Public Key Infrastructure Scalability: the ISE Project Contribution

Pierpaolo Cincilla
ISE Project

**Context**
- Vehicles Broadcasts / Geocasts information to neighbor
  - vehicle dynamics info (position, speed, heading ...)
  - perception of dynamic environment
- **Security and privacy are paramount**

**Challenges**
- Build security infrastructure (PKI)
- Ensure scalability, security and safety
- Methods and Tools to design and validate trustworthy ITS systems
ISE Architecture Overview

ETSI TS 103 097, TS 102 940/941
ISE PKI Architecture

- Enrollment Certificate (EC)
- Authorization Ticket (AT)
- ITS-S
- EA
- AA
- RCA
Large Scale PKI Deployment

- Millions of ITSs, billions of (pseudonyms) identities
  - We must ensure the system scalability
  - A centralized system will saturate at some point
We need to distribute the system

- Replication implications
  - Authorization Tickets (reads) performance improve
  - Enrollment Tickets (writes) performance worsen

![Diagram of Group Communication with expected performances]

**AT (read)**
- Centralized
- Replicated

**EC (write)**
- Centralized
- Replicated
PKI Deployment

To boost the writes…Trade consistency!

- Replication implications
  - Database operation’s execution order (FIFO vs ABCAST)
  - Synchronous vs asynchronous propagation (Local vs Global)

![Group Communication Diagram]

**EC (write)**

- **Write Global**
  - Centralized
  - Rep AB
  - Rep FIFO

- **Write Local**
  - Centralized
  - Rep AB
  - Rep FIFO
See you in Livorno !!!