POSTER

Towards a privacy–respectful telematic verification system for vehicle & driver authorizations*

Ana I. González-Tablas, Almudena Alcaide, Guillermo Suarez-Tangil, José M. de Fuentes, and Israel Barroso-Perez

Computer Science and Engineering Department, Universidad Carlos III de Madrid, Avda. de la Universidad 30, 28911 Leganés, SPAIN,
{aigonzal,aalcaide,jfuentes,ibperez}@inf.uc3m.es,gtangil@pa.uc3m.es

Abstract. The use of ubiquitous technologies to implement a telematic on-the-road verification of driver and vehicle authorizations would provide significant benefits regarding road safety, economic costs and convenience. Privacy-aware digital credentials would enable such a service although some challenges exist. The goal of this on-going work is to address these challenges. The first contribution herein presented is an enhanced data model of driver and vehicle authorizations. Secondly, we provide an analysis of existing privacy-aware digital credential systems that may support the implementation of the system.

Key words: Digital credential, Privacy, Vehicle, Driver, Enforcement, Intelligent Transportation Systems.

1 Introduction

Nowadays, improving road safety is one of the major challenges in developed countries. Valid and up-to-date credentials attesting the conditions of vehicles and drivers are required to prove the suitability of a circulating vehicle from the road safety point of view. Enforcement of this requirement is usually done by human patrols deployed on road stretches. Agents stop vehicles and visually inspect the credentials, most of which are currently issued in paper form. The effectiveness of this procedure to decrease the number or the seriousness of traffic fatalities is related to the intensity of controls. Enforcement systems built on electronic credentials and Intelligent Transportation System (ITS) technologies would enable a more convenient, frequent and effective enforcement. However, some problems must be overcome to develop such a system. Firstly, the current set of driver and vehicle authorizations constitutes an inefficient and complex data model to operate with, in the digital world. Secondly, critical privacy issues arise concerning the traceability and surveillance of drivers and vehicles. Thirdly, the restrictions imposed by ITS environments must be considered. The final goal

* The authors acknowledge the financial support granted by the *Comunidad de Madrid* under CCG10-UC3M/TIC-5174.

Semantic meaning		Credential	Holder	Issuer	Expiration date	Revocability	Verified facts and attributes
Authorizes the vehicle (VIN/ Registration Number) to circulate	Authorizes the vehicle to circulate from a technical point of view	Technical inspection card	Vehicle	Manufacturer / Regional Industry Department	Never	No. Compulsory renewal if attributes change	Holdership, authenticity, authorized issuer.
		Technical inspection report, record (in technical inspection card) and sticker	Vehicle	Technical Inspection Station	Specific number of years		Holdership, authenticity, authorized issuer, up-to-date.
	Authorizes the vehicle to circulate from an administrative point of view	Vehicle registration certificate and registration plate	Vehicle & Keeper	Road Traffic Authority	Never	Yes (documents are usually retained)	Holdership, authenticity, authorized issuer, not revoked.
		Proof of tax payment	Vehicle & Keeper	Local Tax Administration / Bank	Annuity Payment	No	Holdership, authenticity, authorized issuer, up-to-date.
		Proof of compulsory insurance payment	Vehicle & Owner / Keeper	Insurance Company / Bank	Annuity Payment		Holdership, authenticity, authorized issuer, up to date.
Authorizes a person (ID) to drive a vehicle	Authorizes the driver to circulate with a certain type of vehicle	Driving license	Person	Road Traffic Authority	Specific number of years	Yes	Holdership, authenticity, authorized issuer, up to date, not revoked.

Table 1. Summary of the main characteristics of current Spanish credentials.

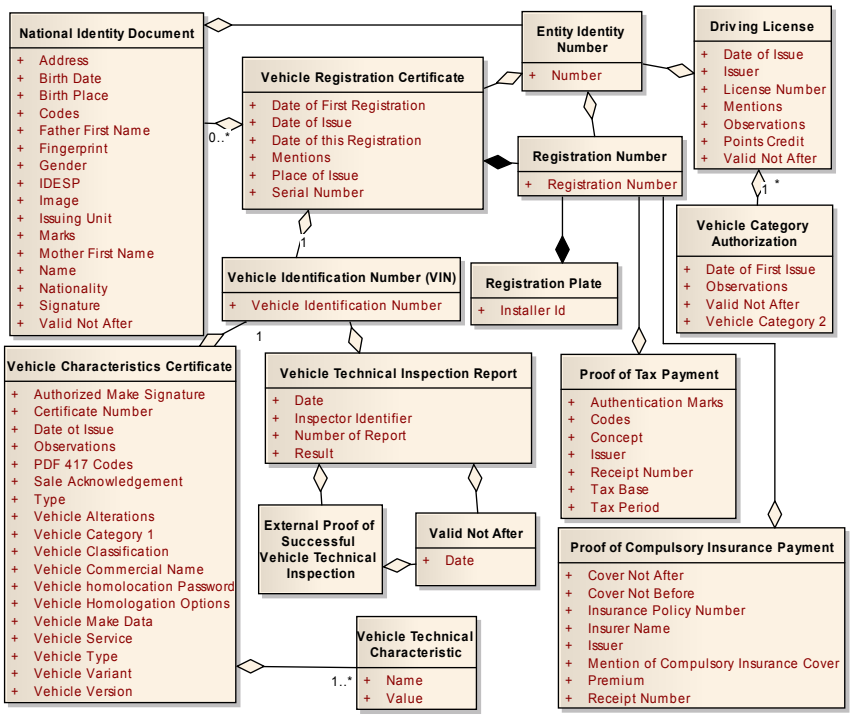

Fig. 1. Improved credential data model.

of this on-going research is to build a privacy-respectful telematic enforcement system for the verification of vehicle and driver authorizations.

	Brands [2]	Kwon [4]	Chameleon [5]	Camenish [3]	Verheul [6]
No. of Certificates	$\alpha\delta$	$\alpha\delta$	1	α	α
Workload	$O(\beta)$	$O(\beta)$	$O(\beta)$	$O(\beta)$	$O(\beta)$
Accept Non Predefined Control Policies?	✓	✓	✓	✗	✗
Commercial Implementation	U-prove	✗	✗	Idemix	✗
Unlinkability (Pseudonyms Changes)	✗	✗	✗	✗	
PKI Standard Compliance	✗	✓	✓	✗	✗
Anonymous Credential Acquirance	✓	✓	✓	✓	✓

Table 2. Summary of the properties analyzed in the schemes. An entity is described by β attributes and wants to unlinkably perform α different verification procedures each one δ times.

2 Proposed Vehicle & Driver Authorizations System

2.1 Improved Credential Model

In this poster, we summarize the first results of our research. First, after analyzing the Spanish legislation (see Table 1), a new credential data model has been developed (see Fig. 1), which significantly improves the current one by eliminating attribute redundancy, and unnecessary relations and credentials.

2.2 Privacy-aware Digital Credential Systems

Second, we have analyzed current credential systems that allow proving the credentials' attributes anonymously (see Table 2). These schemes are the candidates for implementing the privacy-respectful telematic verification system for vehicle and driver authorizations that we envision.

2.3 Deployment on an ITS environment

In order to deploy telematic verification system on an ITS environment, we assume that the vehicle carries its credentials on the vehicle's Hardware Security Module (HSM) and that the driver also carries his credential set in a secured device such as a smart card. We further assume that the vehicle is equipped with different credential readers and that the vehicle's OBU/HSM will act as an intermediary between credentials verification system and the driver's credential platform.

If it is assumed that Road Side Units (RSU) act as verifiers, a vehicle (circulating at 120 km/h) covers the RSU's range (1 km) in 30 s. Therefore, the feasibility of deploying a system such as the envisioned one on ITS environments will strongly depend on the specific scheme or schemes selected to implement the designed set of credentials (see Fig. 1) or others that summarize the attributes that must be verified. Results in [1] throw promising figures as the holdership verification process of a Camenisch credential is said to take around 10.45 s in a Java card.

References

1. P. Bichsel, J. Camenisch, T. Groß, and V. Shoup. Anonymous credentials on a standard java card. In *Proc. of the 16th ACM Conf. on Computer and Communications Security*, CCS'09, pages 600–610, New York, NY, USA, 2009. ACM.
2. S. Brands. *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*. MIT Press, 2000.
3. J. Camenisch, D. Sommer, and R. Zimmermann. A General Certification Framework with Applications to Privacy-Enhancing Certificate Infrastructures. In *Security and Privacy in Dynamic Environments*. 2006.
4. T. Kwon. Privacy preservation with x.509 standard certificates. *Information Sciences*, pages 47–53, 2011. doi:10.1016/j.ins.2011.02.016 Key: citeulike:8971918.
5. G. Persiano and I. Visconti. An efficient and usable multi-show non-transferable anonymous credential system. In *Financial Cryptography*. 2004.
6. Eric R. Verheul. Self-blindable credential certificates from the weil pairing. In *Proceedings of ASIACRYPT '01*, 2001.