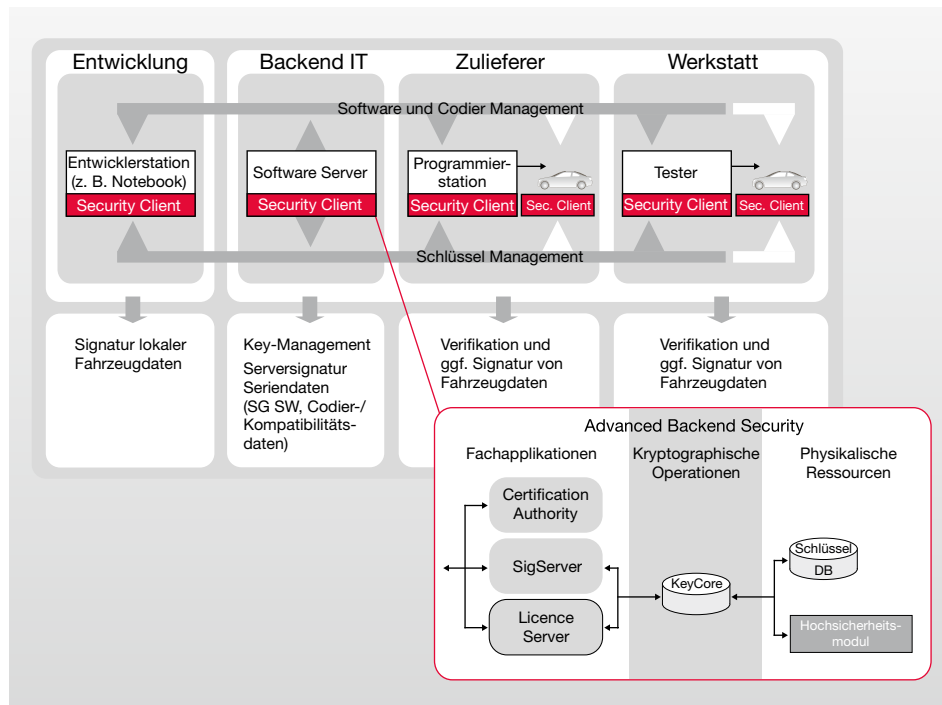


### Absicherung Ihrer Prozesse und Tools durch Advanced Backend Security



#### Ihre Vorteile:

- » Manipulationsschutz der Software
- » Plagiatschutz
- » Verhinderung von Gewährleistungsfällen
- » Schutz von Fahrer und Fahrzeug bei steigendem Softwareanteil

Software hat sich für Fahrer und Hersteller von Automobilen zu einem schützenswerten Gut entwickelt. Nicht nur Unterhaltungsfunktionen sondern auch elementare Fahrzeugfunktionen werden durch sie realisiert. Um Sicherheit für Fahrer und Fahrzeug zu gewährleisten, müssen Plagiate und manipulierte Software vermieden werden.

Ein wirksamer Schutz der Software und Codierdaten vor Manipulation wird erzielt, indem Sicherheitsmechanismen frühzeitig berücksichtigt werden. Der gesamte Lebenszyklus einer Softwarefunktion sowie alle damit in Berührung kommenden Prozesse müssen in die Sicherheitsmaßnahmen einbezogen werden. Dies schließt sowohl die Entwicklung und die Fertigung als auch die Werkstatt und die Serviceorganisation mit ein. Spätere Gefährdungen werden somit frühzeitig neutralisiert.

#### Absicherung der Prozesse und Tools – von der Fertigung bis zur Auslieferung

Eine zuverlässige Lösung bietet die moderne Kryptographie: Um Authentizität und Integrität der Software zu gewährleisten, setzt secunet Signaturverfahren ein, die auf der Verwendung kryptographischer Schlüssel und entsprechender Algorithmen beruhen. Folgende Instanzen müssen dabei berücksichtigt werden:

#### Backend IT

Schlüssel müssen sicher erzeugt und gespeichert werden. Dabei ist es wichtig, den Zugriff zu reglementieren und zu kontrollieren. Gleichzeitig müssen entsprechende Prozesse zur automatisierten Verwendung, Beantragung, Zuweisung und Deaktivierung von Schlüsselmaterial für Entwickler, Lieferanten und Maschinen etabliert werden.

### Entwicklung

Um realistische Szenarien austesten zu können, müssen Schutzmechanismen Software zulassen, die dynamisch verändert und aktualisiert werden können.

### Zulieferer

Das Schlüsselmaterial muss in der Produktion beim Lieferanten in den Steuergeräten gespeichert werden. Der Austausch muss vertraulich und unter Wahrung von Authentizität und Integrität der Schlüsseldaten erfolgen.

### Produktion & Service

Der Zugriff auf signierte Software muss hier zeitnah erfolgen; die Verfügbarkeit aller Daten am Band muss gewährleistet werden.

### Unsere Produktlösung Advanced Backend Security

secunet stellt mit der Advanced Backend Security (ABSec) eine Sicherheitsinfrastruktur bereit, die die spezifischen Anforderungen der Flashdatensicherheit adressiert. Mit der ABSec ermöglicht secunet Ihnen die schnelle und über das Lizenzmodell kostengünstige Integration einer kompletten kryptographischen Sicherheitsinfrastruktur zur Absicherung schutzbedürftiger Anwendungen. Kryptographisches Schlüsselmaterial wird über die ABSec sicher erzeugt, verwaltet, verteilt und genutzt. Die Verfahren werden u.a. für Bereiche wie Fahrzeugprogrammierung, Funktionsfreischaltung und für Anwendungen aus dem Umfeld der Business-to-Vehicle-Kommunikation eingesetzt.

Die Advanced Backend Security besteht aus einer Java-basierten 3-Schicht-Architektur. Neben den anwendungsspezifischen Fachapplikationen enthält sie eine zentrale Managementkomponente. Dieser so genannte KeyCore stellt unternehmensweit kryptographische Dienste bereit und übernimmt das Management des eingesetzten Schlüsselmaterials. Hinsichtlich der Administration ermöglicht der KeyCore eine Verknüpfung des verwendeten Schlüsselmaterials mit Meta- und Stammdaten sowie eine auf Attributen basierte Darstellung der Schlüssel. Dadurch wird die notwendige Kenntnis kryptographischer Verfahren für den Anwender auf ein Minimum reduziert. Zudem verwaltet der KeyCore die angebotenen Krypto-Ressourcen, die für die Ausführung der kryptographischen Verfahren und die sichere Schlüsselspeicherung verantwortlich sind.

Durch den Einsatz der ABSec Produktfamilie profitieren unsere Kunden bei der Konzeption und dem Rollout von Schlüsselmanagementsystemen in der Fahrzeugentwicklung, in den weltweiten Produktionsstätten von Automobilherstellern sowie bei der Einbindung von Vertrags- und freien Werkstätten.

### Unsere Dienstleistungen und Beratungen

Durch unsere Expertise in der klassischen IT-Sicherheit und unseren praktischen Erfahrungen im Bereich Automotive Security sind wir der richtige Partner für Fahrzeughersteller und Zulieferer. Wir unterstützen sie bei der Konzeption und Integration geeigneter kryptographischer Verfahren zur Absicherung existierender IT-Infrastrukturen und Prozesse für die Fahrzeugprogrammierung und -codierung. Dies beinhaltet die Integration einer zentralen Instanz für die sichere Erzeugung, Verwaltung, Verteilung und Nutzung kryptographischen Schlüsselmaterials für die Toolkette und Steuergeräte. Der Integrität und Authentizität der Daten widmen wir besonderes Augenmerk. Auch bei der Umsetzung der dazugehörigen technischen Prozesse bei der Entwicklung, Produktion, Serviceorganisation und bei deren Integration in Logistiksysteme stehen wir unseren Kunden stets zur Seite.

### Daten und Fakten der Advanced Backend Security im Überblick

- Plattformunabhängigkeit durch Java-basierte Umsetzung (J2EE)
- Service orientierte 3-Schicht-Architektur (SOA) – Trennung von Fachapplikationen, kryptographischen Operationen und physikalischen Ressourcen
- Zentralisierung der Sicherheitsmechanismen im KeyCore
- Modularer und skalierbarer Aufbau (Performance, neue Applikationen)
- Hochsicherheitsmodul unabhängig von Applikations-Hardware
- Clusterfähigkeit
- Kostengünstige Wartung und Pflege

Weitere Informationen:  
[www.secunet.com/flashdatensicherheit](http://www.secunet.com/flashdatensicherheit)

**secunet**

secunet Security Networks AG  
Kronprinzenstraße 30  
45128 Essen

Tel.: +49-201-5454-0  
Fax: +49-201-5454-1000  
E-Mail: [info@secunet.com](mailto:info@secunet.com)  
[www.secunet.com](http://www.secunet.com)