escrypt
SECURITY. TRUST. SUCCESS.

CycurACCESS

Secure Vehicle Access and Key Sharing

Share Vehicle Access with Anyone via a Smartphone App

Modern vehicles use a variety of key-based access control methods to restrict use of the vehicle to authorized persons only. These keys are normally either a physical object, or a static piece of secret knowledge such as a PIN code, or newer server-based key sharing via a smartphone. Each of these methods have several disadvantages including significant security issues.

CycurACCESS is a Smartphone based digital key sharing solution for vehicle access with the ability to share access by way of permissions. It removes the need for physical keys and key fobs and does not require network connectivity for the Smartphone or the vehicle in order to access, thus eliminating the potential for being stranded in remote locations or in areas with no cellular or data network coverage.

Advanced cryptographic operations based on Public Key Infrastructure (PKI) are used to provide a high level of security and the solution architecture reduces the threat posed by man-In-the-middle type of security attacks.

All digital identities for vehicle access are generated by ESCRYPT's Key Management Server (KMS). The KMS manages identities and permissions for third party vehicle access and sharing. The KMS also manages vehicle ownership registration and transfers through the lifecycle of the vehicle.

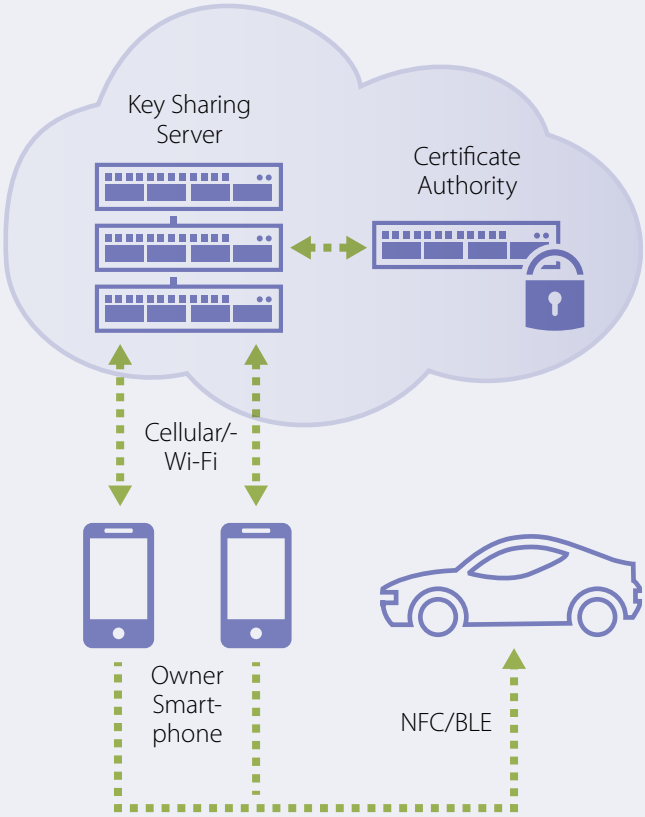
Vehicle access by the CycurACCESS mobile app is completely offline and does not require the use of the secure infrastructure. The mobile app securely stores digital identities for offline vehicle access and is also used to send key sharing invitations and sharing permissions to friends.

ESCRYPT 2018/05

escrypt
SECURITY. TRUST. SUCCESS.

Product Features

- This system can scale to very large sizes without massive increases in infrastructure
  - Leverage Public Key Infrastructure (PKI)
  - Each entity (user or vehicle) only requires a single key pair
- Locks can be completely offline as access verification does not require server access
- Designed to use Government Standard Security Protocols and efficient Elliptic Curve Cryptography for lower resource requirements
- Security protocol is independent of communication layer (NFC or Bluetooth)
- Establishing Credentials for Smartphone App
  - Registers with the Key Management System (KMS)
  - Every registered user is issued a security certificate
  - M2M Certificate Format utilizing ECDSA 256
  - MUST be registered to be able to share keys
  - All keys are signed objects with access properties
- Establishing Credentials Vehicle Capping Module
  - Includes a Secure Element and Stores Car Sharing Root Certificate
  - Able to verify all signed keys
- Mutually Authenticated Key Agreement (NIST SP-800-56A, C(2e, 2s))
- Ideally suited for Fleet Management applications
  - Car sharing companies
  - Rental car companies
  - Commercial fleets



Your Benefits

- **Complete Solution**
  Solutions for embedded on-board equipment in vehicles and roadside infrastructure as well as the backend security infrastructure
- **Easy to Deploy and Manage**
  Turnkey service that scales seamlessly from small early-stage deployments to full-production support.
- **Standards Compliant**
  Adhering to North American and European standards
- **High Performance**
  Components that can scale to manage millions of vehicles and road side equipment,