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

Dr. Andreas U. Schmidt
Andreas.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/Master Thesis

SUBJECT: Trusted Ticket Systems

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, in particular the functions of a privacy CA is interesting in this context.

The thesis shall concretely realise ideas centred around the 'abuse' of TCG attestation processes to obtain a trusted ticket system as a building block for IDM. 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. The core task is to design architectural concepts and data structures for value tickets to be used as one- or many-time authentication credentials for authorisation to universal service access and accounting, and relying on TCG's attestation identity keys. The concepts shall be realised and embedded in an existing authentication system like Kerberos. The combination of attestation of a client system's trustworthiness with user authentication and authorisation is a key issue. The thesis will build on and combine with the results of the concluded thesis "Trusted Infrastructures for Identities"

Prerequisites: Good knowledge of authentication concepts and protocols. Knowledge in cryptography. Elements of Trusted Computing. Fluent in Java and knowledge of contemporary Web-application technology.

Start: Immediately