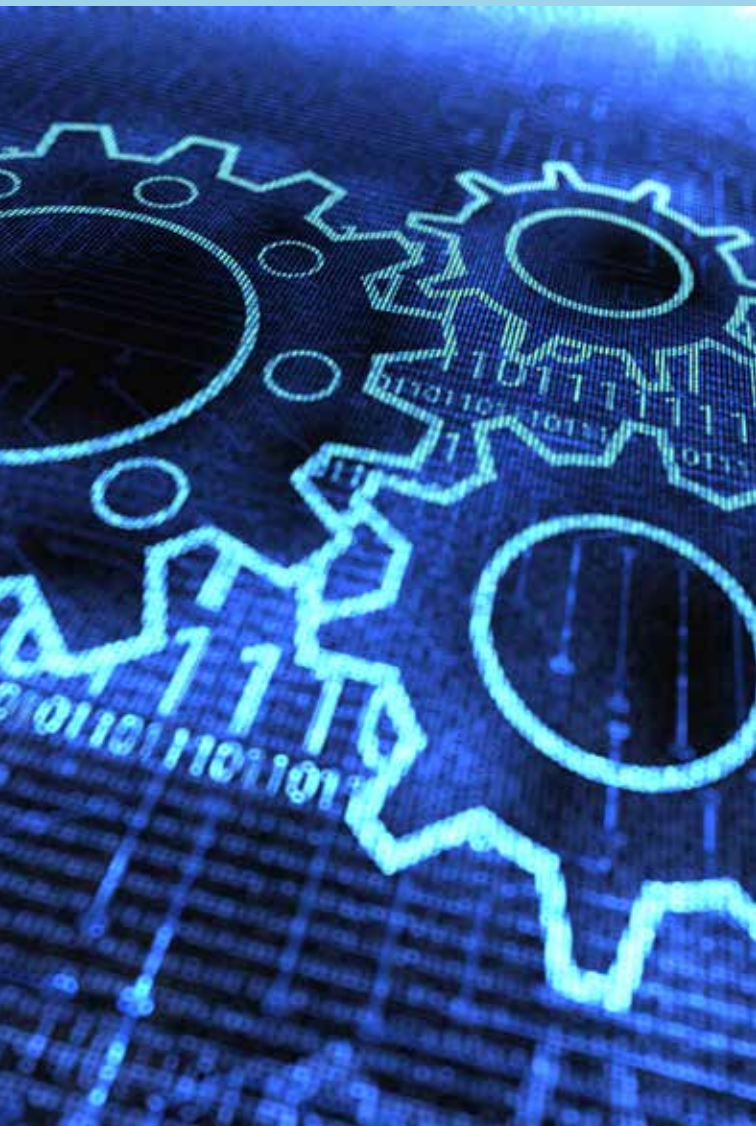
Fraunhofer SIT

TRUSTED COMPUTING FÜR EMBEDDED DEVICES

Sichere Geräteidentitäten und Plattformintegrität



WORUM GEHT'S?

Ob in großen Unternehmensnetzwerken oder im Smart-home-Bereich – jedes einzelne Gerät spielt eine wichtige Rolle für die Sicherheit des Gesamtsystems. Dadurch stellen vernetzte Geräte auch ein **attraktives Ziel für Angreifer** dar.

Für Maschinen im Internet der Dinge sind **Geräteidentitäten** und deren **Integrität** von zentraler Bedeutung: Industrie 4.0, Smart Home oder Smart Traffic funktionieren nur, wenn jede Maschine, jedes Stück Hardware, jedes Gerät eine eigene, nicht klonbare Identität hat, die auch die Integrität der laufenden Firmware umfasst.

Um diesen Herausforderungen zu begegnen, nutzt das Fraunhofer SIT das Prinzip des **Trusted Computing**s. Über den Einsatz von Hardware-Vertrauensankern werden Datenvertraulichkeit und Datenintegrität in eingebetteten Systemen sichergestellt.

In aktiver Zusammenarbeit mit Partnern in Forschung und Industrie entwickelt Fraunhofer SIT die nötigen Technologien und Lösungen zur Umsetzung von Trusted Computing.

UNSERE EXPERTISE

Die Experten des Fraunhofer SIT sind mit mehr als 15 Jahren Erfahrung führend im Bereich Trusted Computing:

- Der standardkonforme **TPM/TSS Software Stack 2.0** ist von Fraunhofer-Experten mitentwickelt worden, die Implementierung sowie die Programmierung sind vollendet und auf Github abrufbar. Hier sind Fraunhofer-SIT-Experten Maintainer und bearbeiten Anfragen, Verbesserungen und Meldungen zu Sicherheitslücken.

- Fraunhofer-Experten halfen bei der Entwicklung einer **OpenSSL-Engine**, die TPM 2.0 und TSS 2.0 nutzbar macht.

- Experten des Fraunhofer SIT sind in der **TPM-Software-Stack-Arbeitsgruppe der Trusted Computing Group (TCG)** vertreten und leiten dort die Standardisierung.

- Unsere Experten werden regelmäßig zu Vorträgen auf einschlägigen Konferenzen wie der **LPC** (Linux Plumbers Conference), der **ELCE** (Embedded Linux Conference Europe) oder der **FOSDEM** (Free and Open Source Software Developers' European Meeting) eingeladen.

UNSERE DIENSTLEISTUNGEN

- Consultancy zu TPM und TSS
- Funktionale Integration in die Systeme selbst
- Integration in TPM-Setups im Herstellungsprozess
- Provisioning
- Technische Beratung, Erstellung von Konzepten und Analysen
- Machbarkeitsstudien und prototypische Implementierungen
- Unterstützung bei der Umsetzung von Trusted-Computing-Projekten

UNSERE KUNDEN

- Industriesteueranlagen-Betreiber
- Netzwerkbetreiber
- Hersteller von Ladesäulen für E-Automobile
- Automobilhersteller
- Hardware- und Chiphersteller
- Softwarehersteller

MÖGLICHE APPLIKATIONEN

- Sichere Firmware-Updates für Kfz-Steuergeräte
- Schutz der Anmeldeinformationen für plug-and-charge-Controller
- Identitätsschutz für Ladestationen, die ungeschützt draußen stehen
- Integritätsbescheinigungen für Industrial Control Systems (ICS)
- Schutz von Funktionen von Mehrzweck-Geräten

MEHR ERFAHREN

www.sit.fraunhofer.de/trustedcomputing

ANSPRECHPARTNER

Fraunhofer-Institut
für Sichere Informationstechnologie SIT

Andreas Fuchs
Rheinstraße 75
64295 Darmstadt

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