



Security and Privacy Issues for Connected Vehicle Safety Applications

André Weimerskirch

COMeSafety – 7th International Workshop on
Vehicle Communications for Safety and Sustainability

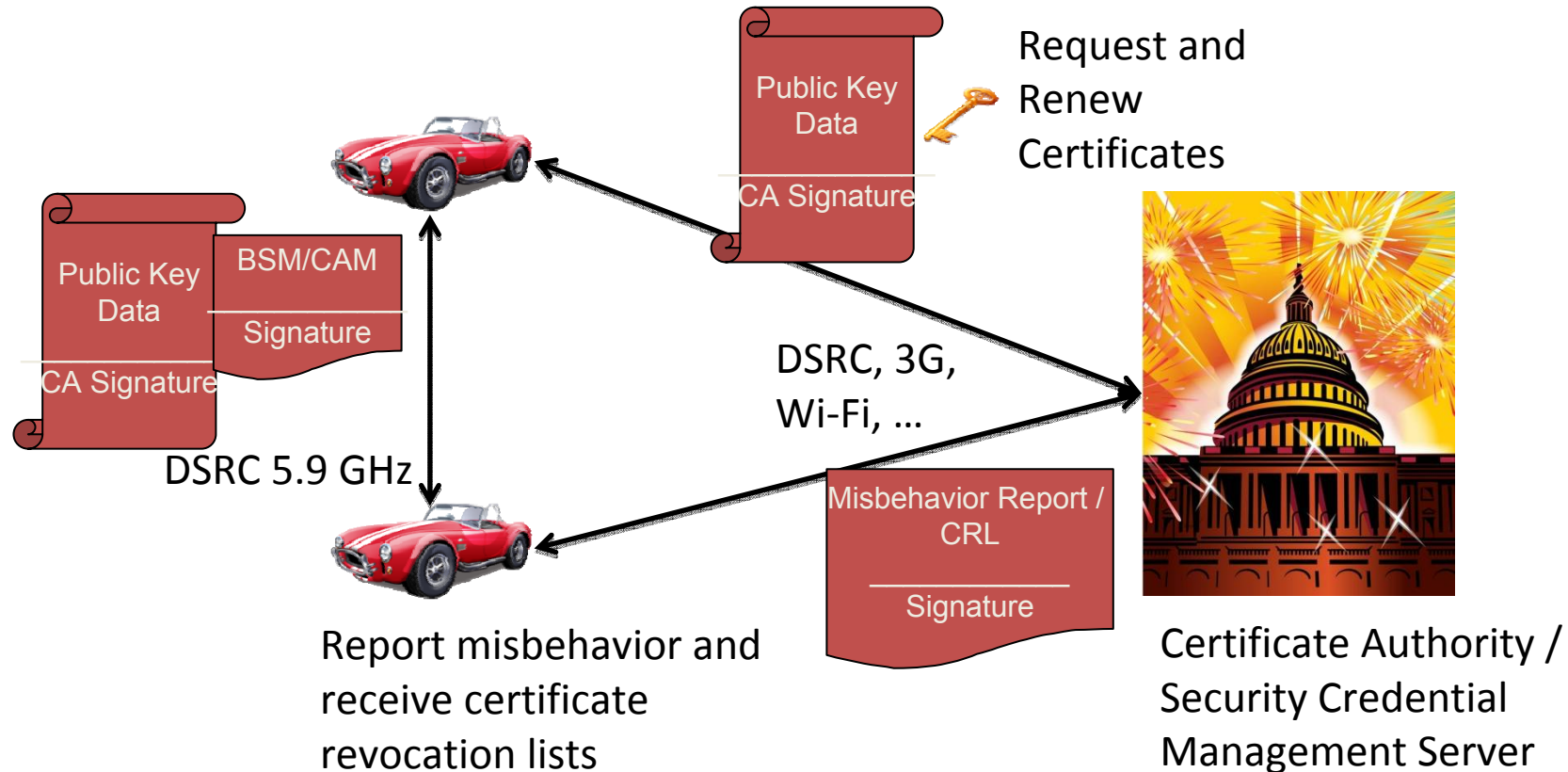
October 21st, 2011

Introduction



- It is commonly agreed that data security mechanisms, especially message authentication, is required in V2V.
- It is also commonly agreed that mechanisms are required to preserve users' privacy
 - In fact, almost all complexity of security design is introduced due to privacy preservation
- It seems that V2V safety applications will be deployed first and that limited DSRC infrastructure will be available for support

Overview of V2V Security



- Main objective is security of V2V
- V2I is required to support V2V security

USA vs. Europe: Security Design Premises



USA	Europe
<p>Crash avoidance safety critical applications will be deployed from day one</p> <ul style="list-style-type: none"> • Driver warnings but no control 	<p>Safety, mobility and efficiency applications will be deployed, but no vehicle control foreseen for day one.</p>
<p>Little infrastructure (e.g. road-side units) will be available at deployment. Then growing with vehicle penetration.</p>	<p>No infrastructure at time of deployment. Then growing with vehicle penetration.</p>
<p>Safety is the objective, design parameters (security, privacy, safety) balanced according to technical and policy objectives.</p>	
<p>Commercially reasonable secure hardware cannot avoid attacks and security design needs to account for most challenging case</p>	<p>Secure hardware planned to protect credentials, in order to lower credential management hurdle</p>

Authentication and Privacy



- Broadcast authentication (V2V)
 - Use IEEE 1609.2 Standard / ETSI 1609.2 Security Profile
 - By the time of deployment, EU and US 1609.2 extensions will (hopefully) be incorporated
 - Same cryptographic primitives are used in USA and EU
- Privacy preserving messages
 - Security credentials: change certificates regularly
 - Similar ideas
 - **But:** US approach requires far more certificates and much higher memory storage requirements in terms of bytes (500 KB vs. 20 MB).
 - Message content: BSMs (USA) and CAM/DENM (Europe)
 - Similar – harmonization in progress

Local Processing

- Misbehavior detection: unclear yet
- Certificate Renewal: defined by VSC3 (1609.2 style), flexible design by C2C-CC
 - Objective: C2C-CC design planned to allow VSC3 compatible design as one option, thus allowing an overlap of implemented cryptographic primitives
- EU does not design misbehavior detection and revocation yet but might naturally evolve later
 - Misbehavior reporting: defined by VSC3 (1609.2 style), n/a in C2C-CC design
 - Certificate revocation list processing: defined by VSC3 (1609.2 style), n/a in C2C-CC design

Security Credential Management Server



- Split roles of authorities to limit ability to violate users' privacy
 - US design driven by privacy preservation
 - EU design emphasizes flexibility
 - No need for harmonization beyond certificate renewal process (→ local processing), thus differences due to regional preferences are possible.
- **Open Question:** does the device identifier security credential (CSR certificate and long-term certificate, respectively) need to be harmonized?

Verify-on-Demand



- US defines minimum requirement to verify those messages leading to a driver warning, finally up to OEM
- EU defines approach to verify as much as possible based on heuristic, finally up to OEM
- Verify-on-demand is not a regional issue but an OEM global decision (car maker X will use same approach in Europe and USA)
- No harmonization needed

What needs to be harmonized?

- Cryptographic mechanisms are already in sync
 - For V2V and V2I (certificate renewal)
 - Allows common cryptographic accelerator, if demanded
- Storage requirements are very different
 - 500 KB and secure key storage, vs.
 - 20 MB but no further requirements
- Privacy parameters and expectations are slightly different
 - But no major design differences
- Security Credential Management Server interface
 - US design might be one of the offered EU server interfaces



What needs to be resolved?

- Misbehavior detection
 - Approaches unclear in EU and US
- Accounting for global production processes
 - Japanese supplier manufacturing a DSRC unit and injecting keys for German car maker that immediately exports this car to the US
 - Any issues that go beyond today's manufacturing processes?
- Security certification
 - Do we need minimum security requirements?
 - How will the minimum requirements be determined?

Security Implementation – Policy Comments / Questions



- Security System: The overall security system should be designed to maintain **privacy by design and policy**, with specific system requirements of: Anonymity for mandatory services; Non-Trackability for mandatory services; Protection from attacks on system Integrity; Prevention of unauthorized access to Personally Identifiable Information (PII); No user fees for mandatory services; Stable, long-term policy and technology with backward compatibility (decades rather than years)¹.
- New Certificates: A vehicle is designed to obtain certificates for a year at a time and decryption keys for a shorter period, about once per month. Q: Is this time period reasonable or should the time period be adjusted, either longer or shorter? **What happens if your vehicle is not able to communicate with the RA and cannot unlock the bundle?** Will your vehicle no longer be able to participate in the cooperative system?
- Fall-Back Certificates: A vehicle will convert to a fall-back certificate if the vehicle runs out of certificates. The vehicle will use the same certificate until it contacts the RA to obtain more certificates. The fall-back certificate is valid for 2-3 years. Q: Does it seem reasonable to include fall-back certificates? What time period for the fall back certificates seems reasonable? What are the implications to not have a fall-back certificate? **What are the privacy implications to have a fall-back certificate?**
- CRL: Once on the CRL, a 'bad' device's linkage ID for a group of certificates is broadcasted to all other vehicles. Q: Does this seem reasonable? What are the rules for revocation? Do you keep sending message or have a policy stated to stop sending messages? (a 'good' vehicle will ignore the 'bad' message only if the 'good' vehicle has the updated CRL) **What legal actions should there be to prevent misbehavior?**

¹ Based on conversation with OEMs.



Dr. André Weimerskirch
CEO
andre.weimerskirch@escrypt.com