End-to-end encryption protects against mass surveillance. Even though there are a number of solutions on the market, such technologies are scarcely used, because on a daily basis their use is much too complicated for most people. With Volksverschlüsselung Fraunhofer SIT is developing a simple potential use for end-to-end encryption. Volksverschlüsselung consists out of two parts: An infrastructure for registering and managing cryptographic codes, and a software that automatically installs these codes at the right location.

Layman-Suitable Software
The heart of Volksverschlüsselung is a software which installs the cryptographic keys at the right locations on the user’s computer. This software ensures that the mail program, browser and other applications on the computer are provided automatically with the codes. The software also generates the codes required for a secure end-to-end encryption and registers the public codes with the central infrastructure while the private codes never leave the user’s environment.

Transparent Infrastructure
Die The central infrastructure provides various services with which keys may be retrieved, reviewed or retracted. In the case of e-mail encryption the software ensures that the Volksverschlüsselung infrastructure (on the server side) will authenticate the public part first. Here the infrastructure functions as a kind of phone book, with which it enquires a user’s public key, in order to send the user an encrypted e-mail, for example.

Software distributes key to local applications.
Enhancements/Add-ons
Fraunhofer SIT is working on various enhancements, among other things a feature with which to transfer the keys securely from a desktop computer to mobile devices.

This is what Volksverschlüsselung supports:
- User friendly software for Windows
- Mac OS X, Linux, iOS and Android versions are in the planning stage
- Certification authority for key authentication
- Directory service for key retrieval
- Blocking service for lost keys
- Construct and continuously maintain a free infrastructure for a nationwide key roll-out

Software generates keys and certifies them.

Software distributes keys to other devices.