EVIDEN

Digital trust in complex ecosystems

The example of the European C-ITS services

Guillaume RICHARD
Security product line manager
19/09/2023

an atos business

Evolution of traditional corporate cybersecurity

Because it's all about communication

Perimetral security

Clear frontiers with clearly identified and separated assets

Need for digital IDs

Interlinked assets with constant need for communication

Zero Trust

No frontiers anymore, multiplication of interconnexions, management of data based on roles and privileges

But what if we have to manage this level of complexity?

Could we ensure a global, secure and native interoperability?

What do we mean by “global, secure and native interoperability”?

The example of the EU C-ITS ecosystem

BEING ABLE TO DELIVER AUTOMATED SERVICES — V2X/C-ITS services

IN A COMPLEX ECOSYSTEM — Road traffic

BETWEEN STAKEHOLDERS THAT DO NOT KNOW EACH OTHER — Cars, traffic lights, bicycles, blue light vehicles, trains, etc.

Which requires:

A COMMON SET OF TECHNICAL AND SECURITY FRAMEWORKS — ETSI Standardization

A LEGAL FRAMEWORK — EU Regulation

A COMMON SET OF WAYS TO HANDLE THE USE CASES — C-Roads/C2C Harmonization

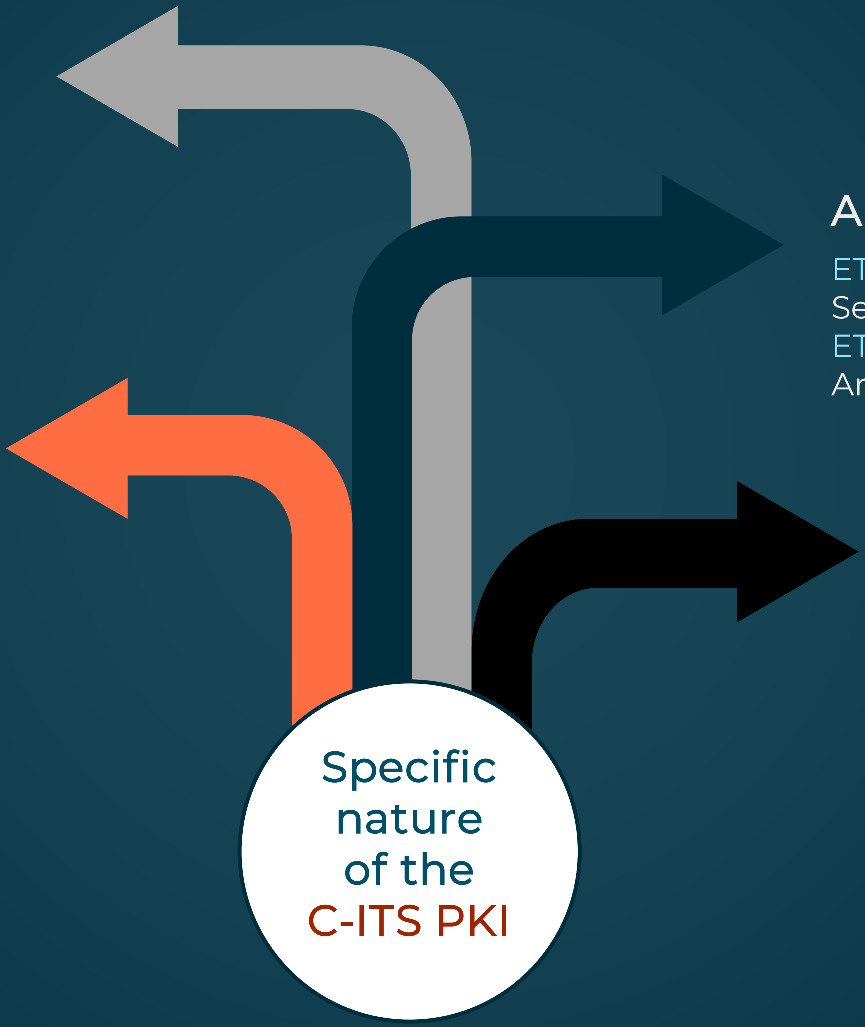
How to guarantee TRUST?

PKI is needed but

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

Specific constraints

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



Specific nature of the C-ITS PKI

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

A PKI conceived as

Foundation of security and trust
Cornerstone of interoperability

C-ITS PKI key functions

ACCESS CONTROL
to C-ITS applications

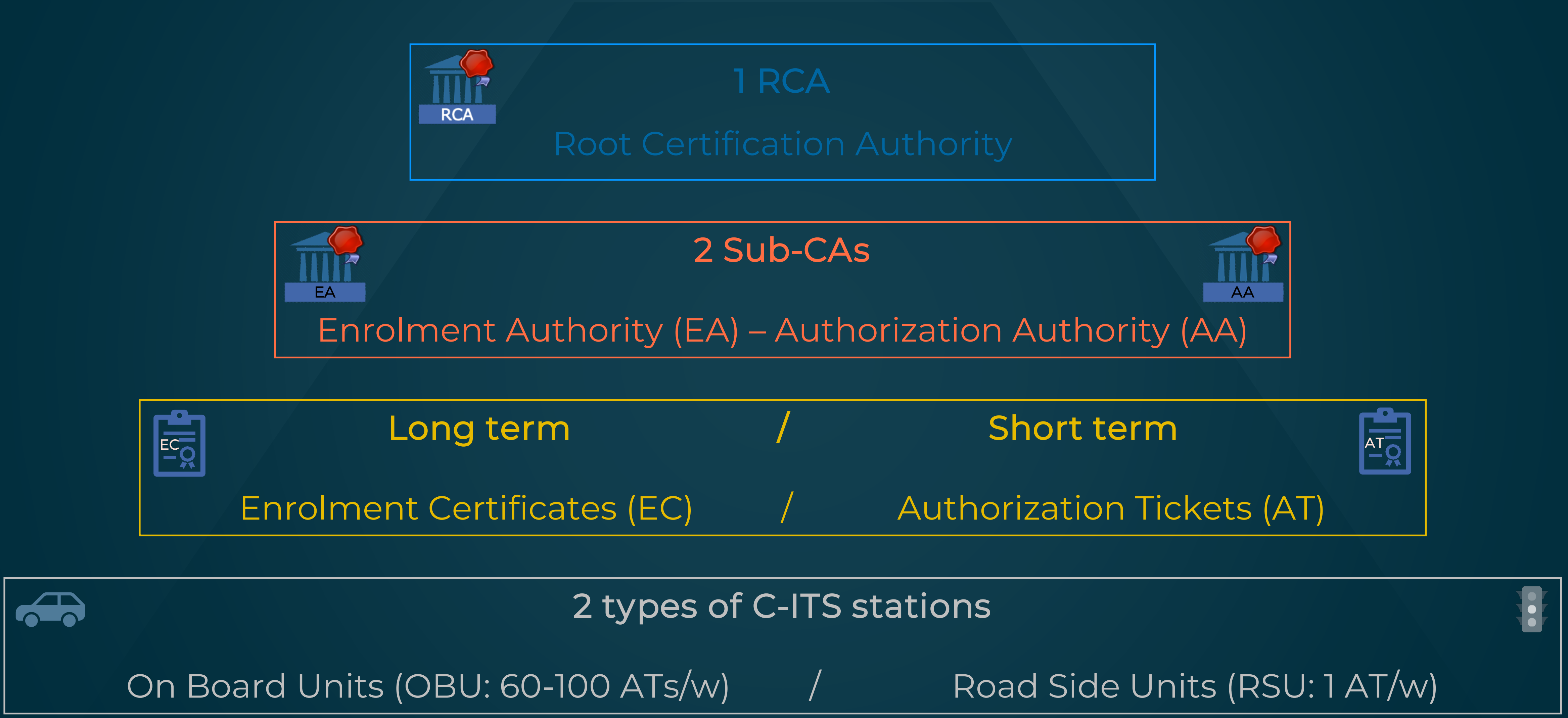
AUTHENTICATION & INTEGRITY of
V2X communications

REVOCATION
of misbehaving entities

PRIVACY
No user’s tracking

Complex ecosystems require **interoperability** & **security**
The **PKI** is the cornerstone of **mutual trust**

C-ITS PKI architecture



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)

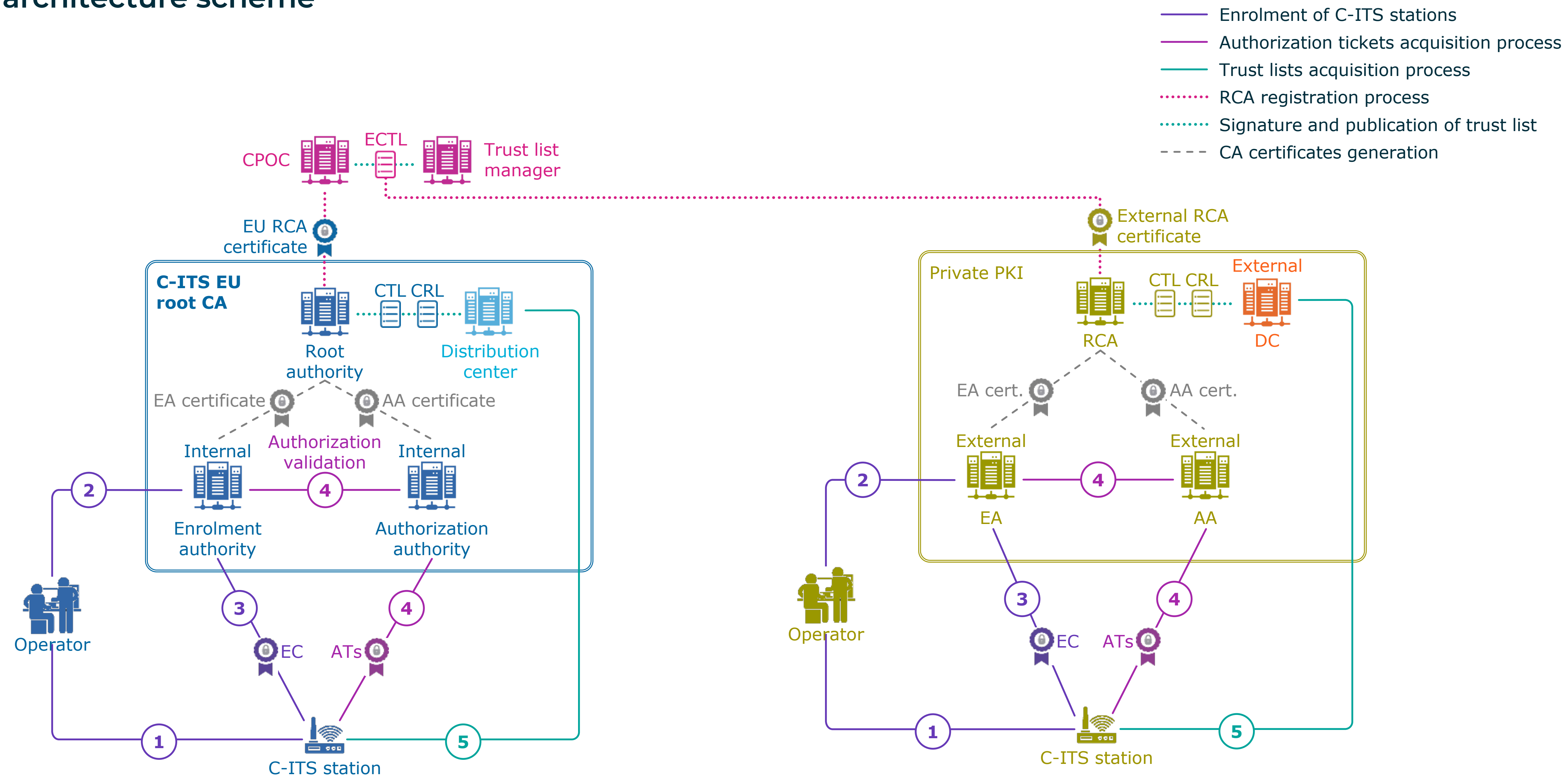
The EU global approach

Security and trust are then ensured at technical level but new questions and challenges arise:

- Is there only one or several PKIs?
- If there are several PKIs, how to enable extension of trust?
- Is a native interoperability possible for the whole EU?
- Can an appropriate level of security be guaranteed by the market?
- Who does what and how?

What do we want to achieve in such a complex ecosystem?

Global architecture scheme



EVIDEN

Thank you!

For more info please contact Axel SANDOT (axel.sandot@eviden.com)

EU Central Security Elements

CPOC
C-ITS Point Of Contact

Hosted and
operated by the
European Commission

Central interface for the
ecosystem

Publication of all EU C-ITS
relevant docs
& objects

TLM
Trust List Manager

Hosted and
operated by the
European Commission

Management of:
TLM certificates
ECTLs (European
Certificate Trust Lists)

EU Root CA
Central C-ITS PKI

Developed and
operated by Eviden
on behalf of the
European Commission

Fully funded by the EC,
in charge of delivering
certificates to all
authorized stations

Main EU C-ITS reference documents

CPOC Protocol

Establishes requirements and rules to request RCA registration in an ECTL

Certificate Policy

Defines the compliance framework applicable to the C-ITS PKI deployment and operation (based on ISO 2700x)

Security Policy

Defines the compliance framework applicable to the C-ITS stations at hardware and software level

EU ecosystem organization

Expert Group
Editing Team

Member states
representatives
+
All involved C-ITS experts

Make evolve and
guarantee coherency of
reference document
(CP, SP, CPOC protocol)

Initiative of
EU Member States
and road operators
for testing C-ITS services
and harmonizing
infrastructure
use cases

C-Roads Platform
Road operators

Car2Car CC
Automotive industry

Organization of
automotive industry
stakeholders that aims
to achieve
accident-free traffic.

Fosters deployments,
specifications and
harmonization of
automotive use cases