Security in der Steuergeräteproduktion

AUTOR

Norbert Bißmeyer ist Security Engineer bei der **ESCRYPT GmbH** in Bochum.

ESCRYPT ist eine hundertprozentige Tochtergesellschaft von ETAS und bietet Sicherheitslösungen im Bereich Embedded Systeme an.

Production Key Server für sicheres Key Management in der Fertigung

Kryptografie schützt vernetzte Embedded Systeme vor Angriffen und unbefugten Zugriffen. Doch gerade in globalen Fertigungsketten ist es eine Herausforderung, die Verfügbarkeit und das sichere Einbringen der Schlüssel zu erreichen. Um die Steuergeräteproduktion bestmöglich abzusichern, bietet ESCRYPT den neuen Production Key Server (PKS) an. Die leicht implementierbare, skalierbare Lösung vervollständigt die Key Management Solution (KMS). Damit ist verlässlicher Schutz der sensiblen Kryptografiedaten über den Gesamtlebenszyklus der Systeme hinweg gewährleistet.

Embedded Systeme übernehmen immer mehr Funktionen. Bestes Beispiel ist die hohe Zahl an Steuergeräten in Automobilen, deren Software immer mehr Antriebs-, Sicherheits- und Komfortfunktionen koordiniert. Bisher waren IT-Systeme in Fahrzeugen geschlossen. Nun steht Vernetzung mit der digitalen Außenwelt an, um Sicherheits- und Servicepotenziale der Car-to-X-Kommunikation oder von Firmware-Over-the-Air-Updates (FOTA) zu erschließen. Neben Potenzialen birgt die Öffnung für die Außenwelt neue Sicherheitsrisiken. Fahrlässige oder mutwillige Eingriffe in Embedded Systeme im Fahrzeug werden möglich, wenn es nicht gelingt, diese zuverlässig abzuschirmen. Die Erlaubnis zum digitalen Datenaustausch muss an eine entsprechende Authentifizierung mit kryptografischen Schlüsseln und Zertifikaten gekoppelt sein. Doch sind sowohl die Bereitstellung und Implementierung dieser Schlüssel und Zertifikate in der Produktion als auch deren Verwaltung über die Gesamtlebensdauer der geschützten Produkte hinweg eine Herausforderung. Das gilt erst recht in Branchen, die wie die Automobilindustrie auf global verteilte Fertigungs- und Lieferketten sowie auf vielfältige Zuliefererstrukturen setzen.

Dezentrale oder zentrale Schlüsselbereitstellung?

Es gibt bisher parallele Ansätze, die das Bereitstellen kryptografischer Daten (unter anderem von Schlüsseln und Zertifikaten) wahlweise dezentralisieren oder es von einer Zentrale aus abwickeln. Beides birgt Probleme. Isolierte Lösungen für jede Produktionsstätte haben den Vorteil, dass sie leicht implementierbar und unabhängig von übergeordneten IT-Systemen sind. Auch die Verfügbarkeit der Schlüssel ist hoch und hängt nicht von der Güte der Internetverbindung vor Ort ab. Doch dafür ist der Sicherheits- und Wartungsaufwand der dezentralen Lösungen hoch. Und für Gerätehersteller ist es schwer, den Überblick über die dezentral vergebenen Schlüssel zu behalten. Erst recht, wenn sie teils in eigenen Werken und teils von Zulieferern erzeugt werden. Umgekehrt haben zentralisierte Lösungen bei Schlüsselverwaltungs- und Security-Fragen Vorteile. Doch beim Ausfall der Internetverbindung oder suboptimalen Übertragungsraten drohen höhere Latenzzeiten beim Einbringen der Schlüssel – woraus Verzögerungen oder sogar Produktionsausfälle resultieren können.

Dezentrale Server und zentrales Backend sind die Lösung

ESCRYPT geht daher einen dritten Weg, der ein zentrales Backend – die Key Management Solution (KMS) – mit der dezentralen Schlüsseleinbringung auf Production Key Servern (PKS) in den Werken verbindet. Dies garantiert höchste Verfügbarkeit, geringe Latenzzeiten und obendrein optimalen Schutz der kryptografischen Daten. Denn jeder PKS ist durch ein leistungsfähiges industrietaugliches Hardware Security Module (HSM) und entsprechende Sicherheitssoftware gegen unbefugte Zugriffe abgeschirmt. Zudem bietet dieser Ansatz größtmögliche Unabhängigkeit von der Internetanbindung. Denn PKS treten nur von Zeit zu Zeit mit dem Backend in Kontakt, um den Datenbestand zu synchronisieren und Updates vorzunehmen. Die Frequenz dieses Austauschs ist variabel einstellbar.

Beim PKS handelt es sich um ein standardisiertes Modul für Server-Racks, das über einen eigenen Stromanschluss, Gigabit-Ethernet-Schnittstellen, das HSM und vorab aufgespielte ESCRYPT-Software verfügt. Nach einmaliger Konfiguration ist er betriebsbereit. Wartung und Administration können online über das KMS-Backend erfolgen. Kritische Ereignisse wie abgelaufene Zertifikate und Schlüsselzugriffsberechtigungen, volle Log-Datenbanken oder auch eine Verknappung der kryptografischen Daten in Puffern melden Production Key Server auf Wunsch automatisiert – beispielsweise per E-Mail.

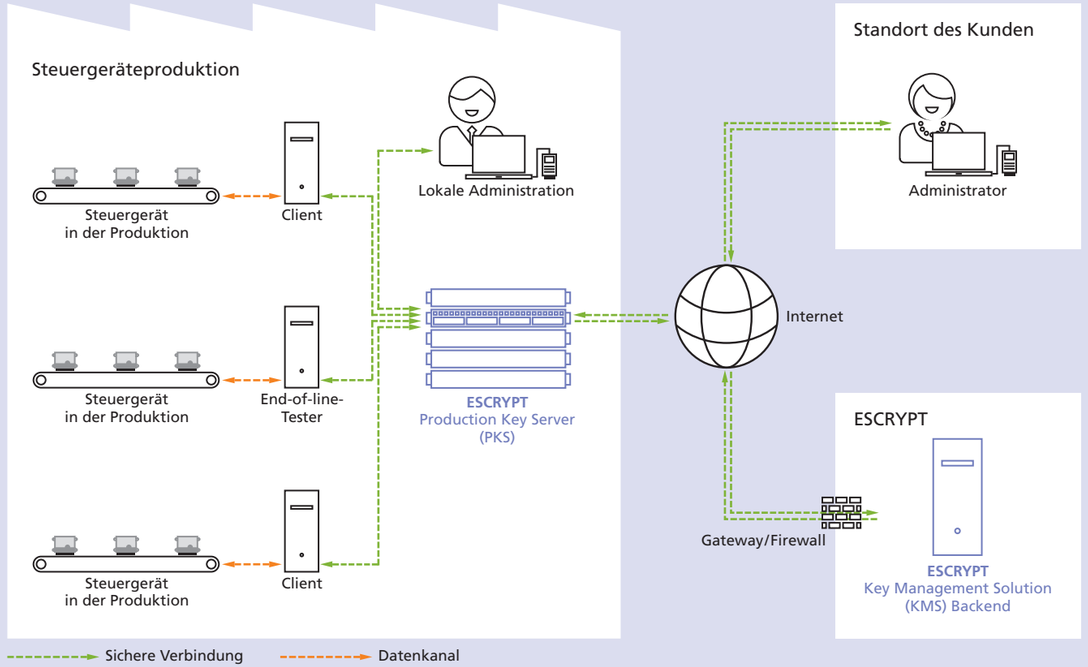
Während die Server weltweit auf die Produktionsstätten verteilt sind, laufen Management und Monitoring der Schlüsselvergabe sowie die Wartung und Konfiguration der PKS im zentralen KMS-Backend. Sollen in der Produktion kryptografische Daten aus einer anderen Quelle verwendet werden, so können diese Daten manuell in das KMS-Backend importiert werden oder das Backend eines Dritten kann sich nach entsprechender Authentifizierung direkt mit der KMS verbinden, um entsprechendes Material auszutauschen. Da sich PKS und KMS in festgelegten Intervallen synchronisieren und dabei ausreichende Puffer an kryptografischen Daten anlegen, sind Steuergerätehersteller bei ihrem Zugriff auf die KMS weitgehend unabhängig von der Stabilität der Internetverbindung.

Die flexible Architektur gewährleistet, dass Hersteller wahlweise selbst die Kontrolle über das Schlüsselmanagement behalten oder dass ESCRYPT das Key Management umsetzt. In beiden Fällen bildet die Verbindung von KMS und verteilten Servern eine leistungsfähige Basis, auf der die PKS-Hardware komplexe kryptografische Operationen nicht nur schnell, sondern auch ausfallsicher umsetzt. Dabei lassen sich PKS auch in Clustern betreiben. Vor allem aber bieten sie maximalen Schutz in Produktionsumgebungen mit problematischem Sicherheitsniveau; auch gegen Diebstahl von geistigem Eigentum. So können vertrauliche Daten, beispielsweise die Sicherheitsschlüssel für befugte Mitarbeiter, auf dem Hardware Security Module gelagert werden. Ihr Abruf kann an vorher festgelegte Routinen und eine Authentifizierung bei der KMS gekoppelt werden. So bleiben sie selbst dann unzugänglich, wenn die komplette PKS-Hardware gestohlen wird. Das HSM dient außerdem als Safe für kryptografische Daten, die auf die Systeme aufgespielt werden, und sichert diese durch zusätzliche Verschlüsselung und eine Sicherheitsprüfung beim Booten ab. Obendrein schützen Firewalls, Verschlüsselung, manipulationsgeschützte Software und HSM-basierte Security-Operationen jeden einzelnen Schritt beim Datenaustausch zwischen Servern, Backend und allen weiteren am Prozess beteiligten Adressaten.

Holistische Sicherheitslösungen sind gefragt

Durch diese Sicherheitsvorkehrungen und die ausgefeilte Architektur wird erreicht, dass typische Automotive-Anwendungen wie das sichere Booten von Mikrocontrollern, das Abschließen von Diagnoseschnittstellen, das Einbringen von Secure-Hardware-Extension-(SHE-) Schlüsseln oder Transport-Layer-Security-(TLS-)Zertifikaten auch im immer stärker vernetzten Fahrzeug der Zukunft sicher bleiben. Das gilt auch für die Absicherung künftiger Car-to-X-Kommunikation oder abschließender Tests von Steuergeräten, für die sich Tester authentifizieren müssen. Die so erreichte Sicherheit lässt sich mit ESCRYPTs holistischem Ansatz für Embedded Security über die Gesamtlebensdauer des Fahrzeugs aufrechterhalten. Denn während PKS für ein sicheres Management und Einbringen von kryptografischen Daten in der Steuergeräteproduktion sorgen, gilt es, Embedded Systeme über den gesamten Lebenszyklus der Fahrzeuge hinweg gegen mutwillige oder fahrlässige Eingriffe abzusichern. ESCRYPT hat entsprechende Sicherheitslösungen und das nötige Know-how für alle Phasen des Lebenszyklus – bis hin zum zuverlässigen Löschen der Schlüssel und Zertifikate nach der Verschrottung.

Production Key Server (PKS)
Sichere Bereitstellung von Schlüsseln und Zertifikaten in der Produktion



Die flexible Lösungsarchitektur zur Absicherung verteilter Fertigungsstätten für Steuergeräte garantiert höchste Verfügbarkeit, geringe Latenzzeiten und optimalen Schutz der eingesetzten kryptografischen Daten.