Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

TRUSTED COMPUTING FOR DIGITAL INDUSTRY

SECURITY FOR EMBEDDED SYSTEMS IN INDUSTRIAL NETWORKS

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Andreas Fuchs
Rheinstraße 75
64295 Darmstadt
Germany

Phone +49 6151 869-228
Fax +49 6151 869-224
andreas.fuchs@sit.fraunhofer.de
www.sit.fraunhofer.de

Industrial plants as well as production and trade processes are getting more and more interconnected and digitized. In this open, connected industry, each device plays an important role in the overall system's security. At the same time, every device embedded in an industrial network also represents an attractive target for attackers. With the help of Trusted Computing methods, hardware components can be identified clearly and a trustworthy state of the software can be ensured (integrity). The Fraunhofer Institute for Secure Information Technology SIT offers consulting, concepts and solutions in the area of Trusted Computing to secure machines and protect industrial networks.

Prior to the digitization and interconnection of industrial production facilities with the Internet, industrial networks were coherent, so that each machine, each device could be clearly identified on the spot. While opening the production facilities to the Internet, the remote maintenance of attachments or the import of updates via remote access, one needs more to prevent manipulations: A secure industry 4.0 only works if every machine, every piece of hardware, each device has its own, not clonable identity, which also includes the integrity of the running firmware. This applies to both large production facilities and critical infrastructures. The computer worm Stuxnet, for example, had changed the software on devices within an industrial network undetected and thus allowed manipulations. With Trusted Computing methods, similar attacks can be effectively prevented.

The Fraunhofer SIT is is developing Trusted Computing-based technologies and solutions for manufacturers to ensure data confidentiality and integrity in embedded systems, including trusted applications and system architectures based on hardware trust anchors. Network provider and supplier companies can be technically advised by the Trusted Computing experts of Fraunhofer SIT.

Our offer:

Consultation, concept, and prototyping

- Technical consultations, generation of concepts and analyses
- Feasibility studies and prototypical implementations
- Support during the implementation phase of Trusted Computing projects

Fraunhofer SIT TPM Software Stack 2.0

- Middleware to use all TPM 2.0 functionalities
- Easy realization of TPM based security solutions and protocols
- Configurability for embedded systems or for reducing storage requirements

Fraunhofer SIT TPM/TSS 2.0 Development Tools

- Support of developmental processes through hardware and software simulations
- Rapid prototyping tools for the quick preparation of feasibility studies
- Extensive and configurable logging and debugging framework