Scalable and Provably Secure Self-Revocation Protocols for V2X

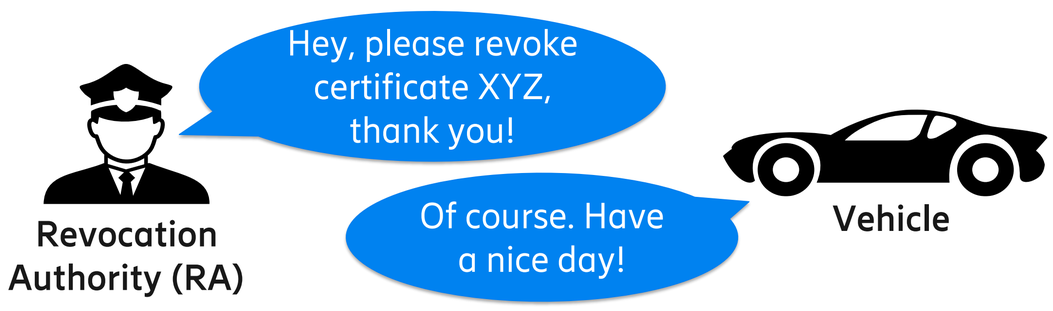
*Revocation in V2X is the **exclusion** of malfunctioning or **malicious** vehicles from interacting with others.*

Challenges

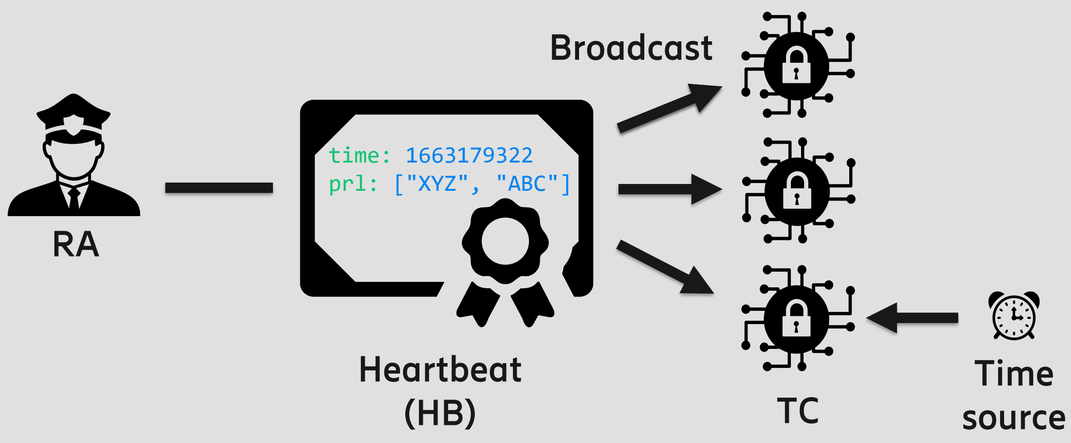
- **Privacy**: vehicles use *pseudonym identities*, which makes revocation harder
- **Security**: revocation must complete *as fast as possible* to maintain road safety
- **Scalability**: the scheme *must scale well* with an increasing number of vehicles

Self-revocation in V2X

Vehicles are equipped with a **Trusted Component (TC)** for attestation and credential management.



Our work

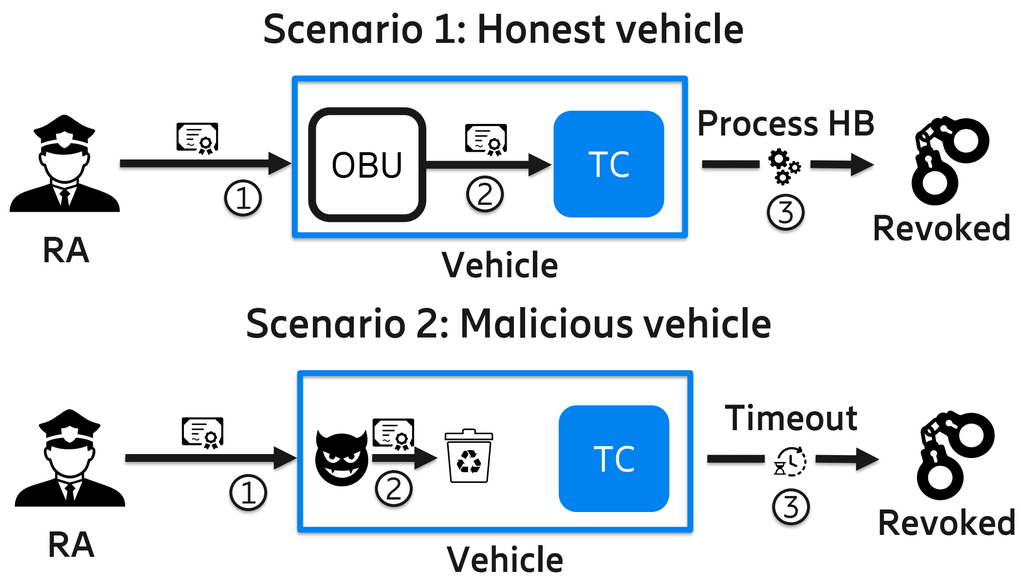


Design

We designed a protocol for self-revocation of V2X credentials, in **two variants**: the first assumes a **trusted time source** available in TCs, the second uses a **logical clock** (“**epochs**”).

Formal verification

We verified both variants with **Tamarin Prover**, showing that we can guarantee actual revocation with an **upper bound on revocation time**, in the presence of different realistic attackers.



Revocation Scheme	Revocation time	Verification time	Network overhead
Active revocation	low	high	high
Passive revocation	moderate	low	moderate
Self revocation	low	low	low

Evaluation

We evaluated the security and scalability of our design, showing that it guarantees a **prompt revocation** and **a low utilization of resources**, even with a high number of participants.

Applicability beyond V2X

Requirements

- Stringent real-time communication
- Use of pseudonymous credentials
- Fast and reliable revocation
- High number of participants

Example use cases

- Smart cities
- Mobile-to-mobile communication
- Peer-to-peer network applications
- Privacy-preserving technologies

Check out our paper!