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

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

Dr.-Ing Martin Steinebach
Martin.Steinebach@sit.fraunhofer.de
Tel. 06151 – 869 349

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

TECHNISCHE
UNIVERSITÄT
DARMSTADT

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 Watermarks

Background and Goal: Watermarking media files offers the possibility to identify a copyright owner or to trace an illegal copy back to its original customer. The latter case is called transaction watermarking and allows for a strong alternative for digital rights management. In working systems like the Apple iTunes Music Store the files are tagged by a centralised authority. As for each centralised architecture such systems have to provide huge resources in terms of computing power and bandwidth. Also certain privacy issues arise. Decentralisation in this area may lead to devices in shops where the music is stored and watermarks are applied on demand. Trusted Computing introduces protocols and hardware to implement trustworthy platforms and by this builds the ground for a high level of trust in devices relying on these platforms.

The aim of this thesis is to develop a concept and to implement a demonstrator how to decentralise this process based on watermarking technology and trusted computing. The information contained in the “trusted watermarks” shall be selected, designed and cast in appropriate data structures. They shall attest to statements like “this watermark is generated and applied by a trustworthy device for customer X on a media file from originator Y”. That is in particular, the trusted watermark will contain some attestation information on the trusted platform on which it is generated. The resulting demonstrator shall provide a working example for trusted watermark application in a concrete media sales scenario.

Prerequisites: Basic knowledge in Web Services and security protocols. Basics of watermarking. Elements of trusted computing.

Start: Immediately