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: Trusted Infrastructures for Identities

Background and Goal: Trusted Computing (TC) as defined by the Trusted Computing Group is usually seen as a protection technology centred on single devices or protection of media (DRM). But this upcoming technology has many facets which applied information security can benefit from. Seen as a platform-neutral security infrastructure, TC offers ways to establish trust between entities that are otherwise separated by technical boundaries, e.g., different access technologies and access control structures. Commercial applications of TC in this respect abound in particular in the mobile sector.

Not surprisingly, some concepts and methods of TC are rather similar to Identity management (IDM) and federation. The thesis shall explore this relationship, in particular it shall

- Thoroughly assess the TC methods of remote attestation and direct anonymous attestation from the viewpoint of IDM,
- Compare existing IDM technology (Kerberos, RADIUS, SAML, etc.) with related TC functionality, and
- Develop a concept to combine (at least one of) the existing IDM technologies with TC *in a way which enables new applications and/or foundation of new trust relations*.

Core concepts of TC-based IDM shall be implemented in the form of a demonstrator. Preferably, the application context shall be that of a state-of-the-art Web application.

Prerequisites: Good knowledge of identity management concepts. Knowledge in cryptography. Fluent in Java and knowledge of contemporary Web-application technology. May have heard of trusted computing. English writing skills.

Start: Immediately