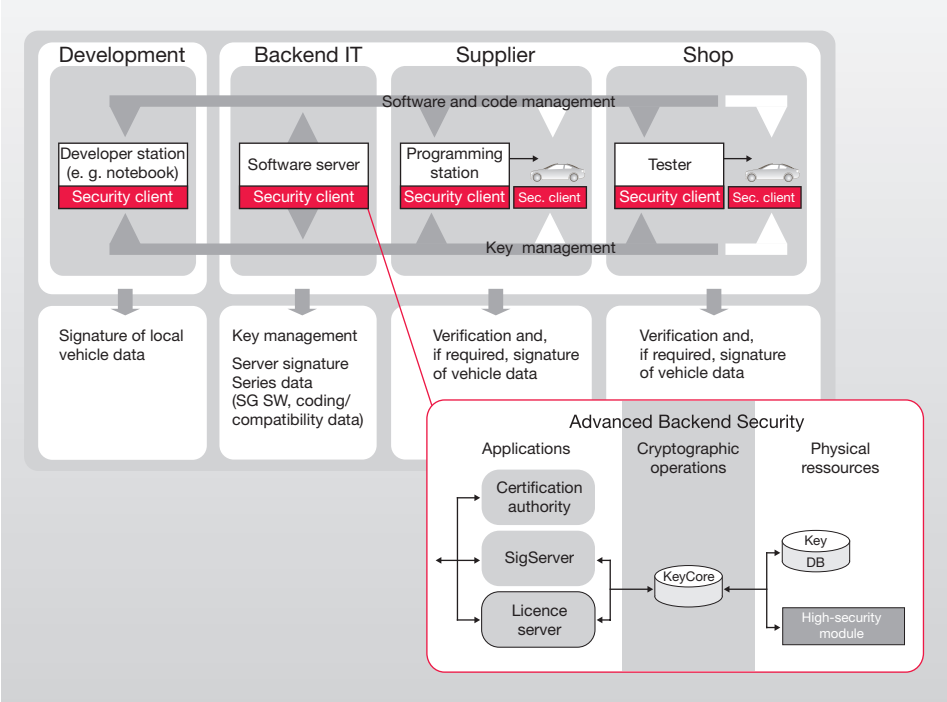
secunet

Flashware Protection

Advanced Backend Security for Protecting Your Processes and Tools



Benefits:

- **Protection of software against manipulation and plagiarism**
- **Prevention of warranty claims**
- **Protection of driver and vehicle in view of the growing proportion of software**

Software has evolved into a commodity that requires protection for drivers and car manufacturers. It enables not only entertainment functions, but also fundamental vehicle functions. In order to ensure the safety and security of the driver and the vehicle, knock-offs, counterfeits and plagiarisms as well as manipulated software must be avoided.

Security mechanisms must be considered at an early stage in order to effectively protect software and code in the vehicle against manipulation and misuse. They must cover the entire lifecycle of a software function as well as all related processes. This includes development and production as well as the shop and the service organisation. Subsequent threats are thus neutralised in time.

Securing processes and tools – from production to shipment

Modern cryptography serves as a basis for a reliable solution: in order to ensure the authenticity and integrity of the software, secunet makes use of signature processes which are based on cryptographic keys and corresponding algorithms. The following instances need to be taken into consideration:

Backend IT

Keys must be securely generated and stored. It is important to regulate and control access. At the same time, the corresponding procedures for the automatic usage, application, assignment and deactivation of key material must be set up for developers, suppliers and machines.

Development
In order to be able to test realistic scenarios, protection mechanisms must permit software which can be dynamically changed and updated.

Supplier
Key material needs to be stored in the control units during production at the supplier's site. The exchange must be made in a way which is confidential and which maintains the authenticity and integrity of the key data.

Production & Service
Access to signed software must occur promptly; the availability of all data on the line must be ensured.

Our Advanced Backend Security product solution

secunet's Advanced Backend Security provides a security infrastructure which addresses the specific requirements of flashware protection. With ABSec, secunet makes it possible for you to integrate a complete cryptographic security infrastructure fast and economically (due to the licence model) to safeguard applications that require protection. Cryptographic key material is generated, administrated, distributed and used securely via ABSec. The processes are used for areas such as vehicle programming and function enabling as well as for applications from the business-to-vehicle communication sector.

Advanced Backend Security includes a central management component in a Java-based 3-tier architecture in addition to specific applications. This so-called KeyCore makes cryptographic services available on a cross-enterprise level and manages the key material used. In terms of administration, the KeyCore enables the key material used to be linked to metadata and master data as well as an attribute-based representation of the keys. As a result, the knowledge of cryptographic methods required by the user is reduced to a minimum. Furthermore, the KeyCore manages the integrated cryptographic resources responsible for execution of the cryptographic methods and the secure storage of the keys.

Our customers benefit by using the ABSec product family for the concept and rollout of key management systems in vehicle development, in production facilities of carmakers world-wide and for the integration of authorised and independent repair shops.

Our services and consulting

Our expertise in classic IT security and our hands-on experience in the field of automotive security make us the right partner for vehicle manufacturers and suppliers. We support them in the design and integration of appropriate cryptographic methods for securing existing IT infrastructures and processes for vehicle programming and coding. This comprises the integration of a central instance for the secure generation, administration, distribution and use of cryptographic key material for the tool chain and control units. We pay special attention to data integrity and authenticity. We provide our customers with ongoing support when it comes to implementing the corresponding technical processes with regard to development, production, service organisation and the integration of such processes into logistics systems.

Advanced Backend Security facts and figures at a glance

- Platform independence through Java-based implementation (J2EE)
- Service-orientated 3-tier architecture (SOA) – separation of applications, cryptographic operations and physical resources
- Centralisation of the security mechanisms in the KeyCore
- Modular and scalable design (performance, new applications)
- High-security module independent of application hardware
- Clusterability
- Cost-effective maintenance

More information:
www.secunet.com/flashwareprotection

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen, Germany

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