Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

PROJEKT VOLKS-VERSCHLÜSSELUNG

EINFACH SICHER

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Michael Herfert
Rheinstraße 75
64295 Darmstadt

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

Ende-zu-Ende-Verschlüsselung schützt vor Massenüberwachung. Obwohl es viele Lösungen für Ende-zu-Ende-Verschlüsselung gibt, werden diese bislang kaum genutzt, weil die Anwendung im Alltag für viele Menschen zu kompliziert ist. Mit der Volksverschlüsselung entwickelt das Fraunhofer SIT eine einfache Nutzungsmöglichkeit für Ende-zu-Ende-Verschlüsselung. Die Volksverschlüsselung besteht aus zwei Teilen, einer Infrastruktur für Registrierung und Management kryptografischer Schlüssel sowie einer Software, welche die Schlüssel automatisch an den richtigen Stellen installiert. Die Verschlüsselung selbst geschieht mit den Programmen, die der Anwender ohnehin benutzt.

Volksverschlüsselung®

Ende-zu-Ende-Verschlüsselung stellt sicher, dass nur Sender und Empfänger Nachrichten im Klartext lesen können. Die Volksverschlüsselung des Fraunhofer SIT vereinfacht die Verteilung kryptografischer Schlüssel derart, dass selbst IT-Sicherheitslaien problemlos damit zurechtkommen.

Benutzerfreundliche Software

Das Herzstück der Volksverschlüsselung ist eine Software, die kryptografische Schlüssel an den richtigen Stellen auf dem Computer des Nutzers installiert. Sie sorgt dafür, dass die Schlüssel dem Mail-Programm, dem Browser und anderen Anwendungen auf dem Rechner automatisch zur Verfügung gestellt werden. Die Software erzeugt auch die Schlüssel, die für eine sichere Ende-zu-Ende-Verschlüsselung notwendig sind, und registriert die öffentlichen Schlüssel bei der zentralen Infrastruktur, während die privaten Schlüssel die Umgebung des Nutzers nie verlassen.

Transparente Infrastruktur

Die zentrale Infrastruktur stellt verschiedene Dienste zur Verfügung, mit denen sich Schlüssel abrufen, überprüfen oder zurückrufen lassen. Im Falle von E-Mail-Verschlüsselung lässt die Software die öffentlichen Anteile von der Infrastruktur der Volksverschlüsselung (Serverseite) beglaubigen. Anschließend fungiert die Infrastruktur als eine Art Telefonbuch, bei dem man die öffentlichen Schlüssel eines Nutzers erfragen kann, weil man ihm zum Beispiel eine verschlüsselte oder signierte Mail schicken möchte.

Zukünftige Versionen

Schlüssel, die von der Volksverschlüsselung unter Windows erzeugt wurden, können heute schon manuell auf Apple-Geräte, sowie auf Linux- und Android - Systeme übertragen werden. Mittelfristig sind eigene Software-Versionen für diese Geräte geplant.

Kommerzielle Nutzung

Eine kostenpflichtige Variante der Volksverschlüsselung, die eine berufliche Nutzung erlaubt, existiert unter dem Namen Key2B. Sie wurde speziell für kleine und mittlere Unternehmen entwickelt. Weitere Informationen unter www.key2b.de .

Das bietet die Volksverschlüsselung:

- Benutzerfreundliche Software für Windows
- Kostenlose private Nutzung
- Quelltext offen einsehbar
- Zertifizierungsstelle für Schlüsselbeglaubigung
- Verzeichnisdienst, um Schlüssel abrufen zu können
- Sperrdienst für verloren gegangene Schlüssel
- Pflege der Infrastruktur zur flächendeckenden Ausrollung von Schlüsseln

So funktioniert die Volksverschlüsselung

1. Der Nutzer lädt sich die Volksverschlüsselungs-Software von www.volksverschluesselung.de herunter und führt die Software auf seinem Rechner aus.
2. Die Volksverschlüsselungs-Software fordert den Nutzer auf, seine Identität nachzuweisen. Der Nutzer kann wählen, ob er dazu die Online-Ausweisfunktion des Personalausweises verwendet oder einen Registrierungscode, den er bei einer Vor-Ort-Registrierung erhalten hat. Eine Alternative zur Vor-Ort-Registrierung ist die Nutzung eines Bürgerterminals. Solche Terminals zur Nutzung des neuen Personalausweises werden mit Unterstützung der Initiative buergerservice.org an allgemein zugänglichen Stellen aufgestellt. Ein solches Terminal ist zum Beispiel in verschiedenen Stadtverwaltungen (Bonn, Darmstadt, etc.) zugänglich.
3. Die Software bittet den Nutzer, die E-Mailadresse auszuwählen, für die er ein Zertifikat beantragen möchte. Der Server schickt eine Mail mit Verifikationscode an den Nutzer, um die Mailadresse zu verifizieren. Der Nutzer bestätigt den Empfang der Mail, indem er den Code in die Volksverschlüsselungs-Software eingibt.
4. Auf dem Rechner des Nutzers werden kryptografische Schlüssel für die gewählte Mailadresse erzeugt. Die privaten Schlüssel werden nur auf dem Rechner des Nutzers gespeichert und die öffentlichen Anteile der Schlüssel zur Zertifizierung an den Server der Volksverschlüsselung geschickt.
5. Die Serverseite zertifiziert die öffentlichen Anteile der Schlüssel und schickt sie an die Volksverschlüsselungs-Software auf dem Rechner des Nutzers.
6. Die Software konfiguriert die auf dem Rechner vorhandenen Mailtools und Browser, so dass diese die Schlüssel unmittelbar nutzen können. Nun kann der Nutzer signierte und verschlüsselte Mails verschicken, entschlüsseln oder ihre Signaturen verifizieren.
7. Die Volksverschlüsselungs-Software bietet dem Nutzer die Verwaltung des Zertifikats an, z. B. das Zertifikat als Datei zu exportieren (Backup), ein Zertifikat zu importieren oder ein Zertifikat (z. B. nach Verlust des geheimen Schlüssels) mittels Sperrkennort zu widerrufen, d. h. dauerhaft für ungültig erklären zu lassen

Registrierungskarte mit Registrierungscode für Nutzer, die sich nicht über das Internet authentifizieren können.