Making message encryption easier

February 15 2016

Sending emails is as easy as pie. However, until now a lot of know-how has been required to securely encrypt them. This is bound to change: Deutsche Telekom and the Fraunhofer Institute for Secure Information Technology SIT in Darmstadt will be making encryption easy – with a popular encryption named Volksverschlüsselung. The Volksverschlüsselung software provides the required keys and configures the existing e-mail programs for the users to be able to encrypt and decrypt.

Developed by Fraunhofer, the Volksverschlüsselung solution will be operated by Deutsche Telekom in a high-security data center. The software is due to be available in the first half of 2016 and will be expanded in stages after its launch. The core of Volksverschlüsselung is

a software that makes it possible even for users without special IT-knowledge to overcome the technical obstacles of encryption. The software generates the requisite keys, and certifies and integrates them into applications. To be able to send encrypted emails, you have to install the program and identify yourself, whether through Deutsche Telekom's established log-in procedure or using your electronic ID card. The software then generates the cryptographic key on the user's device, allowing emails and data to be encrypted and signed. For the actual encryption itself, most users do not require a new program, as almost all e-mail programs have built-in encryption capability provided the relevant keys are available. Fraunhofer and Deutsche Telekom only receive the public keys. The private keys will never leave the user's computer, so only he will be able to encrypt or sign messages.

"Through our Volksverschlüsselung solution, we want to take cryptographic methods that are already established in research and finally make them available to everyone," emphasizes the director of Fraunhofer SIT, Professor Michael Waidner. The particular advantages offered by the method are described by Dr. Thomas Kremer, member of the Deutsche Telekom board of management responsible for data privacy: "Volksverschlüsselung is simple, free, and transparent. For us, it is the best tool for establishing e-mail end-to-end encryption among the public at large."

In the first stage, Volksverschlüsselung will enable Windows users to encrypt emails sent via programs such as Outlook or Thunderbird. Plans are to roll out versions for Mac OS X, Linux, iOS and Android. The software will initially support the S/MIME standard, and will eventually support OpenPGP as well. Fraunhofer will make the source code generally available. In this way, experts will be able to verify for themselves that Volksverschlüsselung does not have any back doors.

Provided by Fraunhofer-Gesellschaft