

Future Security Modules for Trusted Computing

Motivation

Small hardware security modules allow to project trust from a small, certified chip on their host computer.

For future generations of such chips, different hardware interfaces and software architectures to support them are under discussion.

Novel cryptographic solutions and protocols wait to be analyzed.

Project description

We want you to study recent proposals, experiment with emulators and modify existing libraries to become compatible with the future.

A non-disclosure agreement may have to be signed.



Deliverables

- Software experiment results
- Documentation, Report
- Presentation (15-20 min)

Scope and Credits

Studies: INF SEW TEL MATH

The scope, effort, and credits of this project are scalable.

Advisor / contact

ronald.toegl@iaik.tugraz.at