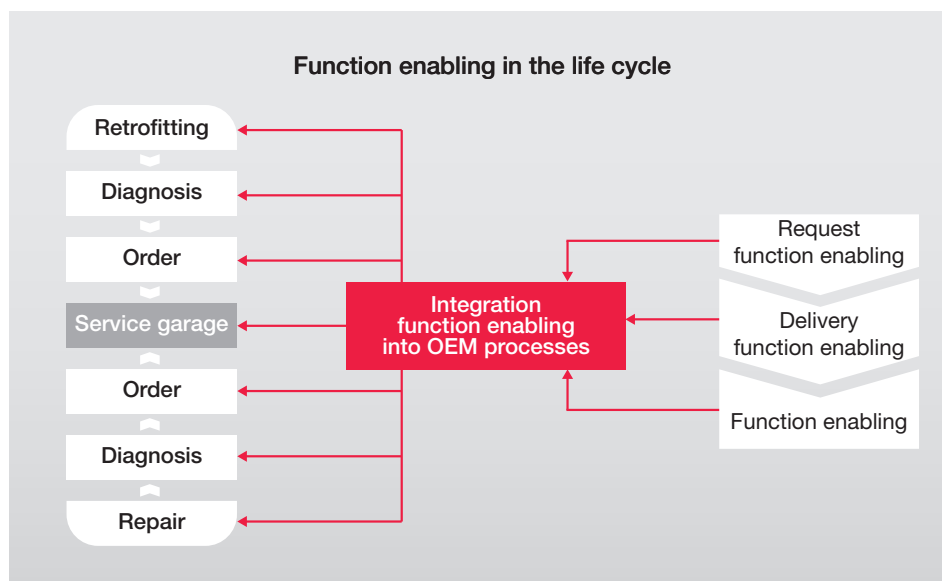


# Rights Management for the Use of Vehicle Functions



## Benefits:

- » Reduced number of hardware variations to lower the costs of logistics
- » Reduced licensing costs as a result of individual software enabling
- » New revenue models as a result of controlled software enabling

Digital Rights Management (DRM) established itself years ago in the PC sector. Media suppliers sell music, videos and entire software packages via Internet download and then activate them for use. **The advantage for the supplier is self-evident: margins of up to 80 % are possible for direct sales using electronic distribution methods without hardware. Such distribution models are now catching the interest of the automotive market.**

This trend is the result of the rising number of electronic control units and software-based functions in the vehicle plus the rapid increase in levels of internal and external vehicle networking.

### Rights management as protection and enabler

The use of a rights management system in a vehicle's onboard network facilitates numerous different applications: on the one hand, it is possible to personalise individual components on a per vehicle basis. If implemented properly, this can, for instance, minimise the risk of the device being replaced without authorisation. On the other hand, new business models can be established as a result of personalisation. Vehicle makers no longer have to install new hardware to upgrade functions; instead they can make upgrades available as cost-effective software. Processes for rights management serve as a means of "enabling" new sources of revenue in the networked vehicle.

Such systems are normally based on cryptographic methods. They ensure that only authorised users – the driver of the vehicle or the vehicle itself – are permitted to use the functions in question. In addition to solutions that people are already familiar with in the area of DRM, automotive-specific solutions are available. These have been specified by the Manufacturer Initiative Software (HIS), for example. All of these processes ultimately lead to the enabling of a specific function in a particular context.

**Factors for successful and secure function enabling**

In order to securely implement rights management or enabling in the vehicle, a few basic rules need to be observed:

- Protection of the software against manipulation in the control unit
- Secure authentication of the rights owner
- Secure exchange of reference data internally and externally

These fundamental security aspects must be taken into consideration to arrive at a well-balanced solution. Since system attacks generally aim at the weakest point, users should opt for a solution which is well balanced in all areas as opposed to a solution which is strong but very local.

**Protection of the processes from production to shipment**

Not only must attention be given to the purely technical solution for enabling in the control unit, but also to related processes in the areas of development, production, sales/distribution, service and billing. This involves analysing, for example, whether the required enabling data is provided via a central instance from the background systems or via distributed systems in the vehicle. In the case of central enabling, there are two ways of transmitting enabling data: via the vehicle's online connection or via service processes available offline.

In order to optimise processes, logistical and system-technical issues need to be resolved: for instance, whether and how the enabling request can be processed independent of the installed hardware as well as how the prompt availability of the enabling data on the line is ensured. The integration of the enabling procedure in the supplier's production process and the quality assurance processes must also be taken into consideration. If enabling is extended to include the service organisation, it must be guaranteed that the required data is available in a global, heterogeneous infrastructure at all times.

If software which is not free of charge is to be enabled, the enabling processes must be linked to existing billing processes. In addition, it is necessary to determine how a record of completed enabling processes can be clearly represented to a third party, in this case the software supplier.

**secunet's solution portfolio**

In the area of function enabling, secunet has extensive production experience. secunet has designed solutions from the concept phase to implementation for various German carmakers. For a German OEM, secunet was actively involved in the creation of the Manufacturer Initiative Software (HIS) specification for function enabling.

In addition to creation of the concept alone, the range of services includes putting the necessary processes in place at the customer's site as well as implementation, further development and optional operation of the required backend IT systems. With its ABSec (Advanced Backend Security) solution, secunet provides a powerful key management and crypto service component which also generates HIS-compliant (HIS=Manufacturer Initiative Software) enabling codes.

**secunet – your experienced partner for automotive security**

secunet supports vehicle manufacturers and suppliers in the implementation of effective rights management systems in the areas of development, production and service organisation as well as in the integration into logistics and finance systems. The customer profits from the expertise of our specialists in the fields of authentication, identity management, cryptography, biometrics and secure payment solutions.

More information:  
[www.secunet.com/functionenabling](http://www.secunet.com/functionenabling)



secunet Security Networks AG  
Kronprinzenstraße 30  
45128 Essen, Germany

Phone: +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)