AutoCrypt® Digital Key

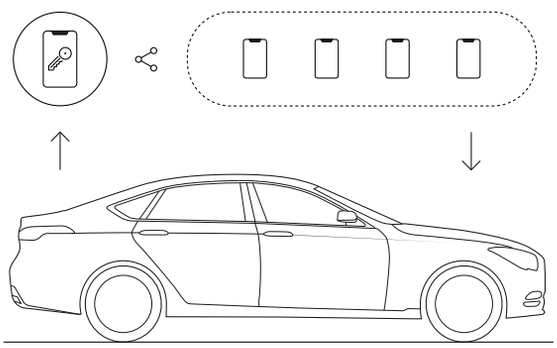
Secure, seamless vehicle access solution based on CCC 4.0 standards

AUTOCRYPT's Digital Key Solution provides a secure and interoperable lock-and-key system for vehicles, ensuring seamless operation across diverse mobile devices and vehicle platforms.

Ensuring Safe, Seamless Vehicle Access

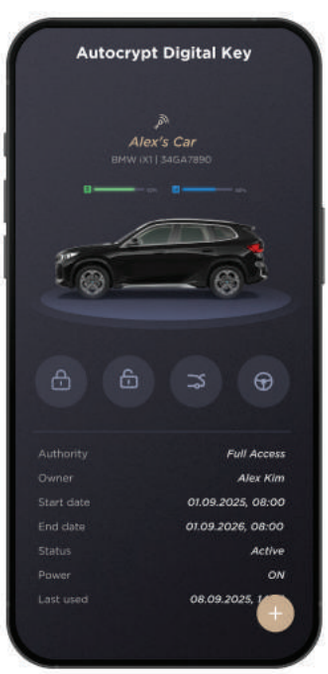
Digital Keys enable secure locking, unlocking, and access sharing for vehicles, operating across multiple stages of the vehicle lifecycle – from user registration to key sharing and key revocation.

AutoCrypt® Digital Key is a custom-developed solution based on the CCC Digital Key 4.0 standard, featuring a customizable high-security applet that strengthens credential protection and enables seamless integration with diverse OEM vehicle architectures and security policies.



Capabilities Complete Vehicle Access Control

Vehicle Access Control

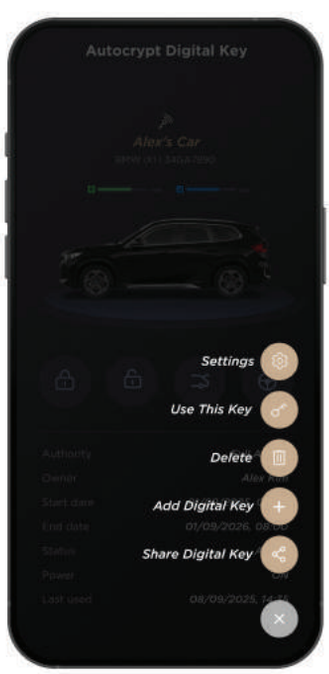


- Remote access and control of the vehicle as an owner or authorized shared user
- Seamless operation of vehicle functions including door access, engine start via smartphone

Key Registration and Sharing

- Easily register vehicle within the Digital Key app to activate key functionality
- Share keys with multiple users through secure credentials or invitation links

Restrictions and Settings



- Flexible owner-controlled settings for usage restrictions and permissions
- Configure access levels, sharing boundaries, and user-specific limitations

Benefits

Adaptable for OEMs, Fleet Operators and Users

Designed to meet diverse needs, the solution supports multiple deployment models to establish secure vehicle access infrastructure for OEMs, fleet operators and users, fully aligned with CCC Digital Key 4.0 standards for interoperability, scalability and data integrity.

OEMs

On-Premise Server Deployment

- Provides centralized, server-based control over key issuance and revocation
- Cloud-accessible via API and seamless integration with third-party services
- Compliant with CCC Digital Key 4.0 standard

Fleet Operators

Centralized Access Control

- Allows instant, automated key generation for drivers, optimizing large-scale fleet operations
- Enables remote, software-driven vehicle access control
- Consulting available for user and vehicle authentication workflow setup

Users

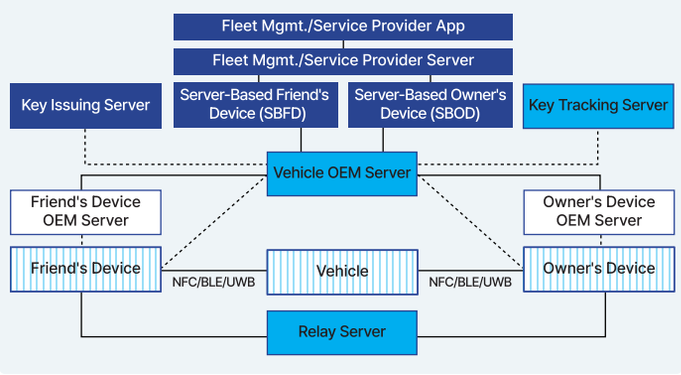
Simple Access Protection

- Offers immediate secure vehicle access without approval from owner
- Delivers a simplified, convenient experience for rentals, shared mobility, and temporary access scenarios
- Flexible key sharing options with peers and service providers

Infrastructure

Securing Vehicle-to-Device Communications

Based on a certificate-chain-of-trust authentication system for vehicle-to-device (V2D) communications, the solution supports secure communication channels between the Key Tracking Server, Vehicle OEM Server, Vehicle CCC Applet & Host API, and the Relay Server. Furthermore, using the key-sharing capabilities of the 4.0 servers, the solution enables server-generated keys, allowing third parties (such as fleet providers) to operate independently from the vehicle owner.



Legend: Full support, Partial support, Standardized, Proprietary
CCC Standard: CCC R4.0, CCC R3.0

Module (CCC R4.0)	Function
Fleet Mgmt. / Service Provider App	User Access Request and Vehicle Interaction
Fleet Mgmt. / Service Provider Server	Driver Assignment and Access Authorization
Server-Based Friend's Device	Temporary Key Retrieval and Access Execution
Server-Based Owner's Device	Primary Key Control and Permission Delegation
Key Issuing Server	Server-Based Digital Key Generation and Provisioning

Roadmap

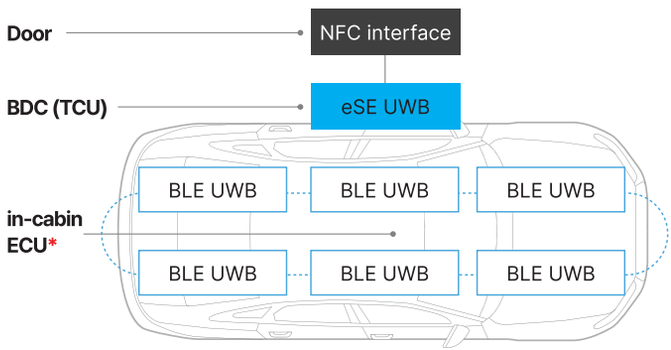
End-to-End Vehicle Security Architecture

AUTOCRYPT extends secure digital key operations across all layers of the vehicle security stack — from backend servers and authentication layers to in-vehicle key management and smartphone interface. AUTOCRYPT's solutions are consequently advancing through a structured roadmap, with additional features and communication layers to be strengthened.

As-is: Delivers owner pairing (BLE/NFC), key sharing, and key termination features, supported by URSK derivation & authentication

To-be: WCC1 (Door & Console NFC Trans.), WCC2 (BLE RKE Trans.), WCC3 (BLE+UWB Passive Entry & Start Trans.) features, complemented by Access Control/Logic layer (WCC3), and BLE data communication

Partner Integration: Capable of integrating partner-provided features (Key Localization and Gesture Detection), partner-based Localization Engine, UWB/BLE Anchors, UWB Radar, and Smartphone/Key functions



*in case of 6 UWB MCUs

APAC | Autocrypt Co., Ltd. | Seoul, South Korea | domestic@autocrypt.io
NORTH AMERICA | Autocrypt Inc. | San Jose, CA, USA | global@autocrypt.io
EUROPE | Autocrypt Technologies GmbH | Munich, Germany | europe@autocrypt.io

AUTOCRYPT