# Digitale Schutzimpfung für das Steuergerät

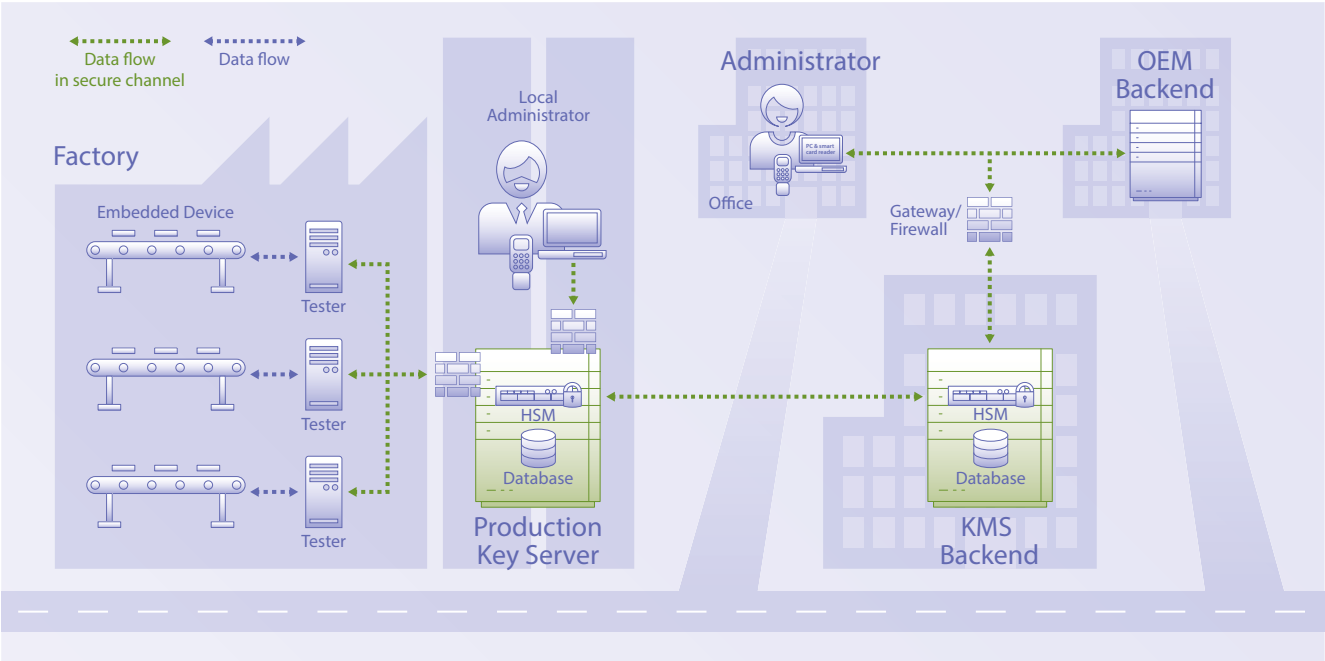
## IT-Security für das vernetzte Fahrzeug beginnt in der Steuergeräteproduktion

**Wie kann das für einen sicheren Datenaustausch notwendige kryptografische Schlüsselmaterial anforderungsgerecht in die ECUs eingebracht werden? Die Antwort liefert eine integrierte Lösung aus zentralem Key Management Backend und dezentralen Production Key Servern.**

Beim Schutz vor Cyberangriffen kommt den Steuergeräten im Fahrzeug im wahrsten Sinne des Wortes eine Schlüsselrolle zu: Erst kryptografische Schlüssel erlauben es den ECUs, sich zu authentifizieren und damit den Datenaustausch innerhalb des Bordnetzes, aber auch nach außen hin zu legitimieren. Die besondere Herausforderung dabei: Die Steuergeräte für die verschiedenen Fahrzeugplattformen müssen initial mit dem OEM-spezifischen Schlüsselmaterial und Zertifikaten versorgt werden – und das idealerweise bereits bei deren Produktion durch den ECU-Hersteller.

### Sichere Distribution des OEM-Schlüsselmaterials

Die probate Lösung liegt in einer Verbindung aus klassischem Key-Management-System (KMS) als zentralem Backend und mit dem KMS kommunizierenden, dezentral installierten Production Key Servern (PKS) in den Produktionsstätten. Vorteil für den OEM: Die Bestückung seiner spezifischen elektronischen Steuergeräte mit dem eigenen Schlüsselmaterial lässt sich vollständig in die bestehende Produktionsinfrastruktur des ECU-Zulieferers integrieren. Dabei werden die Datenpakete mit dem vom jeweiligen Autohersteller bereitgestellten Schlüsselmaterial in das KMS eingespeist.




Integrierte Key Distribution und Injection mit Key Management Solution und Production Key Server.

Das Schlüsselmaterial wird zentral gespeichert, per sicherer Datenübertragung bedarfsgerecht an die Produktionsstandorte verteilt und dort auf Production Key Servern bevorratet (siehe Bild).

### Einbringen der Schlüssel per End-of-Line-Tester

Das Einbringen des Schlüsselmaterials in die Steuergeräte erfolgt vor Ort in der Fertigung durch angebundene End-of-Line-Tester. Diese rufen die einzelnen Schlüsselpakete dann beim Production Key Server im Werk ab und „injizieren" sie – einer „digitalen Schutzimpfung" gleich – während der Produktion in die einzelnen Steuergeräte. Gleichzeitig protokolliert der PKS, welche kryptografischen Schlüssel in welche ECU eingebracht wurden. Auf Wunsch werden abschließend sogenannte Verification Files aus der Fertigung vom PKS über das zentrale KMS-Backend zum OEM zurückgespielt. Der Autohersteller hat so die Gewissheit, dass die Fahrzeugsteuergeräte mit seinem Schlüsselmaterial korrekt bedatet sind.

### Sichere Bevorratung ohne ständige Online-Anbindung

Besonderer Vorteil der Lösung ist die Symbiose aus hoher Sicherheit und Verfügbarkeit. Denn die Production Key Server sind sowohl durch ein robustes und leistungsfähiges Hardware-Sicherheitsmodul (HSM) als auch durch eigene Sicherheitssoftware vor unerlaubtem Zugriff geschützt. Zudem treten die PKS nur von Zeit zu Zeit in Kontakt mit dem Backend, um den Datenbestand zu synchronisieren, etwaige Updates vorzunehmen und ausreichende Puffer mit kryptografischen Daten anzulegen. Das heißt, sie sind nicht auf eine permanent stabile Internetanbindung angewiesen und so vor potenziellen Online-Attacken weitgehend gefeit.

Wie oft die Kontaktaufnahme zum KMS-Backend erfolgen soll, können die Nutzer bedarfsgerecht bestimmen. Sinkt der Bestand unter ein vorgegebenes Mindestkontingent, werden vom Server automatisch neue Schlüssel angefordert. Auf diese Weise ist gewährleistet, dass stets genügend Schlüsselmaterial für die Bestückung der Fahrzeugsteuergeräte in der Fertigung vorrätig ist. Ein potenziell kostspieliger Produktionsausfall durch eine unterbrochene Netzwerkverbindung ist ausgeschlossen. Der Production Key Server bleibt stets einsatzbereit.

### Weltweit in der ECU-Produktion im Einsatz

Eine sichere und präzise Bedatung von Fahrzeugsteuergeräten mit kryptografischen Schlüsseln bildet das Fundament für nahezu alle weiteren IT-Sicherheitsfunktionen im Fahrzeug. Die integrierte KMS-PKS-Gesamtlösung ermöglicht es, den komplexen Auslieferungsmechanismus von kryptografischem Material des OEM über ein sicheres Key Management, die sichere Bevorratung und Injektion des Schlüsselmaterials in die ECUs bis hin zur Protokollierung und Verifikation zu meistern. Aus gutem Grund ist dieses Verfahren heute weltweit bei der Steuergeräteproduktion für verschiedene Automobilhersteller im Einsatz. ■

### Autoren

**Christian Wecker** ist Product Manager PKS bei ESCRYPT.
**Michael Lueke** ist Senior Program Manager KMS bei ESCRYPT.