EVIDEN

IDnomic C-ITS PKI

La PKI pour un trafic connecté, plus intelligent et plus sûr

Dans un monde révolutionné par les TIC, les voitures et autres véhicules ont commencé à communiquer entre eux et avec l'infrastructure routière avec en ligne de mire les systèmes de conduite entièrement autonomes. Cela permet d'éviter de nombreux accidents, de réduire les embouteillages et de rendre le transport plus respectueux de l'environnement. Les technologies utilisées à cette fin sont appelées « systèmes de transport intelligents coopératifs » (Cooperative Intelligent Transport Systems, C-ITS) et reposent sur la communication entre les véhicules (V2V) ou l'infrastructure routière (V2I), résumées sous le nom de "vehicle-to-everything" (V2X).

.

Dans le contexte du C-ITS, tous les éléments actifs (« stations ») d'un système de transport communiquent entre eux. Une station représente généralement un véhicule ou un élément d'infrastructure, tel qu'un feu de signalisation. Une station peut être embarquée dans un véhicule (unité embarquée, OBU) ou déployée sur l'infrastructure routière (unité de bord de route, RSU).

Les normes internationales exigent une infrastructure à clé publique (PKI) spécifique, chargée de protéger la communication V2X et de la production des véhicules.

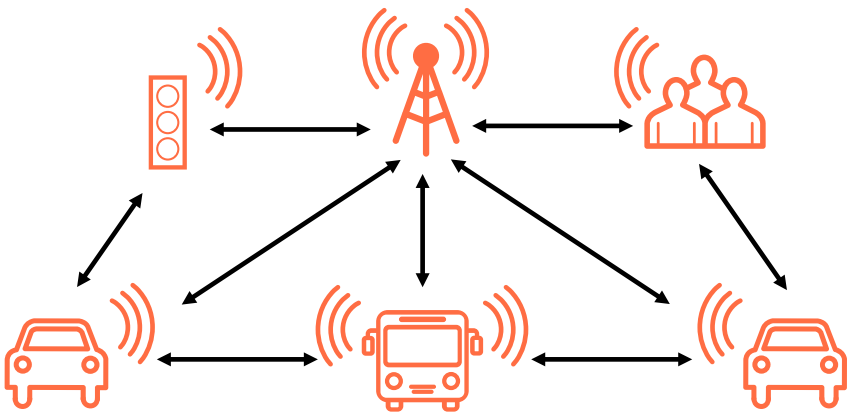
La sécurité joue un rôle central dans les C-ITS, car l'information (privée) et la sécurité physique sont des exigences obligatoires. Il convient de se concentrer sur l'un d'entre eux en particulier, notamment

- *Cybersécurité* : Les systèmes doivent être protégés contre les pirates informatiques, les terroristes et les autres criminels.
- *Utilisation contrôlée* : L'accès à des droits (permissions) d'utilisation doivent être validés.
- *Protection des données* : L'intégrité du contenu des messages doit être garantie.
- *Pseudonymisation et protection de la vie privée* : L'identité des stations doit être pseudonymisée pour empêcher que les véhicules soient tracés en suivant leurs messages signés par le C-ITS.

IDnomic C-ITS PKI est une suite logicielle spécialement conçue pour se conformer aux normes internationales pour les C-ITS et les V2X. Le format de certificat spécifié dans les normes IEEE et ETSI est basé sur des structures de données simples et optimisées pour que les stations puissent rapidement analyser et traiter un certificat.

Parmi d'autres références, IDnomic C-ITS a été choisie comme solution technique pour l'AC racine européenne, exploitée par le Centre Commun de Recherche (Joint Research Centre, JRC) de l'UE à Ispra, Italie.

IDnomic C-ITS PKI - Maturité, Performance et Conformité

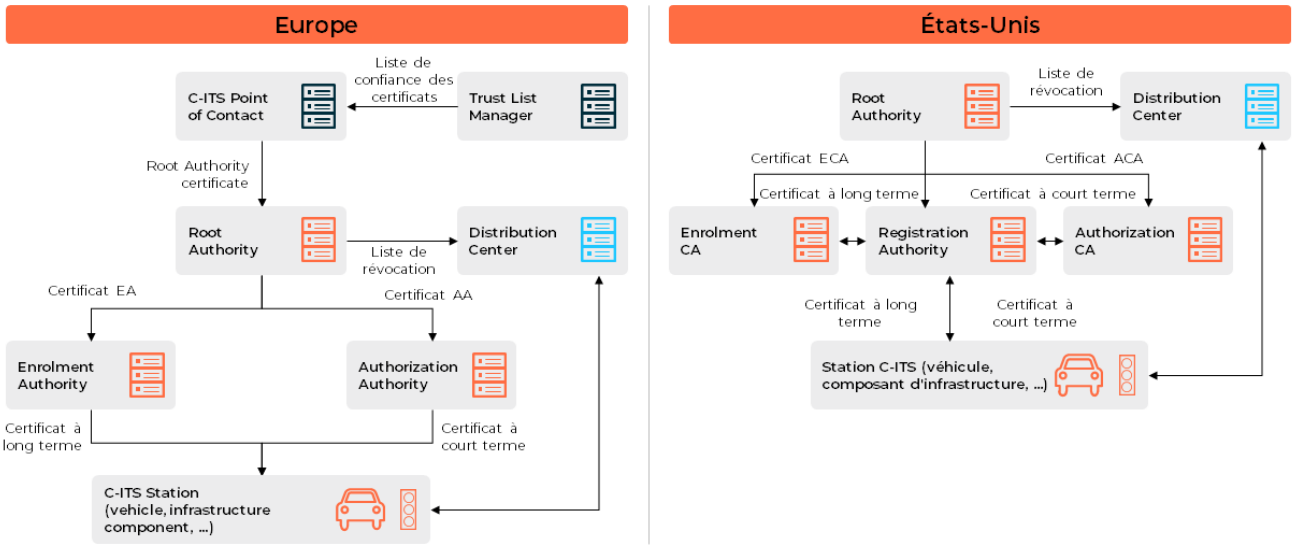


Les systèmes de transport intelligents coopératifs sont une technologie d'avenir importante, dans laquelle la sécurité joue un rôle central.

Composants de l'IDnomic C-ITS PKI

IDnomic C-ITS PKI se concentre sur une conformité rigoureuse par rapport aux normes européennes et américaines. Les composants clés suivants sont mis en œuvre :

- *Autorité racine* : Elle délivre les certificats de ses sous-AAC, les autorités d'inscription et d'autorisation.
- *Autorité d'inscription (EA)* : Utilisée pour enregistrer les stations et délivrer des certificats à long terme appelés "Enrolment Certificates" (EC), elle reçoit les demandes de validation envoyées par l'autorité d'autorisation et y répond.
- *Autorité d'autorisation (AA)* : Délivre aux stations des certificats à court terme appelés tickets d'autorisation (AT), reçoit et répond aux demandes de certificats envoyées par l'autorité d'autorisation.
- *Centre de distribution (DC)* : Service d'annuaire fournissant des certificats d'AC, des certificats d'abonnés, des listes de confiance de certificats et des listes de révocation à télécharger.
- *Autorité d'enregistrement (RA)* : Point central de validation et de distribution des autorisations entre les stations du C-ITS et les AC (uniquement pour le schéma PKI américain).



Les avantages clé pour nos clients

- Strictement conforme aux normes internationales ETSI et IEEE
- Solutions matures - produit exploité depuis 2016. Résultats probants lors des tests d'interopérabilité internationaux.
- Déploiements - Plusieurs pilotes et productions mis en œuvre dans le monde entier.
- Fiabilité - IDnomic C-ITS PKI est la solution choisie pour l'autorité de certification racine de l'UE par la JRC à Ispra, en Italie.
- Évolutivité/élasticité - Architecture compatible avec tous les architecture Cloud
- Haute performance et sécurité - Déploiement en mode actif/actif, y compris l'intégration complète du HSM

Normes et spécifications techniques

- ETSI TS 102940, 102941 et 103097 pour l'Europe
- IEEE 1609.2 et 1609.2.1 pour l'Amérique du Nord

En savoir plus sur nous: www.cryptovision.com

Connectez-vous avec nous

eviden.com