



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Contact:

Fraunhofer-Institute
Secure Information Technology
Dolivostr. 15
64293 Darmstadt

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

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: Signed Voice Transactions

Background and Goal: The latest successful example for the ever ongoing convergence of information technologies is internet based telephony, transporting voice over the internet protocol (VoIP). Voice based information portals and ticket reservation services are already using VoIP as a backbone, as do many corporate telephony systems.. With operators of mobile and fixed line telephony networks already embracing the new technology, one can envisage the horizontal integration of services enabled through VoIP, enhancing functionality, e.g., by enriching internet based business-to-consumer services by (semi-automatic) voice communication.

On this background, does it make sense to apply sophisticated digital signature technology to voice data in VoIP streams? While authenticity proofs by signing a data stream or using audio watermarks are trivial, we believe that electronic signatures applied to voice data on a transactional level, serving purposes such as formation of binding contracts, non-repudiation, voice supported authentication and access control (e.g., for establishing trustworthy contact between unacquainted persons), and, of course, enabling handicapped persons to use electronic signatures, comprise an area of considerable of novelty and potential interest.

In this thesis, the fundamental principles of signed voice transactions shall be developed and exemplified in a demonstration environment for realistic application scenarios, which are also to be devised. While the theory can rest on the known basics of trustworthiness through signed transactions, special care has to be taken of the particularities of the voice channel (perceived one-dimensionality and duplex character). In particular, protocols for the seamless voice presentation (e.g. using SpeechML) of signatures and certificates, taking ergonomic factors into account, are to be developed, as well as the proper integration into an ongoing conversation. The problem of archiving signed voice transactions and applying lossful compressions establishes contact to the project TransiDoc (www.transidoc.de).

Prerequisites: Good knowledge of VoIP technology. A little background in audio compression and data formats. Digital signature basics. English writing skills.

Start: Immediately