



Vehicular PKI Scalability-Consistency Trade-Offs in Large Scale Distributed Scenarios

Omar Hicham

Vehicles **communicate**
and **cooperate**



New Complexity

Lane Keeping



Entertainment

Adaptive Cruise Control

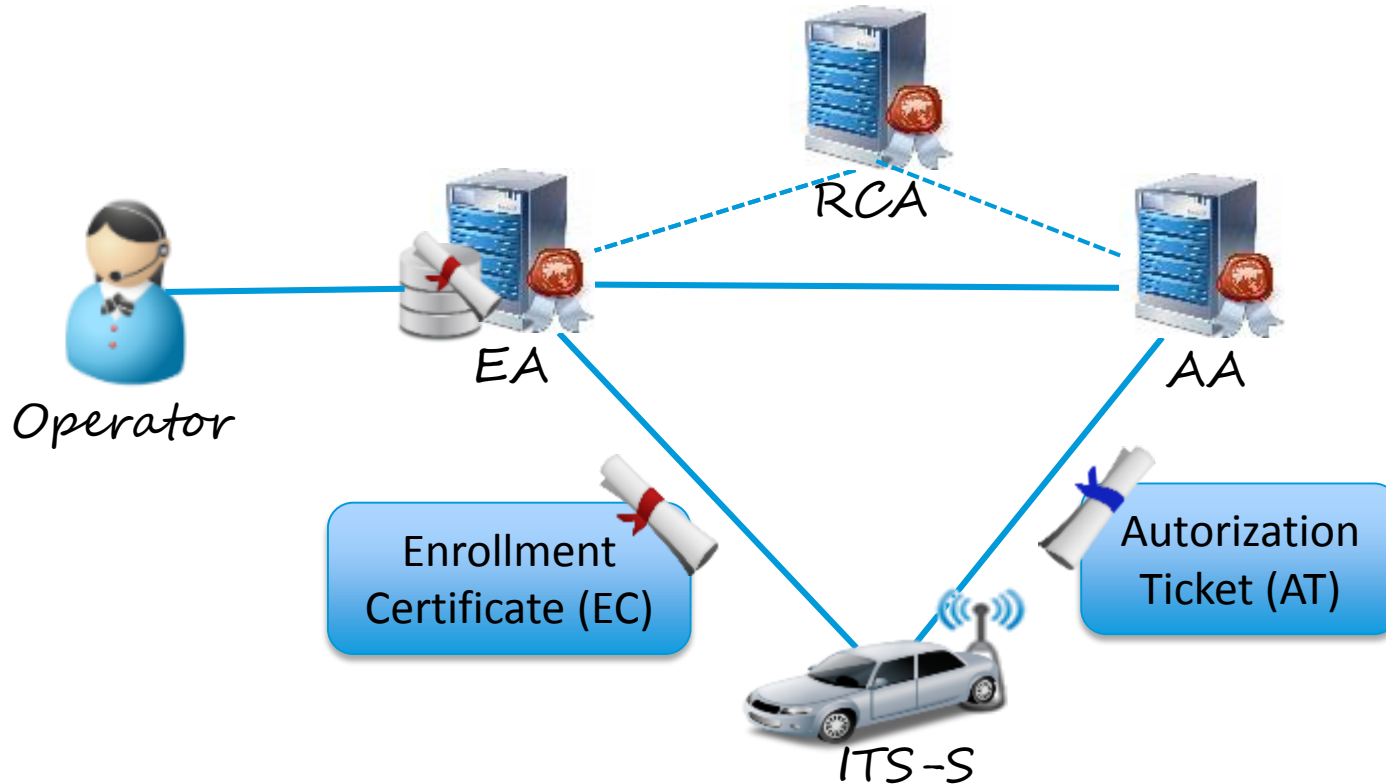
New Applications

New Threats

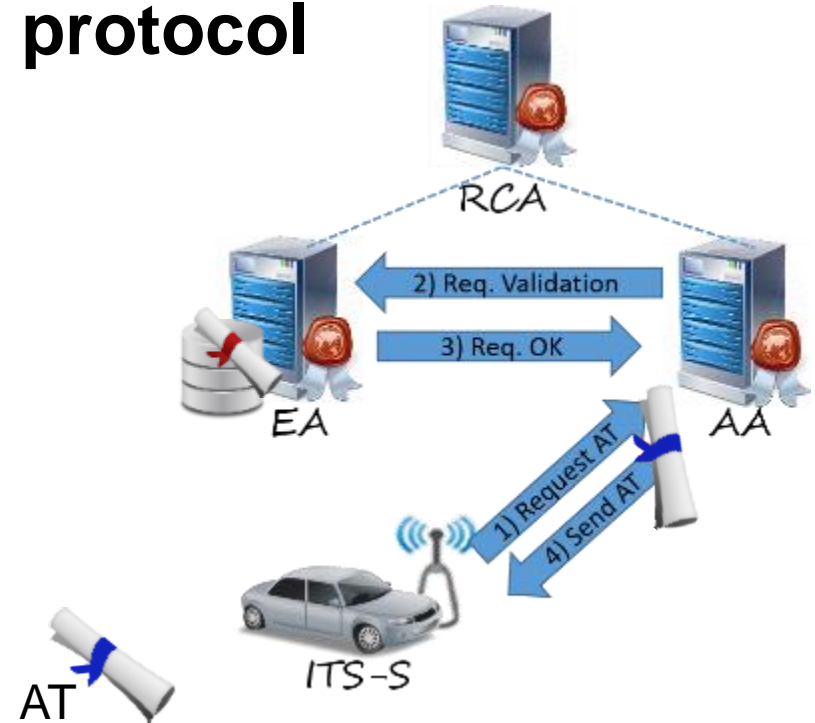
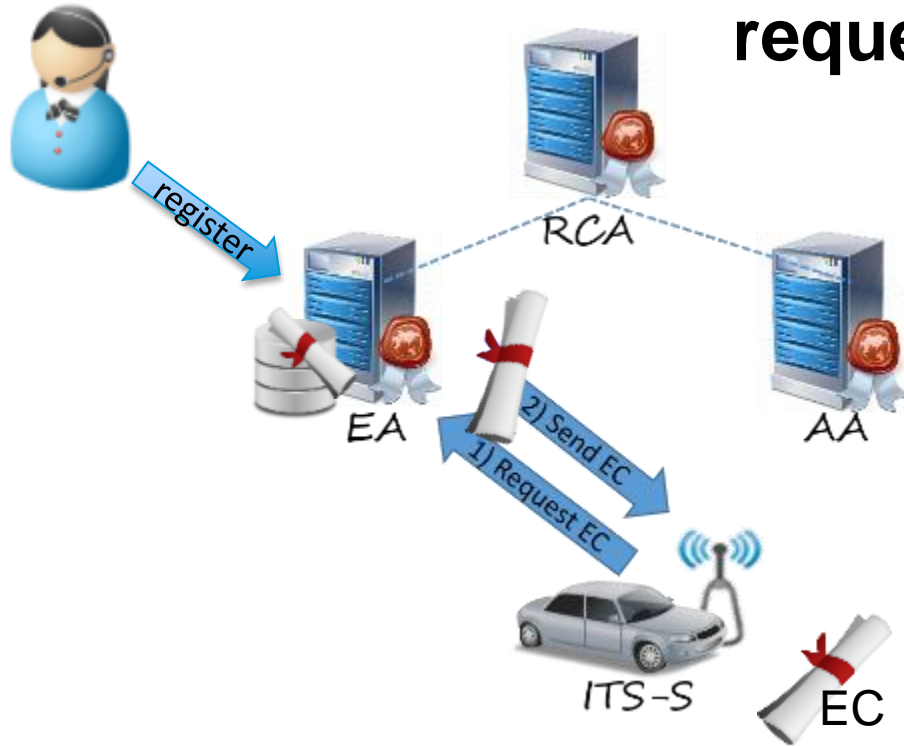


- Communications between ITS and the infrastructures are fundamental to improve traffic management, road safety, mobility and comfort services
- EU and US standards define the Public Key Infrastructure (PKI) as the base of trust for vehicular communication
- No one has investigated the **PKI scalability** in large scale deployment.
- We assess PKI performance and scalability **replicating the system** on hundreds of machines.
- We evaluate different replication strategies in terms of **performance and consistency implications**.

ISE PKI Architecture



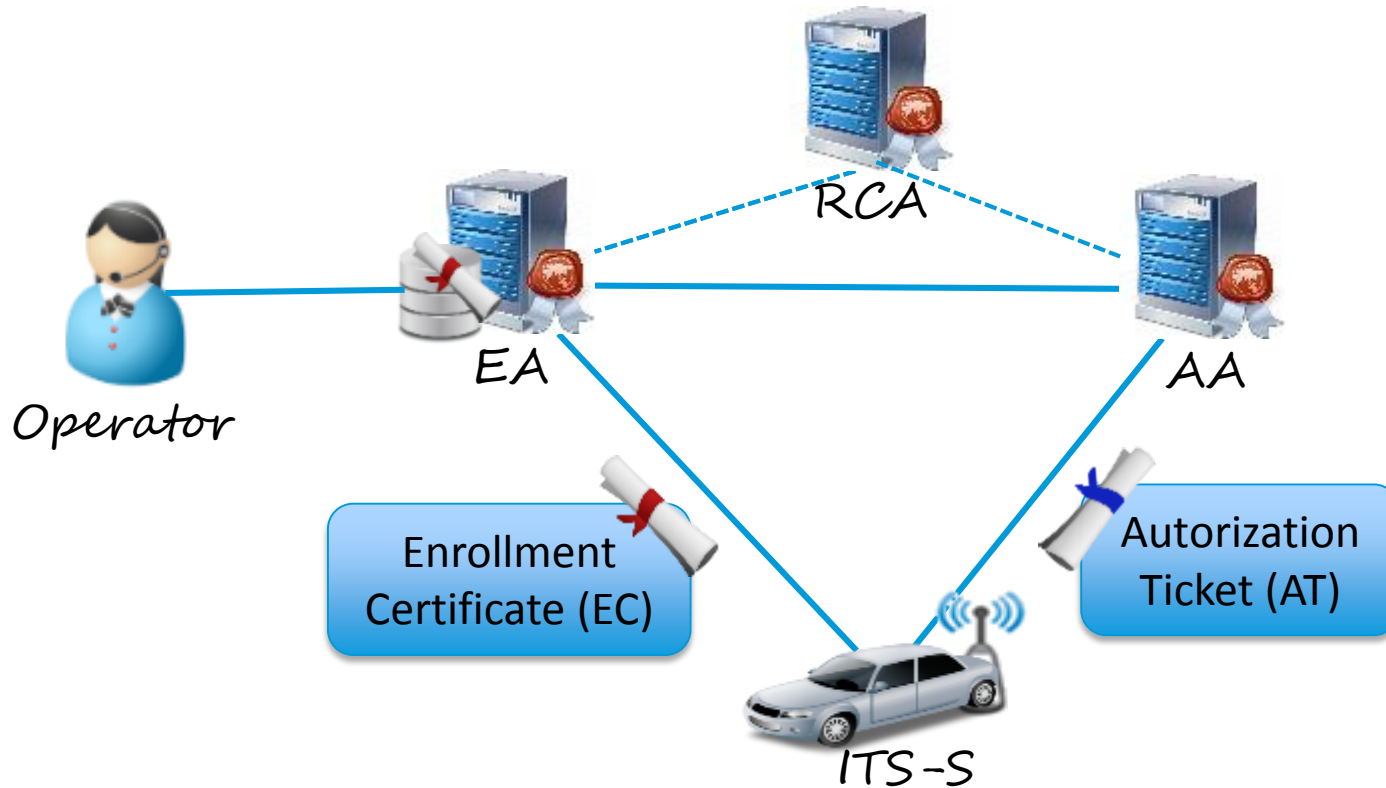
EC and AT request protocol



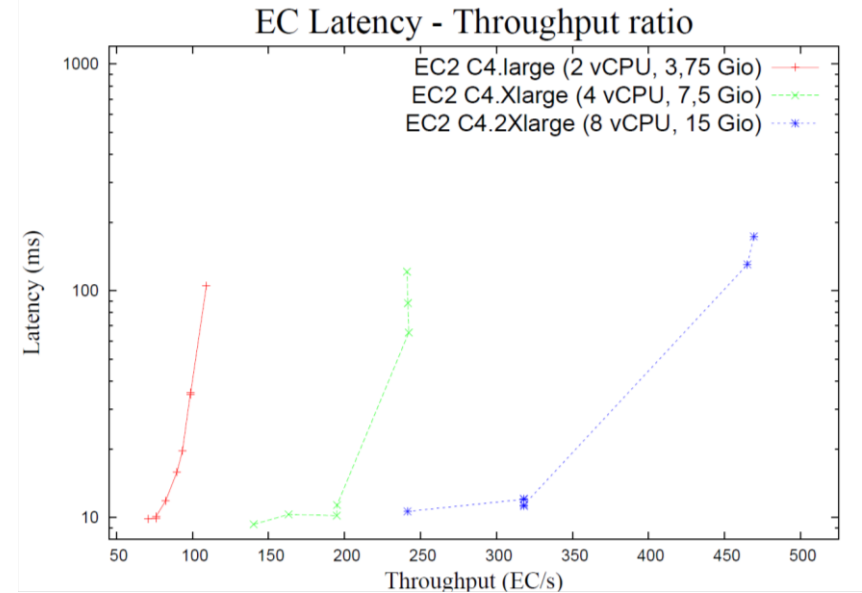
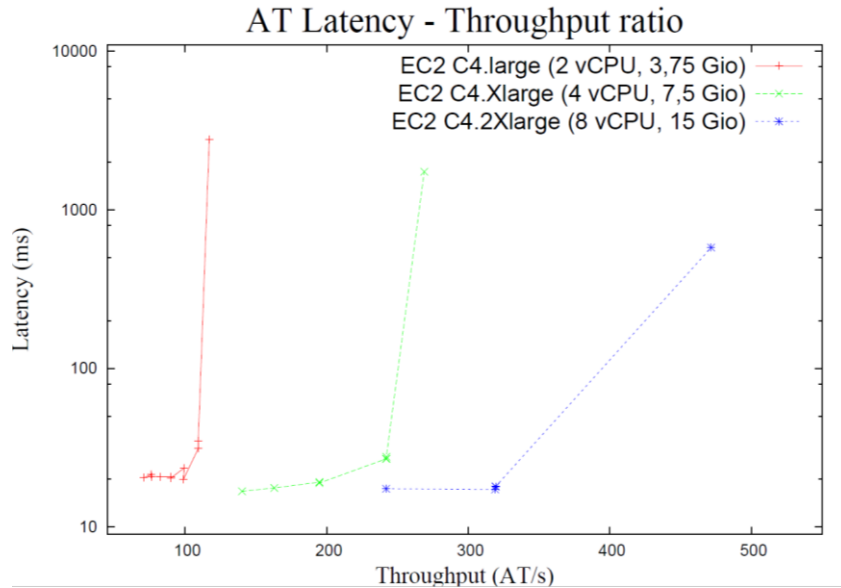
- **Why is it important to study VPKI Scalability ?**

Millions of ITSs, billions of (pseudonyms) identities

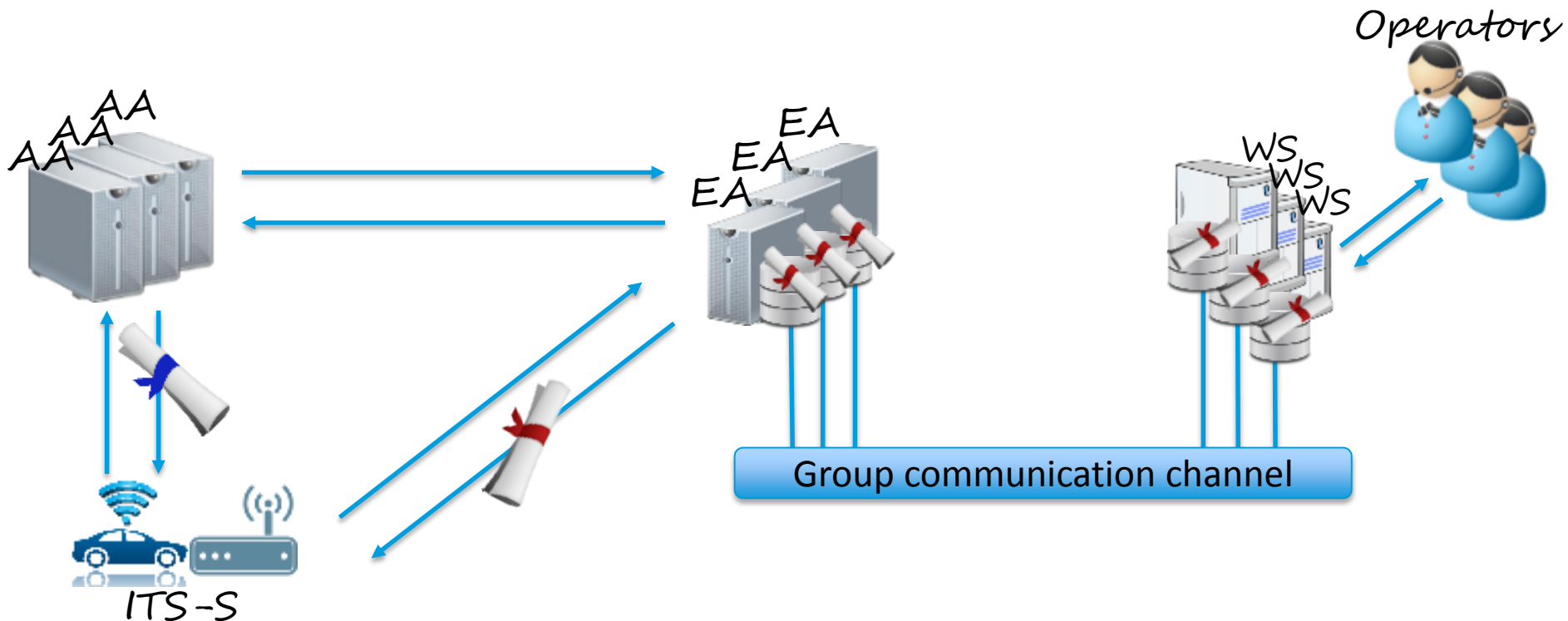
- **Amazon EC2 instances**
- **EU Ireland Data Center**
- **US Northern California Data Center**
- **C4.large (2 vCPU, 3.75GB RAM)**
- **C4.xlarge (4 vCPU, 7.5GB RAM)**
- **C4.2xlarge (8 vCPU, 15GB RAM)**



System saturation !

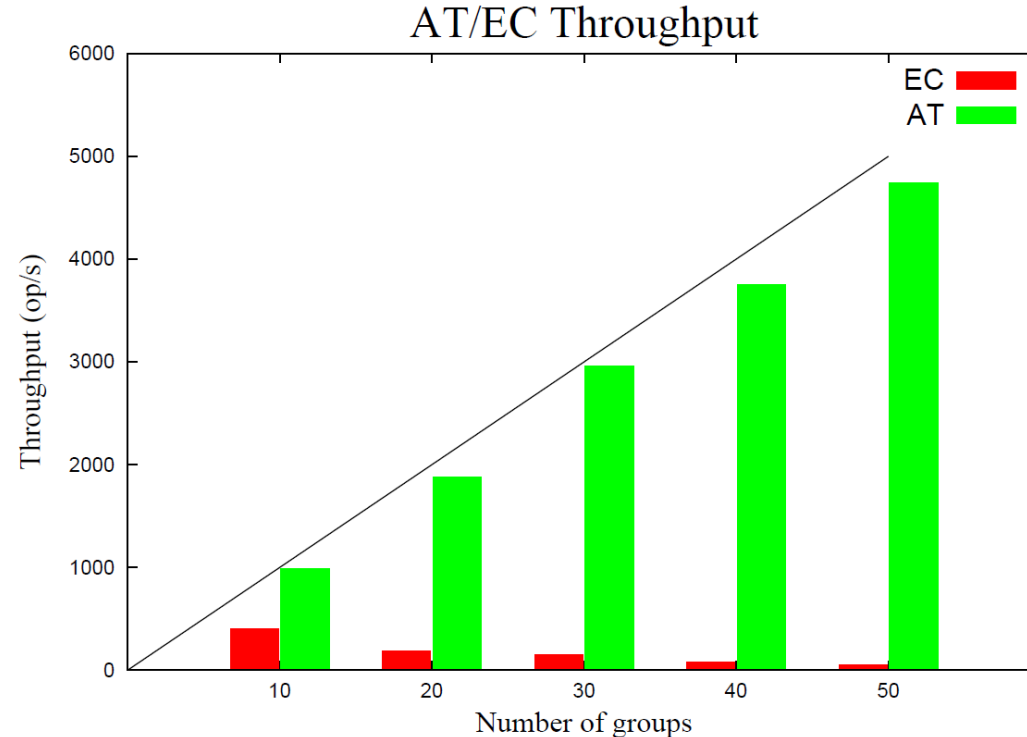


We need to distribute the system



2.Replicated PKI Deployment

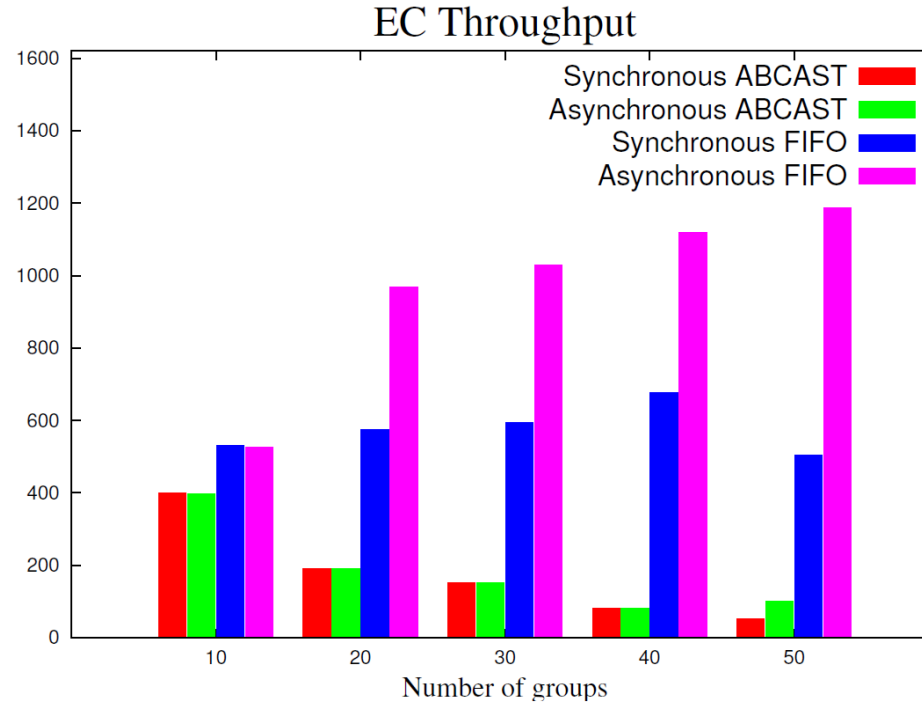
- ✓ AT delivery throughput scales well (representing majority of requests)
- ✗ EC delivery throughput degrades augmenting the number of replicas.

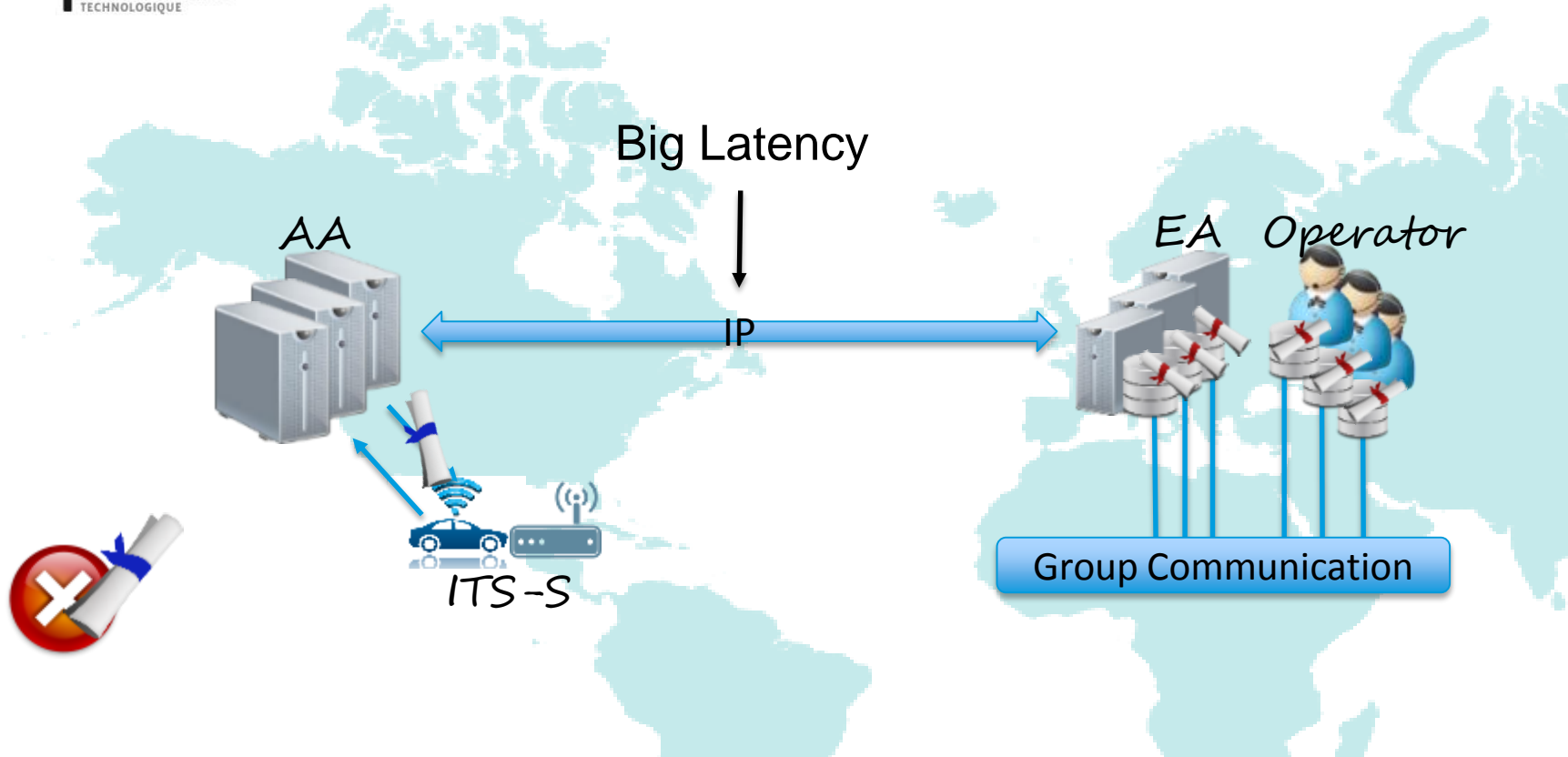


- **Synchronous vs asynchronous** updates propagation (Local vs Global)
- Database operation's execution order (**FIFO vs ABCAST**)



To **boost** EC delivery performance we must **relax** the storage consistency properties

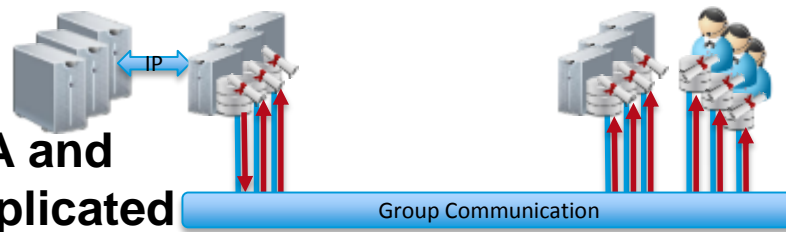
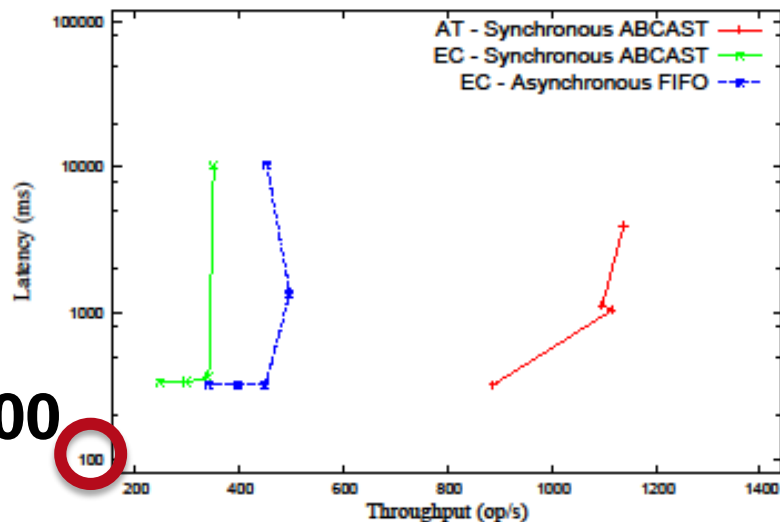






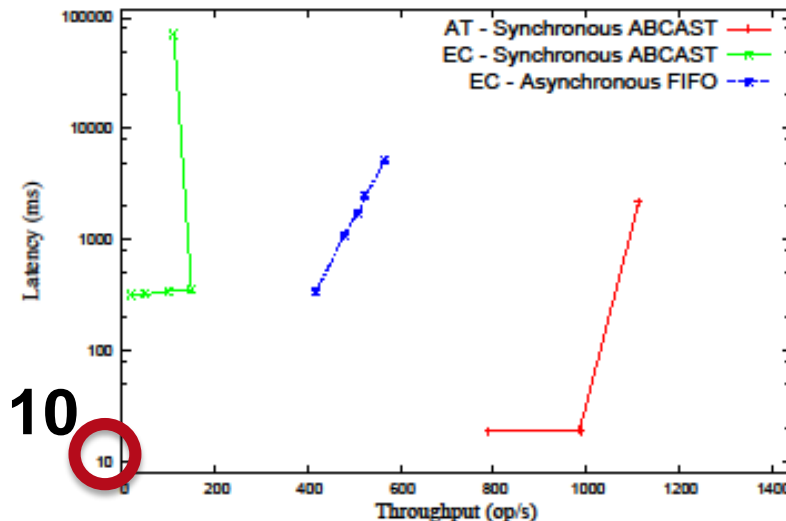
**10 AA in US
and 10 EA in Europe**

AT and EC Latency - Throughput Ratio



**10 AA and
10 replicated
EA in US**

AT and EC Latency - Throughput Ratio



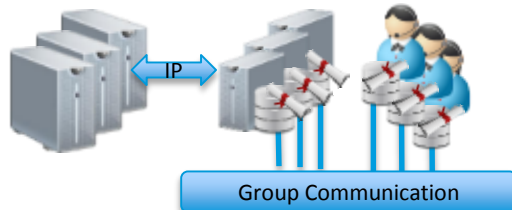
100

10

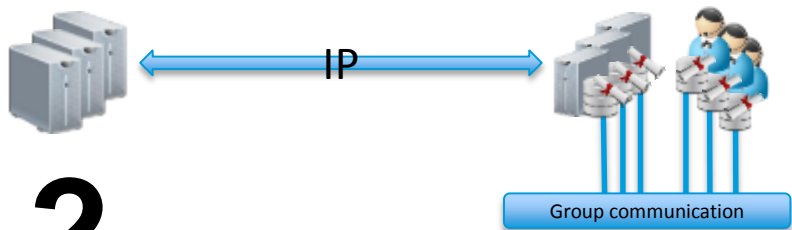
3. Geographic Replication

Autorisation Tickets
all settings

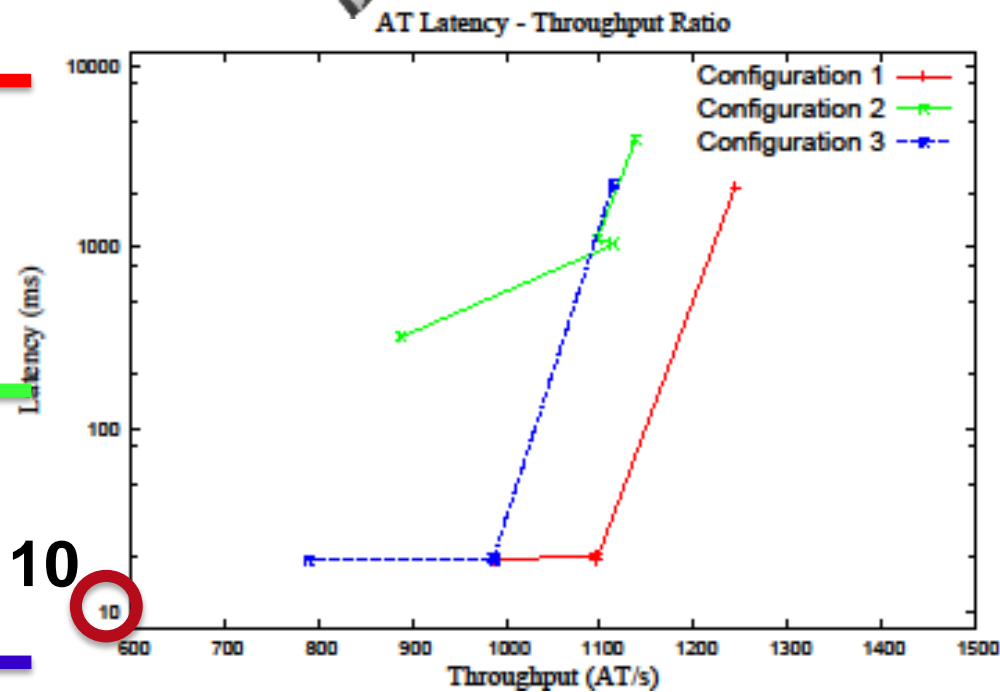
1



2



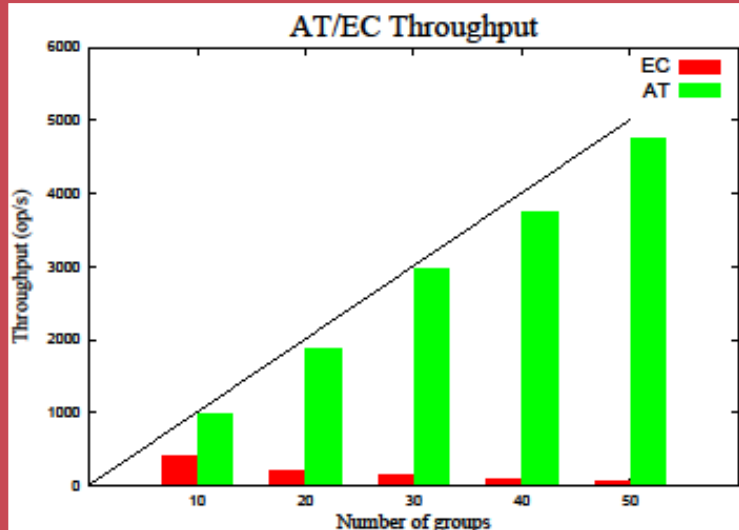
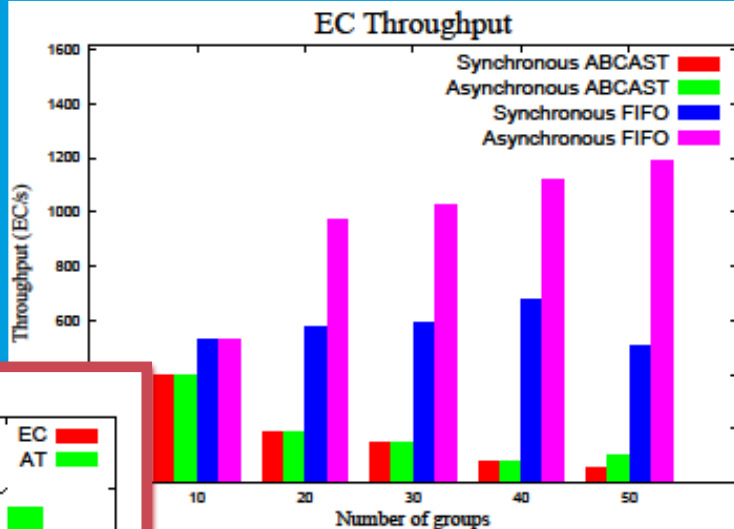
3



- **Centralized deployment doesn't scale and has saturation points**
- **Replication scales well for AT, for EC we need to relax the consistency to gain scalability**
- **Geo-replication gives better performance for AT, and for EC as long as we relax the consistency constraint**

AT / EC
Distributed

Geographic
Deployment



Enrollment Certificate
weak consistency

