

Automotive KMI Solution

Comprehensive key management solution for vehicle production

AUTOCRYPT's Automotive KMI Solution provides an automated and standardized cryptographic key management system for automotive OEMs and suppliers, ensuring trusted authentication across every layer of the manufacturing lifecycle. The solution streamlines cybersecurity operations by supporting certificate issuance, key generation, and secure provisioning.

Secure, Automated Key Management for Vehicle Manufacturing

Automotive KMI centralizes certificate and key lifecycle management, overseeing secure generation, controlled distribution, and reliable storage through an integrated PKI-KMS middleware structure.

Composed of **AutoCrypt® PKI**, **AutoCrypt® KMS**, **AutoCrypt® KeyLink**, the solution delivers seamless key management aligned with modern automotive cybersecurity requirements such as FIPS PUB 186-2 and PKCS #11.

The system consists of three core components that establish an end-to-end chain of trust for automotive manufacturing.



AutoCrypt® PKI

Digital Certificate Issuance

- Issues and manages SSL/TLS digital certificates based on X.509 across Root, Sub, and Leaf CA structures
- Built on UNECE R155, ISO/SAE 21434 standards with unified dashboard visibility
- Provides flexible on-premise and SaaS deployment options



AutoCrypt® KMS

Key Generation, Storage Engine

- Generates high-entropy cryptographic keys using TRN/PRN with HSM-backed secure storage
- Compliant with ISMS (ISO/IEC 27001), PCI DSS and certified to FIPS 140-2 Level 3
- Enables centralized lifecycle operations with admin-friendly management tools



AutoCrypt® KeyLink

Key Distribution Middleware

- Manages certificate trust chains, key retrieval, and scheduled batch provisioning
- Supports firmware signing within the production process
- Integrates with *MES, **EOL, and diagnostic tools to enforce client-specific security policies

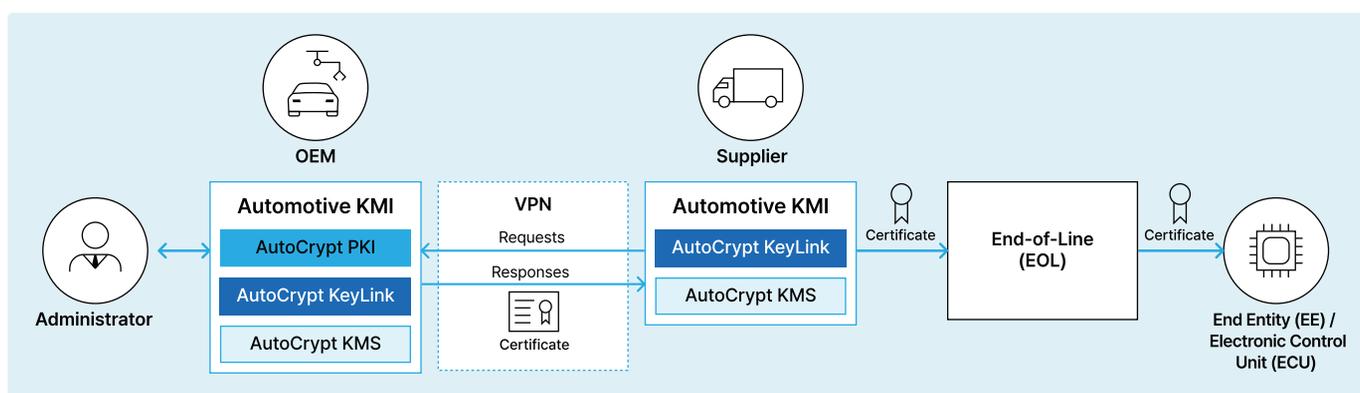
* MES: Manufacturing Execution System

** EOL: End-of-Line

Architecture

Securing Vehicle-to-Device Communications

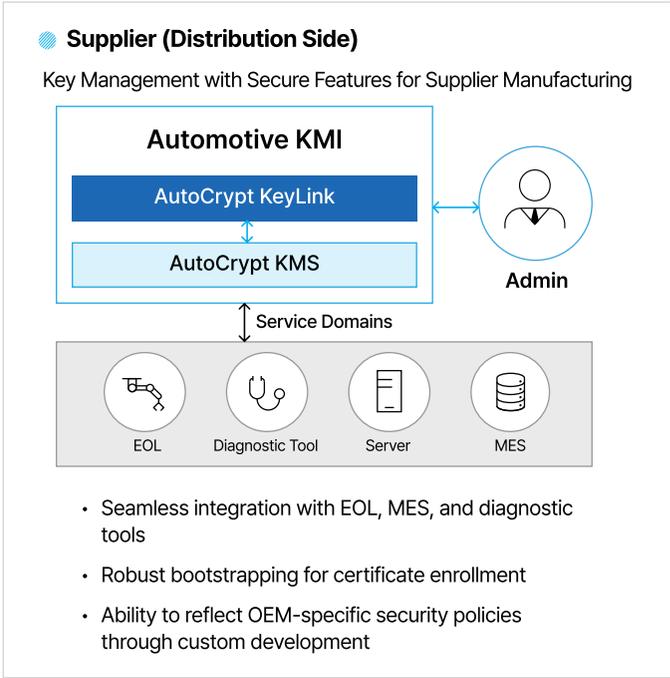
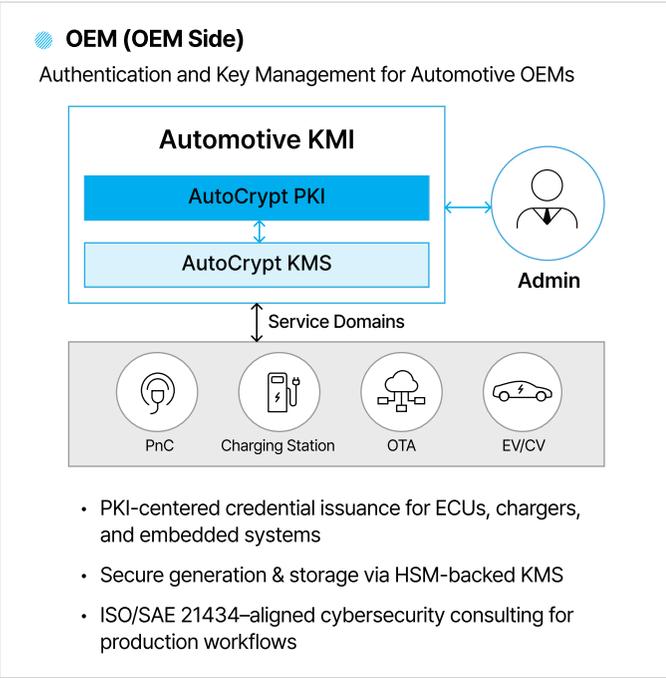
Automotive KMI provides a secure, production-ready credential pipeline that links OEMs and suppliers. Both parties can share a unified workflow that enables certificate issuance, distribution, and EOL validation for authenticated ECU key provisioning.



Benefits

Tailored for OEMs and Suppliers

Designed to support the full automotive supply chain, Automotive KMI provides a unified credential management foundation for both OEMs and suppliers, enabling secure, scalable, and production-ready key operations across a wide range of manufacturing environments.



Capabilities

Enhanced Usability and Flexibility

Combining advanced security functions with production-specific enhancements, Automotive KMI delivers flexible deployment options, an administrator-centered UX/UI, and ISO/SAE 21434-aligned consulting. This ensures secure, efficient, and policy-driven key management across diverse OEM and supplier environments.

● Differentiation Points

- Diverse deployment models: Supports both on-premise and SaaS deployment models
- Administrator-centered UX/UI: Intuitive monitoring, batch management, and maintenance workflows
- Production-site consulting: ISO/SAE 21434-aligned architecture and policy design adapted to EOL environments

