Third public workshop of the
Amsterdam Group and CODECS

C-ITS Deployment in Europe: Common Security and Certificate Policy

14 February 2017 Amsterdam
Gerhard Menzel
European Commission - DG MOVE

C-ITS Platform
WG Security

Scope: Cyber Security ←→ C-ITS?

- The scope of the work conducted in the C-ITS Platform Work Group security currently concentrates on the **security of communications for V2V and V2I exchange of messages.**
- The C-ITS Platform WG does not deal with the internal security of vehicles or the topic of security for the topic of access-to-in-vehicle-data.
- The discussions of C-ITS compliance assessment also heavily links to the topic of C-ITS security of communications.
- Further there is an important link to privacy & data protection.

C-ITS Platform
WG Security

C-ITS Platform 2014-2016: C-ITS Trust Model Analysis

- In 2015, the C-ITS platform set up Working Group 5 to identify the most appropriate trust model in Europe for C-ITS platforms.
- The trust model shall be based on a Public Key Infrastructure (PKI) as recommended by the standardization results and by similar initiatives in the world (Connected Vehicles in USA and Australian GateKeeper).
- In addition, Europe has already a working PKI used in the Digital Tachograph application (millions of commercial vehicles in Europe).

C-ITS Platform
WG Security

European Commission

C-ITS Platform 2014-2016: C-ITS Trust Model Analysis

Member of the working group for security in C-ITS:

- Telematics manufacturers
- Vehicle manufacturers
- Member states
- Roadside authorities
- Standardization bodies
- Security experts

Experience from similar and parallel initiatives was used:

- Biometrics passports
- Connected Vehicles in USA
- Digital Tachograph
- Australian Gatekeeper

European Commission

C-ITS Platform 2014-2016: C-ITS Trust Model Analysis

These options were evaluated on the basis of different metrics:

1. Maintainability
2. Scalability
3. Crypto-Flexibility
4. Trust Model flexibility
5. Robustness (Reliability and Resiliency)
6. Simplicity (Antonym to Complexity) – Organizational and Technical
7. Support for life cycle of C-ITS stations
8. Liabilities, contractual aspects
9. Support for revocation
10. Misbehavior detection and countermeasures
11. Robustness against lack of harmonized standards
12. Cost efficiency for investment costs-(CAPEX)
13. Cost efficiency for Running costs (OPEX)
14. Performance efficiency
15. Storage minimization

C-ITS Platform
WG Security

C-ITS Trust model:

- The results of the qualitative analysis based on expert opinion for different categories of stakeholders recommended **Certificate Trust List as main option** with single root CA as close second option.

- These conclusions were completed by additional work items in C-ITS Platform Working Group Security for compliance assessment, crypto agility and revocation.

- In 2016, the work started to define a potential deployment scenario for Europe.

C-ITS Platform
WG Security

European Commission

C-ITS Trust model defined in …

Security policy (SP): rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems, particularly those which impact the systems and associated elements (ISO/IEC 21827:2008-10-15)

Certificate policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. (IETFRFC 3647)

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. (IETF RFC 3647)

European Commission

C-ITS Trust model: Roles (1/2)

The Policy Authority is a role composed by the representatives of public and private stakeholders (e.g. Member States, Vehicle Manufacturers, etc.) participating to the C-ITS trust model, where a majority consensus based voting scheme applies.

The Central Point of Contact (CPOC) is a unique entity appointed by the Policy Authority. It has responsibility to establish and contribute to secure communication exchange between the Root CA to collect the Root CA certificates and provide them to the Trust List Manager (TLM). The CPOC is also responsible for distributing the ECTL to any interested entities in the trust model. The ECTL is needed to ensure interoperability among European member states and vehicles from different manufacturers.

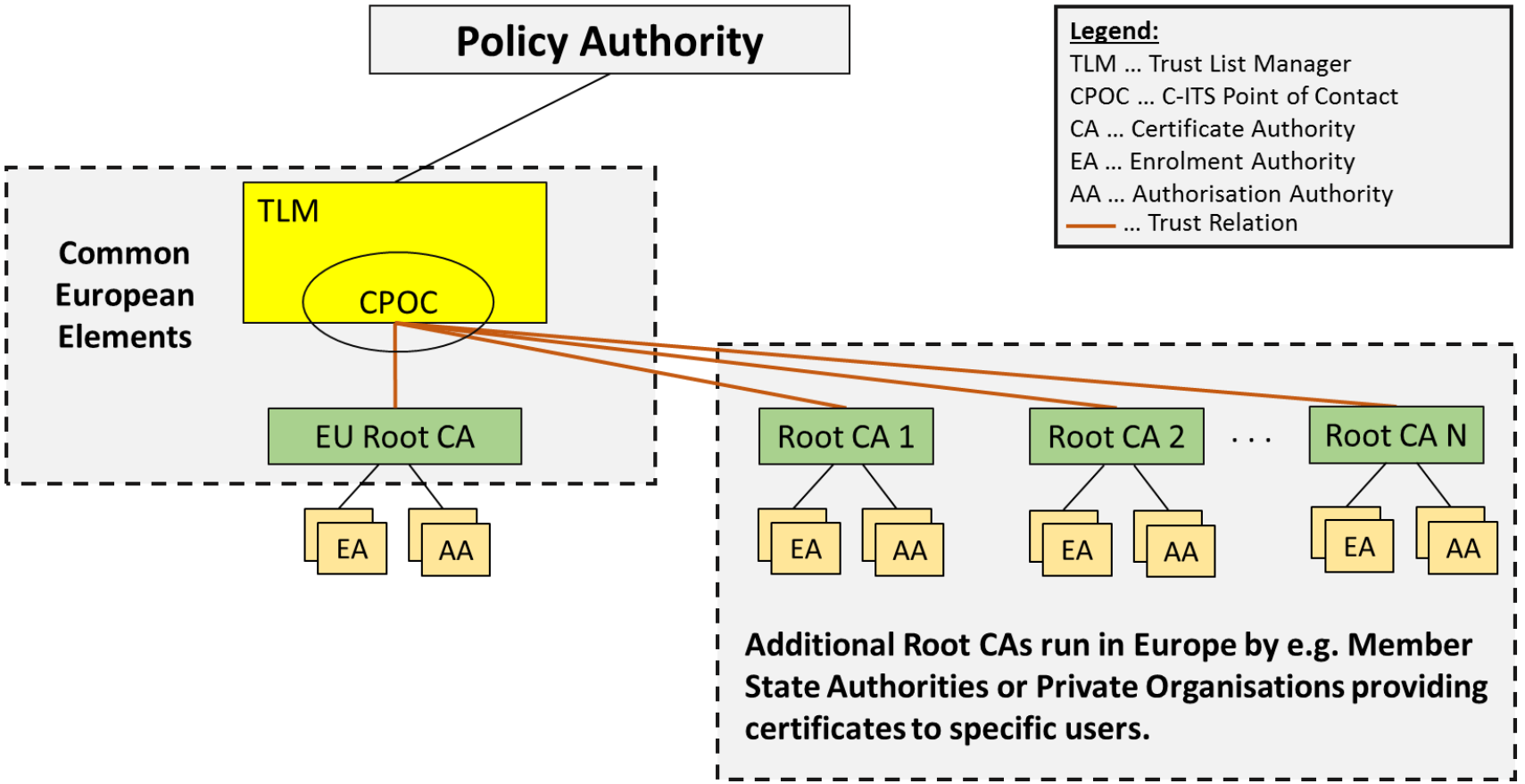
Root Certification Authority provides EA and AA with proof that it may issue enrolment credentials and authorization tickets. A root CA can be both a government (i.e., Member State) or a private entity (i.e., industry)

European Commission

C-ITS Trust model: Roles (2/2)

The Trust List Manager (TLM) is responsible for creating the list of root CA certificates and signing it. The signed list of root CA certificates is the European Certificate Trust List (ECTL)

European Trust Model Architecture



WG Security to implement EU C-ITS Strategy

European Commission

COM (2016) 766 - Ch 3.2 C-ITS Security:

- The Commission will work together with all relevant stakeholders in the C-ITS domain to steer the development of **a common security and certificate policy** for deployment and operation of C-ITS in Europe. It will publish guidance regarding the European C-ITS security and certificate policy in 2017.
- **All C-ITS deployment initiatives** should participate in the development of this common security policy by committing from the beginning to implement future-proof C-ITS services in Europe
- The Commission will analyse the roles and responsibilities of the European C-ITS Trust Model, and whether some operational functions and governance roles should be taken over by the **Commission** (as, for instance, in the case of the Smart Tachograph).

WG Security

COM (2016) 766 - Ch 3.7. Legal framework:

The Commission will consider, where appropriate, making use of its mandate under the ITS Directive to adopt delegated act(s) by 2018 on:

- ensuring continuity of C-ITS services
- laying down **rules to ensure security of C-ITS communications**
- ensuring the practical implementation of the General Data Protection Regulation in the area of C-ITS
- ensuring a forward looking hybrid communication approach
- laying down rules on interoperability
- laying down rules on the **compliance assessment processes**

WG Security

COM (2016) 766 - Ch 3.5. Interoperability at all levels:

The Commission will make full use of the C-Roads platform as the coordination mechanism for C-ITS deployment at operational level.

→ Crucial for **secure and interoperable operation** of C-ITS in Europe for both V2I (Member States / Authorities !) and V2V

→ There is only 1 Trust Model in Europe – **any deployment initiative** (no matter if OEMs or public authorities) needs to stick to common security and certificate policy!

→ Cooperation with C-ROADS therefore an important requirement for CEF co-funded projects

WG Security

Next Steps?

- C-ITS Platform WG Security to deliver final draft of C-ITS certificate policy by early 2017.
- EC to follow-up on actions defined in C-ITS strategy COM 766/2016
- Close involvement of all European stakeholders and international partners needed!
- Target of 2019 very close – urgent need to avoid interoperability and security issues in deployment in Europe NOW!

More Information

Directorate-General for Mobility and Transport:
http://ec.europa.eu/transport/index_en.htm

ITS Action Plan and Directive:
http://ec.europa.eu/transport/its/road/action_plan_en.htm

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

Thank you for your attention!

Gerhard Menzel
gerhard.menzel@ec.europa.eu
European Commission - DG MOVE
B.4: Sustainable & Intelligent Transport