



# SOFTWARE-PLATFORM FOR TPM 2.0

## SECURITY FOR AUTOMOTIVE IT

*Fraunhofer Institute for Secure  
Information Technology SIT*

*Contact:  
Andreas Fuchs  
Rheinstrasse 75  
64295 Darmstadt  
Germany*

*Phone 06151 869-228  
Fax 06151 869-224  
andreas.fuchs@sit.fraunhofer.de  
www.sit.fraunhofer.de*

Several innovations in the automotive industry are based on IT systems and their internet connection. However, increasing connectivity also poses new vulnerabilities. Fraunhofer SIT has developed a software platform where secure control units can be developed based on a TPM 2.0.

The combination of IT with the physical world is playing an ever increasing role in many industries. For example, in the automobile industry: The previously closed system within a car now has more than 100 embedded control devices, sensors, and other mini-computers that communicate with each other and the manufacturers' backend systems or are connected with the internet. On the one hand, this results in a variety of new application possibilities. On the other, it leads to many more risks for automobiles. Hackers procure personal as well as manufacturer-specific data, car thieves bypass the immobilizers. Should maps within navigation systems be tampered with, there could be grave consequences for the driver and passengers.

### **More Security**

Considering the large number of weaknesses identified in the past years, there is a need for new concepts to ensure the integrity of the control units installed. To meet this need, Fraunhofer SIT has developed a software platform based on manufacturer-independent open standards. Fraunhofer SIT's solution uses a hardware security module (HSM), the Trusted Platform Module (TPM) 2.0. The software portion of the solution communicates with the TPM, which functions as the trust anchor and storage for cryptographic

keys. These are only released when the devices are in perfect condition. If an attack is registered, e.g. if the brakes are tampered with, the motor's control unit could refuse to start as a means of protecting the passengers. These functions can be used to check if firmware updates are from trustworthy sources and, if not, prevent access to cryptographically secure storage. Moreover, this mechanism can be expanded to prevent outdated and possibly vulnerable original firmware versions from being reinstalled. Additionally, the installation of counterfeit replacement parts can be recognized and prevented using this approach, because the keys stored in the TPM, which are neither readable nor able to be copied, can identify whether a device is an original part. Thus, the manufacturer is protected from piracy, and the car owners are not in danger of causing an accident due to poor quality and improperly functioning parts.

Fraunhofer SIT's solution is a prototype available via licensing. In addition to this product, Fraunhofer SIT offers further development of solutions for device protection based on TPM 2.0.

### **Software-Platform for TPM 2.0 offers**

- Recognition of firmware and protection from its manipulation
- Protection of personal and manufacturer-specific data
- Protection from product piracy
- Easy realization of further security protocols
- Only small amount of storage & computing capacity necessary
- Support of development process via hard- & software simulators