IDnomic C-ITS PKI

PKI for a connected, smarter, and safer traffic

In a world revolutionized by ICT, cars and other vehicles started to communicate with each other and with the road infrastructure. The future is set for fully autonomous driving systems. As a result, many accidents are avoided, traffic congestions decreasing, and transport more environmentally friendly. Technologies used for this purpose are referred to as Cooperative Intelligent Transport Systems (C-ITS), based on communication between vehicles (V2V) or traffic infrastructure (V2I), summarized as vehicle-to-everything (V2X).

In the C-ITS context, all active elements ("stations") of a traffic communicate with each other. A station usually represents a vehicle or an infrastructure element, such as a traffic light. A station can be either embedded inside a vehicle (on-board unit, OBU) or deployed on the road infrastructure (road-side unit, RSU).

International standards require a specific Public Key Infrastructure, in charge of protecting the V2X communication and production of vehicles.

Security plays a central role in C-ITS, as both (private) information and physical safety are mandatory requirements. One has in particular to focus on:

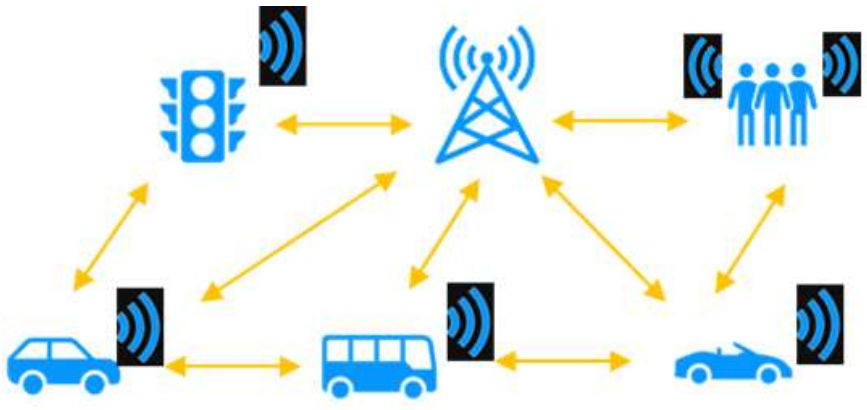
• *Cyber security:* The systems must be protected from hackers, terrorists, and other criminals.
• *Controlled use*: Access to specific rights (permissions) of use must be validated.
- *Data protection*: The integrity of messages' content must be guaranteed.
- *Pseudonymity and privacy:* The identity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

.

IDnomic C-ITS PKI is a software suite, specifically designed to comply with international standards for C-ITS and V2X.

The certificate format specified in the IEEE and ETSI standards is based on simple data structures and optimized so that stations can quickly parse and process a certificate.

Amongst other references, IDnomic C-ITS PKI has been chosen to be the technical solution for the European Root CA, operated by the Joint Research Center (JRC).



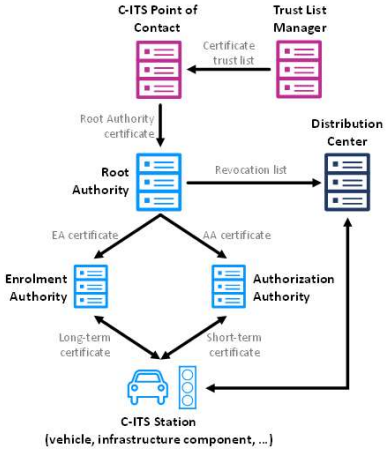
Collaborative Intelligent Transport Systems (C-ITS) Scheme

Atos

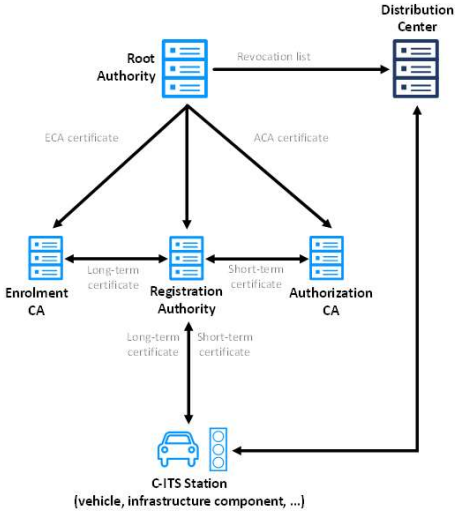
IDnomic C-ITS PKI – maturity, performance and compliance

IDnomic C-ITS PKI focuses on stringent compliance with European and US standards. The following key components are implemented:

- Root Authority: Issuing 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.
- Distribution Center (DC): Directory service providing CA certificates, subscriber certificates, certificate trust lists, and revocation lists for download.
- Registration Authority (RA): Central permission validation and distribution point between the C-ITS stations and the CAs (only for the US PKI scheme)



EU C-ITS Scheme



US C-ITS Scheme

Benefits for our customers

- Strictly compliant with international standards ETSI and IEEE
- Mature solutions – product operated since 2016. Successful results during international interoperability tests.
- Deployments - Several pilots and production implemented worldwide
- Reliability – Idnomic C-ITS PKI is the chosen solution for EU Root CA by JRC in Ispra, Italy
- Scalability/Elasticity – Architecture compatible with any public cloud
- High performance & Security – Deployed in Active/Active mode, including full HSM integration.

Standards and technical specifications

- ETSI TS 102940, 102941 and 103097 for Europe
- IEEE 1609.2 & 1609.2.1 for North America

Find out more about us atos.net/en/solutions/cyber-security/trusted-digital-identities