Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

Fraunhofer-Institut für Sichere Informationstechnologie

Kontakt:
Michael Herfert
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-329
Fax 06151 869-224
michael.herfert@sit.fraunhofer.de
www.sit.fraunhofer.de

PROJEKT VOLKS-VERSCHLÜSSELUNG

EINFACH SICHER

Ende-zu-Ende-Verschlüsselung schützt vor Massenüberwachung. Obwohl es eine Vielzahl von Lösungen gibt, werden entsprechende Technologien 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 und einer Software, welche die Schlüssel automatisch an den richtigen Stellen installiert.

Software verteilt Schlüssel an lokale Anwendungen.

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.

Laientaugliche 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

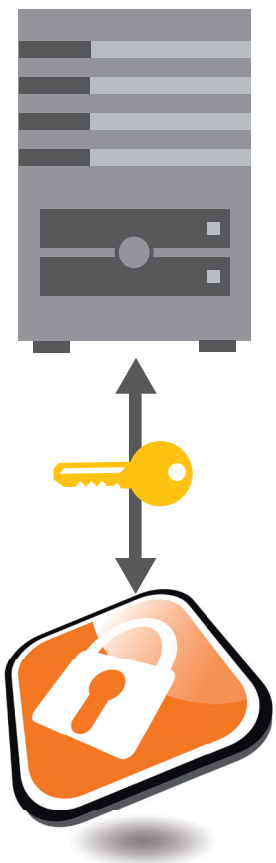
Die zentrale Infrastruktur stellt verschiedene Dienste zur Verfügung, mit denen sich Schlüssel abrufen, überprüfen oder zurückrufen lassen. Im Falle von E-Mail-Verschlüsselung lässt die Software zuerst die öffentlichen Anteile von der Infrastruktur der Volksverschlüsselung (Serverseite) beglaubigen.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

Erweiterungen/Ergänzungen

Fraunhofer SIT arbeitet an diversen Erweiterungen, unter anderem an einer Version, mit der sich die Schlüssel auch sicher vom Desktop-Computer an Mobilgeräte übergeben lassen. Darüber hinaus plant das Institut eine Ergänzung zur Ad-hoc-Verschlüsselung, mit der Benutzer auch spontan verschlüsseln können, ohne sich vorher bei der zentralen Infrastruktur registrieren zu müssen.

Das kann Volksverschlüsselung:

- Benutzerfreundliche Software für Windows
- Versionen für Mac OS X, Linux, iOS und Android sind geplant
- Zertifizierungsstelle für Schlüsselbeglaubigung
- Verzeichnisdienst, um Schlüssel abrufen zu können
- Sperrdienst für verloren gegangene Schlüssel
- Aufbau und kontinuierliche Pflege einer kostenlosen Infrastruktur zur flächendeckenden Ausrollung von Schlüsseln



Software erzeugt Schlüssel und lässt sie zertifizieren.

Software verteilt Schlüssel an weitere Geräte.