Fully managed cryptography service for automotive use cases **ESCRYPT Automotive Key Management Platform**

Automotive key management for software-defined vehicles

Enabling seamless communication between vehicles and automotive backends is essential for unlocking innovative features in the transition to the software-defined vehicle (SDV). Authenticity and confidentiality are crucial for secure data exchange, particularly in over-the-air updates and cloud services. Implementing secure key management, however, poses challenges, requiring a system that spans the entire lifecycle of a diverse vehicle fleet and complies with evolving safety and security regulations.

Managing all cryptographic challenges with one solution

To address all these demands, ETAS offers the ESCRYPT Automotive Key Management Platform. This managed, scalable cryptography Software-as-a-Service (SaaS) provides a comprehensive solution for various use cases, such as signing and encrypting vehicle software and firmware files.

By utilizing the platform, you can efficiently achieve your security objectives while cost-effectively outsourcing complexity to an external partner with decades of cybersecurity expertise and a proven solution.

Highly reliable, available, and scalable

The ESCRYPT Automotive Key Management Platform seamlessly integrates into native IT environments and product lifecycle solutions, offering full management with high reliability and availability. Additionally, it adheres to common standards such as ISO 27001 and addresses all security use cases for SDVs.

Field proven
Used for millions of ECUs and vehicles

Globally available
Fully managed key management (SaaS)

Easy integration
into existing software lifecycle mgmt. systems

Specialized
for automotive security use-cases

ESCRYPT Automotive Key Management Platform at a glance

Software Development	Software Update	Vehicle Communications	Digital Services/ Access
Container Signing	Encryption of Firmware	Securing communication in vehicle networks	Locking and unlocking devices/vehicles
Code Signing	Signing of Firmware/Hash	Securing vehicle external communication using certificates	Accessing/Authorization of digital services like charging

Setups and use cases

- Digital Signing – Ensures that only authentic software / configurations can be deployed on ECUs/vehicles/fleets
- Digital Certificates and Device Specific Keys – Enables secure communication within and beyond the vehicle, e.g. SecOC, cloud connectivity, smart charging
- Digital Access Codes – Ensures that only authorized users/devices (e.g., testers) get access, e.g. for diagnostic services or telematics
- Encryption – Prevents eavesdropping
- Secure key injection and update – Supports end-to-end authentication and encryption of key material

Features & supported protocols

- Asymmetric key and X.509v3 certificate creation including management following RFC 5280
- Certificate revocation management with CRL and OCSP following RFC 6818 and RFC 6960
- Signing and encryption of software and firmware files supporting CMS following RFC 5652
- Signing of software and firmware files or hash values supporting CMS following RFC 5652
- Export of symmetric file encryption key encrypted with a public key of a certificate of the target device supporting CMS following RFC 5652
- Symmetric key and password creation / derivation including management
- AUTOSAR Secure Hardware Extension (SHE)
- Keyless Entry certificates following Car Connectivity Consortium (CCC) Digital Key Specification
- User Management with multi-factor authentication with the option to connect the customer's identity provider
- Role-based access control
- Fine-grained assignment of cryptographic material permission to users

Your benefits with ESCRYPT Automotive Key Management Platform

- Completely managed key management service covering all SDV security use cases
- Easy integration into native IT environments and product lifecycle solutions
- Fully managed with high reliability and availability
- Compliant with common standards like ISO 27001
- Already in use in millions of devices
- ETAS cybersecurity experts provide comprehensive support to individualize all parameters according to your needs

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/key-management-platform

ETAS/COM2_AS/06/2024