Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

SECURE VoIP

ENCRYPTED INTERNET TELEPHONY FOR CONVENTIONAL CELLULAR TELEPHONES

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Matthias Ritscher
Rheinstrasse 75
64295 Darmstadt, Germany

Phone +49 6151 869-313
Fax +49 6151 869-224
matthias.ritscher@sit.fraunhofer.de
www.sit.fraunhofer.de

Companies can reduce their telephone costs considerably with IP telephony. Many of the VoIP solutions available on the market can easily be manipulated or eavesdropped on, however, as voice information is generally not encrypted. This is why there's already a first generation of products available that provide encryption for VoIP enabled telephone lines. Since cellular telephones should also be supporting VoIP telephony in the future, the Fraunhofer Institute SIT has developed a software solution that enables an encrypted connection between two conventional cellular telephones. Secure VoIP guarantees end-to-end security for VoIP-based voice connections.

Protection in insecure environments

Secure VoIP offers end-to-end security for voice communication and does not require special hardware. Companies can use this software to protect security-sensitive telephone conversations from unauthorized listening. This is particularly important when data connections are not sufficiently secure, for example when using a public hot-spot.

Works with almost every device

The prototype uses an AES algorithm for encrypting the voice channel and is based on J2ME, a programming platform supported by numerous cellular telephone manufacturers. When a voice connection is established, a cryptographic key is first negotiated between the end devices in a secure way (Diffie-Hellman method). The software then secures the voice transmission using this secret session key. The AES encryption with Secure VoIP works with almost every J2ME-capable cellular telephone, regardless of the manufacturer or data connection used (WLAN, UMTS or GPRS).

Speech quality

Encryption has no effect whatsoever on the acoustic quality of the transmission; noise, crackling and other interferences do not arise. Conventional cellular telephones do experience delays, however, which impede real-time communication. This is why a push-to-talk solution was chosen for the first implementation. The project team is also working on a port for other cellular telephone platforms, such as Symbian, to make optimum use of the performance capability of future end devices. To accelerate development, a tool was created within the framework of Secure VoIP that tests the performance capability of mobile telephones and their suitability for VoIP voice services.

What's next?

The Fraunhofer Institute SIT is providing support in the securing and further development of existing systems to manufacturers and suppliers of VoIP solutions.