Encryption for everyone

March 16 2015

The aim of Public Encryption is to bring end-to-end encryption to the masses. Credit: Fraunhofer SIT

In the wake of the revelations that intelligence agencies have been engaged in mass surveillance activities, both industry and society at large are looking for practicable encryption solutions that protect businesses and individuals. Previous technologies have failed in practice because they were too expensive or not user friendly enough. Fraunhofer has launched an open initiative called "Volksverschlüsselung" with the aim of bringing end-to-end encryption to the masses. Fraunhofer researchers

will be presenting a prototype of their easy-to-use software and the infrastructure concept behind it at CeBIT 2015 (Hall 9, Booth E40).

Encryption is the most effective antidote to unwarranted, mass surveillance of people, companies and authorities. Although there are any number of computer programs designed to, say, make e-mail communication more secure, most people find them to be too much of a hassle. This is why the German government made establishing universal and easy-to-use encryption part of its Digital Agenda. A research team from the Fraunhofer Institute for Secure Information Technology SIT in Darmstadt developed a public encryption concept that factors in user friendliness from the outset. The software automatically installs the cryptographic keys in the right places on your computer. The researchers are also working on an infrastructure that will be available to everyone and is compatible with existing encryption services.

"With this initiative and what it's developing, Fraunhofer is supporting the German government's efforts to better protect people and companies," says Prof. Michael Waidner, Head of Fraunhofer SIT. This is why "Volksverschlüsselung" is to be made available as open-source software.

Key allocation for beginners

The software is the centerpiece of the solution. It relieves the user of the previously difficult task of allocating keys by recognizing which applications – different e-mail programs, for example – on your computer, smartphone or tablet can use cryptography and automatically allocates the right key to each one. The software also generates cryptographic keys that can be used to encrypt e-mails or files.

If you want to send someone an encrypted e-mail, you need the public key. In the "Volksverschlüsselung" model, you can obtain this from the

central infrastructure. "It works like a phone book," says project manager Michael Herfert. "Anyone can look up and download public keys. The central infrastructure also ensures that the keys actually belong to the person requesting them and helps prevent identity fraud." At CeBIT 2015, Fraunhofer researchers will demonstrate how people can register using the eID function of the German identity card. Other ways of registering are to be made possible in the future. To make it possible for a vast number of people to use the "Volksverschlüsselung" infrastructure, it would ideally have to be set up to handle several million keys. This calls for an infrastructure that is as efficient as it is secure. The current plan is to install the infrastructure on a high-security server at the Fraunhofer Institute Center in Birlinghoven near Bonn, and other trusted partners will also be able to participate soon.

Companies also stand to benefit from the results of the "Volksverschlüsselung" project – especially from the software. Solutions developed as part of the project could help small and medium-sized enterprises in particular by making it easier for them to implement encryption and thus better protect trade secrets.

Provided by Fraunhofer-Gesellschaft