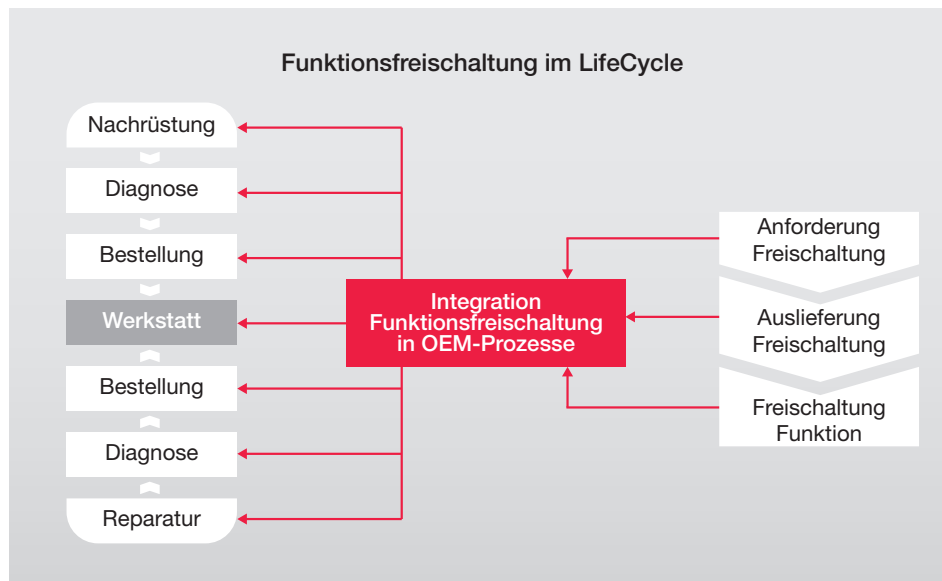


Rechtmanagement zur Nutzung von Fahrzeugfunktionen



Ihre Vorteile:

- » **Reduzierte Variantenanzahl von Hardware und damit sinkende Logistikkosten**
- » **Reduzierte Lizenzkosten durch individuelle Software-Freischaltung**
- » **Neue Erlösmodelle durch kontrollierte Freischaltung der Software**

Im PC-Umfeld hat sich Digital Rights Management (DRM) bereits seit Jahren erfolgreich durchgesetzt. Medienanbieter verkaufen Musik, Videos und vollständige Softwarepakete über Downloads im Internet und schalten diese anschließend zur Nutzung frei. **Der Vorteil für den Anbieter liegt auf der Hand: Durch die elektronische Verteilung der Software ohne Hardware erreicht er im Direktvertrieb Margen von bis zu 80%. Solche Vertriebsmodelle werden nun auch für den Automotive Markt interessant.**

Der Grund dafür liegt in dem steigenden Anteil an elektronischen Steuergeräten und softwarebasierten Funktionen im Fahrzeug und der rasanten Zunahme der internen und externen Vernetzung des Fahrzeugs.

Rechtmanagement als Schutz und Enabler

Der Einsatz eines Rechtmanagement-Systems im Bordnetz eines Fahrzeugs ermöglicht eine Vielzahl unterschiedlicher Anwendungen: Zum einen können einzelne Komponenten auf ein bestimmtes Fahrzeug personalisiert werden. Richtig umgesetzt minimiert dies z.B. die Gefahr eines unberechtigten Gerätetausches. Zum anderen lassen sich durch die Personalisierung neue Geschäftsmodelle etablieren. Fahrzeughersteller müssen Funktionen nicht mehr durch neue Hardware nachrüsten, sondern können sie günstig als Software bereitstellen. Verfahren zum Rechtmanagement stellen somit eine „Enabler“-Technik für neue Umsatzträger im vernetzten Fahrzeug dar.

Die Grundlage für solche Systeme sind dabei in der Regel kryptographische Verfahren. Sie stellen sicher, dass nur berechtigte Anwender – der Fahrer selbst oder das Fahrzeug – die entsprechenden Funktionen nutzen dürfen. Neben bekannten Lösungen im Bereich DRM gibt es Automotive spezifische Lösungen. Diese wurden z. B. durch die Hersteller Initiative Software (HIS) spezifiziert. All diese Verfahren dienen letztendlich der Freischaltung einer bestimmten Funktion in einem speziellen Kontext.

Erfolgsfaktoren für eine sichere Freischaltung

Um ein Rechtemanagement bzw. eine Freischaltung sicher im Fahrzeug umzusetzen, sind einige grundsätzliche Regeln zu beachten:

- Schutz der Software vor Manipulation im Steuergerät
- Sichere Authentisierung des Rechteinhabers
- Sicherer Austausch von Referenzdaten intern und extern

Diese grundlegenden Sicherheitsaspekte müssen berücksichtigt werden, um eine ausgewogene Lösung zu erhalten. Da Angriffe auf ein System grundsätzlich auf das schwächste Glied abzielen, sollten Anwender eine ausgewogene Lösung in allen Bereichen immer einer starken aber sehr lokalen Lösung vorziehen.

Schutz der Prozesse von der Fertigung bis zur Auslieferung

Neben der rein technischen Lösung für die Freischaltung im Steuergerät sind ebenfalls die angrenzenden Prozesse in den Bereichen Entwicklung, Fertigung, Vertrieb, Service und Abrechnung zu betrachten. Hierbei wird u. a. analysiert, ob die erforderlichen Freischaltinformationen über eine zentrale Instanz aus den Hintergrundsystemen heraus oder über dezentrale Systeme am Fahrzeug zur Verfügung gestellt werden. Bei einer zentralen Freischaltung können die Freischaltinformationen auf zwei Wegen übermittelt werden: über eine Online-Verbindung des Fahrzeugs oder offline über verfügbare Service-Prozesse.

Um die Prozesse zu optimieren, müssen logistische und systemtechnische Fragen geklärt werden: Beispielsweise ist zu erarbeiten, ob und wie die Anforderung einer Freischaltung unabhängig vom Verbau der Hardware erfolgen kann und wie die zeitnahe Verfügbarkeit der Freischaltinformationen am Band gewährleistet wird. Die Integration des Freischaltvorganges in den Zulieferer-Produktionsprozess und die Abläufe der Qualitätskontrolle müssen ebenfalls in die Betrachtung einbezogen werden. Wird die Freischaltung um die Serviceorganisation erweitert, muss sichergestellt werden, dass die benötigten Daten jederzeit in einer weltweiten, heterogenen Infrastruktur verfügbar sind.

Handelt es sich bei der Freischaltung um eine kostenpflichtige Software, müssen die Freischaltprozesse mit den bestehenden Abrechnungsprozessen verknüpft werden. Zudem ist zu ermitteln, wie der Nachweis über erfolgte Freischaltungen einem Dritten, in diesem Fall dem Softwarelieferanten, transparent dargestellt werden kann.

Lösungsangebot von secunet

secunet verfügt über umfassende Serienerfahrung im Bereich Funktionsfreischaltung. Im Auftrag verschiedener deutscher Automobilhersteller hat secunet Lösungen von der Konzeptphase bis zur Serieneinführung gestaltet. Im Auftrag eines deutschen OEMs war secunet an der Erstellung der HIS-Spezifikation zur Funktionsfreischaltung beteiligt.

Das Leistungsspektrum umfasst neben der reinen Konzepterstellung auch die Einführung der notwendigen Prozesse beim Kunden sowie die Umsetzung, Weiterentwicklung und optional den Betrieb der notwendigen Backend IT-Systeme. Mit der Produktlösung ABSec (Advanced Backend Security) stellt secunet eine leistungsfähige Key-Management- und Krypto-Service-Komponente bereit, die zudem HIS-konforme Freischaltcodes erzeugt.

secunet – Ihr erfahrener Partner für Automotive Security

secunet unterstützt Fahrzeughersteller und Zulieferer bei der Umsetzung eines wirksamen Rechtemanagements in den Bereichen Entwicklung, Produktion, Serviceorganisation sowie bei der Integration in die Logistik- und Finanzsysteme. Unser Kunde profitiert durch die Expertise unserer Spezialisten aus den Bereichen Authentisierung, Identity Management, Kryptographie, Biometrie und sichere Payment Solutions.

Weitere Informationen:
www.secunet.com/funktionsfreischaltung

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

Tel.: +49-201-5454-0
Fax: +49-201-5454-1000
E-Mail: info@secunet.com
www.secunet.com