EVIDEN

IDnomic C-ITS PKI

Die PKI für einen vernetzten, intelligenten und sichereren Straßenverkehr

In einer von Informationstechnologien revolutionierten Welt haben Autos und andere Fahrzeuge begonnen, untereinander und mit der Straßeninfrastruktur zu kommunizieren, mit Hinblick auf vollständig autonome Fahrsysteme. Dadurch können viele Unfälle vermieden, Staus reduziert und der Verkehr umweltfreundlicher gestaltet werden. Die dafür eingesetzten Technologien werden als "kooperative intelligente Verkehrssysteme" (Cooperative Intelligent Transport Systems, C-ITS) bezeichnet und basieren auf der Kommunikation zwischen Fahrzeugen (V2V) oder der Straßeninfrastruktur (V2I), zusammengefasst als "vehicle-to-everything" (V2X) bezeichnet.

Im Konzept des C-ITS kommunizieren alle aktiven Elemente ("Stationen") eines Verkehrssystems miteinander. Eine Station stellt in der Regel ein Fahrzeug oder ein Infrastrukturelement, wie z. B. eine Ampel, dar. Eine Station kann sich in einem Fahrzeug befinden (On-Board-Unit, OBU) oder auf der Straßeninfrastruktur eingesetzt werden (Roadside Unit, RSU).

Sicherheit spielt bei C-ITS eine zentrale Rolle, da (private) Informationen und physische Sicherheit zwingende Anforderungen sind. Internationale Standards fordern daher eine spezielle Public-Key-Infrastruktur (PKI), die für den Schutz der V2X-Kommunikation und der Fahrzeugproduktion zuständig ist.

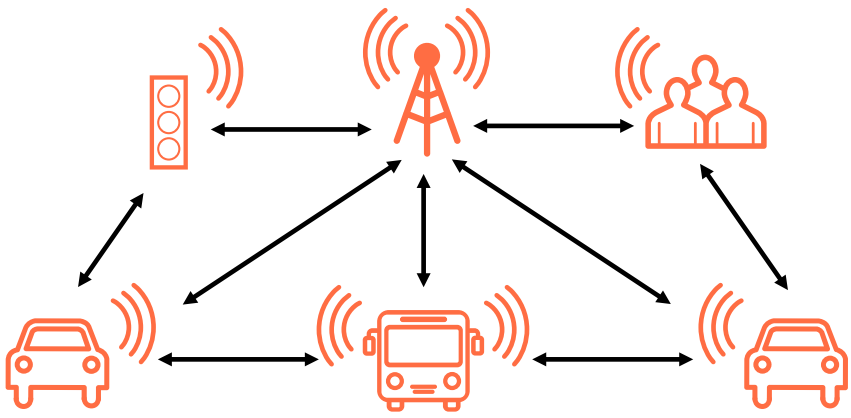
Mit dieser PKI sollen folgende Ziele erreicht werden:

- *Cybersicherheit*: Die Systeme müssen vor Hackern, Terroristen und anderen Kriminellen geschützt werden.
- *Kontrollierte Nutzung*: Der Zugriff auf Nutzungsrechte (Berechtigungen) muss validiert werden.
- *Schutz der Daten*: Die Integrität des Inhalts von Nachrichten muss gewährleistet sein.
- *Pseudonymisierung und Schutz der Privatsphäre*: Die Identität der Stationen muss pseudonymisiert werden, um zu verhindern, dass Fahrzeuge durch die Verfolgung ihrer von C-ITS signierten Nachrichten zurückverfolgt werden können.

IDnomic C-ITS PKI ist ein Softwarepaket, das speziell zur Einhaltung der internationalen Standards für C-ITS und V2X entwickelt wurde. Das in den IEEE- und ETSI-Standards spezifizierte Zertifikatsformat basiert auf einfachen Datenstrukturen, die so optimiert sind, dass die Stationen ein Zertifikat schnell analysieren und verarbeiten können.

Neben anderen Referenzen wurde IDnomic C-ITS als technische Lösung für die europäische Root CA ausgewählt, die von der Gemeinsamen Forschungsstelle (Joint Research Centre, JRC) der EU in Ispra, Italien, betrieben wird.

IDnomic C-ITS PKI – Eine ausgereifte Lösung, leistungsstark und konform

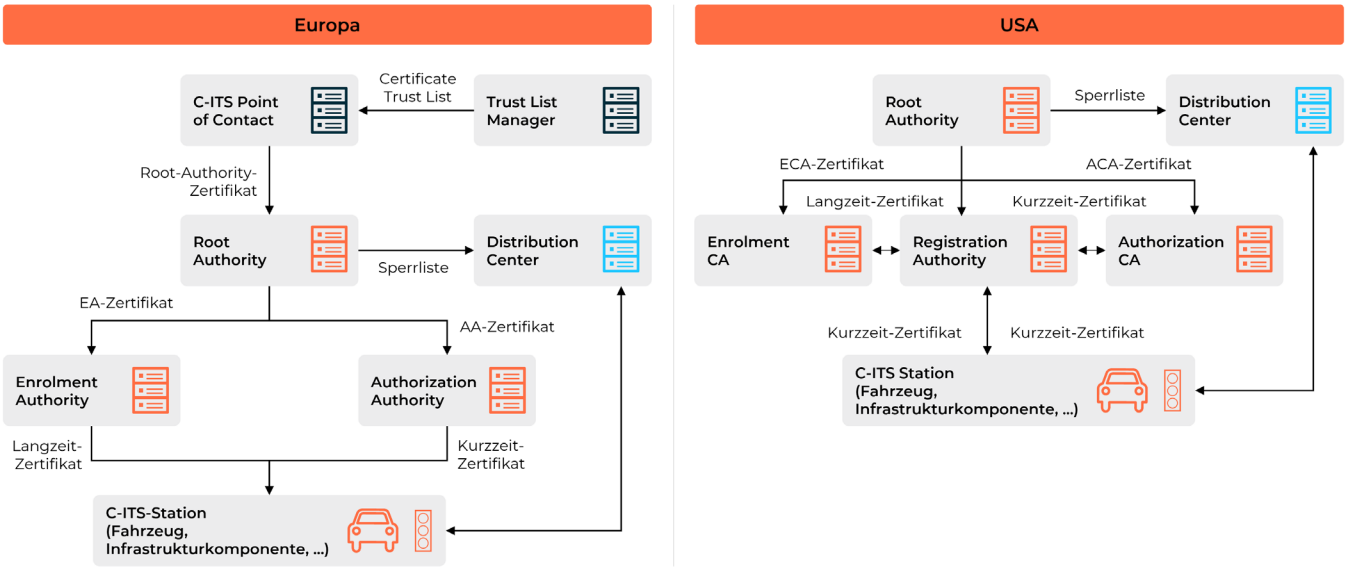


Kooperative intelligente Verkehrssysteme sind eine wichtige Zukunftstechnoligie, bei der die Sicherheit eine zentrale Rolle spielt.

Komponenten der IDnomic C-ITS PKI

IDnomic C-ITS PKI hält sich an europäische und US-Standards. Folgende Schlüsselkomponenten sind in dieser Lösung enthalten:

- *Root Authority*: Sie stellt die Zertifikate ihrer Sub-CAs, der Registration Authority und der Authorization Authority aus.
- *Registrierungsbehörde (EA)*: Wird verwendet, um Stationen zu registrieren und langfristige Zertifikate, sogenannte "Enrolment Certificates" (EC), auszustellen; sie empfängt die von der Autorisierungsbehörde gesendeten Validierungsanfragen und beantwortet diese.
- *Autorisierungsbehörde (AA)*: Stellt den Stationen kurzfristige Zertifikate aus, die als Autorisierungstickets (AT) bezeichnet werden, empfängt und beantwortet die von der Autorisierungsbehörde gesendeten Zertifikatsanfragen.
- *Distributionszentrum (DC)*: Verzeichnisdienst, der CA-Zertifikate, Teilnehmerzertifikate, Vertrauenslisten von Zertifikaten und Widerrufslisten zum Herunterladen bereitstellt.
- *Registrierungsbehörde (RA)*: Zentrale Stelle für die Validierung und Verteilung von Berechtigungen zwischen C-ITS-Stationen und CAs (nur für das US-PKI-Schema).



Vorteile für unsere Kunden

- Strikte Einhaltung der internationalen Standards von ETSI und IEEE
- Ausgereifte Lösungen – unser Produkt wird seit 2016 betrieben
- Überzeugende Ergebnisse bei internationalen Interoperabilitätstests
- Implementierungen – mehrere Pilotprojekte und Produkte, die weltweit implementiert wurden
- Zuverlässigkeit – IDnomic C-ITS PKI ist die Lösung, die von der JRC in Ispra, Italien, für die EU-Root-Certificate-Authority ausgewählt wurde.
- Skalierbarkeit/Elastizität – die Architektur ist mit jeder Cloud-Architektur kompatibel.
- Hohe Leistung und Sicherheit – Einsatz im Aktiv/Aktiv-Modus, einschließlich vollständiger HSM-Integration

Standards und technische Spezifikationen

- ETSI TS 102940, 102941 und 103097 für Europa
- IEEE 1609.2 und 1609.2.1 für Nordamerika

Weitere Informationen: www.idnomic.com

Soziale Medien

eviden.com