



セキュアな 車両アクセスと鍵共有

スマホアプリで誰とでも車両アクセスを共有

最近の車両は、さまざまな鍵をベースとしたアクセス制御を使用して、オーサライズされた人だけに車両の利用を制限しています。この鍵は目に見える鍵の場合もあれば、PIN 番号のような静的な暗号の場合、あるいは最近ではスマートフォンを利用したサーバベースの鍵共有の場合があります。いずれの方法もセキュリティ上の課題を抱えており、完璧とは言えません。

CycurACCESS は、スマートフォンをベースとして車両へのアクセスを許可するデジタル鍵共有ソリューションです。物理的な鍵やキー FOB を携帯する必要がなく、スマートフォンや車両がネットワークにアクセスする必要もないため、遠隔地や携帯の電波が届かない場所でも問題なくご利用いただくことができます。

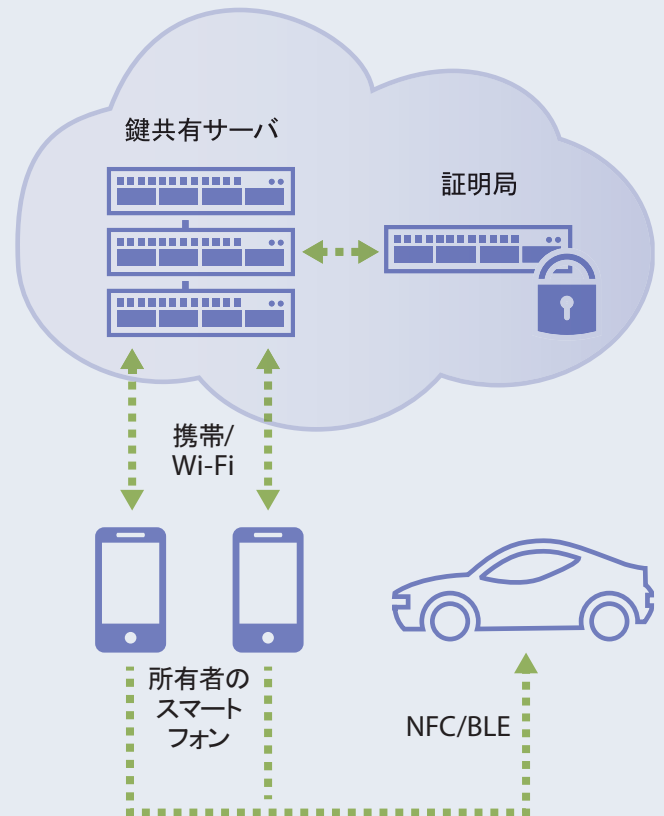
公開鍵基盤 (PKI) をベースとした先進的な暗号技術が、高いレベルのセキュリティを確保し、製品のソリューションアーキテクチャが、中間者攻撃といったセキュリティ攻撃からの脅威を低減します。

車両アクセス用のデジタル ID は ESCRYPT の鍵管理システム (KMS) で生成されます。KMS は車両をアクセス・共有するための ID とアクセス許可を管理します。KMS はまた、車両のライフサイクル全般において所有者の登録および変更を管理します。

CycurACCESS モバイルアプリによる車両アクセスは完全にオフラインで行われ、セキュアなインフラストラクチャを必要としません。モバイルアプリはオフラインの車両に安全にデジタル ID を格納し、鍵共有の招待と共有許可を、共有したい相手に送信します。

製品の特長

- 大規模なスケールアップにもインフラストラクチャの大きがかりな拡張は不要
 - 公開鍵基盤（PKI）を利用
 - 各エンティティ（ユーザまたは車両）が必要なのは単一のキーペアのみ
- アクセス認証はサーバアクセスを必要としないため、鍵は完全にオフライン
- 各国標準のセキュリティプロトコルに適合し、楕円曲線暗号の効率的な利用でリソース要件を低減
- 通信レイヤ（NFCまたは Bluetooth）に依存しないセキュリティプロトコル
- スマートフォンアプリ向けの資格情報を確立
 - 鍵管理システム（KMS）で登録
 - 登録された各ユーザにセキュリティ証明書を発行
 - ECDSA 256 を利用した M2M 証明書フォーマット
 - 鍵共有には登録が必要
 - すべての鍵はアクセスプロパティ付きの署名済みオブジェクト
- 車両モジュール向けの資格情報を確立
 - セキュアエレメントを内蔵し、車両共有ルート証明書を格納
 - 署名済み鍵をすべて検証可能
- 相互認証鍵規約（NIST SP-800- 56A, C(2e, 2s)）
- フリート管理アプリケーションに最適
 - カーシェアリング会社
 - レンタカー会社
 - 商用車



お客様の利点

- **トータルなソリューション**
車両の組み込みオンボード装置、路端のインフラおよびバックエンドのセキュリティインフラストラクチャ用ソリューション
- **容易な展開と管理**
初期の小規模な展開から量産まで、シームレスな拡張が可能なターンキーサービス
- **標準規格に準拠**
北米およびヨーロッパのセキュリティ標準規格に準拠
- **高性能**
車両および路側装置を数百万点まで拡張、管理可能なコンポーネント

