

EVIDEN

Eviden C-ITS PKI

PKI for connected, smarter and safer traffic

In an ICT-revolutionized world, vehicles communicate with each other and with road infrastructure, paving the way for fully autonomous driving systems. This advancement, known as Cooperative Intelligent Transport Systems (C-ITS), relies on Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, summarized as V2X.

Interconnected traffic

In the C-ITS context, all active elements ("stations") of traffic communicate. A station typically represents a vehicle or an infrastructure element like a traffic light. Stations can be embedded in vehicles (onboard unit, OBU) or deployed on road infrastructure (road-side unit, RSU). International standards mandate a specific Public Key Infrastructure to protect V2X communication and vehicle production.

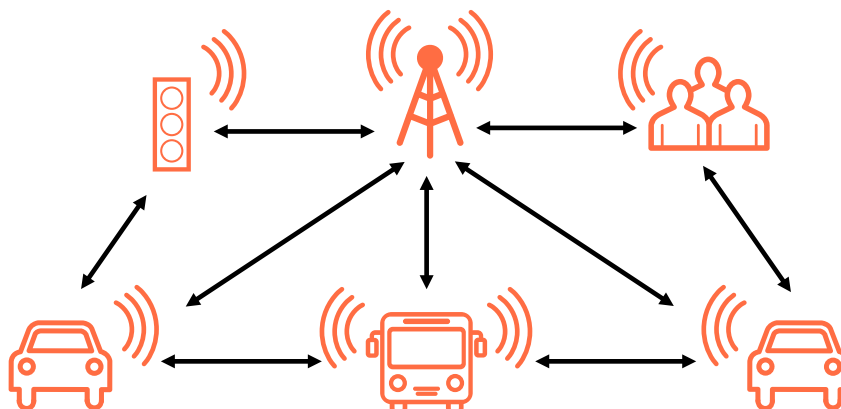
Security and driver's privacy

Security is paramount in C-ITS, as both physical safety and driver's private information need to be assured. All digital assets that are produced for vehicle identity and information exchange confidentiality and integrity must be protected against cyberattacks. Industrial C-ITS security solutions must therefore cover all critical areas such as cyber security, access control, data protection, and pseudonymity to prevent vehicle tracking.

Best-of-breed technology

C-ITS PKI is a software suite designed to comply with international standards for C-ITS and V2X. The certificate format specified in IEEE and ETSI standards is optimized for quick parsing and processing by stations. Notably, C-ITS PKI is chosen as the technical solution for the European Root CA operated by the Joint Research Center (JRC).

C-ITS PKI – A mature solution, powerful and compliant

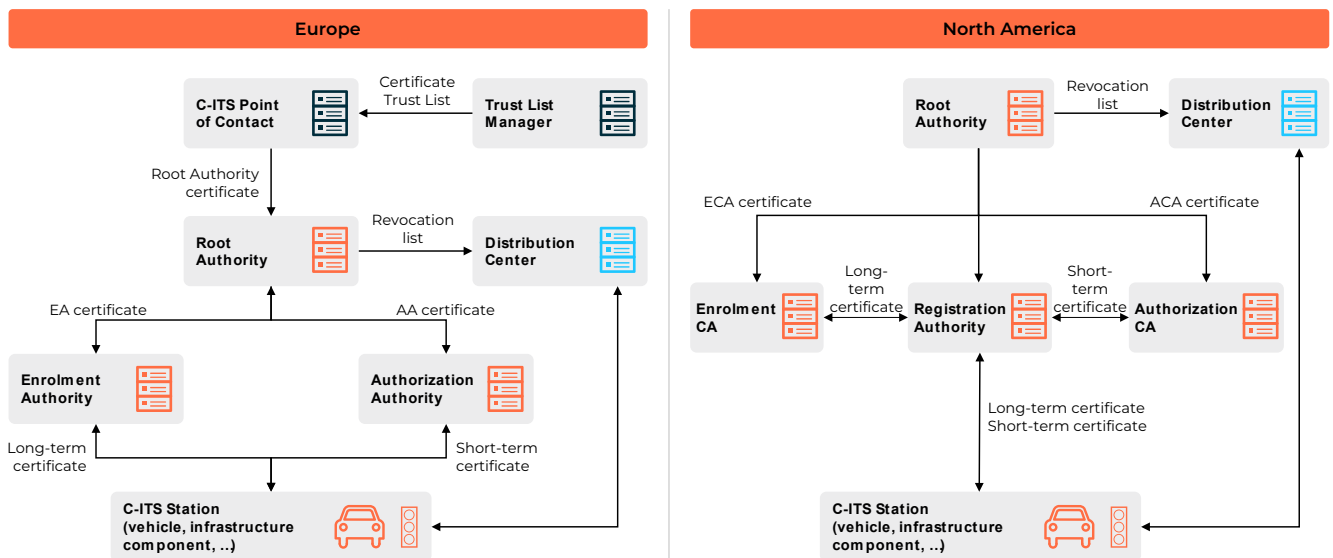


Cooperative intelligent transportation systems are an important future technology in which security plays a central role.

Components of the C-ITS PKI

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

- **Root Authority:** Issues certificates for its sub-CAs, i.e. the Enrolment Authorities and the Authorization Authorities.
- **Enrolment Authority (EA):** Registers C-ITS stations and issues long-term certificates (Enrolment Certificates). Receives and replies to validation requests sent by the Authorization Authority.
- **Authorization Authority (AA):** Issues short-term certificates (Authorization Tickets) to the C-ITS stations. Receives and replies to certificate requests sent by the C-ITS stations.
- **Distribution Center (DC):** This component is a directory service providing CA certificates, subscriber certificates, certificate trust lists, and revocation lists for download.
- **Registration Authority (RA):** This central permission validation and distribution point between the C-ITS stations and the CAs only exists in the US scheme.



Benefits for our customers

- **Compliance with International Standards:** Our product strictly adheres to recognized international standards set by ETSI and IEEE.
- **Proven Track Record:** With a history of operation since 2016, our mature solutions have consistently demonstrated successful results in international interoperability tests.
- **International Deployment Experience:** Our solutions have been deployed in several pilots and production environments worldwide.
- **Reliability:** C-ITS PKI has been selected as the solution for the EU Root CA by the prestigious Joint Research Center (JRC) in Ispra, Italy.
- **Scalability and Elasticity:** Our architecture is designed to be compatible with any public cloud infrastructure.
- **High Performance and Security:** Deployed in Active/Active mode with full Hardware Security Module (HSM) integration, our solution ensures both high performance and robust security.

Standards and technical specifications

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

Find out more about us: www.eviden.com

Connect with us



eviden.com