

# C-ITS PKI

## The European trust approach

---

**Axel Sandot**

Digital ID

V2X & IoT Security Business Manager



# The EU C-ITS PKI Foundation of mobility digital trust

---



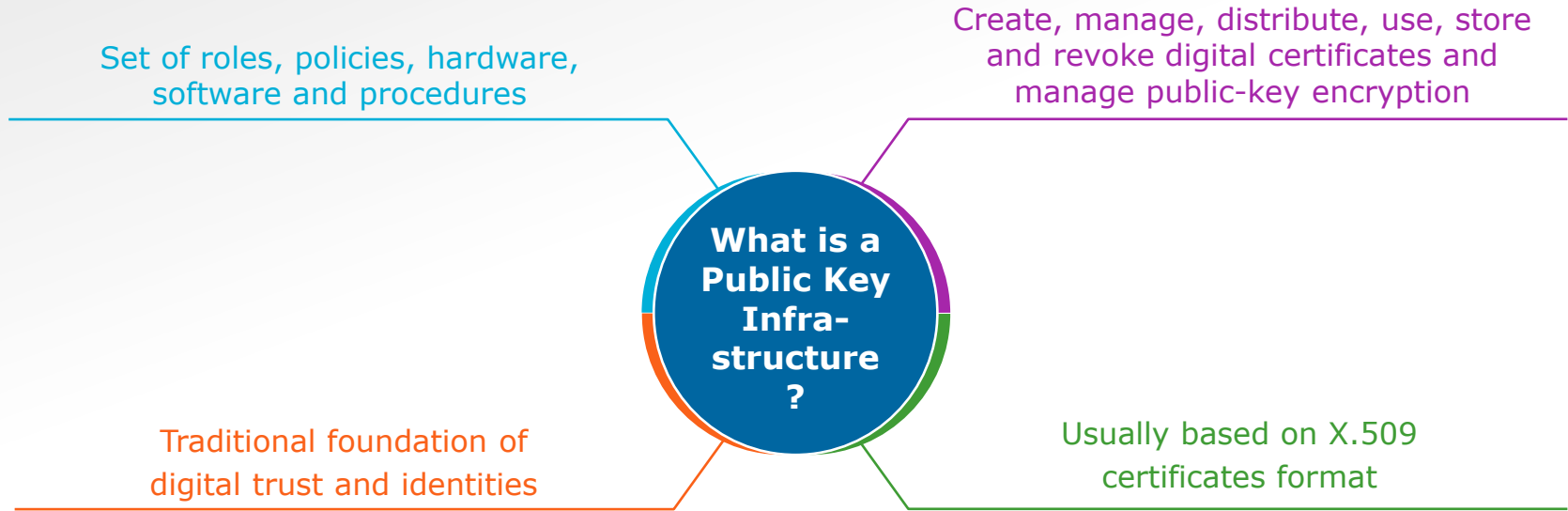
# Safety needs security

If I want to send and receive messages...



... How can I guarantee **TRUST**?

# Guaranteeing security and trust



# The specific nature of the C-ITS PKI

C-ITS messages must allow almost **instantaneous reactions** when facing **unexpected road events**

## Problematics

**X.509** certificates formats are **not adapted to C-ITS needs**:  
high computation power, long delays

A new kind of PKI is required:

**ETSI TS 103 097**

Security requirements + C-ITS certificates format

**ETSI TS 102 940/941**

Architecture + related information exchange protocol

## Solutions

The PKI is conceived as:  
**Foundation of security and trust**  
**Cornerstone of interoperability**

# Key-functions and parameters

---



# C-ITS PKI key functions

**ACCESS CONTROL**  
to C-ITS applications

**AUTHENTICATION & INTEGRITY**  
of V2X communications

**REVOCATION**  
of misbehaving entities


**PRIVACY**  
No user's tracking




# Why V2X communication?



**1 RCA**  
Root Certification Authority



**2 Sub-CAs**



Enrolment Authority (EA) – Authorization Authority (AA)



**Long term**

Enrolment Certificates (EC)

/

**Short term**



Authorization Tickets (AT)



**2 types of C-ITS stations**

On Board Units (OBU: 60-100 ATs/w) / Road Side Units (RSU: 1 AT/w)





# EU central security elements

---



# EU C-ITS central PKI

## Scope

### Different Needs = Different Models

#### Internal

- ▶ **Direct registration** of C-ITS stations in the internal C-ITS EU PKI

#### External

- ▶ Private **C-ITS Sub-CAs trusted** by the **EU Root CA**

### Different Purposes = Different Services

#### L0

- ▶ **Testing** and integration works, less mature pilot projects

#### L1

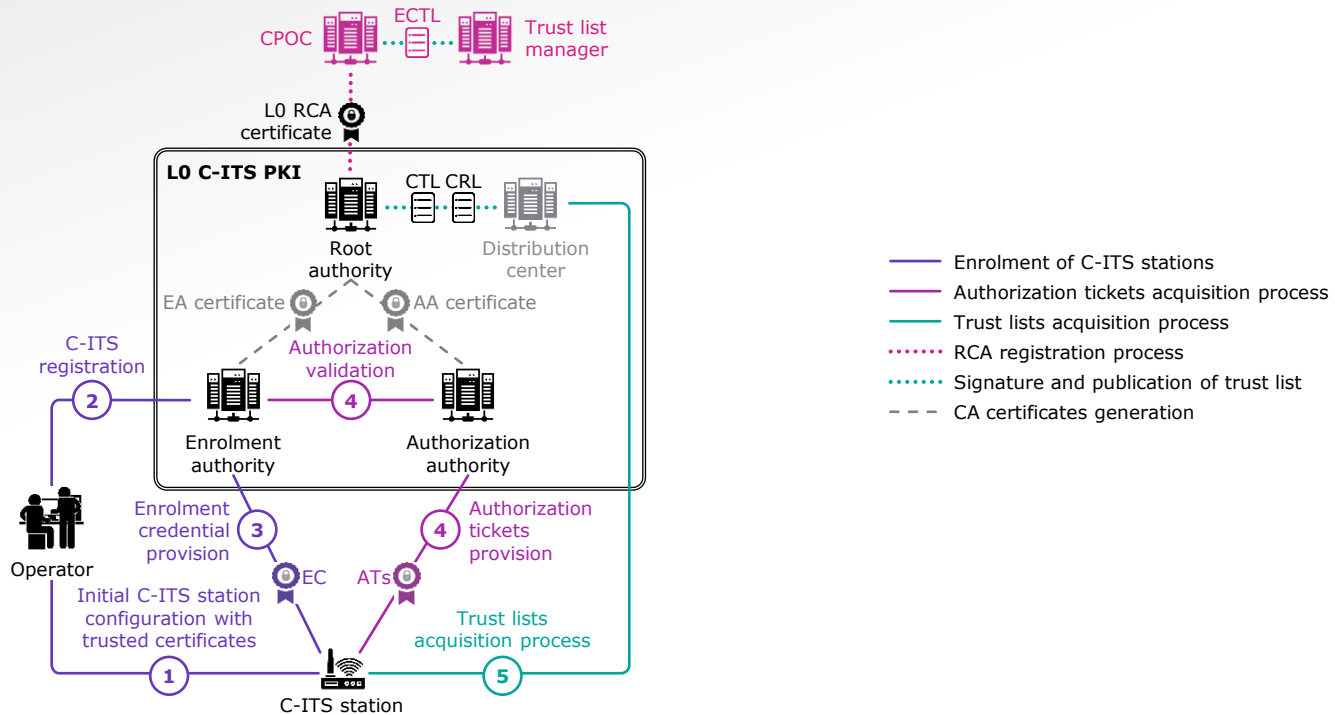
- ▶ **Stable pilot** operation, full-scale production **not CP certified**

#### L2

- ▶ Full-scale **EU CP certified** production

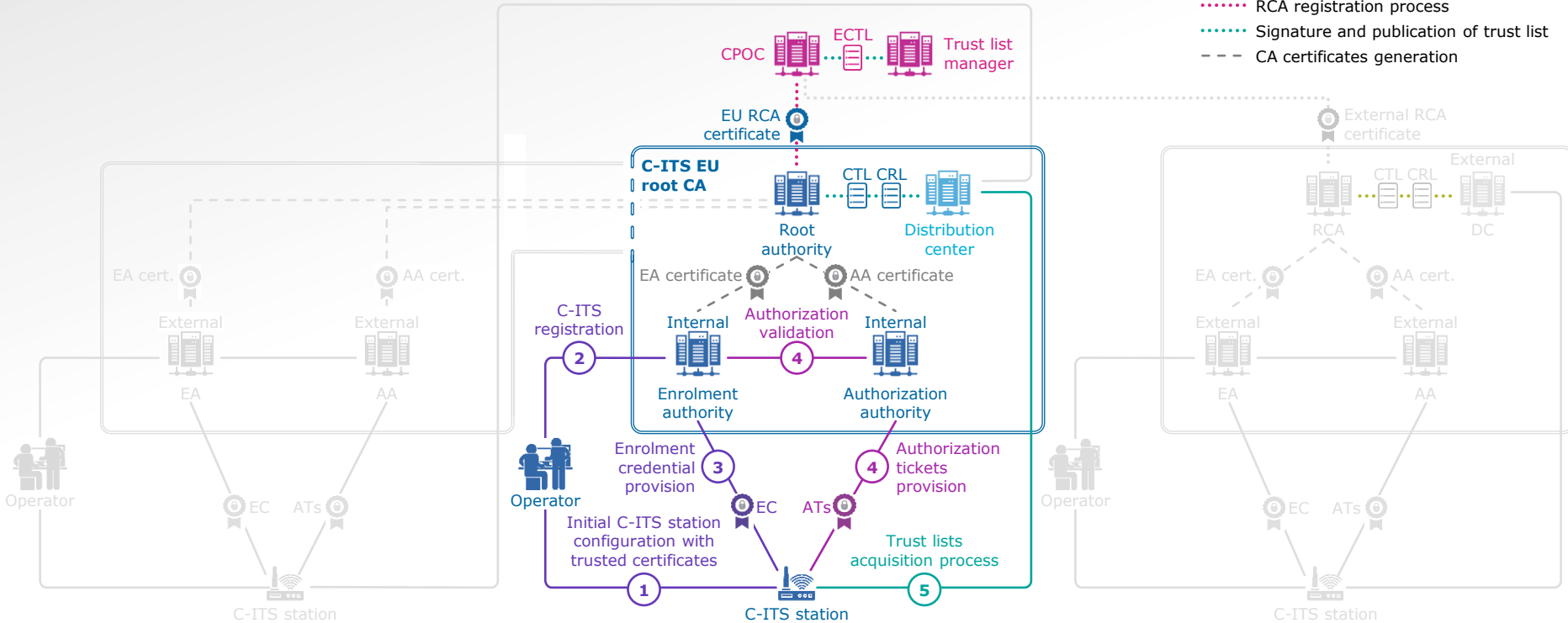
[IDnomic C-ITS PKI video](#)

# Shared C-ITS PKI for testing L0 service



# Shared C-ITS EU PKI – *Internal* L1 & L2 services

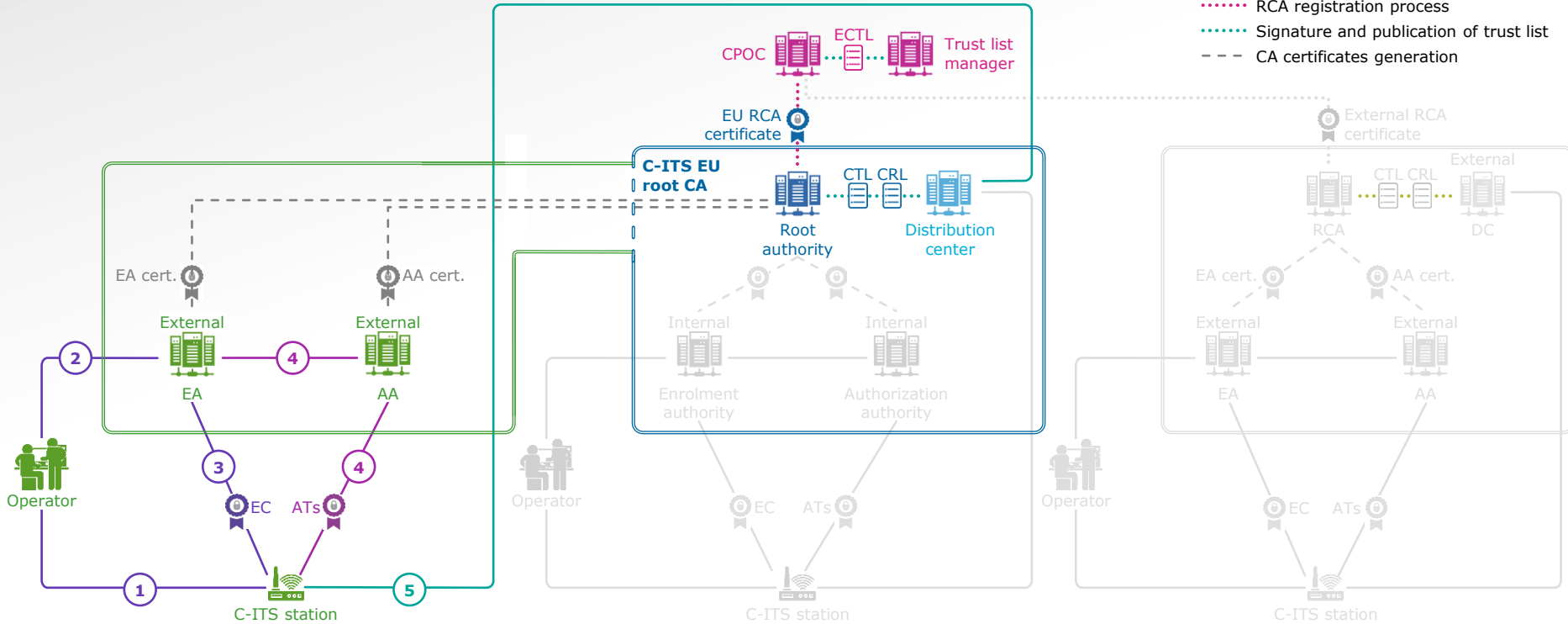
- Enrolment of C-ITS stations
- Authorization tickets acquisition process
- Trust lists acquisition process
- ⋯ RCA registration process
- ⋯ Signature and publication of trust list
- - - CA certificates generation



# Dedicated Sub-CAs with EU RCA – External

## L1 & L2 services

- Enrolment of C-ITS stations
- Authorization tickets acquisition process
- Trust lists acquisition process
- ..... RCA registration process
- ..... Signature and publication of trust list
- - - CA certificates generation



# Key-take Aways



## Europe as C-ITS leader

- ▶ World 1st continental certified C-ITS PKI



## EC guarantees trust and security availability

- ▶ Any stakeholder can request for central EU C-ITS digital certificates



## European institutions pull the ecosystem maturity

- ▶ L0 already praised by the ecosystem
- ▶ L1 & L2 technically ready and waiting for opening

# Thank you

For more information please contact:

---

**Axel Sandot**

Digital ID

V2X & IoT Security Business Manager

[axel.sandot@atos.net](mailto:axel.sandot@atos.net)

