Contact:
Fraunhofer-Institute
Secure Information Technology
Rheinstraße 75
64295 Darmstadt

Dr. Andreas U. Schmidt
Andreas.U.Schmidt@sit.fraunhofer.de
Tel. 06151 – 869 60 227

Nicolai Kuntze
Nicolai.Kuntze@sit.fraunhofer.de
Tel. 06151 – 869 60 054

Prof. Dr. Claudia Eckert
Fachbereich Informatik
FG Sicherheit in der Informationstechnik
Hochschulstr. 10
64289 Darmstadt
Telefon +49 (0) 61 51/16-6591
Telefax +49 (0) 61 51/16-3514

Fraunhofer Institut
Sichere Informationstechnologie SIT
Institutsleitung
Prof. Dr. Claudia Eckert

Rheinstraße 75
64295 Darmstadt

E-Mail: eckert@sit.fraunhofer.de
http://www.sit.fraunhofer.de

Diploma Thesis

SUBJECT: Virtualisation of a SIM card using trusted computing

Background and Goal: The Subscriber Identity Module (SIM) is the industry standard for user authentication in the mobile domain today. With the upcoming Trusted Computing (TC) technology and its adoption for the mobile domain by the Trusted Computing Group (TCG, through its Mobile Phone Working Group) a new hardware based security and trust enabling system for mobile devices is established.

TC offers ways to establish trust between entities by providing metrics of the system state and the ability to create, store and use asymmetric key pairs inside a shielded hardware device, the Trusted Platform Module (TPM).

As two hardware security tokens in one device are not desired by the industry the question arises if it is possible to emulate the behaviour of an SIM protected by the methods of a TPM. Aim of the diploma thesis is to implement a mobile TPM emulation based on existing frameworks for a Linux platform using the specification of the TCG.

On this fundament concepts for SIM virtualisation shall be developed and implemented

Prerequisites: Good knowledge of identity management concepts. Knowledge in cryptography. Fluent in C++ and Linux. May have heard of trusted computing. English writing skills.

Start: Immediately