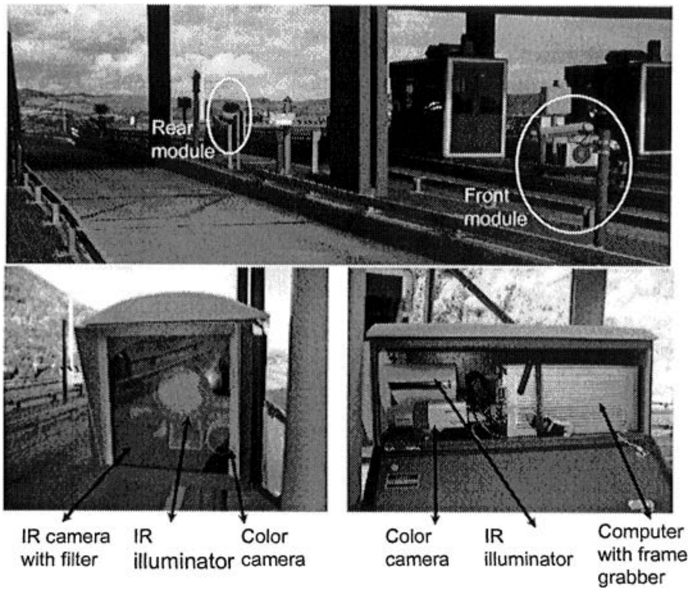

Figure 5 – Physical architecture of the ALPR system. Above: the front and rear modules. Below: detail of the rear module.

4. SECURITY OF THE COLLABORATIVE FRAMEWORK

Whenever a document is to be used as evidence, the possibility of falsification or forgery must be taken into account, whether or not the document exists in electronic format. The developed security collaborative framework takes into account the fact that several types of attack are possible (Coulouris, 2001), (Macgregor, 1996), namely:

- Replacement of a legitimate ALPR unit with a duplicate, built by a third party with knowledge of the technology
- Introduction of a "Trojan horse" into an ALPR unit, either during scheduled maintenance or by unauthorized access through the private network
- Eavesdropping into the messages exchanged through the private network, during transactions
- Tampering with the picture, for example editing the image to change license plate characters

Protection against these types of attack requires organizational as well as technological measures. Physical access to the units must be restricted, validated using, for instance, PINs or codes and smart-cards, and recorded for future traceability. Network security is also a concern. Sensitive information, such as PINs or passwords, should never be sent in clear text.

Encryption and digital signature are a key technological component of the security system, and so are the monitoring capabilities of the ITSIbus. For example, if an ALPR unit is removed, even temporarily, an exception is generated by the ITSIbus, either through sensors connected to the physical system or by detecting a loss of communication. Pictures from that particular unit will no longer be trusted until the source of the exception is investigated.

As for ensuring the integrity of the JPEG pictures, a digital signature scheme is used, as illustrated in Figure 6. The system uses the public key infrastructure (PKI), and the picture is digitally signed. This process may take place directly in the ALPR using the optional Certification module, as in Figure 4, or it may take place at a later point instead. Which option is used depends on whether or not the communication link with the central services is considered secure enough.

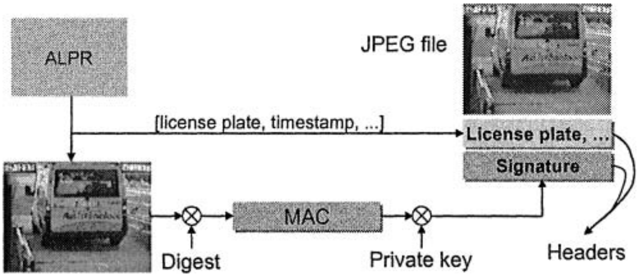

Figure 6 – Integrity control model.

The signature process is based on the concept of asymmetric cryptography (Schneier, 1996), where a private key encodes the message and a corresponding public key decodes it. The private key must be kept confidential within the organization that is responsible for the digital signature, while the public key may be issued to message readers. Both the private and the public key are associated with a certificate issued by a legally authorized entity. Access and use of the certificate is done securely.

For computational performance reasons, a Message Authentication Code (MAC) is signed instead of the entire message (in this case is a picture, which may have considerable size). A MAC is the output of a *digest function* which, given two distinct inputs, produces significantly smaller outputs that are almost certainly distinct as well (the probability of having the same output for different inputs is vanishingly small). Thus, the MAC is digitally signed and the resulting signature is placed in the JPEG file header, together with additional information such as the vehicle class, the recognized license plate number and a timestamp. If the picture is altered in any way, the change can be detected by recomputing the MAC and confronting it with the one present in the file header, after decoding the later with the public key. This operation can be performed by a validation application.

This security collaborative framework is compatible with the requirements expressed in Portuguese and European law, respectively Decreto-Lei 62/2003 and Directive 1999/93/CE, for electronic signatures. Certifying organizations are also members of the established collaborative network and are regulated by the

Portuguese Instituto das Tecnologias de Informação na Justiça, according to Decreto-Lei 234/2000.

5. CONCLUSIONS

The establishment of a collaborative network based on certification of electronic documents is still in a preliminary stage, the relevant legislation having been produced in 2003. Within this legal collaborative framework, a certification system has been developed for enforcement in motorway electronic toll collection, based on the ALPR system and a digital signature scheme.

Organizational as well as technical issues have been taken into account when developing the overall security collaborative framework. This certification is intended to contribute to the success of the toll enforcement system, by establishing trust between the partners involved in this collaborative network. Although complete invulnerability to attack can never be guaranteed, the presently afforded degree of protection is considered adequate in face of the types of attack that are foreseeable in the near future.

A direction for further development is the establishment of procedures for managing the issuing, validation and revoking of certificates, which should be agreed upon between the network members.

6. ACKNOWLEDGMENTS

This work was partially supported by BRISA group, through the research and development ITSIBus-Vision project. The research groups M2A and GIATSI from ISEL-DEETC in collaboration with DIT, the Innovation and Technology Department of BRISA, are developing the work. We also acknowledge the valuable contributions from Joaquim Pereira, Rui Gonçalves and Rui Lopes.

6. REFERENCES

(Camarinha-Matos, 2004) - Camarinha-Matos, L. M.; Afsarmanesh, H.; Supporting Infrastructures for New Collaborative Forms, in Collaborative Networked Organizations, pg. 175-192, Kluwer Academic Publishers 2004.

Coulouris, G., Dollimore, J.; Kindberg T. - Distributed Systems - Concepts and Design, 3rd edition, Addison-Wesley, 2001.

Duc Duan, T., Hong Du, T., Vinh Phuoc, T., Viet Hoang, N. - Building an Automatic Vehicle License-Plate Recognition System, Int. Conf. in Computer Science, RIVF'05, Vietnam, February 2005.

Gomes J. Sales, Jacquet G., Machado M, Osório A. Luís, Gonçalves C., Barata M. - An Open Integration Bus for EFC: The ITS IBus, in ASECAP2003, 18 - 21 May 2003 in Portoroz, Slovenia

Macgregor R. S., Aresi, A., Siegert A., WWW.Security, How to Build a Secure World Wide Web Connection, IBM, Prentice Hall PTR, 1996.

Osório A. L., Abrantes A. J., Gonçalves J. C., Araújo A.; Miguel J. M., Jacquet, G. C.; Gomes, J. S. - Flexible and Plugged Peer Systems Integration to ITS-IBUS: the case of EFC and LPR Systems, PROVE'03 – 4th IFIP Working Conference on Virtual Enterprises, published by Kluwer Academic Publishers, ISBN: 1-4020-7638-X, pages 221-230, 2003-b.

Osório, A. Luís; Osório; L., Barata, M.; Gonçalves, C.; Araújo, P.; Abrantes, A.; Jorge, P.; Gomes, J. Sales; Jacquet G.; Amador, A. - Interoperability among ITS Systems with ITS-IBus framework, BASYS 2004, Vienna, Austria 27-29 September 2004.

Rahman, A., Radmanesh, A. - A Real Time Vehicle's License Plate Recognition, Proceedings of the IEEE on Advanced Video and Signal Based Surveillance, 2003

Schneier B. - Applied Cryptography, 2nd Edition, John Wiley & Sons, 1996