



Accès véhicule et partage de clés sécurisés

Partager l'accès au véhicule à travers une application smartphone

Les véhicules modernes utilisent diverses méthodes de contrôle d'accès basées sur des clés, pour limiter l'utilisation du véhicule aux seules personnes autorisées. Ces clés sont généralement soit des objets physiques, soit des données secrètes statiques comme un code PIN, soit un partage, via un smartphone, de clé hébergée sur un serveur. Chacune de ces méthodes présente plusieurs inconvénients, notamment des problèmes de sécurité importants.

CycurACCESS est une solution numérique de partage de clé du véhicule via le Smartphone à travers un système de gestion de permissions. Elle élimine le besoin de clés physiques et de porte-clés et ne nécessite pas de connectivité réseau pour le Smartphone ou le véhicule pour y accéder, éliminant ainsi la possibilité d'être bloqué dans des endroits isolés ou dans des zones sans couverture réseau.

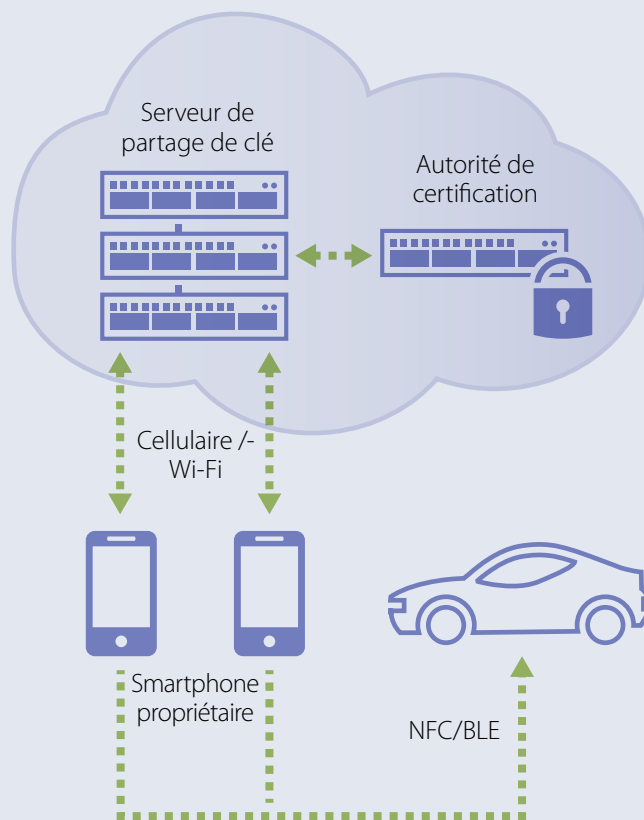
Cette solution utilise des traitements cryptographiques avancés basés sur l'infrastructure à clés publiques (PKI) pour assurer un niveau de sécurité élevé et son architecture réduit la menace représentée par des attaques de sécurité de type « man-in-the-middle ».

Toutes les identités numériques pour l'accès véhicule sont générées par le serveur de gestion de clés (KMS) d'ESCRYPT. Le KMS gère les identités et les autorisations pour l'accès et le partage de véhicules avec des tiers. Le KMS gère également l'enregistrement et les transferts de propriété du véhicule tout au long de son cycle de vie.

L'accès véhicule par l'application mobile CycurACCESS est totalement déconnecté et ne nécessite pas l'utilisation de l'infrastructure sécurisée. L'application mobile stocke les identités numériques pour l'accès véhicule hors ligne en toute sécurité et est également utilisée pour envoyer à des amis des invitations de partage de clé et gérer les autorisations de partage associées.

Caractéristiques du produit

- Ce système peut être redimensionné à grande échelle sans augmentation forte de l'infrastructure
 - Exploite l'infrastructure à clés publiques (PKI)
 - Chaque entité (utilisateur ou véhicule) ne nécessite qu'une seule paire de clé
- Les verrouillages de porte peuvent se faire complètement hors ligne car les contrôles ne nécessitent pas l'accès au serveur
- Conçu pour utiliser les protocoles de sécurité standard gouvernementaux et la cryptographie sur les courbes elliptiques efficace pour diminuer les besoins de ressources
- Le protocole de sécurité est indépendant de la couche de communication (NFC ou Bluetooth)
- Création d'identifiants pour l'application smartphone
 - Enregistrement avec le système de gestion de clés (KMS)
 - Chaque utilisateur enregistré reçoit un certificat de sécurité
 - Format de certificat M2M utilisant ECDSA 256
 - DOIT être enregistré pour pouvoir partager les clés
 - Toutes les clés sont signées avec des propriétés d'accès
- Création d'un module de recouvrement de clés
 - Comprend un élément sécurisé et stocke un certificat racine de partage de voiture
 - Capable de vérifier toutes les clés signées
- Accord sur les clés mutuellement authentifiées (NIST SP-800-56A, C(2e, 2s))
- Idéal pour les applications de gestion de flotte
 - Sociétés de covoiturage
 - Sociétés de location de voitures
 - Flottes commerciales



Vos avantages

- **Solution complète**
Solutions pour les équipements embarqués intégrés dans les véhicules et l'infrastructure routière ainsi que l'infrastructure de sécurité back-end
- **Facilité de déploiement et de gestion**
Un service clé en main qui évolue facilement, des petits déploiements initiaux à la production complète
- **Conformité aux normes**
Respect des normes nord-américaines et européennes
- **Hautes performances**
Des composants qui peuvent évoluer pour gérer des millions de véhicules et d'équipements routiers

