Security in ECU Production

AUTHOR

Norbert Bißmeyer is Security Engineer at **ESCRYPT GmbH** in Bochum, Germany.

ESCRYPT is a 100-percent subsidiary of ETAS GmbH and offers security solutions for embedded systems.

Production Key Server for secure key management

Cryptography protects connected embedded systems against attacks and unauthorized access. However, ensuring availability and secure injection of keys is a challenge – particularly in global production chains. To secure ECU production to the greatest extent possible, ESCRYPT offers its new Production Key Server (PKS). This easy-to-implement, scalable solution complements ESCRYPT's Key Management Solution (KMS) and guarantees reliable protection of sensitive cryptographic data over the entire system lifecycle.

Embedded systems are taking on more and more functions. The large number of ECUs in vehicles is a prime example, with their software coordinating more and more powertrain, safety, and convenience functions. Previously, IT systems in vehicles were isolated and independent. Now it is time to provide connectivity with the outside digital world in order to take advantage of the security and service potential of Car-to-X communication, or of Firmware-over-the-Air updates (FOTA).

Opening up to the outside world harbors not only opportunities, but also new security risks. Negligent or willful tampering with embedded systems in vehicles will become possible if we fail to protect them reliably. Permission for digital data exchange must be made dependent on an appropriate authentication with cryptographic keys and certificates. However, providing and implementing these keys and certificates in production, as well as managing them over the entire life of the protected products, is challenging – especially in business areas that rely on globally distributed production and supply chains and on a diverse array of supplier structures, such as the automotive industry.

Decentralized or centralized key provisioning?

To date, there have been parallel approaches that either decentralize the provisioning of cryptographic data (keys, certificates, etc.) or manage it from a central location. Neither solution is perfect. The advantage of isolated, decentralized solutions for each production site is that they can be implemented easily and are independent from higher-level IT systems. Additionally, key availability is high and does not depend on the quality of the local internet connection. However, the security and maintenance overhead of decentralized solutions is high. In addition, it is difficult for device manufacturers to maintain an overview of the keys generated and assigned, especially when some of the keys are generated in the manufacturers' own plants and some by suppliers. Conversely, centralized solutions offer advantages in terms of key management and security issues. However, if the internet connection fails or transfer rates are suboptimal, there is a risk of longer latency times when injecting the keys, potentially resulting in delays or even production downtimes.

The solution: decentralized servers and centralized backend

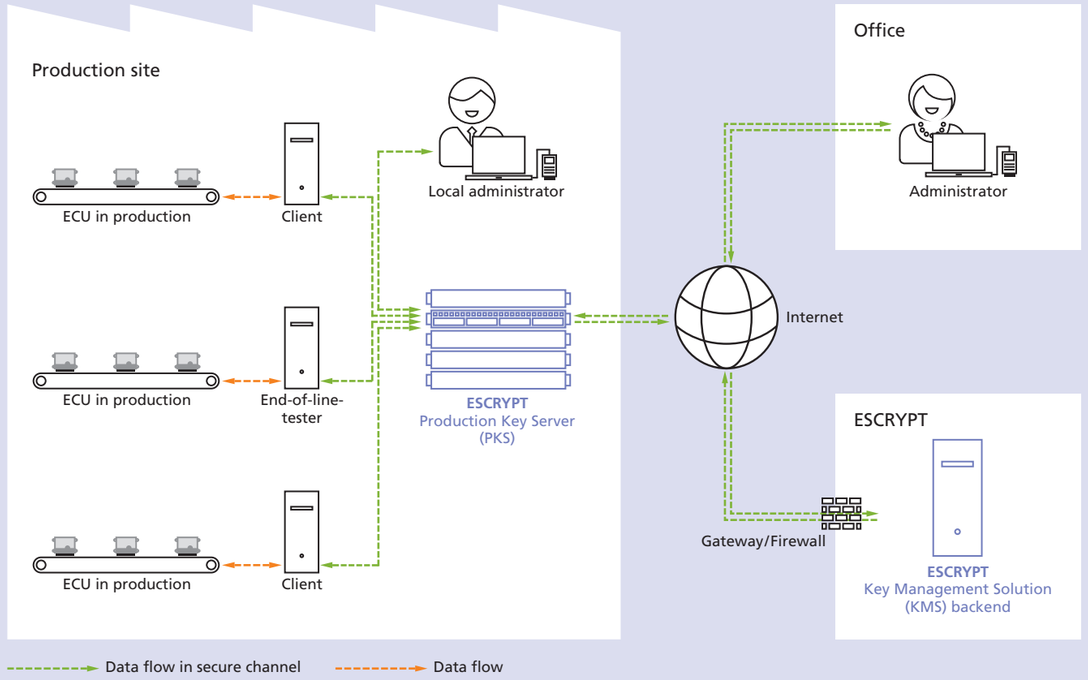
ESCRYPT is following a third path, which combines a centralized backend – the Key Management Solution (KMS) – with decentralized key injection on Production Key Servers (PKS) in the plants. This guarantees not only maximum availability and low latency times, but also optimum protection of cryptographic data, as every PKS is protected against unauthorized access by a powerful Hardware Security Module (HSM) that is suitable for industrial use, and appropriate security software. Furthermore, since the PKSs are only occasionally in contact with the backend – to synchronize the data and perform updates – this approach offers the greatest possible independence from the internet connection. The frequency of this exchange is adjustable.

The PKS is a standardized module for server racks and has its own power connection, Gigabit Ethernet interfaces, an HSM, and pre-installed ESCRYPT software. After a one-time configuration, it is ready for operation. Maintenance and administration can be done online through the KMS backend. If desired, PKSs can automatically report – for instance by e-mail – critical events such as expiring certificates, key access authorizations, full log databases, or a shortage of cryptographic data in local buffers.

While the servers are distributed across production sites around the world, management and monitoring of key assignment, as well as maintenance and configuration of the PKSs, is handled in the centralized KMS backend. If cryptographic data from another source is to be used in production, this data can be manually imported into the KMS backend. Another option is to use the backend of a third party that can connect through authentication directly to the KMS to exchange the relevant cryptographic material. Since the PKS and the KMS backend synchronize at specified intervals, thus creating sufficient buffers of cryptographic data, ECU manufacturers are largely independent from internet connection stability when accessing the KMS.

The flexible architecture ensures that manufacturers can either maintain control over key management themselves or have ESCRYPT implement the key management. In both cases, the connection between the KMS and the distributed servers forms a powerful basis on which the PKS hardware can execute complex cryptographic operations quickly and reliably. PKSs can also be operated in clusters. Importantly, they offer maximum protection – also against intellectual property theft – in production environments where providing an adequate level of security is an issue. With confidential data (such as security keys for authorized associates) stored on the HSM, and their retrieval tied to previously determined routines and authentication on the KMS, data will remain inaccessible even if the entire PKS hardware is stolen. Furthermore, the HSM serves as a safe for cryptographic data installed on the systems; it secures this data through additional encryption and a security check when booting up. On top of all this, firewalls, encryption, tamper-proof software, and HSM-based security operations protect each individual step when data is exchanged between servers, the backend, and all other recipients involved in the process.

Production Key Server (PKS)
Keys/Certificate injection



Holistic security solutions are needed

These security precautions and the sophisticated architecture ensure that typical automotive use cases – such as secure booting of microcontrollers, locking of diagnostic interfaces, and injection of Secure Hardware Extension (SHE) keys or Transport Layer Security (TLS) certificates – remain secure even in the increasingly connected car of the future. This also applies to securing future Car-to-X communication and final testing of ECUs that require testers to authenticate themselves. The security achieved in this way can be maintained over the entire life of the vehicle – using ESCRYPT's holistic approach for embedded security. While PKSs ensure secure management and injection of cryptographic data in ECU production, embedded systems need to be protected over the entire vehicle lifecycle to prevent willful or negligent tampering. ESCRYPT has the appropriate security solutions and the required expertise for all stages of the vehicle's lifecycle, including reliable deletion of keys and certificates after vehicles are scrapped.

The flexible solution architecture for securing distributed production sites for ECUs guarantees maximum availability, low latency times, and optimum protection of the cryptographic data used.