Im Folgenden haben wir **zentrale Fragen und Antworten** zur Volksverschlüsselung zusammengestellt. Weitere Fragen und Antworten, sowie Informationen zum Thema Volksverschlüsselung und Verschlüsselung allgemein finden Sie unter www.telekom.com/verschluesselung und unter www.volksverschluesselung.de.

Was ist die Volksverschlüsselung?

Mit der Volksverschlüsselung hat das Fraunhofer SIT eine Initiative gestartet, um die Nutzung von Ende-zu-Ende-Verschlüsselung in der Bevölkerung zu verbreiten und damit den Schutz der elektronischen Kommunikation von Privatpersonen sowie Unternehmen zu erhöhen. Mit der Veröffentlichung der Volksverschlüsselungs-Software starten das Fraunhofer SIT als Entwickler und die Deutsche Telekom AG als Betreiber der Infrastruktur das erste kostenfreie Angebot der Volksverschlüsselung.

Warum soll ich als Nutzer meine Mails überhaupt verschlüsseln?

Mit Verschlüsselung können Nutzer zum Beispiel sensible persönliche Daten besonders schützen, etwa E-Mails mit medizinischen oder finanztechnischen Informationen. Die unerlaubte Massenüberwachung von E-Mails verstößt zudem gegen das deutsche Grundrecht und bedroht auch die Meinungsfreiheit. Mit der Ende-zu-Ende-Sicherheit der Volksverschlüsselung sichern Nutzer deshalb zugleich ihre digitale Souveränität.

Was ist Ende-zu-Ende-Verschlüsselung?

Ende-zu-Ende-Verschlüsselung stellt sicher, dass ein Absender eine Nachricht so verschlüsselt, dass nur der intendierte Empfänger sie wieder entschlüsseln kann. Auch wenn die Nachricht auf ihrem Weg viele Server passiert, bleibt ihr Inhalt immer vertraulich. Das garantiert die Kryptografie.

Wie arbeitet die Volksverschlüsselungs-Software?

Die Software erzeugt zunächst auf dem Gerät des Nutzers die kryptografischen Schlüssel, mit denen sich E-Mails und Daten verschlüsseln und signieren

lassen. Nachdem der Nutzer seinen Registrierungsschlüssel eingegeben hat oder sich erfolgreich per DTAG Telekom Login (entspricht dem Anmeldeverfahren etwa an dem Kundencenter) oder dem elektronischen Personalausweis identifiziert hat, werden bei der Zertifizierungsstelle der Volksverschlüsselung digitale Zertifikate für Verschlüsselung, Authentisierung und Signatur erzeugt.
Nach Empfang der Zertifikate sucht die Software automatisch auf dem Gerät des Nutzers nach E-Mailprogrammen, Browsern und anderen Anwendungen, die Kryptografie nutzen können. Die Schlüssel und Zertifikate werden dann automatisch in die vorhandenen Anwendungsprogramme zur Nutzung der Zertifikate eingebracht.
Nach diesem einmaligen Schritt lassen sich E-Mails etwa in MS Outlook und Thunderbird einfach verschlüsseln und signieren.

Was ist das Besondere an der Volksverschlüsselung?
Die Volksverschlüsselung setzt auf Benutzerfreundlichkeit. Die Software übernimmt automatisch alle Schritte des Prozesses, angefangen von der Schlüsselerzeugung über die Zertifizierung bis hin zur Einrichtung und Konfiguration der Anwendungsprogramme auf den verschiedenen Geräten des Nutzers. Der Nutzer muss sich nicht mehr um die Installation der Schlüssel und Zertifikate und die Konfiguration der Anwendungen kümmern. Auch technisch weniger bewanderten Nutzern ist es somit möglich, ohne großen Aufwand ihre E-Mails und Daten zu verschlüsseln.

Welche Kosten/Gebühren fallen an?
Die Nutzung von Infrastruktur und Software ist für Privatanwender kostenlos.

Kann die Volksverschlüsselung auch mit Web-Mail genutzt werden?
Die Volksverschlüsslung stellt X.509-Zertifikate aus und unterstützt damit alle S/MIME-fähigen E-Mail-Clients. Die Integration in Web-Mail-Dienste ist anbieterabhängig und erfordert die Zusammenarbeit mit den Dienstanbietern. Eine enge Zusammenarbeit mit den Dienstanbietern wird vom Fraunhofer SIT

angestrebt, damit E-Mail-Verschlüsselung sich weit verbreitet und auch im Web zur Normalität wird.

Was ist S/MIME?

S/MIME heißt Secure / Multipurpose Internet Mail Extensions. Das ist ein internationaler Standard, der festlegt, wie verschlüsselte E-Mails verschickt werden. S/MIME nutzt X.509-Zertifikate.

Kann die Volksverschlüsselung auch mobil über Apps genutzt werden?

In einem ersten Schritt ist die Volksverschluesselung für Windows PCs ausgelegt. Perspektivisch soll die Verschlüsselungs-Software auch auf mobilen Geräten so einfach nutzbar sein wie im ersten Schritt für Windows. Hierzu ist geplant, Versionen für Android und iOS zu entwickeln, siehe nächste Frage.

Auf welchen Systemen läuft die Volksverschlüsselungs-Software?

Die Software gibt es bislang für Windows. Versionen für Mac OS X, Linux, iOS und Android sind geplant.

Ist die Volksverschlüsselung auf Hintertüren überprüfbar?

Ja. Wir wollen allen Interessierten freie Einsicht in den Source Code ermöglichen. So können sich Experten selbst davon überzeugen, dass keine Hintertüren (Backdoors) in der Software existieren. Außerdem veröffentlichen wir auch das Kommunikationsprotokoll, über das die Volksverschlüsselungs-Software mit der Zertifizierungsstelle kommuniziert.

Warum muss ich mich identifizieren?

Von der Volksverschlüsselung werden hochwertige Klasse 3-Zertifikate ausgestellt. Ein wesentliches Sicherheitsmerkmal dieser Zertifikate ist, dass die Identität des Zertifikatsinhabers im Rahmen der Zertifizierung zuverlässig festgestellt werden konnte.

Welche Anwendungen werden unterstützt?

Die Volksverschlüsselung erzeugt Zertifikate, die von allen E-Mail-Clients, Browsern und Web-Anwendungen genutzt werden können, die X.509 unterstützen. Von der neuen Software können aktuell die E-Mail-Clients MS Outlook und Thunderbird, sowie die Browser Internet Explorer, Chrome und Firefox automatisch zur Nutzung der Zertifikate konfiguriert werden. Die automatische Integration ist für weitere Anwendungen geplant, ebenso eine Unterstützung von OpenPGP in einem späteren Release.

Worin liegt der Unterschied zwischen Verschlüsseln und Signieren einer Nachricht?

Eine verschlüsselte Nachricht ist eine Nachricht, die auf dem Transportweg vollkommen unlesbar ist. Nur der Empfänger der Nachricht kann die Nachricht entschlüsseln, das heißt „lesbar“ machen.

Eine signierte Mail klärt eindeutig die Urheberschaft einer Mail. Das bedeutet: Mails können nicht mehr unter falschem Namen und vorgetäuschter Mailadresse verschickt werden.

Kann ich mithelfen, die Volksverschlüsselung weiterzuentwickeln?

Ja. Bitte wenden Sie sich dazu an Fraunhofer SIT (info@volksverschluesselung.de).