nPA-VoIPS
SECURE VOIP TELEPHONY WITH THE NEW IDENTITY CARD

With the new German identity card businesses can quickly, conveniently and reliably determine the identities of internet users, even when using internet telephony. The new identity card allows internet telephone conversations to be recorded so they are both legally secure and audit-proof, as in the case of contract negotiations, for example. Fraunhofer SIT has developed a user-friendly procedure for recording tamper-proof internet telephone conversations and integrated the new identity card. The solution uses the electronic identity functions (eID) of the new German identity card (nPA) to guarantee confidentiality, integrity and authenticity as well as the signature function for archiving. Possible areas of application for this are the finance and insurance industry and the medical and legal fields.

Cloud Telephony Scenario
The nPA-VoIPS solution offers great flexibility in terms of its integration into various telephony infrastructures. Even cloud-based telephony services (IP Centrex) are supported. IP Centrex suppliers can offer services such as caller authentication and conversation archiving. The IP Centrex supplier’s offer can therefore be adapted to the service supplier’s individual needs, e.g. only authentication or archiving or both. This version is particularly cost-effective for the service supplier as its existing telephony infrastructure remains unchanged.

Fraunhofer SIT has developed a demonstration service and an associated client application. The service provides for a reliable authentication of the dialogue partners in VoIP telephone conversations by means of a two-factor authentication using the eID function of the nPA. Furthermore, the conversation content of the VoIP connections is transferred confidentially and with integrity. In addition, the signature procedure developed and patented at Fraunhofer SIT offers legally secure conversation archiving, both in terms of the service provider and client. Both dialogue partners receive a record of the recorded conversation.

The solution is particularly ideal for telephone applications which legally require authentication of the dialogue partners. This primarily concerns communication with persons who are committed to confidentiality for professional purposes, such as solicitors or doctors,
and the communication with authorities regarding applications and requests for information made over the telephone as well. Use in the commercial environment to increase security in telephone traffic is also planned. The new German identity card introduced in November 2010 forms the universal trust anchor. It has an ISO 14443 compliant RFID chip for the contactless reading of the holder’s data stored in the card. The new identity card allows every federal citizen to verify the identities of transaction partners on the internet and to build a secure connection for the confidential exchange of information.

Alongside the eID function, the new identity card also offers a certificate for the qualified electronic signature and thus represents the first signature card available nationwide. nPA-VoIPS uses the signature function of the identity card to legally sign documents. nPA-VoIPS thus allows the card holder as well as the service provider to file telephone conversations in a legally secure manner.

The eID function can also be used to authenticate dialogue partners in telephone conversations. The developed solution has the potential to be used in the entire German population as a result of the legal requirement to possess an identity card. Previous authentication solutions failed because of the lack of an infrastructure which could be applied nationwide as well as the high costs for purchasing additional hardware.

Further Information

Demonstrator-Website: http://voice-over-ip.sit.fraunhofer.de