



Public Key Infrastructure Scalability: the ISE Project Contribution

Pierpaolo Cincilla



ISE Project

Start :
July 2014
3 Years

◆ Context

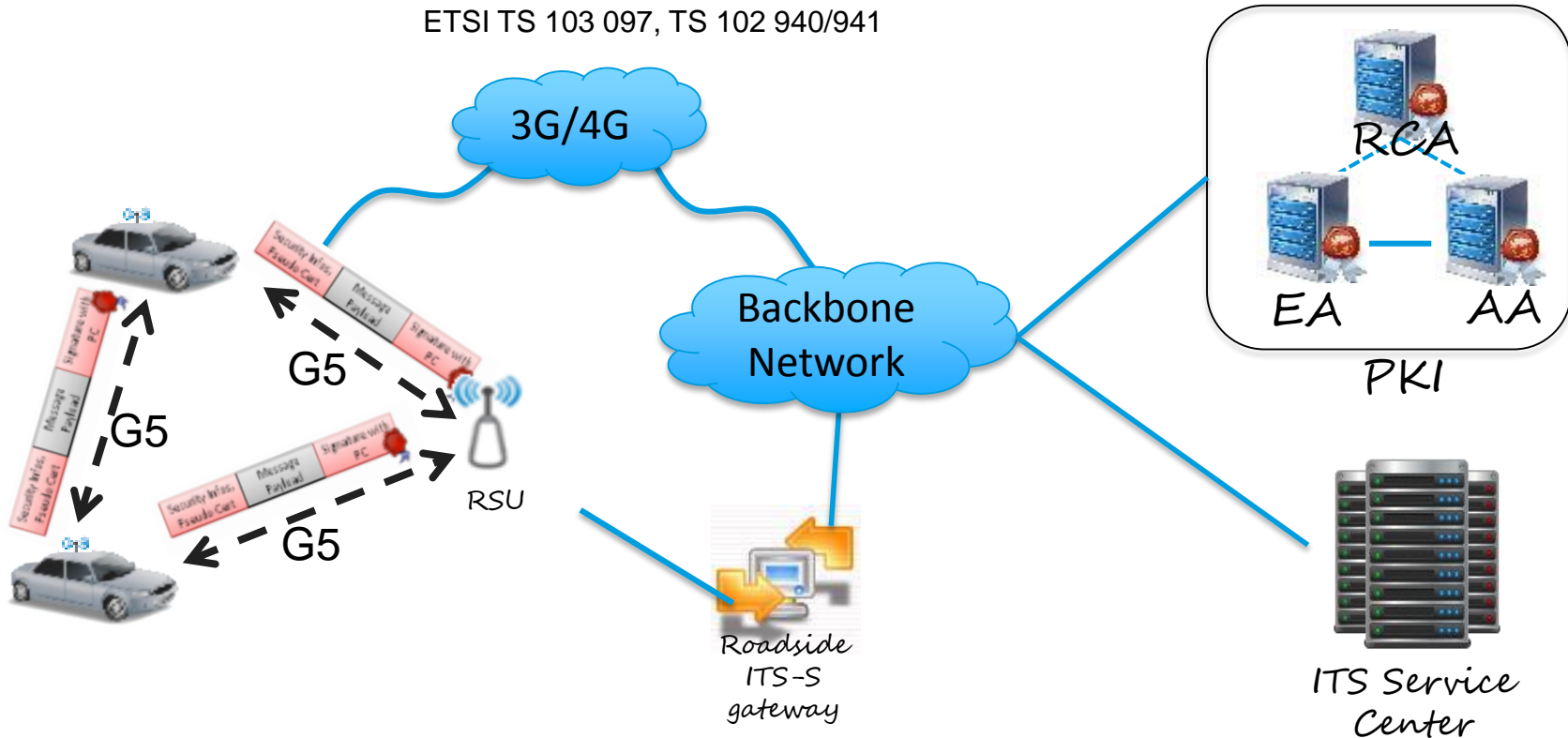
- ◆ Vehicles Broadcasts /Geocasts information to neighbor
 - ◆ vehicle dynamics info (position, speed, heading ...)
 - ◆ perception of dynamic environment
- ◆ **Security and privacy are paramount**

◆ Challenges

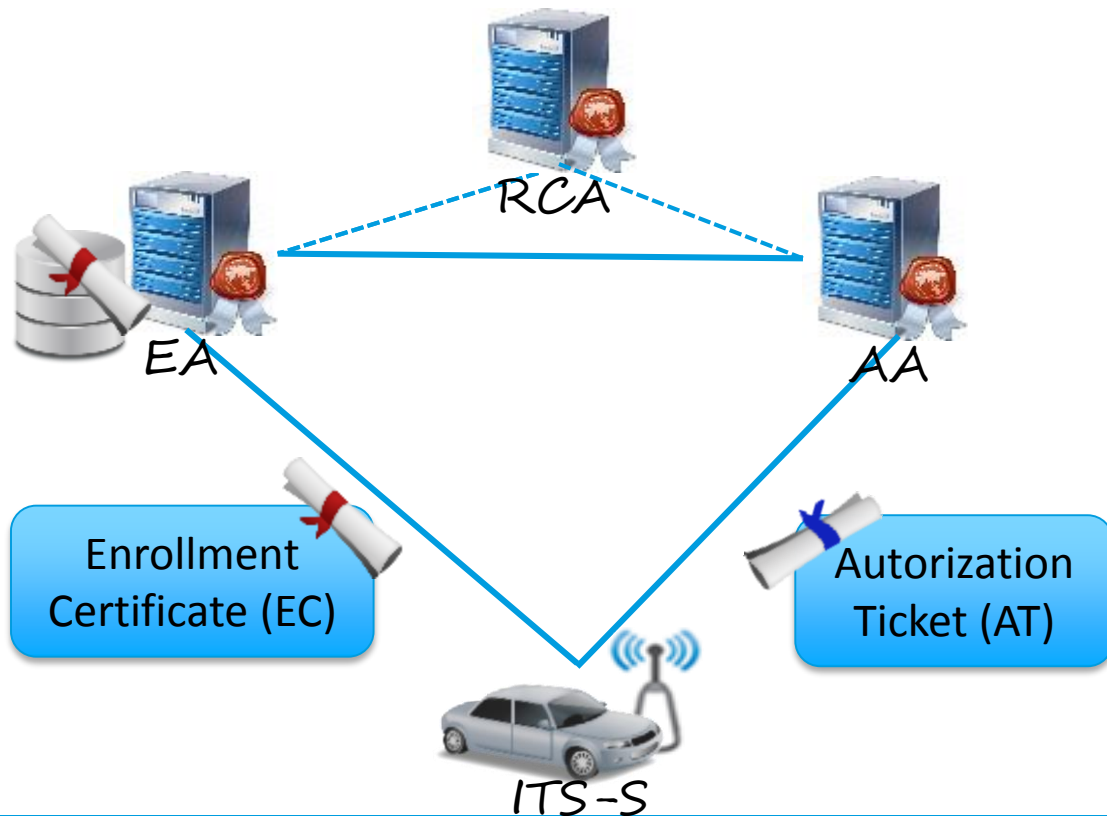
- ◆ Build security infrastructure (PKI)
- ◆ Ensure scalability, security and safety
- ◆ Methods and Tools to design and validate trustworthy ITS systems

ISE Architecture Overview

ETSI TS 103 097, TS 102 940/941

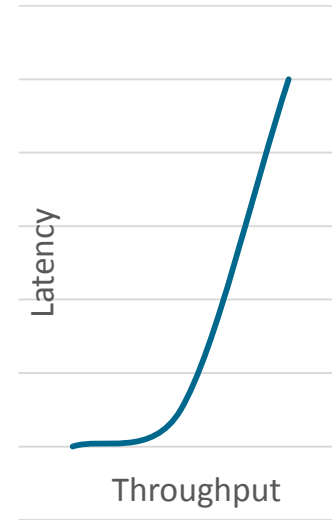
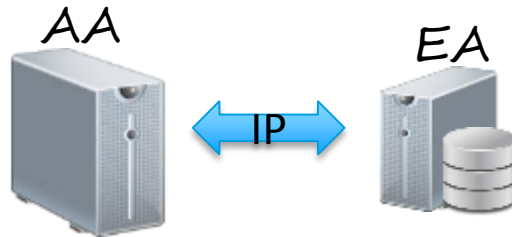


ISE PKI Architecture



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



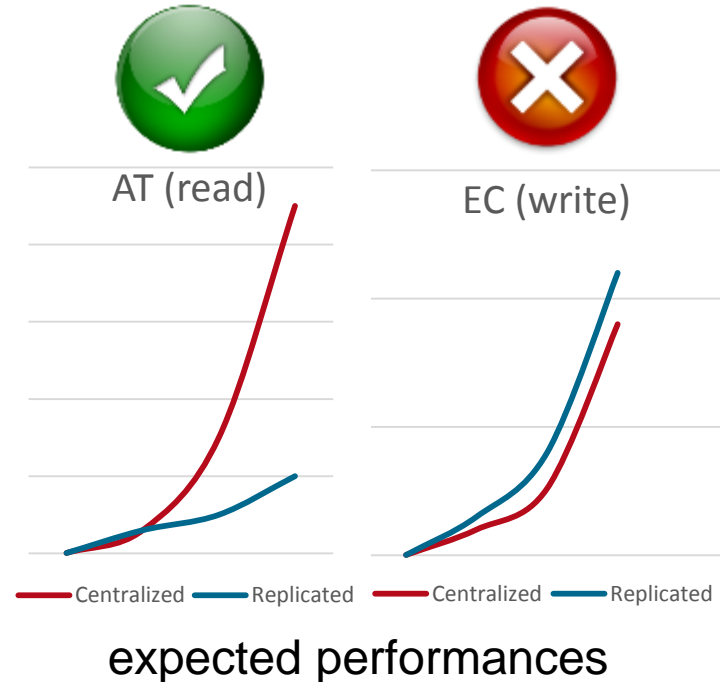
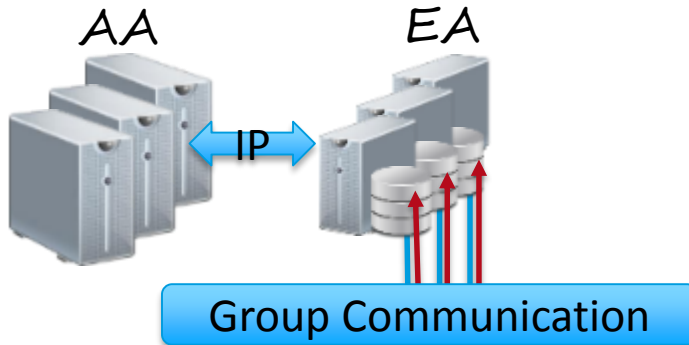
AT expected performances



EC expected performances

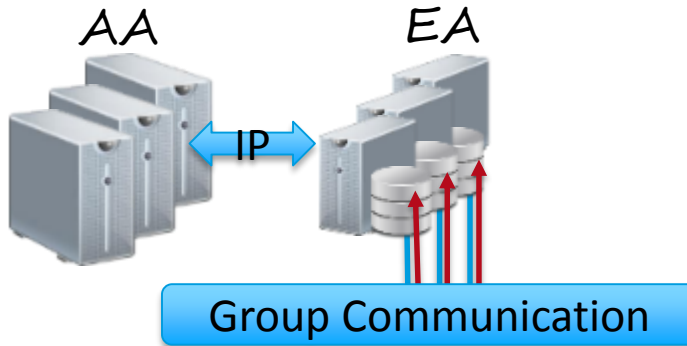
We need to distribute the system

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



To boost the writes... Trade consistency!

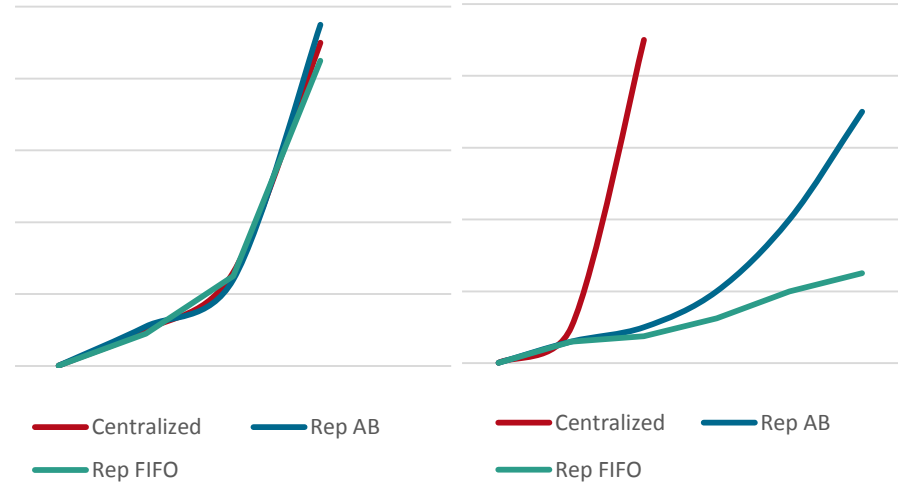
- ◆ Replication implications
 - ◆ Database operation's execution order (FIFO vs ABCAST)
 - ◆ Synchronous vs asynchronous propagation (Local vs Global)



EC (write)

Write Global

Write Local



ITS Cooperative Mobility Services Event 5

See you in
Livorno !!!

