Whether it is in companies’ large networks or the smart home area, every single device plays a significant role with regard to the overall system security. Thus, they represent an attractive target for attackers. For equipment in the internet of things, device identities and their integrity are of central importance: Industrial Internet, smart home or smart traffic can only work reliably if every device has its own non-clonable identity, which includes the integrity of the running firmware. From the heating control system in a private smart home environment to the big production plants, device identity and integrity is crucial.

The Fraunhofer Institute for Secure Information Technology SIT is one of the leading experts in this area with more than ten years of experience in the field of trusted computing, secure data processing, and an active participation in relevant standardization bodies. To meet these challenges, Fraunhofer SIT works in cooperation with research and industry partners to develop technologies and solutions to assure data protection and confidentiality in embedded systems, utilizing trustworthy applications and system architectures based on hardware trust anchors.

Furthermore, Fraunhofer SIT works on proof of concept solutions and analyzes trusted computing based concepts and implementations. Based on the in-house developed and standard-conform TPM Software Stack 2.0 and the development tools for TPM 2.0 the institute offers solutions for the latest technologies in this field.

Our offerings:

**Fraunhofer SIT TPM Software Stack 2.0**
- Middleware for the use of all TPM 2.0 functionalities
- Easy realization of TPM based security solutions and protocols
- Configurability for embedded devices e.g. for the reduction of the storage needs
- Licensable implementation

**Fraunhofer SIT TPM/TSS 2.0 Development Tools**
- Support of the development process through hard- and software simulators
- Rapid prototyping tools for a fast preparation of feasibility studies
- Extensive and configurable logging and debug framework
- Licensable implementation

**Consultation**
- Technical consultation, creation of concepts and analyses
- Feasibility studies and prototypical implementations
- Support with the implementation of trusted computing projects

**Our Applications:**

**Trusted Core Network**
- Hardware based security for industrial networks
- Usage of the trusted platform module (TPM)
- Intrusion alert directly to central monitoring
Automotive Runtime Software Product Lines

- One unified firmware image for the whole product line
- Individually encrypted and TPM protected product features
- TPM secured model numbers and encryption keys

Monitoring of device integrity in industrial network

- Network protocol: Time based unidirectional attestation (TUDA)
- Continuous information about the software's / firmware's condition of all devices with TPM
- Further use of SNMP as standard protocol
- Compatibility with constrained application protocol (CoAP) and RESTconf
- Usability in unidirectional network environments such as high-to-low-security communications
- Time stamp based attestations suitable for auditing logs