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

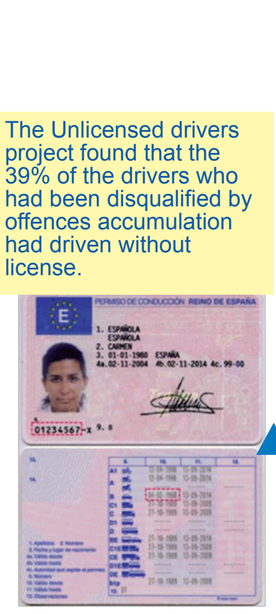
Ana I. González-Tablas, Almudena Alcaide, Guillermo Suárez-Tangil, José M. de Fuentes, Israel Barroso-Perez
Computer Science and Engineering Department. SeTI Research Group. University Carlos III of Madrid

Universidad Carlos III de Madrid

MobiQuitous 2011
8th International ICST Conference on Mobile and Ubiquitous Systems

1. Current enforcement of vehicle & driver authzs.

The Unlicensed drivers project found that the 39% of the drivers who had been disqualified by offences accumulation had driven without license.



In Spain there were 1.4 million of uninsured vehicles in 2006.

The amount of untaxed vehicles in Britain has been estimated in 2.1 million in 2006.

In Spain, 400.000 cars were reported of being driven without having passed the mandatory technical inspection in 2009.

1. The effectiveness of the enforcement procedure to decrease the number or the seriousness of traffic fatalities is related to the intensity of controls.

2. Enforcement systems built on electronic credentials and Intelligent Transportation Systems (ITS) technologies would enable a more convinient, frequent and effective enforcement.

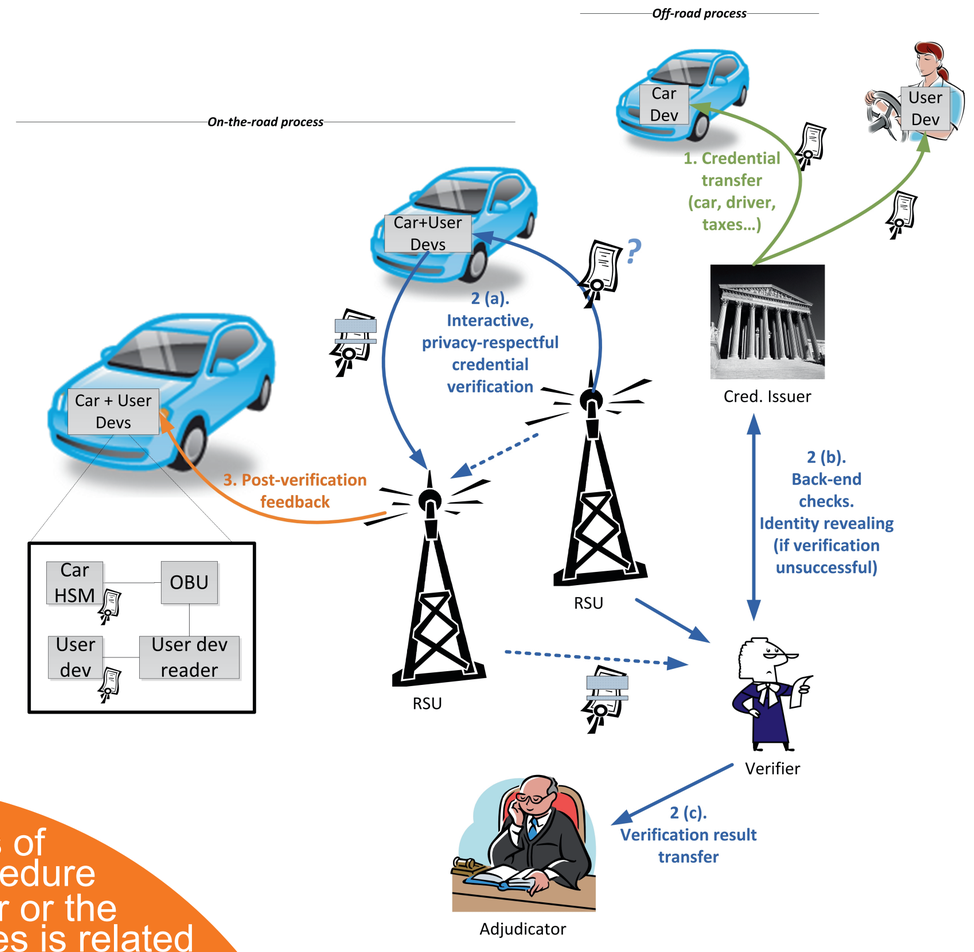
Some problems must be overcome:

P1. The current set of driver and vehicle authorizations constitutes an innefficient and complex data model to operate with, in the digital world.

P2. Critical privacy issues arise concerning the traceability and surveillance of drivers and vehicles.

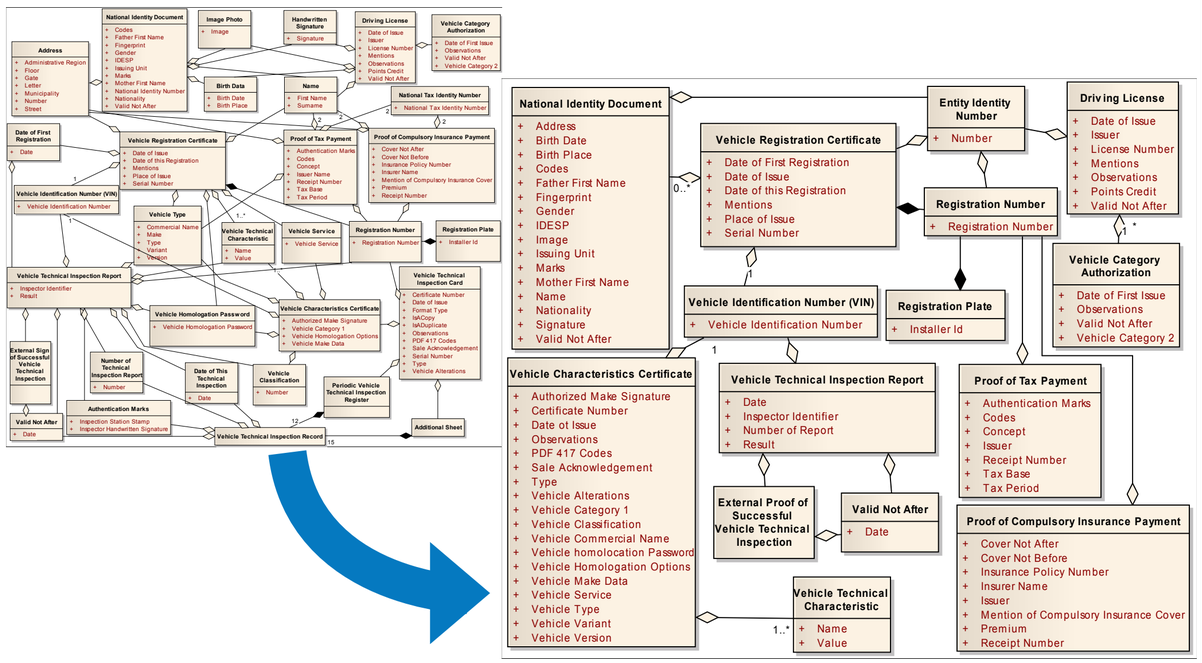
P3. The restrictions imposed by ITS environments must be considered.

2. Proposed privacy-respectful telematic verification system for vehicle & driver authzs.



P1: Improved credential model

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.



P2: Analysis of privacy-aware digital credential systems

A non anonymous digital credential will always disclose the actual values of the holder's attributes.

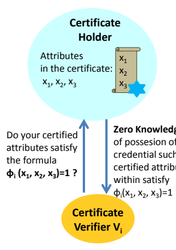
An anonymous digital credential will allow to verify the holder's set of attributes without knowing their actual value.

	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	✓	✓	✓	✓	✓

ONE PASS CREDENTIALS: Consecutive uses of the same anonymous credential are linkable.

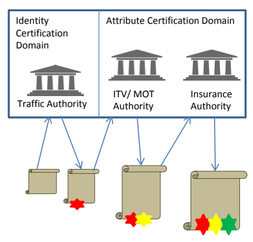
Brand's Credentials

The holder can proof that the set of attributes specified in the credential satisfy a Boolean formula, without disclosing the attributes' actual values.



Kwon's Credentials

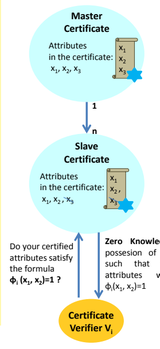
Different authorities certify different attributes belonging to the same credential such that, each authority only sees the actual value of the set of attributes it is certifying.



MULTI-SHOW CREDENTIALS: Consecutive uses of the same anonymous credential are NOT linkable.

Persiano's Credentials

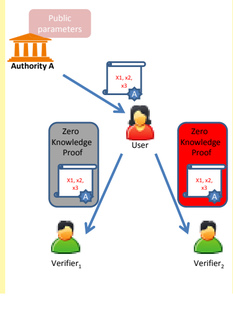
From a master certificate, there could be various slave certificates for different subsets of attributes. Slave certificates are not linkable.



The actual attribute values are never disclosed.

Camenisch's Credentials

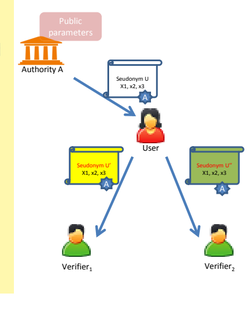
Different zero knowledge proofs (ZKP) can be generated to proof posesion of the same credential. The ZKPs are not linkable.



The actual attribute values are never disclosed.

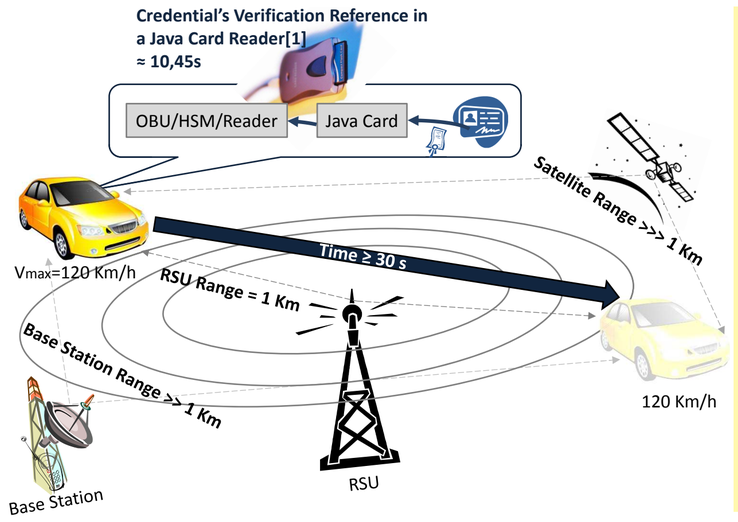
Verheul's Credentials

Different blinded versions of the same pseudonym can be generated from an initial certificate. The new blinded certificates are unlinkable.



The actual attribute values are disclosed each time a certificate is shown. The identity is not.

P3: Restrictions of ITS environments



Feasibility of deploying the proposed system on ITS environments will strongly depend on:

- the specific scheme selected to implement the designed set of credentials,
- the computational capacity of the involved platforms, and
- the responsiveness required for safety-related services.

Holdership verification process of a Camenisch credential is said to take around 10,45s in a Java card [1].

A vehicle (circulating at 120 km/h) covers the RSU's range (1 km) in 30s. If other communication networks are used, other possibilities arise.

References

[1] P. Bischel, J. Camenisch, T. Groß, V. Shoup. Anonymous credentials on a standard Java card. In *Proc. of the 16th ACM Conf. on Computer and Communications Security, CCS'09*, 2009.
[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*, 2011. doi:10.1016/j.ins.2011.02.016.
[5] G. Persiano and I. Visconti. An efficient and usable multi-show non-transferable anonymous credential system. In *Financial Cryptography*, 2004.
[6] E.R. Verheul. Self-blindable credential certificates from the weil pairing. In *Proc. of ASIACRYPT '01*, 2001.

Acknowledgments & Contact Information

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

Authors' emails: aigonzal (at) inf.uc3m.es, aalcaide (at) inf.uc3m.es, gtangil (at) pa.uc3m.es, jfuentes (at) inf.uc3m.es, ibperez (at) inf.uc3m.es