European Commission

Atos

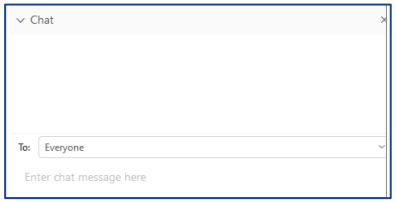
Welcome!

C-ITS EU Root CA Webinar

Practicalities:

- Please mute your microphone!

- Please use the chat function for any question during the webinar. We will answer them at the end of the presentation.



- This presentation will be made available after the webinar

European Commission

Atos

Webinar Outline

1. EC introduction on EU central elements of C-ITS security
   C-ITS Point of Contact, Trust List Manager and EU Root CA

2. Atos presentation on C-ITS EU Root CA
   Main project phases, architecture and services description, conditions of service, integration in the EU C-ITS ecosystem

3. Questions (CHAT!) & Answers

EU Root CA

- Open Tender procedure JRC/IPR/2019/OP/0365
  - Date of publication: 19/04/2019
  - Date of contract signature: 09/12/2019
  - Successful tenderer: Keynectis S.A. (Atos)

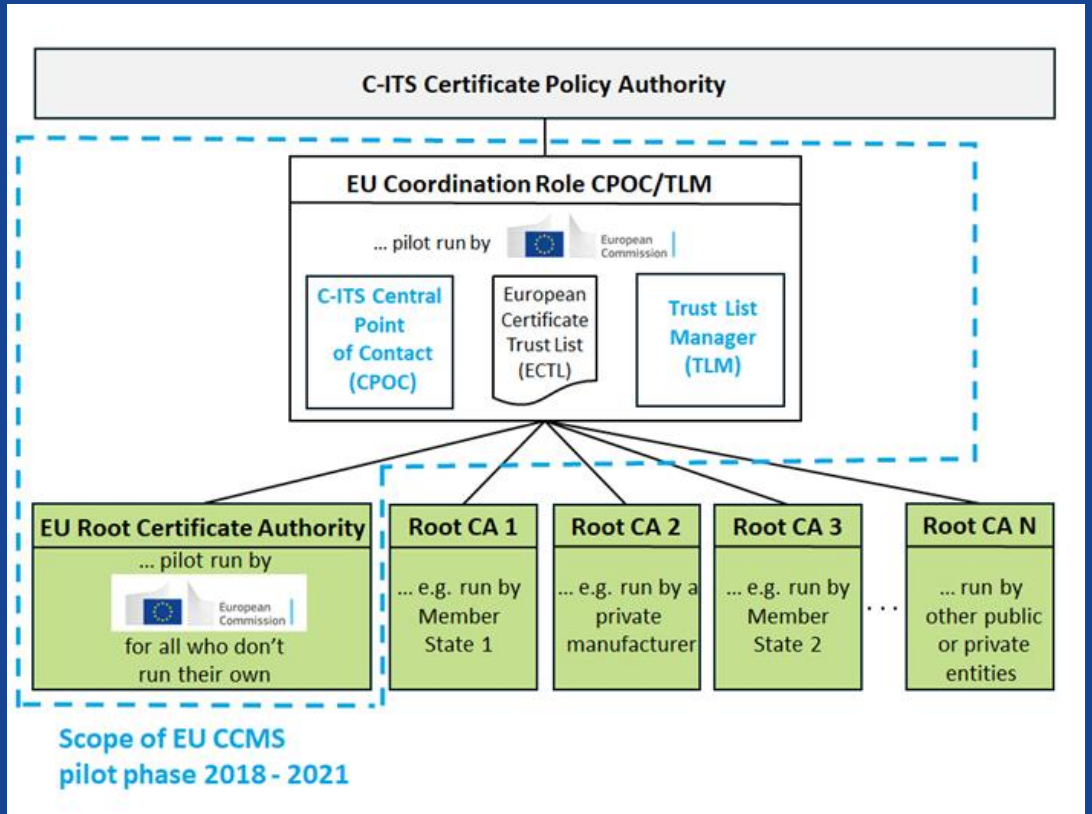
- Project scope
  - Phase I - until end of 2022, fully-funded by the European Commission
  - No charge for end-users
  - Optional Phase II 4x1 year until end of 2026

Open Tender procedure was performed in 2019

All information regarding tenders of the European Commission is published in the Official Journal of the European Union (OJEU)

https://ted.europa.eu/

EU CCMS – Scope of activities



C-ITS Point of Contact (CPOC)

- **CPOC is fully hosted by the European Commission**
  - CPOC Entry
  - CPOC Website https://cpoc.jrc.ec.europa.eu/
  - E-mail: JRC-CPOC@ec.europa.eu
  - Note: CPOC WEB currently under revision – M2M interface currently in implementation, based an CPOC protocol definitions

- **C-ITS Point of Contact (CPOC) Protocol**
  - Definition of a secure protocol for exchange of root CA certificates between Root CAs and the CPOC, first release January 2019

  <u>Currently under revision</u>

  - New Annex I with necessary technical updates of ETSI Standards following findings of 2019 plugtests
  - Significant amount of clarifications and implementation relevant requirements & recommendations

  → A lot of work done together with expert volunteers – will now also become topic of **the new sub-group!***

CPOC Website launched since end of November 2019!

For more info on the subgroup on C-ITS of the Commission Expert Group on Intelligent Transport Systems: https://ec.europa.eu/transport/themes/its/news/2020-04-27-cits_en

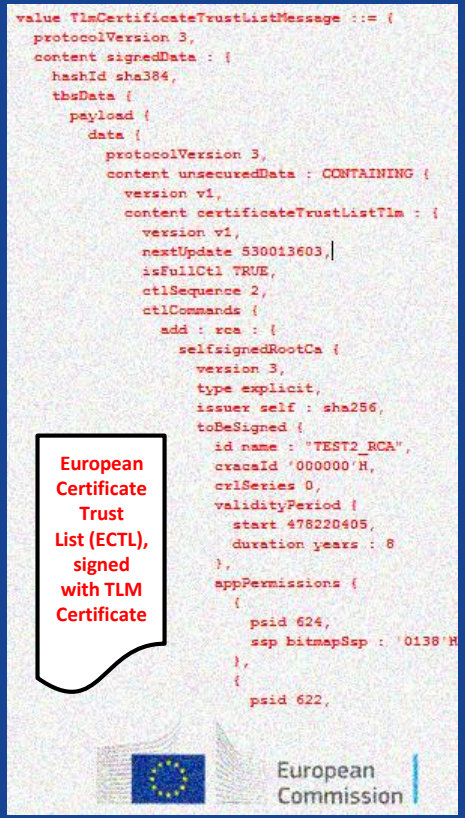
Trust List Manager (TLM)

- TLM is fully hosted by the European Commission and is implemented on Commission premises in ISPRA, Italy
- TLM functionalities have already been supplied at the ETSI plug-tests in 2019

Most frequently asked question these days:

- "When is the ECTL available and how do I get on it?"

→ The European Commission aims to offer support for European C-ITS deployment with **<u>3 different Levels of TLM Services</u>**



TLM – Level 0

EU CCMS: TLM Services

- **TLM LEVEL 0 Service (L0)**
  - **LEVEL 0 TLM CERTIFICATE**
  - **LEVEL 0 ECTL**
- **TLM LEVEL 1 Service (L1)**
  - **LEVEL 1 TLM CERTIFICATE**
  - **LEVEL 1 ECTL**
- **TLM LEVEL 2 Service (L2)**
  - **LEVEL 2 TLM CERTIFICATE**
  - **LEVEL 2 ECTL**

- TLM L0:
  - Offered on the basis of requests for interoperability testing sessions (e.g. C-Roads interoperability test sessions, etc.)
- No CP audit is needed.
- Time Plan:
  - L0 is implemented, available and has already been provided for two ETSI plug-tests in 2019
  - L0 TLM/ECTL scope needs to be agreed by testing stakeholders and EC on a case by case basis
  - next publication soon and including EU RCA L0

Results of the last plug-test are currently published on:
https://cpoc.jrc.ec.europa.eu/

TLM – Level 1

EU CCMS: TLM Services

- **TLM LEVEL 0 Service (L0)**
  - **LEVEL 0 TLM CERTIFICATE**
  - **LEVEL 0 ECTL**
- **TLM LEVEL 1 Service (L1)**
  - **LEVEL 1 TLM CERTIFICATE**
  - **LEVEL 1 ECTL**
- **TLM LEVEL 2 Service (L2)**
  - **LEVEL 2 TLM CERTIFICATE**
  - **LEVEL 2 ECTL**

- Longer operation intervals, longer validities of certificates, **but limited in time, as deployments shall move to L2.**
- No CP audit needed but requirements and processes very close to full compliance and audit against the CP (limited exceptions and operation scope clearly defined by the CPA)
- For RCAs and C-ITS stations that meet CPA requirements and start to operate C-ITS Day 1 services in regular and well defined operation periods
- Time Plan: depends on the stakeholders (CPA) that want to make use of the TLM LEVEL 1 service --> key role for new sub group
- TLM ready to support signing of L1 ECTL (including L1 EU root CA) as of June 2020 with TLM software version of last plugtest

TLM – Level 2

EU CCMS: TLM Services

- **TLM LEVEL 0 Service (L0)**
  - **LEVEL 0 TLM CERTIFICATE**
  - **LEVEL 0 ECTL**
- **TLM LEVEL 1 Service (L1)**
  - **LEVEL 1 TLM CERTIFICATE**
  - **LEVEL 1 ECTL**
- **TLM LEVEL 2 Service (L2)**
  - **LEVEL 2 TLM CERTIFICATE**
  - **LEVEL 2 ECTL**

- L2 is enabled by the CPA and operates according to the CP with no exceptions
- Hence, full audits are required
- Time Plan: Since the EU Root CA will be fully audited by the end of 2020, the TLM intends to provide such LEVEL 2 ECTL by the end of 2020, including (at least) the EU root CA on this LEVEL 2 ECTL. Details are subject to discussion in the CPA.

More Information

Cooperative, connected and automated mobility:
https://ec.europa.eu/transport/themes/its/c-its_en

CPOC Website:
https://cpoc.jrc.ec.europa.eu

Thank you for your attention!

Gerhard Menzel

European Commission - DG JRC
E.3: Cyber & Digital Citizens' Security

JRC-C-ITS-EU-RCA@ec.europa.eu
JRC-CPOC@ec.europa.eu

IDnomic

EU Root CA & Sub-CAs

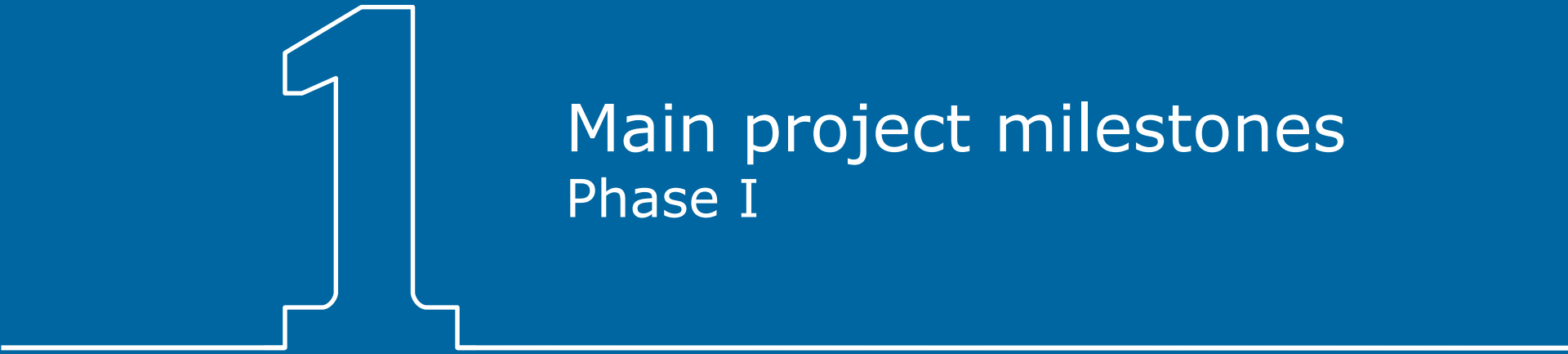
Foundation of mobility digital trust

18-06-2020

Trusted partner for your **Digital Journey**

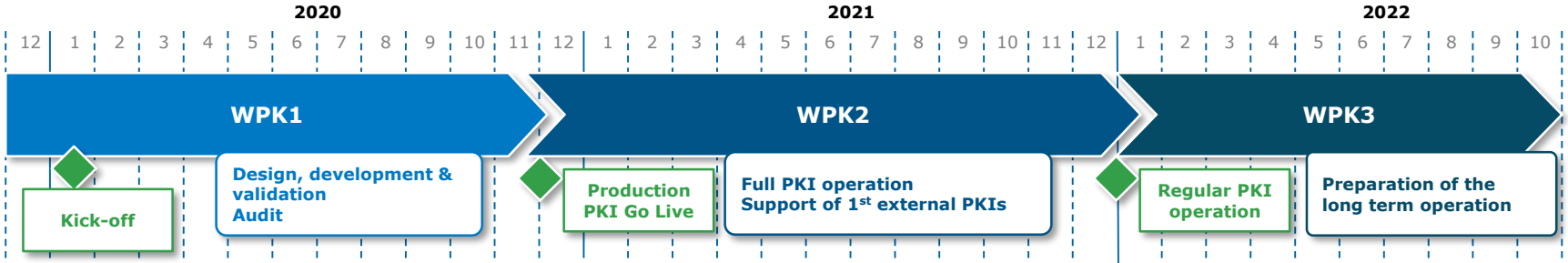
European Commission

Atos



Main project milestones
Phase I

1. Main project milestones
Phase I



- WPK1 : 12 Months
- WPK2 : 13 Months
- WPK3 : 10 Months
- Phase 1 runs until end of October 2022

2

Architecture schemes and services

2. Architecture schemes and services

IDnomic

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

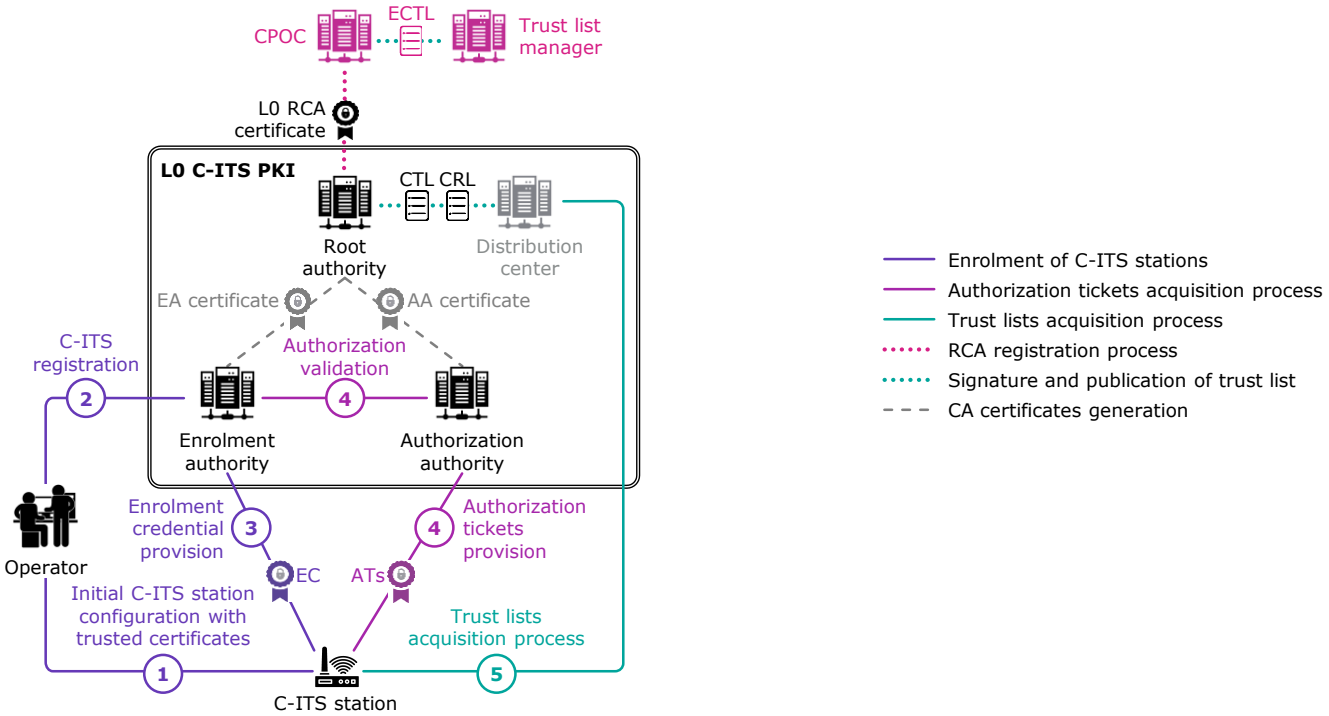
- **L0**: testing and integration works, less mature pilot projects
- **L1**: stable pilot operation, full-scale production not CP certified
- **L2**: full-scale CP certified production

Phase I capacity

- Stations: 150.000 units
- External Sub-CAs: 11 EA+AA

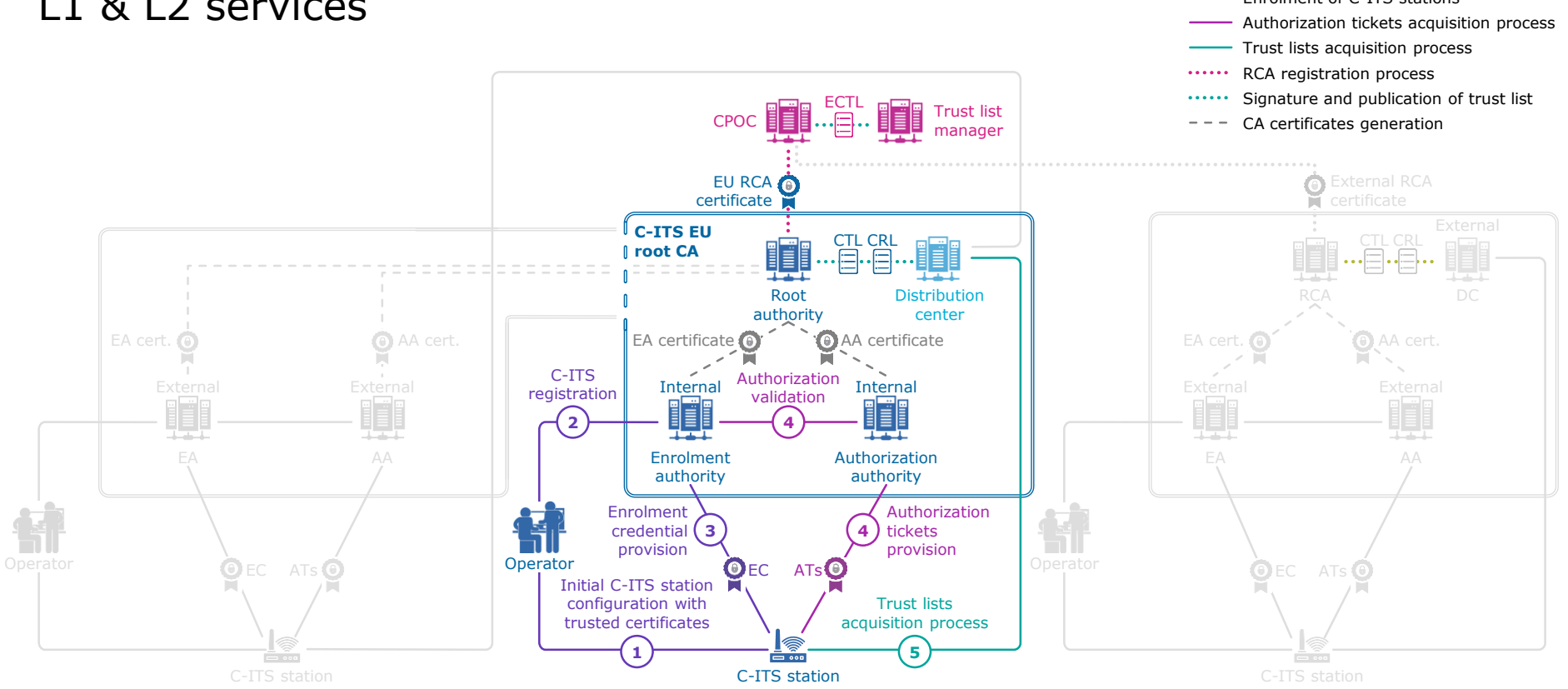
Shared C-ITS PKI for testing

L0 service



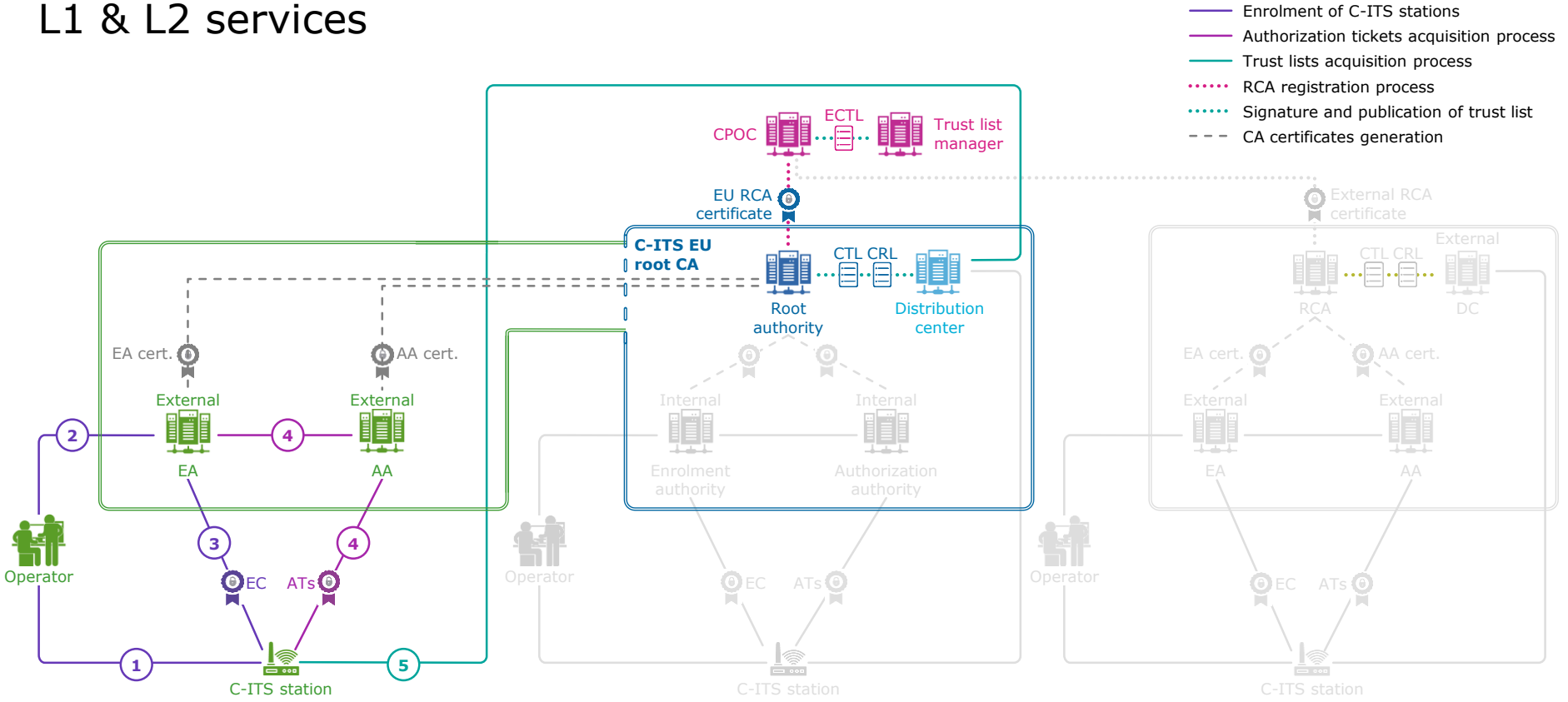
Shared C-ITS EU PKI – *Internal*

L1 & L2 services



Dedicated PKI with EU RCA – *External*

L1 & L2 services



Available service conditions

3. Available service conditions

IDnomic

L0

- **Access conditions:** correct use and guaranty of station's behavior similar to real operation
- **Availability**: best effort

L1

- **Access conditions:** stable operation in conditions as close to real-scale production as possible
- **Availability**: internal goal at 99,5%

Deployed means to reach this goal:

- L1 platform is a copy of L2 platform
- Cloud platform: 99,99% of availability guaranty
- Redundancy: systematic redundancy (hardware and software) spread over 2 physical distant sites
- Monitoring: deployment of monitoring processes to maintain a fine control of the service activity

SLA: PKI service vs. C-ITS service

- Availability of the PKI service is not the same as availability of the C-ITS services themselves
  - The certificate management protocol is built to preserve the C-ITS services continuity

Integration with the C-ITS EU Central Elements

4. Integration with the C-ITS EU Central Elements

IDnomic

L0	L1	L2
L0 EU Root CA **AVAILABLE**	L1 EU Root CA **AVAILABLE**	L2 EU Root CA **END OF 2020**
L0 EU RCA in L0 ECTL **ABOUT TO BE INCLUDED**	L1 EU RCA in L1 ECTL **READY TO BE INCLUDED**	L2 EU RCA in L2 ECTL **TO BE INCLUDED**

Registration process

5. Registration process
Step 1

1. E-mail request submission

✉ Point of contact: registration@c-its-eu-rca.eu
+ Copy: jrc-c-its-eu-rca@ec.europa.eu

✉ Subject:
- ✓ "EU RCA L*[0,1]* service registration – [*Organization name*]"

Example: EU RCA L1 service registration - Atos

✉ Content description:
- ✓ project needs (*internal developments, name and type of project, etc.*)
- ✓ expected duration
- ✓ quantities of OBUs and RSUs

5. Registration process
Step 2

2. E-mail documents submission

✉ Point of contact: registration@c-its-eu-rca.eu
+ Copy: jrc-c-its-eu-rca@ec.europa.eu

✉ Agreement:
- ✓ Filled out and signed "C-ITS EU ROOT CA & SUB-CAs SAAS AGREEMENT"
- ✓ Legal registration proof of your organization

5. Registration process
Step 3

3. Service access

- ✉ Confirmation e-mail of authorization to use the service
- ✉ Follow instructions
- ✉ Use and send Atos template file with the information of the stations to be enrolled

5. Registration process
Stations enrollment

	Name	Max EC validity period	Max AT validity period	Max AT preloading period	Validation request requires privacy	Allowed permissions
Attribute format	*ASCII*	*Integer:Unit*	*Integer:Unit*	*Integer:Unit*	*Optional, True, or False*	*PSID:SSP ; PSID:SSP ; PSID:SSP ; …*
Default profile	Default Profile	3:Years	7:Days	30:Days	Optional	36 : 010000 ; 36 : 01E500 ; 36 : 01FFFC ; 37 : 01000000 ; 37 : 01FFFFFF ; 137 : 01E0 ; 138 : 01C0 ; 139 : 01744000FFF8 ; 140 : 01FFFFE0 ; 141 ; 623 : 01C0
Profile01						
Profile02						
Profile03						
…						

	Canonical name	Public key	Attached profile name	Station status	*Tags (optional)*
Attribute format	*ASCII (possible in HEX also)*	*RFC 5480*	*ASCII*	*Status*	*ASCII*
Example	Company_MyStation0001	3059 3013 0607 2A86 48CE 3D02 0106 082A 8648 CE3D 0301 0703 4200 0462 83FD 5D98 9904 8B76 E3E7 AABC 05C4 0A45 46C1 30C6 56F6 BDD3 97D1 1125 4114 EB01 0631 9254 9D45 67D7 1EF2 3C56 F596 2064 0867 CB88 868C 986C 227D E721 2BAA BD	Default Profile	Activated	*EmailOfOperator1 Compagny_name1 Operator1 Station_usage1*
Station01					
Station02					
Station03					
…					

Questions & answers

6. Questions and answers

We will try to answer to all questions!

If we do not manage to answer your question(s) during the webinar, we will gladly do it after.

For this, please send us an e-mail to the right points of contacts.

POINTS OF CONTACT

General information

- ✉ EC JRC: gerhard.menzel@ec.europa.eu
- ✉ Atos: axel.sandot@atos.net

EU RCA services access

- ✉ EC JRC: jrc-c-its-eu-rca@ec.europa.eu
- ✉ Atos: registration@c-its-eu-rca.eu

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

FURTHER BACKGROUND INFORMATION

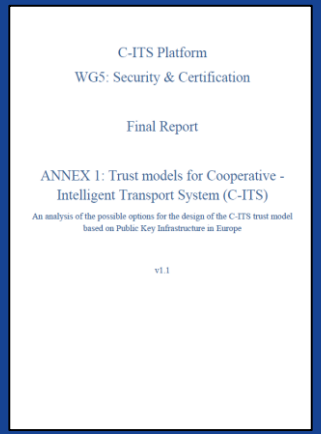
EU Policy on C-ITS Security

- COM (2016) 766 - A European strategy on C-ITS, a milestone towards cooperative, connected and automated mobility
- **May 2018:** COM(2018) 283 final - On the road to automated mobility: An EU strategy for mobility of the future
  - Commission will **"implement a pilot on common EU-wide cybersecurity infrastructures and processes needed for secure and trustful communication between vehicles and infrastructure for road safety and traffic management related messages according to the published guidance on the certificate and security policy"**

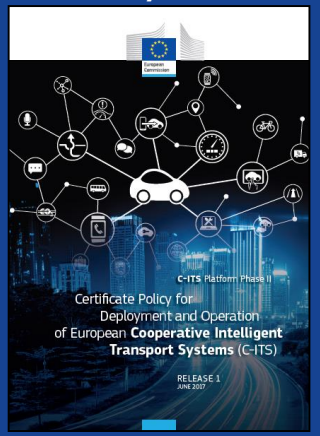
EU Policy on C-ITS Security

.... from guidance & testing ....

2014 -

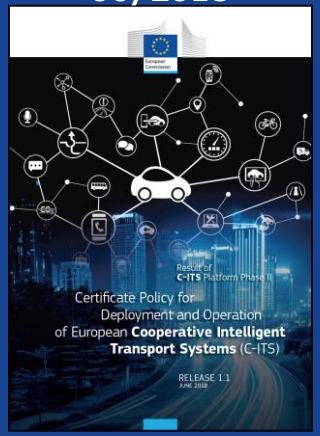


06/2017



12/2017

06/2018



(all outdated versions)

EU Policy on C-ITS Security

…. to implementation ….

All C-ITS security activities of the Commission are based on the CP and SP of the preparatory phase of the C-ITS Delegated Regulation[1]:

Certificate Policy (CP): Annex 3

EUROPEAN COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

ANNEX 3

ANNEX

to the

Commission Delegated Regulation

supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

Security Policy (SP): Annex 4

EUROPEAN COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

ANNEX 4

ANNEX

to the

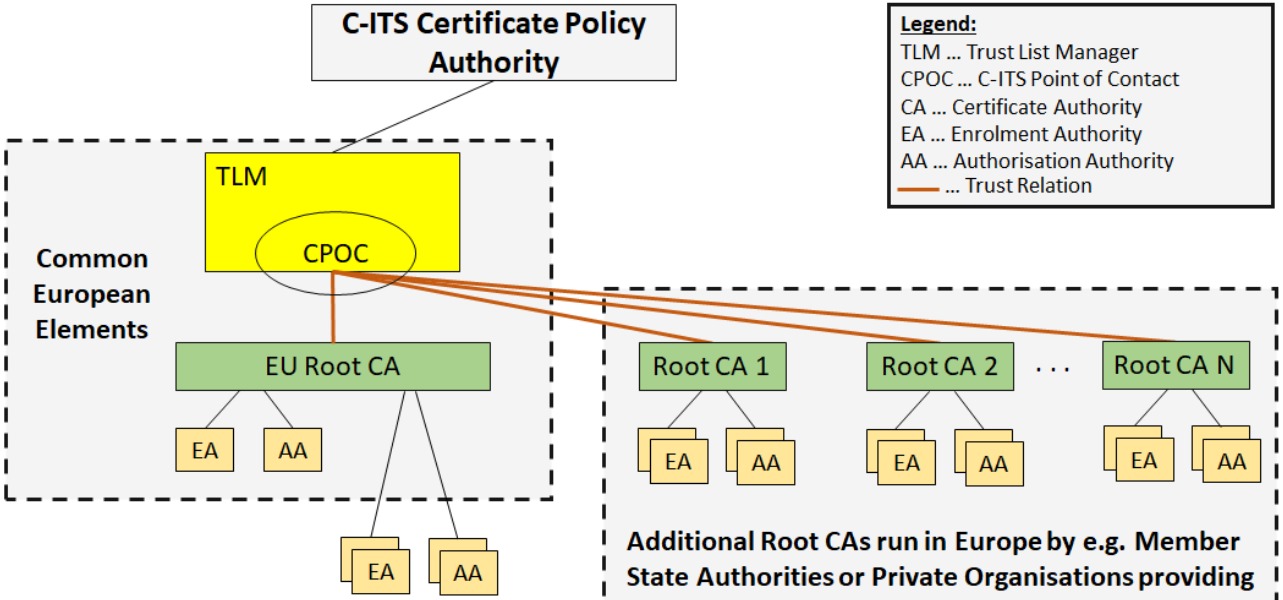
Commission Delegated Regulation

supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

1: Regulation adopted by the Commission that did not enter into force – the contents of Annex 3 (CP) and 4 (SP) are however still the basis for the EU CCMS activities of the Commission for C-ITS deployment support:
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552572526215&uri=PI_COM:C(2019)1789

EU Trust Model according to Certificate Policy



IDnomic

European Commission

EU Root CA

Level 0 registration guide

v1.06

Trusted partner for your **Digital Journey**

Atos

Context

1. The C-ITS EU Root CA is funded by the European Commission

2. The different services provided to the C-ITS ecosystem are deployed and operated by Atos on behalf of the European Commission

3. The different EU Root CA services are provided against no charge

Registration process steps

1. Send your request to use the **EU RCA L0 service** to registration@c-its-eu-rca.eu, putting jrc-c-its-eu-rca@ec.europa.eu in copy, indicating "EU RCA L0 service registration – *[Organization name]*" in the subject of your e-mail and briefly describe your **project needs** (*e.g. internal developments, C-Roads pilot, interoperability tests, client project*), its **expected duration** and **quantities of OBUs and RSUs**.

2. When receiving the **C-ITS EU ROOT CA & SUB-CAs SAAS AGREEMENT**, fill it out and sign it, join the legal registration proof of your organization and send both documents to the same e-mail addresses. Please name **two trusted persons** of your organization responsible for PKI related interactions.

3. After receiving the confirmation of your authorization to use the service, please follow the instructions to send the information of the **stations to be enrolled** in the L0 PKI (e.g. ID and key, permissions – template file to be provided by ATOS). In return, PKI information (certificates & URLs) will be provided.

Terms & Conditions overview

- The EU RCA L0 service is provided by ATOS (IDnomic) on behalf of the European Commission. ATOS reserves the right to grant access to the service
- The EU RCA L0 service is operated by ATOS and data are located in France
- The EU RCA L0 service is delivered against no charge and shall be used for testing purpose only
- The EU RCA L0 service is compliant with ETSI TS 103 097 V1.3.1 and ETSI 102 941 V1.3.1
- The EU RCA L0 service is open 24/7. However technical interventions with possible impact on the service may happen during working hours. ATOS support is only operating during working hours (week days, 9am-6pm Paris time); this includes stations registration and incident recovery.
- ATOS may temporarily or definitely deactivate access to the PKI in case of inappropriate behavior; in particular for clients having stations significantly overcharging the PKI with certificate requests
- Configuration of the EU RCA L0 service (esp. RCA and AA certificates) may evolve on a regular basis. ATOS will inform all enrolled clients prior to configuration update
- The European Commission remains involved and informed on the enrolment and service usage of the C-ITS EU RCA L0 Service from Atos
- Name of organizations using the EU RCA L0 service may be used in ATOS or European Commission public communication in relation to the EU RCA service