Digital vaccination for the ECU

IT security for networked vehicles starts with ECU production

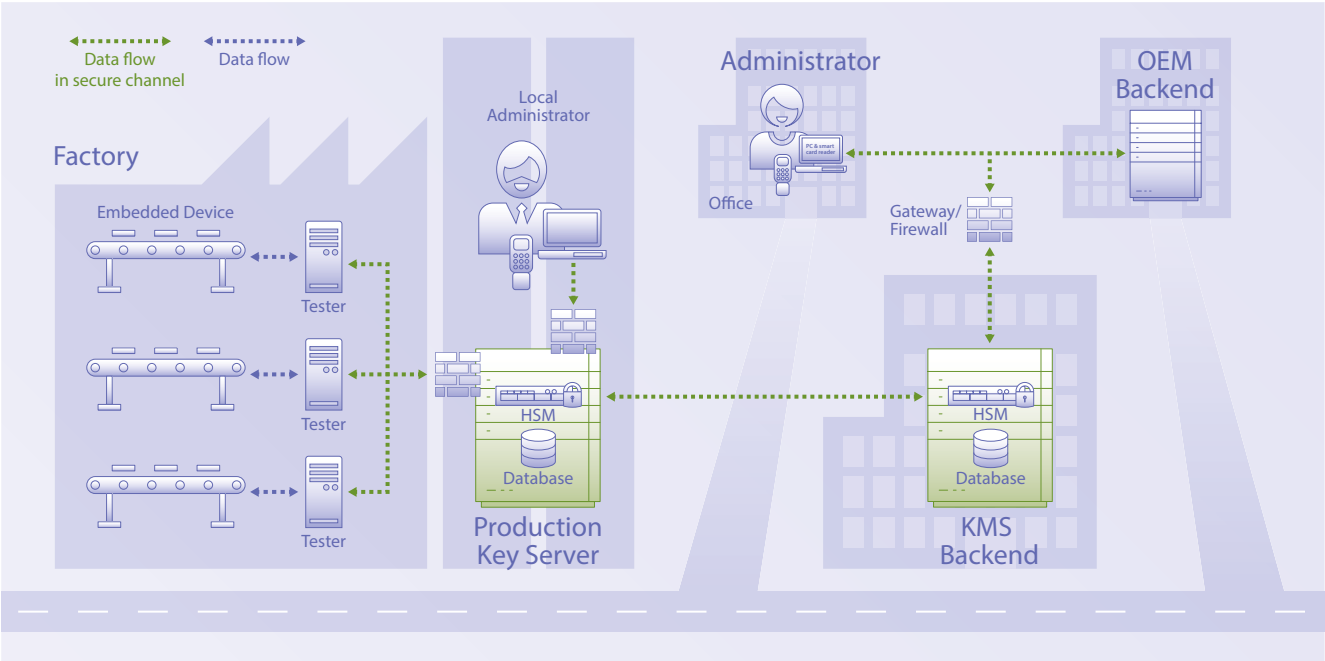
How can the cryptographic key material necessary for secure data exchange be introduced into the ECUs securely and according to requirements? The answer is an integrated solution consisting of a central key management backend and decentralized production key servers.

When it comes to protecting against cyber attacks, the control units in the vehicle play a key role – in the truest sense of the word: only cryptographic keys enable ECUs to authenticate themselves and thus legitimize data exchange within the electrical system as well as with the outside world. The special challenge here is that the ECUs for the various vehicle platforms must initially be supplied with OEM-specific key material and certificates – and ideally during their production by the ECU manufacturer.

Secure distribution of OEM key material

The effective solution combines a classic key management solution (KMS) as the central backend with decentralized production key servers (PKS) that are installed in the production facilities and communicate with the KMS. This is of benefit to the OEM because it means the process of equipping the OEM's specific ECUs with its own key material can be fully integrated into the ECU supplier's existing production infrastructure.

First, the KMS is fed the data packets with the key material provided by the respective car manufacturer. The key material is stored centrally, distributed via secure data transfer as needed among production sites, and stored on production key servers in readiness (see Figure).



Integrated key distribution and injection with key management solution and production key server.

Key insertion via end-of-line tester

The key material is introduced into the ECUs on site during production by connected end-of-line testers. These then retrieve the individual key packages from the production key server in the plant and "inject" them – like a "digital vaccination" – into the individual ECUs during production. At the same time, the PKS logs which cryptographic keys have been introduced into each ECU. Finally, on request, the PKS sends back what are known as verification files from production via the central KMS backend to the OEM. This gives automotive manufacturers certainty that the ECUs are correctly equipped with key material.

The solution combines high security and availability.

Secure storage without permanent online connection

A particular advantage of the solution is the symbiosis of high security and availability. The production key servers are protected against unauthorized access both by a robust and powerful hardware security module (HSM) and by their own security software. In addition, the PKS make contact with the backend only from time to time to synchronize data, carry out any updates, and create sufficient buffers with cryptographic data. This means that they are not dependent on a permanently stable internet connection, which means they are largely immune to potential online attacks.

Users can freely determine how often contact should be made with the KMS backend as required. If the stock falls below a predefined minimum quota, new keys are automatically requested from the server. This ensures that there is always enough key material available for equipping the ECUs in production, which precludes a potentially costly production outage due to an interrupted network connection. The production key server always remains operational.

In use worldwide in ECU production

Secure and precise ECU data assignment with cryptographic keys forms the basis for almost all other in-vehicle IT security functions. The integrated KMS-PKS solution makes it possible to master the complex delivery mechanism for OEMs' cryptographic material, from secure key management to secure storage and injection of the key material into the ECUs and, finally, logging and verification. For good reason, today this process is used worldwide in ECU production for various automotive manufacturers. ■

Authors

Christian Wecker is Product Manager PKS at ESCRYPT.
Michael Lueke is Senior Program Manager KMS at ESCRYPT.