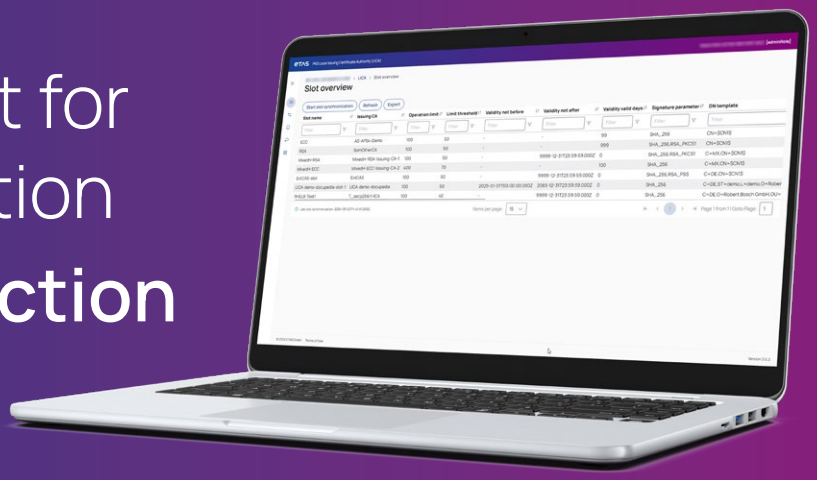
Empowering Tomorrow's Automotive Software
www.etas.com

Central key management for secure key injection **ESCRYPT Production Key Platform**



Maximizing efficiency and reliability in key management for automotive production

In today's fast-paced manufacturing environment, the increasing complexity of electronics and the critical need for secure data make robust key management essential, particularly for automotive production. This is where the **ESCRYPT Production Key Platform** comes into play, addressing the major challenges in key management: safeguarding sensitive data, protecting against cyber threats, and ensuring smooth, error-free processes. These capabilities help OEMs and Tier-1 suppliers remain competitive and protected in a rapidly evolving market.

Areas of application

- Secure communication within the vehicle's internal network: ECUs must be provisioned with symmetric cryptographic keys to protect network messages
- Secure external communication to the OEM backend or third-party backends: Equipping the vehicle with digital certificates enables secure connection and authentication
- Secure access: Ensure that only authorized machines and users get access to device interfaces, e.g. for diagnostics or software flashing
- Secure data distribution: Transport third party cryptographic keys or data securely to production plants

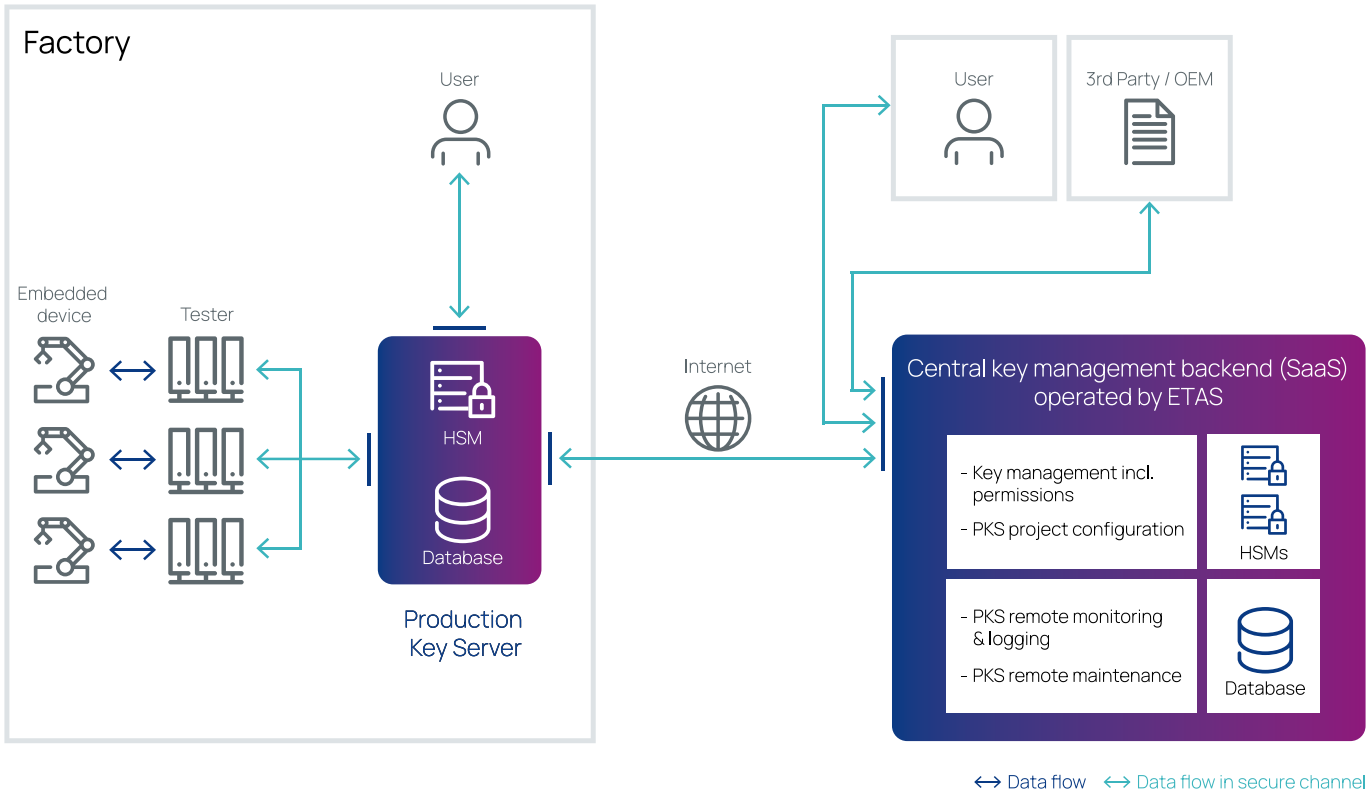
Features

- Generate device specific symmetric keys with key sizes 128, 192 and 256 bit
- Generate device specific asymmetric keys, e.g. RSA keys
- Support key format of AUTOSAR Secure Hardware Extension (SHE)
- Issue X.509 device certificates following RFC 5280 with a wide support for cryptography
- Provide cryptographic functions, such as digital signatures, to implement secure access protocols

Benefits

- **High availability**: Operation is guaranteed by the Production Key Server despite internet disruptions
- **Fast and easy scalability**: Many production plants can be served by one central key management platform
- **Maximum security**: HSM technology and end-to-end key protection provide a very high level of security
- **Seamless integration**: Ensures interoperability with existing plant IT infrastructure and various third-party key management backends

Architecture of the end-to-end key management solution



The ESCRYPT Production Key Platform provides comprehensive key management, including key/certificate injection, for high-volume ECU production across multiple lines. The core of the solution is the Production Key Server (PKS), which incorporates a cutting-edge hardware security module (HSM) for secure storage of sensitive data. A central key management backend also distributes keys to the PKS and securely forwards data to both the PKS and customer backends.

Production Key Server (PKS)

Core elements

- HSM: A physical device that securely generates, stores, and manages cryptographic material
- Database: A system that stores and manages the relevant certificates

Technical functions

- Hosting and handling of cryptographic material
- Distribution of cryptographic material to connected production lines
- Generation of device certificates
- Generation of cryptographic keys
- Signing data cryptographically

Central Key Management Backend

Core elements

- Two HSMs: The physical devices, which securely generate, store, and manage cryptographic material
- Database: A system that stores and manages the relevant certificates

Technical functions

- Establish connection to third-party/OEM backend
- Distribute cryptographic material and parameters to the PKS
- Upload data to the third-party/OEM backend
- Manage permissions
- Manage keys
- Monitor, log, and maintain the PKS remotely

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

Further product information:
etas.com/escrypt-production-key-platform

ETAS/COM2_FS/05/2025