Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

PROJECT VOLKS-VERSCHLÜSSELUNG

SIMPLY SECURE

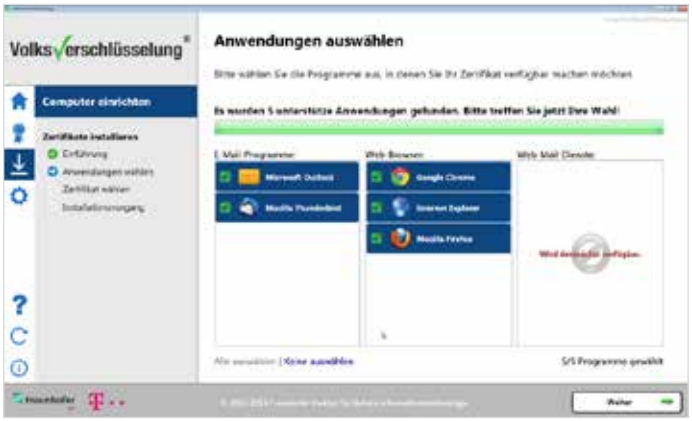
Fraunhofer Institute for Secure Information Technology SIT

Contact:
Michael Herfert
Rheinstrasse 75
64295 Darmstadt
Germany

info@volksverschluesselung.de
www.sit.fraunhofer.de
www.volksverschluesselung.de

End-to-end encryption protects against mass surveillance. End-to-end encryption ensures that only the sender and the recipient of an encrypted message will be able to read the message in plain. Even though many encryption solutions exist, they are hardly used. The reason for this is simple: the users don't have cryptographic keys. Fraunhofer SIT's Volksverschlüsselung simplifies the generation and distribution of cryptographic keys such that even IT nonprofessionals can easily manage it. Volksverschlüsselung consists of two parts: a software that automatically generates and installs the keys in the right places on a user's computer and an infrastructure for the registration and management of cryptographic keys. The programs, which the user is using anyway, will carry out the encryption itself e.g. email clients.

Volksverschlüsselung®



User Friendly Software

At its heart, Volksverschlüsselung is a software that generates cryptographic key pairs and installs them in the right places on a user's computer. It ensures that the keys will be provided to installed mail tools, browsers and other applications. The public parts of the keys pairs, required for end-to-end encryption, are registered with Volksverschlüsselung's central infrastructure. The private parts stay with the user and never leave the user's environment.

Transparent Infrastructure

Volksverschlüsselung's central infrastructure provides various services for retrieving, reviewing, or revoking keys. In addition, keys intended for email encryption will be certified by Volksverschlüsselung's infrastructure. When the certification process is completed, the infrastructure works similar to a phone book where everyone can look up and retrieve a user's public key, e.g., to send an encrypted or digital signed mail to a friend.

Future Versions

The Volksverschlüsselung's keys generated in Windows nowadays can be exported to Apple-Devices, Linux- and Android - Systems. In the medium term, separate software versions for these devices are planned.

Commercial Usage

A business version of the Volksverschlüsselung for commercial use, liable to pay costs, will be available soon.

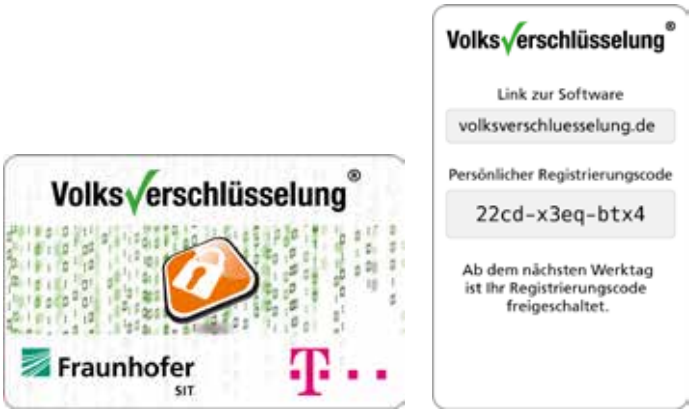
The free use for private purposes is not affected thereby.

This is what Volksverschlüsselung offers:

- User friendly software for Windows
- Free of charge for private purposes
- Source code is open
- Certification authority for public key accreditation
- Directory service for public key retrieval
- Revocation service for lost keys
- Maintenance of the central infrastructure for comprehensive roll-out of keys

This is how Volksverschlüsselung works

1. The user downloads the Volksverschlüsselung software at www.volksverschluesselung.de and runs it.
2. The Volksverschlüsselung software requests the user to perform a proof of identity at the Volksverschlüsselung server. For this, the user can choose between the online identification function of the German identity card, identification through an existing customer account at Deutsche Telekom, or a registration code obtained from an on-site registration. An alternative to on-site registration is the use of a citizen's terminal. Such terminals for the use of the new ID card will be made available in generally accessible places with the support of the buergerservice.org initiative.
3. The software asks the user to choose the email address for certification. The server sends an email with a verification code to the given email address in order to verify the user's ownership of the email account. The user confirms the email by entering the provided code into the Volksverschlüsselung software.
4. Cryptographic key pairs for the selected email address are generated on the user's computer. The private keys will be stored on the user's computer only. The public keys will be sent to the Volksverschlüsselung server for certification.
5. The server certifies the public keys and sends them back to the Volksverschlüsselung software at the user's computer.
6. The software configures the mail tools and browsers installed on the computer with the generated keys and certificates. After this, the user will be able to sign, encrypt and decrypt emails or verify its signatures.
7. The Volksverschlüsselung software offers certification management, for example certificate export to file (backup), certificate import, or certificate revocation (for example when the secret key has been lost) by using a lock-out password in order to permanently invalidate a certificate.



Registration card with the registration code for persons that have neither the online identification function on their identification card or a Telekom account.