C-ITS
Cooperative Intelligent Transport Systems

Security and Privacy Aspects

Gianmarco Baldini
DG.JRC.E3
Gianmarco.Baldini@ec.europa.eu

Joint Research Centre

C-ITS Challenges

In Cooperative Intelligent Transport Systems (C-ITS) vehicles are capable of broadcasting or receiving data that allow them to communicate with each other and/or with the infrastructure. In addition to what drivers can immediately see around them, and what vehicle sensors can detect, all parts of the transport system are increasingly sharing information to improve driver decision-making and optimise transport operations and safety.

©Car2Car Communication Consortium

The systems must be:

1° Trusted

2° Publicly accepted

3° Harmonized

4° and Law Compliant

The very nature of sharing information provides that C-ITS equipped vehicles are **constantly broadcasting** data, including for example speed and location. This broadcasting is an inherent part of the system and hence raises potential concern as how to guarantee **privacy** and **data protection**, while **securing** the operations.

Role of Security in C-ITS

European Commission

Protection of Critical Assets

Personal information. For instance:

- Information identifying the device or user as a person
- Information about activities: Location (GPS), MAC address, other header info, e.g., IP addresses, PSID/App ID, RF fingerprint of radio
- Application data
- Proprietary codes, algorithms, etc.

Other resources

- Processing time on general purpose CPU or on special purpose processors,
- Other resources in system such as SPECTRUM: Channel usage

Protection of Access

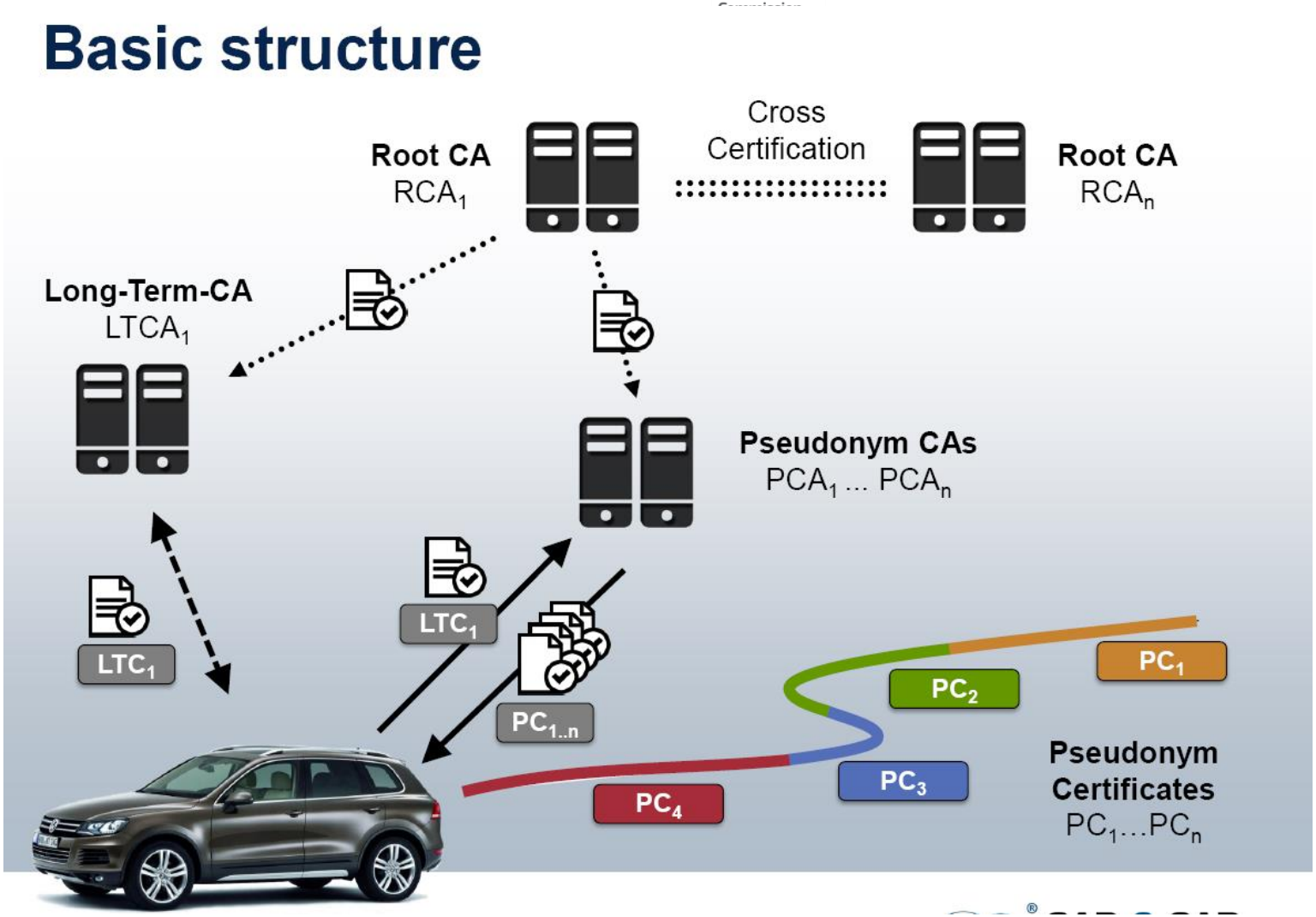
Access to services:

- Ability of a user to access a service or the resources needed
- Ability to discover a service in time to use it
- Ability to trust exchanged data: (a) trustworthy provider; (b) provider with whom the User has a relationship; (c) data has not been modified

Access to resources on a device or system to perform intended functions

Availability of safety-of-life channels and other resources for safety-of-life uses

C-ITS Security



From CAR2CAR: https://www.car-2-car.org/fileadmin/user_upload/OEM_Workshop_WOB/Security-Workshop_Deployment_Options.pdf

Trust Model for C-ITS

The implementation of appropriate levels of security is essential to provide a level of trust among the main elements of the C-ITS architecture: vehicles, road side infrastructures, drivers personal ITS stations, road authorities, service providers and other entities.

C-ITS has specific features, which must be taken in consideration:

- the cooperative aspect implies that mutual trust among the elements of the architecture must be supported,
- the importance of safety applications means that security requirements are high to protect the lives of the citizen,
- the high speed of the vehicles implies that real-time exchange of secure information is needed,
- the huge size of the automotive market spanning many nations entails complex organization and technical dependencies

Trust Model for C-ITS

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).

Different trust model options can be considered with a PKI:

1) Single Root CA
2) Federation of Cross-certified Root CAs
3) Bridge CA
4) Certificate Trust List

Trust Model for C-ITS

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

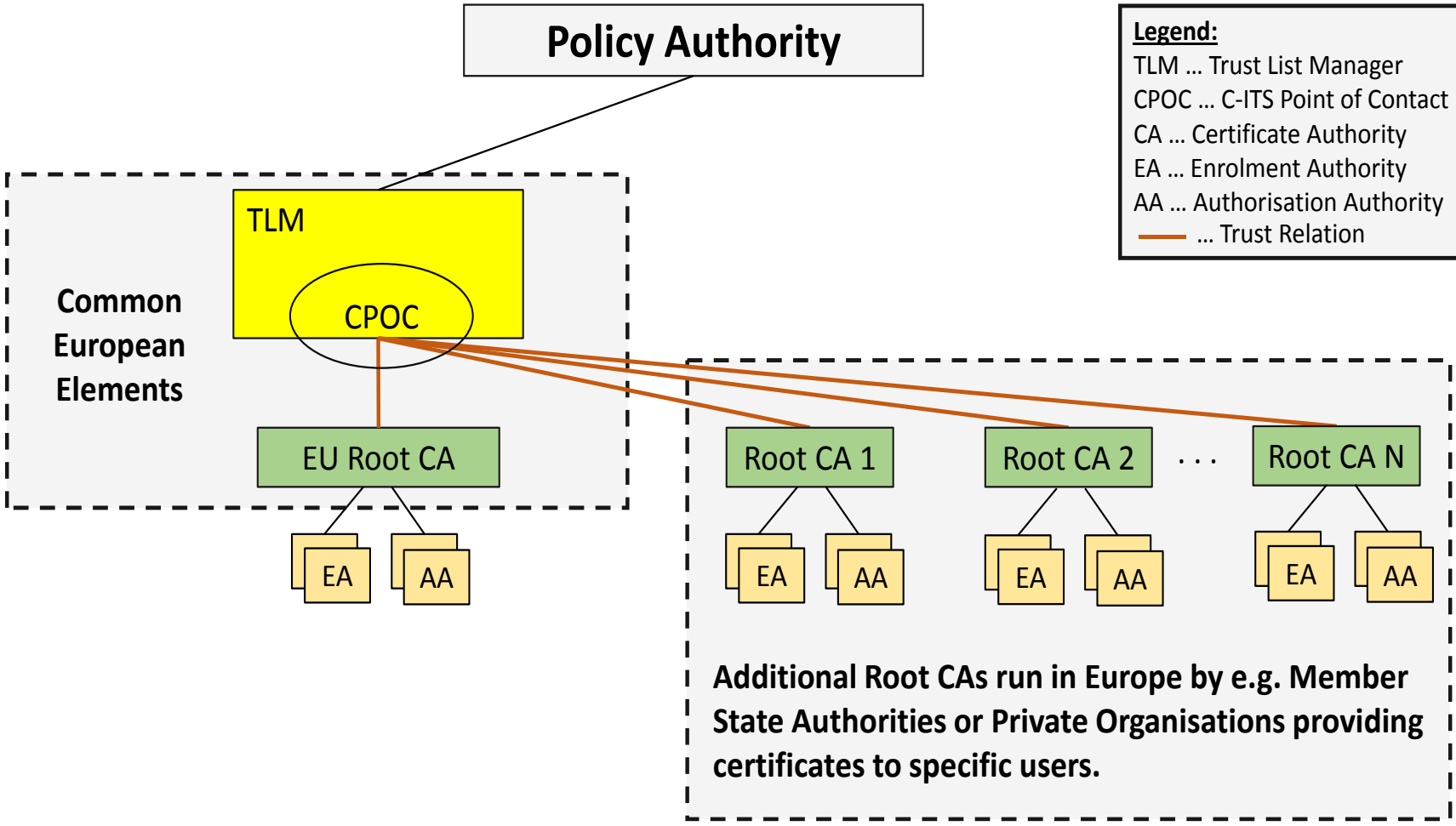
- Telematics manufacturers
- Vehicle manufacturers
- Member states
- Roadside authorities
- Standardization bodies
- Security experts

Experience from similar and parallel initiatives was used:

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

C-ITS Security

Towards a common C-ITS certificate and security policy in Europe



Trust Model for C-ITS: Roles

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)

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).

C-ITS Security

Security policy: 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. (IETF RFC 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)

C-ITS

©Car2Car Communication Consortium

Our Unit "Digital Citizen Security" is supporting:

1° DG MOVE C.3 ITS unit

C-ITS platform WG4 DATA PROTECTION
C-ITS platform WG5 SECURITY

2° Harmonization Task Group HTG#6

Candidate Harmonized Policies for Cooperative ITS Security Implementation

3° Harmonization Task Group HTG#7

C-ITS Standards Analysis

C-ITS Masterplan

DG MOVE C.3 ITS unit

C-ITS form an integral part of the **Commission's Energy Union Strategy** by decreasing energy consumption and increasing energy efficiency in road transport with better traffic management and less congestion. It also contributes to the **Commission's Digital Single Market Strategy** as C-ITS can incorporate ICT-solutions in transport and will create massive volumes of electronic data exchanges.

ROADMAP			
TITLE OF THE INITIATIVE	A Master Plan for the deployment of Interoperable Cooperative Intelligent Transport Systems in the EU		
LEAD DG – RESPONSIBLE UNIT – AP NUMBER	MOVE.DDG1.C.3	DATE OF ROADMAP	07/04/2016
LIKELY TYPE OF INITIATIVE	Commission Communication		
INDICATIVE PLANNING	*http://ec.europa.eu/atwork/pdf/planned_commission_initiatives_2016.pdf*		
ADDITIONAL INFORMATION	*http://ec.europa.eu/transport/themes/its/index_en.htm*		

C-ITS Harmonization HTG#6

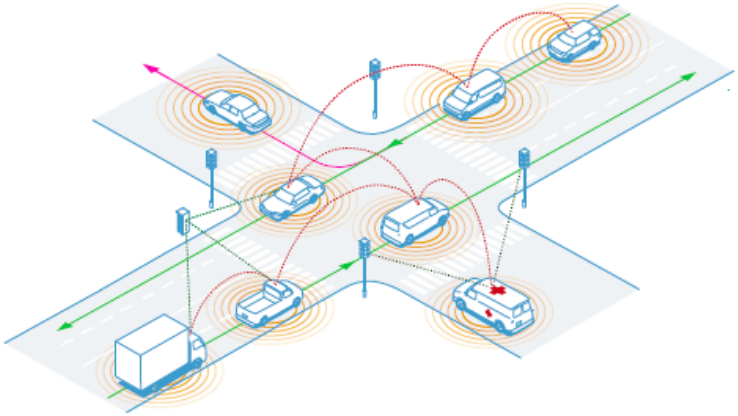
Results
http://ec.europa.eu/digital-agenda/en/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international

EU-US-AU Task Group to Harmonize Cooperative ITS Security Policy

EU-US ITS COOPERATION

EU-US Joint Intelligent Transportation System (ITS) Technical Task Force

The European Union (EU) and the United States (US) signed an Implementing Agreement in 2009 to develop coordinated research programs, focusing on cooperative ITS systems. The task force executes work programs under the agreement.



Standard Harmonization Working Group (HWG)

Other Working Groups include Safety Applications, Sustainability Applications, Assessment Tools, Driver Distraction and HMI, European Technical Roadmap, and Glossary.

Harmonization Task Group (HTG) #6: "Candidate Harmonized Policies for Cooperative ITS Security Implementation"

Among the completed HTGs, the HTG#1, on security standards, identified a range of gaps related to security management policies and approaches - HTG#6 seeks to address many of these gaps.
Australia has joined as an equal participant HTG#6.

Aim and Objectives
Harmonize cooperative ITS vehicle security policy.
JRC Direct Support to DG CNECT H.5 (Smart Cities Unit).

Co-leadership
EU Commission - US DOT - TCA

U.S. Department of Transportation

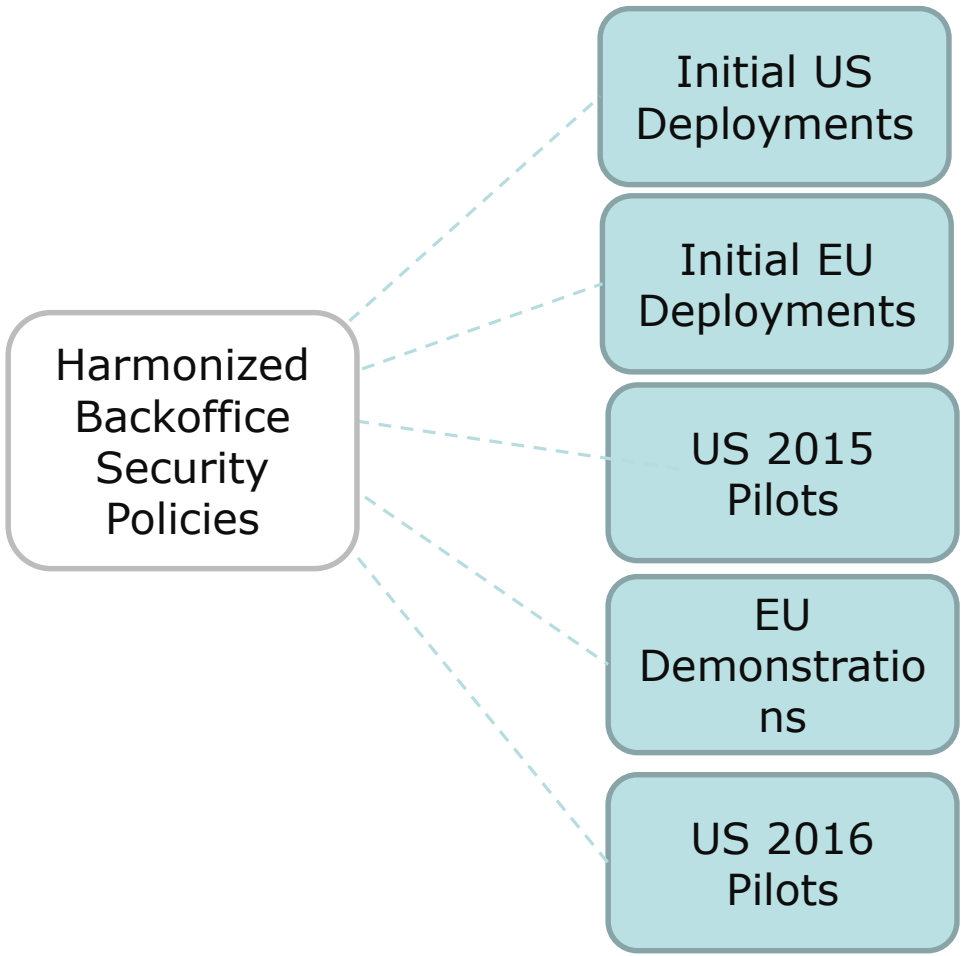
Team
Multidisciplinary team made of experts from US EU AU.
Observers from Japan and Canada.

Deliverables
Outcomes are expected to include:

- Implementation guidance and recommendation
- Roadmaps and policy requirements; identification of gaps; identification of those areas that are not suitable for harmonization
- Candidate harmonized policies
- Exchange of best practices between countries/region

Importance of Security Policy Harmonization

- Ensures trust across the system
- Risk management
  - Security risks are not taken into consideration during planning, procurement, installation, and integration activities
  - Current standards do not address cooperative/interdependent environments
- Opportunities
  - Harmonized security policies will reduce uncertainty for implementers
  - New, future applications and devices can be built in a consistent manner to meet security risks if policies are understood beforehand



C-ITS Harmonization HTG#7

C-ITS Standards Analysis

Harmonization Task Group 7 Workshop

INTERNATIONAL ITS COOPERATION

June 6, 2016 | 8H30 – 14H30 | Alsh Room 1, Scottish Exhibition and Conference Centre (SECC)

Harmonization Task Group 7 ("HTG7") is a cooperation of the European Commission, Transport Certification Australia, and U.S. Department of Transportation to recommend a comprehensive set of standards for an overall system architecture to support large-scale Cooperative-Intelligent Transportation Systems (C-ITS) deployment. The work is being performed in a manner that is extensible to include emerging technologies including connected Automated Vehicle (AV) deployments, urban ITS deployments, and smart cities (among other evolutions in the future).

HTG7 OBJECTIVES:

- Support implementers in identifying candidate standards that are available to them for planning and use; and, in particular, for implementers to have a clear understanding about which functions and interfaces are critical for interoperability and where standards are available to support interoperability;
- Support governments, standards organizations, and interested stakeholders in identifying gaps for those interfaces and information flows that are of significant public interest so that we can work with experts to address gaps in three ways—
    1. Recommend available standards to adopt, including an identification of how the standard meets cooperative-system requirements, when known;
    2. Identify interfaces and functions where adapting existent standards is best, and describe the needs/requirements that need to be met through adaptation; and
    3. Identify gaps and describe the needs/requirements where there is a need to create new content, which offer key opportunity for collaborative standards development.

Research Centre

Thank you for your attention.

Joint Research Centre (JRC)
Web: www.jrc.ec.europa.eu