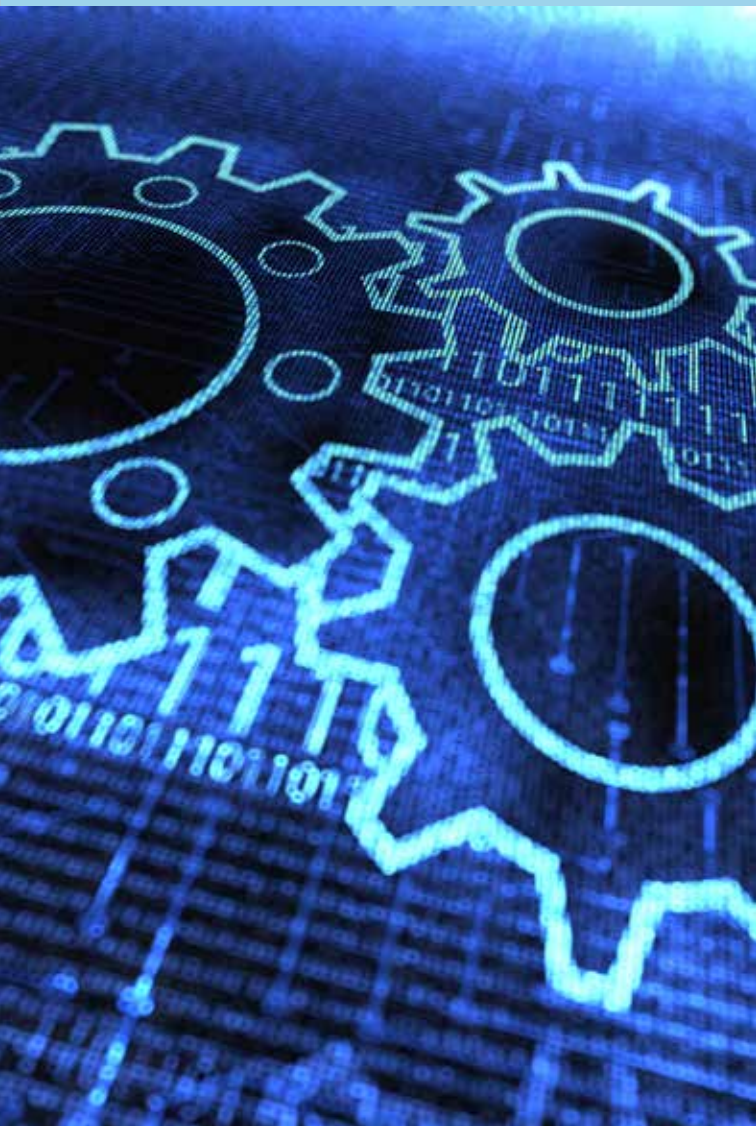
Fraunhofer SIT

TRUSTED COMPUTING FOR EMBEDDED DEVICES

Secure Device Identities and Platform Integrity



ABOUT

Whether in large corporate networks or in the smart home area – each individual device plays an important role in the security of the entire system. As a result, embedded devices also represent an **attractive target for attackers**.

For devices in the Internet of Things, identities and their integrity are of central importance: Industrie 4.0, Smart Home or Smart Traffic only work if each machine, each piece of hardware, each device has its own non-clonable identity, which also includes the integrity of the running firmware.

To meet these challenges, Fraunhofer SIT uses the principle of Trusted Computing. The use of hardware trust anchors ensures data confidentiality and data integrity in embedded systems.

Fraunhofer SIT develops the necessary technologies and solutions to implement Trusted Computing in cooperation with partners in research and industry.

OUR EXPERTISE

With more than **15 years of experience**, the experts at Fraunhofer SIT are leading in the field of Trusted Computing:

- The standard-compliant **TPM/TSS Software Stack 2.0** has been co-developed by Fraunhofer experts, the implementation as well as the programming is completed and available on Github. Here, Fraunhofer SIT experts are maintainers, and they handle requests, improvements and messages about security flaws.

- Fraunhofer experts helped to develop an **OpenSSL engine** that makes TPM 2.0 and TSS 2.0 usable.

- Fraunhofer SIT experts are leading the standardization in the **TPM software stack working group** of the Trusted Computing Group (**TCG**).

- Our experts are regularly invited to speak at relevant conferences such as the **LPC** (Linux Plumbers Conference), the **ELCE** (Embedded Linux Conference Europe), or the **FOSDEM** (Free and Open Source Software Developers' European Meeting).

OUR SERVICES

- Consultancy on TPM und TSS
- Functional integration into the systems
- Integration in TPM setups in the manufacturing process
- Provisioning
- Technical consulting, preparation of concepts and analyses
- Feasibility studies and prototype implementations
- Support in the implementation of Trusted Computing projects

OUR CUSTOMERS

- Industrial control system operators
- Network operators
- Manufacturers of charging stations for electric cars
- Car manufacturer
- Hardware and chip manufacturers
- Software producer

POSSIBLE APPLICATIONS

- Secure firmware updates for automotive head units
- Credential protection for plug-and-charge controllers
- Identity protection for charging stations in the field
- Integrity attestation for Industrial Control Systems (ICS)
- Feature protection for multi-purpose devices

MORE INFORMATION

www.sit.fraunhofer.de/en/trustedcomputing

CONTACT

Fraunhofer Institut
for Secure Information Technology SIT

Andreas Fuchs
Rheinstrasse 75
64295 Darmstadt

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