Public-Key-Infrastructures for Cooperative Intelligent Transport Systems (C-ITS)

Today's automotive industry is being moved by deep trends that are drastically changing the driving experience, the vehicles, and their environment: electrification, automated driving, software defined vehicles and connected cars. Vehicles are not isolated entities on the road anymore; they can connect and exchange information with the infrastructure and the other users through Vehicle-to-Everything (V2X) communications. The V2X technology is being used to deliver Cooperative Intelligent Transport Systems (C-ITS) services, which are meant to make transport safer, more efficient, and more environmentally friendly.

C-ITS are considered an important technology for the future and are therefore a focus of standardization and research on a worldwide level (ETSI in Europe, IEEE in the USA, ISO, etc.). Beyond these standardization works, the C-ITS ecosystem also needs harmonization work to ensure that the same implementation concepts are shared by the different stakeholders for the widest possible interoperability. Several initiatives took place in that sense, like the Omniair consortium, the Car-to-Car consortium, or the C-ROADS platform that directly involves 18 EU member States and other non-European countries.

All kinds of cyber communication in complex ecosystems require high security requirements, and C-ITS are no exception. C-ITS must be protected from hackers, terrorists, and other criminals, while the user's privacy needs to be enforced. The operating mode based on constant exchanges of qualitative trustful information between unknown third parties requires the management of cyber trust.

For this reason, V2X communication and C-ITS services must be equipped with cryptographic security measures. Thus, the standardization bodies chose the Public Key Infrastructure (PKI) as C-ITS backbone for security and interoperability. The C-ITS PKI issues dedicated digital certificates to vehicles and infrastructure components to ensure the correct use of specific permissions, the authenticity of messages and the pseudonymization of the issuers' identity, among others.

This whitepaper introduces the C-ITS ecosystem, its purposes, the C-ITS PKI concepts, and its operation by Atos.

Contents

Introduction

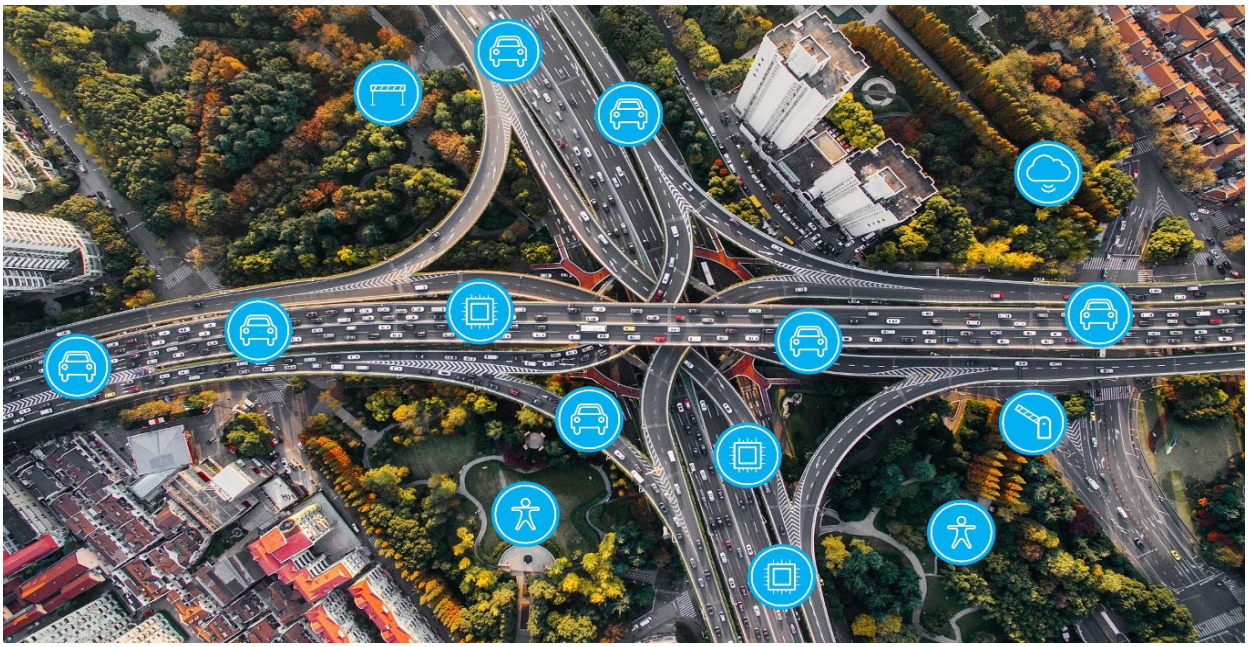
In automotive history, the 1900s can be referred to as the mechanical century since most innovations and improvements affected the hardware. From a safety standpoint and despite a limited human perception, the vehicles' behavior was 100% driver-dependent and was relying on the human capacity to react.

At the beginning of the 2000s, an electronical shift occurred. The car manufacturers started to embed more and more electronic driving assistance such as GPS navigation, lane keeping warning or sleep detection. The driver became part of an extended perception system able to detect, warn and even react in an automated way. However, this evolution didn't fundamentally modify the way safety was handled: it remained based on reaction, which was often too late.

Around the beginning of the 2020s, road vehicles fully embraced the multiplied capacities of telecommunication, cloud computing, big data, and artificial intelligence to enter the digital era. In this transition phase towards advanced automated driving functions, not only the safety challenges, but also pollution reduction and traffic efficiency can be tackled by new solutions.

By delivering valuable information from beyond the direct environment of the vehicle, digital communication technology provides an enhanced perception. Key-information can be shared much earlier, which enables anticipation instead of hazardous reaction. Still, each entity of this complex ecosystem, from cars to road infrastructure through vulnerable road users, must be able to fully trust this information to take appropriate measures when necessary.

This implies to establish interoperable services where information quality levels are guaranteed, use cases are harmonized, and security is applicable to all stakeholders at hardware and software level, with clear requirements and compliance frameworks.



Cooperative Intelligent Transport Systems

C-ITS

In a world revolutionized by the Internet and telecommunication, cars and other vehicles started to communicate with each other and with the road infrastructure. As a result of this communication, many accidents are now avoided, traffic congestions become rarer, and transport becomes more environmentally friendly. The impacts will even be greater with fully autonomous driving systems.

Technologies used for this purpose are referred to as **Cooperative Intelligent Transport Systems (C-ITS)** and are based on communication between vehicles (V2V) or between vehicles and traffic infrastructure (V2I), summarized as **vehicle-to-everything (V2X) communication**.

V2X communication and C-ITS are considered important future technologies. The global V2X market was estimated at[1] 2.5 billion USD in 2019 and at 11,7 billion USD in 2027. The last impact assessment ordered by the European Commission established that the impact of the deployment of C-ITS services in total saved money until 2040 would be of 145 billion EUR, and 30 billion EUR in reduction of accident's costs. During the same period, the total cost, mainly car integration, deployment, and operation, would reach 21 billion EUR. It must be noted that these figures do not even take into account the positive effects that such C-ITS services will have on multimodality and highly automated services.

In the C-ITS context, communication takes place between stations. A station usually corresponds to a vehicle or an infrastructure component, such as a traffic light. When a station is embedded inside a vehicle, we call it an on-board unit (**OBU**), and when it is deployed on the road infrastructure, we talk about a road-side unit (**RSU**). Each station is given an identity.

Security

Cyber communication in complex ecosystems requires high security requirements and C-ITS aren't an exception to this rule:

- *Cyber security*: The systems must be protected from hackers, terrorists, and other criminals.
- *Controlled use*: Access to specific rights (permissions) of use must be validated.
- *Data protection*: The integrity of messages' content must be guaranteed.
- *Pseudonymity and privacy*: The identity of stations must be pseudonymized to prevent vehicles to be tracked by following their C-ITS signed messages.

[1] alliedmarketresearch.com/automotive-v2x-market-A07120

Standardization

V2X communication is currently a focus of standardization and research at worldwide level. There are activities in the USA, Europe, Asia, and Africa.

In Europe, the European Commission addressed in 2009 the standardization mandate that in 2012/13 led to a first minimum set of standards for the interoperability of the C-ITS in the European Community. The reference standardization bodies are the IEEE in the USA and the ETSI in Europe.

At a global level, the main C-ITS standards are ETSI TS 102940, 102941 and 103097 for Europe, IEEE 1609.2 & 1609.2.1 for North America, and YD/T CCSA "Technical Requirement of Security Certificate Management System for LTE-based Vehicular Communication" in China.

Since 2016, 18 EU member states participate in the C-Roads platform, which fosters the deployment of C-ITS pilot projects and harmonization works.

Depending on their level of technical and implementation complexity, the C-ITS services are classified into different groups. The easiest ones are the Day 1 services, and the others with more complex challenges belong to the Day 1.5, Day 2, Day 3 and more. The present European regulation and central security elements only include the Day 1 services at this stage.

The C-ITS-PKI

Overview

The C-ITS standardization defined as a prerequisite for interoperability the use of public key infrastructures known as **C-ITS PKI**. The C-ITS PKI issues digital certificates to OBUs and RSUs. The use of these certificates by the stations enables secure V2X communication.

The C-ITS PKI has been designed to meet several requirements, like making it possible to:

- React instantaneously on unexpected road events to enhance road safety.
- Authenticate via digital certificates stations delivering C-ITS services.
- Protect data and communication between stations with certificate based digital signature.
- Know which messages to trust or to ignore in an automated way.
- Block a misbehaving station if necessary.
- Preserve privacy by making it impossible to track the movements of an OBU through certificate pseudonymization.

Structure

The certificate format specified in the IEEE and ETSI standards is the same and does not correspond with the X.509 format. It is based on simple data structures and optimized so that stations can quickly parse and process a certificate. This format was specifically developed for C-ITS.

In Europe, trust domain extension beyond the Root Certificate Authority (RCA) is made possible through a central European Certificate Trust List (ECTL). The ECTL is managed by a Trust List Manager (TLM) operated by the European Commission's Joint Research Center (JRC) in line with the C-ITS Point

of Contact (CPOC) protocol. Compliant RCAs can be included in the ECTL to enable automated interoperability between stations from different trust domains.

The European C-ITS PKI has the following key components (see Figure 1):

- *Root Authority*: As root of trust, this offline authority trusts and signs the certificates of its Sub-CAs, the Enrolment and Authorization Authorities.
- *Enrolment Authority (EA)*: Used to register stations and issues long-term certificates named Enrolment Certificates (EC), receives and answers to validation requests sent by the Authorization Authority.
- *Authorization Authority (AA)*: Issues short-term certificates named Authorization Tickets (AT) to the stations, receives and answers to certificate requests sent by the C-ITS stations.

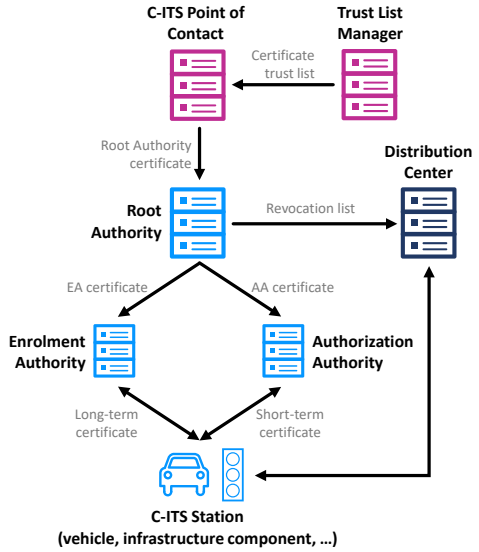


Figure 1: Simplified architecture scheme of ETSI C-ITS PKI (EU)

- *Distribution Center (DC)*: This directory service provides CA certificates, subscriber certificates, certificate trust lists, and revocation lists for download.

The North American C-ITS PKI is more complex than its European counterpart and has a slightly different architecture (see Figure 2). In North America, the expression "V2X PKI" is more common. Among others and in addition to the four elements mentioned above, the North American V2X PKI includes:

- *Registration Authority (RA)*: Acts as central permission validation and distribution point between the C-ITS stations and the CAs.

The C-ITS PKI protocols are completely independent from the communication technologies used by the stations.

A distinction is made between long-term certificates (valid for several years) and short-term certificates (valid for a few hours or days). Each station initially receives a long-term certificate (EC). This EC is exclusively used for communications with the PKI, mainly to request short-term certificates (AT). The ATs are constantly changed and exclusively used for signing the C-ITS messages sent to other stations on the field.

The technical and organizational separation of roles between the EA and the AA enables the pseudonymization of the identity contained in the long-term EC. Combined with the high rotation of ATs used to sign C-ITS messages, it guarantees privacy by preventing the vehicle to be tracked during its journey.

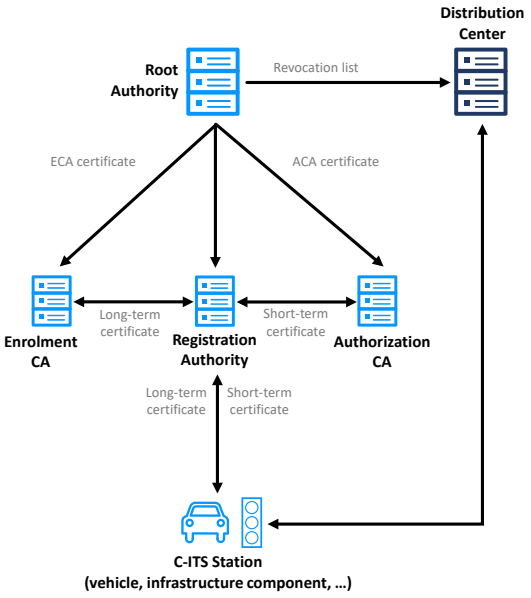


Figure 2: Simplified architecture scheme of IEEE V2X PKI (USA)

Central security elements and operation levels

To complement the C-ITS PKI, Europe also deployed central security elements that are part of the European C-ITS Credential Management System (EU CCMS):

- *Trust List Manager (TLM)*: Issues and signs the European Certificate Trust List (ECTL).
- *C-ITS Point of Contact (CPOC)*: Central interface between the C-ITS ecosystem and the TLM, especially for the inclusion of Root CA certificates in the ECTL.

To define coherent trust environments at continental level, three levels of operation were defined for PKI, stations, and ECTL:

- *L0*: for testing and integration works, less mature pilot projects.
- *L1*: for more stable pilot operation, full-scale production but not certified against the EU reference documents (Certification Policy and Security Policy), it is conceived as a temporary transition level that will turn into a legacy platform.
- *L2*: for full-scale production certified against the EU reference documents (Certification Policy and Security Policy).

Operation of the IDnomic C-ITS PKIs by Atos

The IDnomic team, part of Atos group, develops, deploys, and operates the IDnomic C-ITS PKIs, which represent a significant part of the current C-ITS PKI. Run as a service in public clouds, the C-ITS PKIs are compliant with both latest versions of the European (ETSI) and North American (IEEE) standards.

Due to high scalability/elasticity operational needs, the architectures are compatible with any public cloud provider proposing a Kubernetes service. The Hardware Security Modules (HSM) are connected in a performant and secure way to the cloud platform.

The infrastructure chosen for Europe consists in minimum two Active-Active sites, where each site is able to handle 100% of the service load and plays the role of a recovery site of the other. Data storages are replicated on three sites. Each datacenter is minimum TIER 3 certified and physically distant from the others.

The first public cloud chosen for the North American V2X PKI is the Google Cloud Platform (GCP).

In Europe, Atos deploys and operates IDnomic C-ITS PKIs since 2016, operates on L0 since the first L0 ECTL was published in 2020, already deployed an L2 certified platform for the European Commission and an L1 platform aligned on L2. The L1 service is ready to be referenced in the L1 ECTL when it is made available by the European Commission.

Ecosystem leverage points

As for all industrial subjects, the deployment of V2X communication and C-ITS services can directly be impacted by several elements that must be identified by the stakeholders and the public administrations. This is especially true for topics driven by standardization and seeking for native interoperability. These elements are the following:

- *Regulation*: The existence or absence of regulation, as well as the clarity of the regulation content is without any doubt the main factor that can affect the C-ITS services deployment. Even if such services are not made mandatory, the frameworks defined by the regulation become the reference points for the whole ecosystem and a strong basis to unlock strategical investments. As the goal of C-ITS is global and native interoperability, the ideal situation is to have a regulation applicable at continental level (Europe, North America, etc.). On the contrary, local regulatory constraints should be avoided, especially when considered unnecessary or dangerous for the ecosystem harmonization.

- *Certificate and Security Policies*: C-ITS solutions must guarantee a high and uniform level of security across the whole ecosystem. Without a clear Certification Policy and Security Policy, manufacturers, Road operators and other users will be reluctant to open their trust domains to third parties, which will block native interoperability. The Security Policy also has direct impacts on the hardware design and on the manufacturing process.

- *Euro NCAP*: The inclusion of C-ITS services in the Euro NCAP list of security features could push V2X into all vehicles (97% of the new vehicles sold in Europe are Euro NCAP rated, and 89% of new vehicles have 4- or 5-star ratings). Any technology added to Euro NCAP has reached nearly all new vehicles within a few years after receiving the rating.

Conclusion

Thanks to the C-ITS activities in the EU and other parts of the world, cooperative intelligent transport systems are on a good way, Nevertheless, the C-ITS technology is still in an early stage. By considering the potential of this technology, we can expect a rapid growth in the years and decades to come. This market penetration will only be sustainable if the components and processes of C-ITS are adequately protected while ensuring a global, native interoperability. For this reason, cyber security and trust will always play a major role in C-ITS standardization, governance, and regulation. The PKI is therefore entrusted a big responsibility by being the C-ITS ecosystem angular stone of trust and interoperability.

For the years to come, one of the major challenges will be to scale up the C-ITS PKI to support several million stations who will request billions of certificates.

In parallel, harmonization groups and activities of synchronization between the different stakeholders and the different geographical regions will have to take place to reach the broadest possible interoperability and avoid an unnecessary and complex fragmentation of the ecosystem.

For more information please contact: **axel.sandot@atos.net**

About Atos

Atos is a global leader in digital transformation with 112,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

More about us:
atos.net
atos.net/career

Let's start a discussion together.

For more information: www.atos.net

Editor:
Atos Cybersecurity Products, Axel Sandot, Klaus Schmeh

Source of supply:
Atos
River Ouest, 80 quai Voltaire
95877 Bezons cedex – France

Published in February 2023

Figures: Atos