IDnomic

C-ITS Public Key Infrastructure

The European trust approach

18-06-2020

Trusted partner for your **Digital Journey**

Atos

European context and C-ITS goals

1. European context and C-ITS goals

IDnomic

The European economy directly relies on the ability to

- Promote, implement and regulate innovative and sustainable means of transport
- Develop a modern infrastructure network
- Guarantee quicker, safer and free movement of people, services and goods

Transport, cornerstone of mobility

- Supervised by the European Commission
- Highly strategical
- One of the most sensitive

C-ITS goals

- Greener: reduce environmental impact
- Safer: reduce road accidents
- Smarter: make traffic more fluid

European C-ITS strategy

2. European C-ITS strategy

IDnomic

Innovation Challenge

- No side effects on other very sensitive aspects of the European sovereignty and regulation:
  - security & safety
  - privacy & data protection
- guaranty that the interoperability will be ensured across Europe despite a high diversity of stakeholders

Strategy

- Not (only) regulated by the business and free-market competition
- Standardisation: all solutions must follow technical and security standards requirements
- Regulation: national or supra-national institutions define regulations or guidelines

Means

- EU Certificate Policy
- EU Security Policy
- EU Central Elements:
  - EU TLM/CPOC
  - ECTL
  - EU Root CA & and Sub-CAs (PKI)

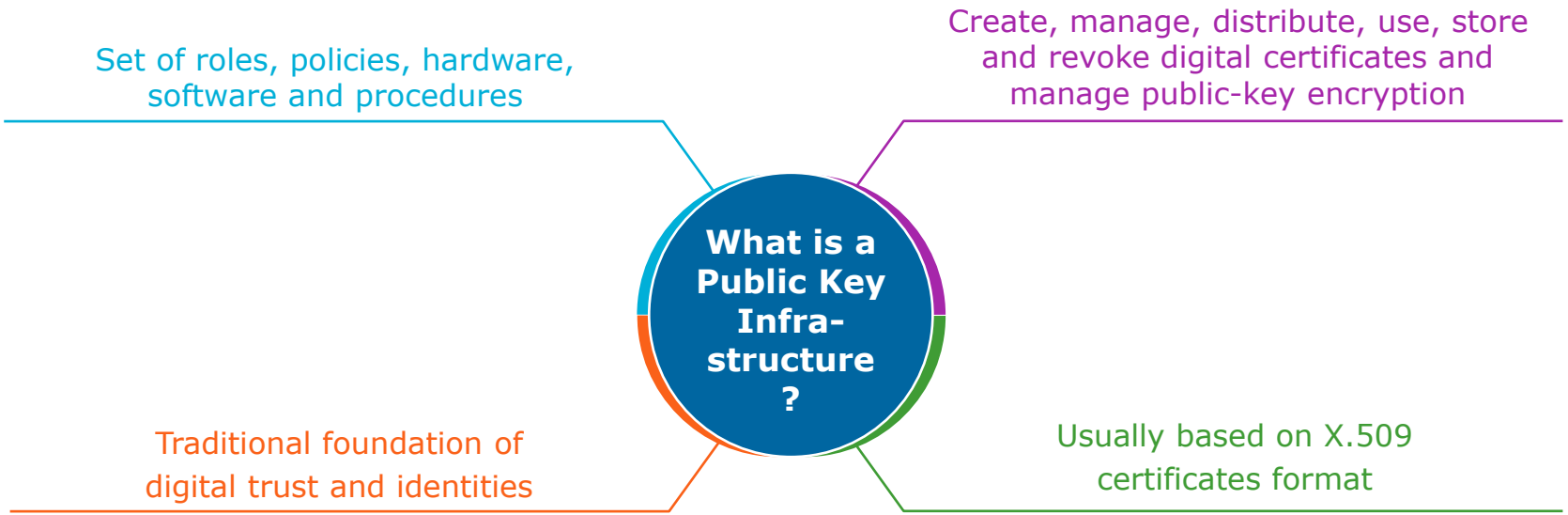
3

C-ITS PKI

Foundation of mobility digital trust

3. C-ITS PKI

Foundation of mobility digital trust



3. C-ITS PKI

Foundation of mobility digital trust

IDnomic

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 102 941
Architecture + related information exchange protocol

Solutions

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

Key-functions & parameters

4. Key-functions & parameters

IDnomic

4. Key-functions & parameters

IDnomic

1 RCA

Root Certification Authority

2 Sub-CAs

Enrolment Authority (EA) – Authorization Authority (AA)

Long term	/	**Short term**
Enrolment Certificates (EC)	/	Authorization Tickets (AT)

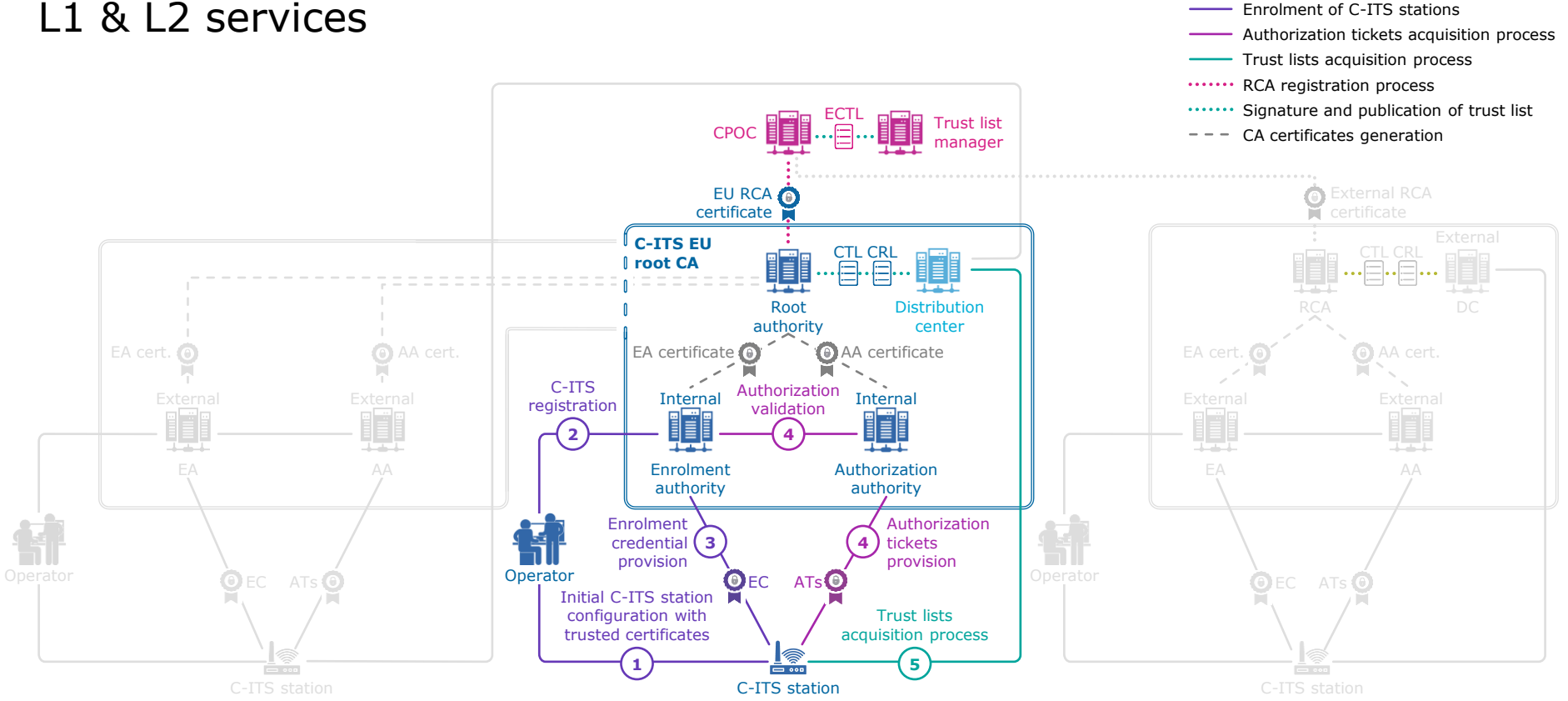
2 types of C-ITS stations

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

EU central security elements

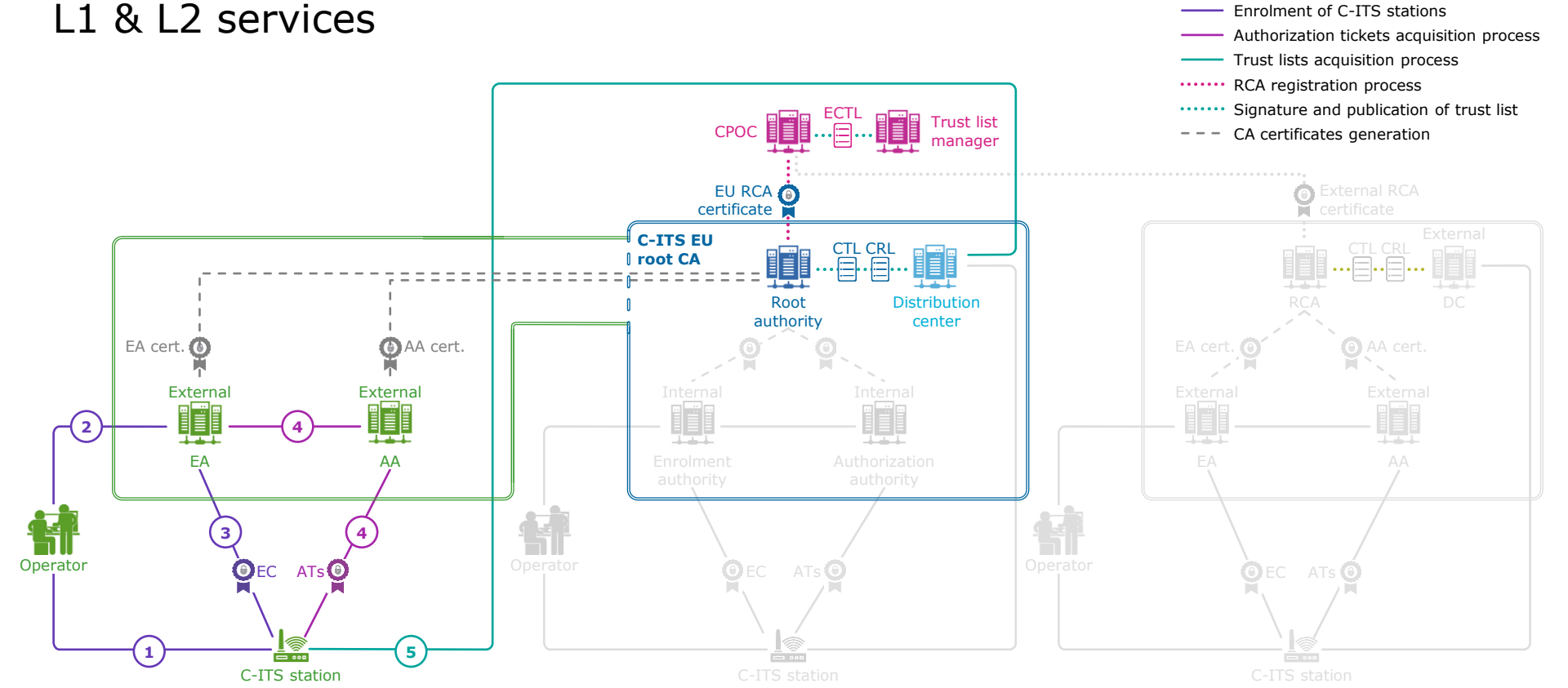
Shared C-ITS EU PKI – *Internal*

L1 & L2 services



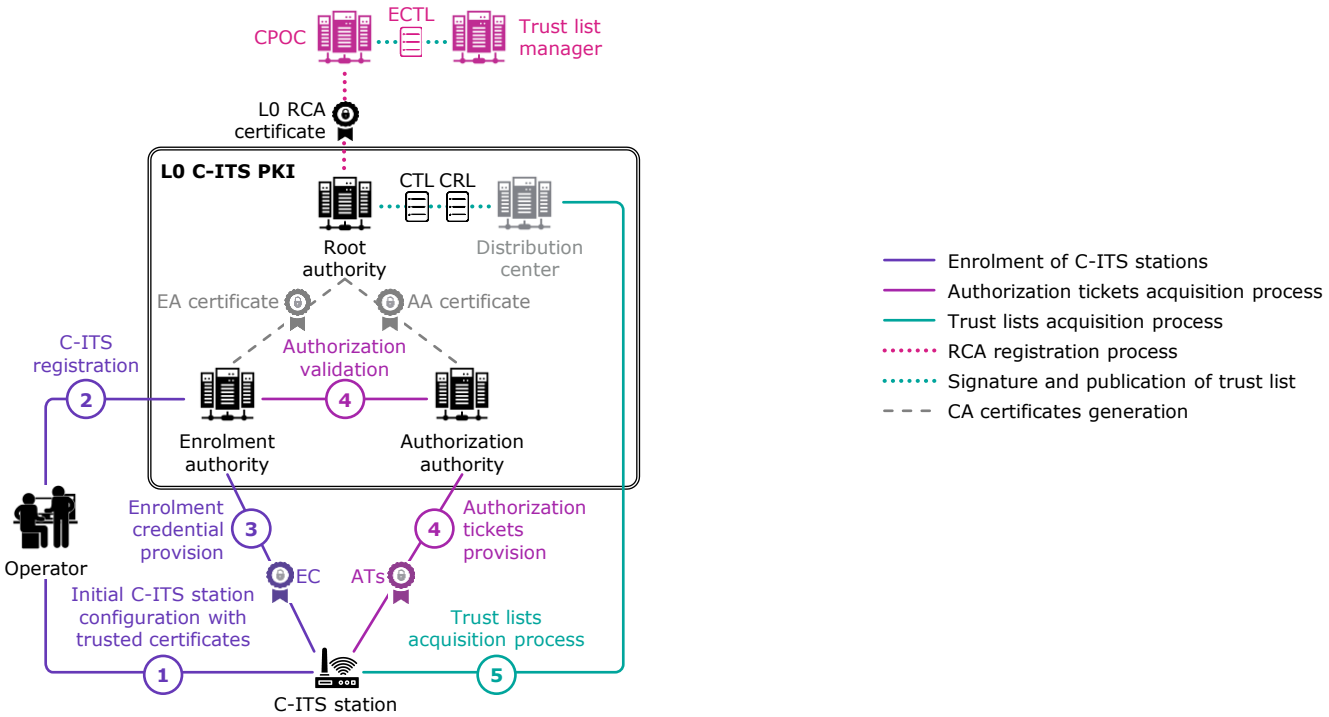
Dedicated PKI with EU RCA – *External*

L1 & L2 services



Shared C-ITS PKI for testing

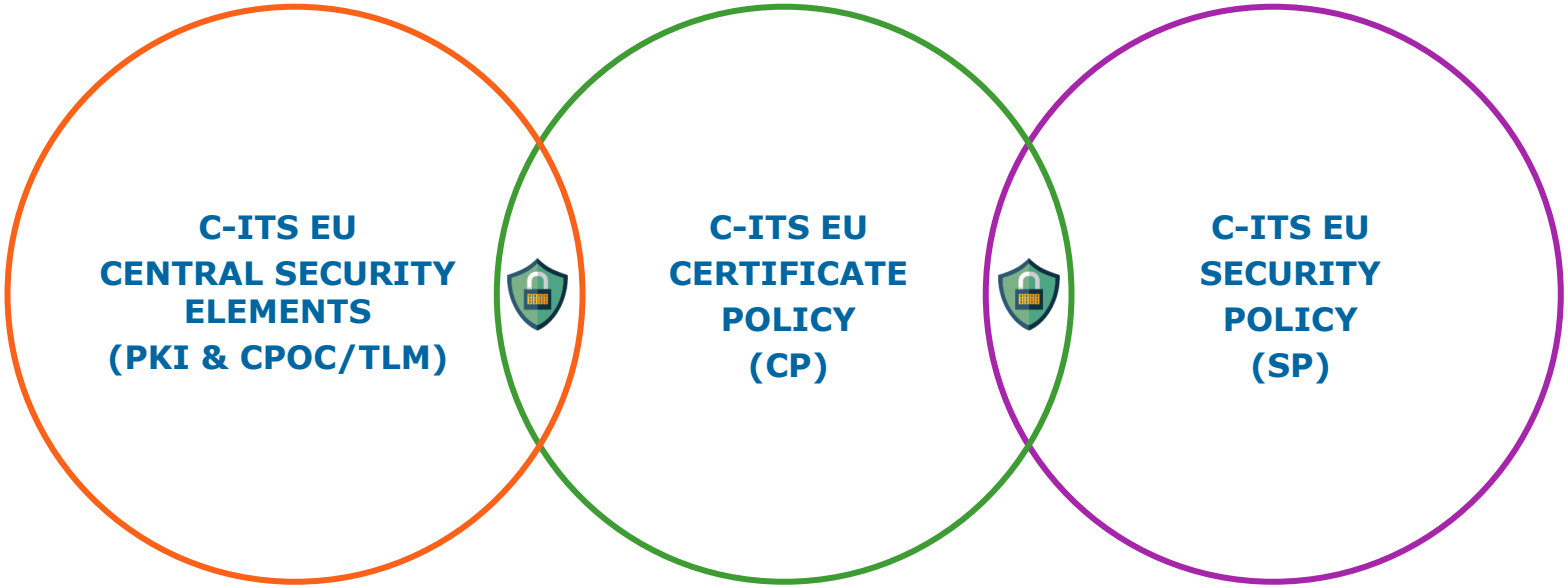
L0 service



Integral security

6. Integral security

IDnomic



IDnomic

Thank you

Contact

Axel Sandot
Big Data & Security - Digital ID
V2X & IoT Security Business Manager – IDnomic
M: +33 (0) 7 86 58 00 05
@: axel.sandot@atos.net

Atos