FAQ
Krypto-Kampagne der c’t

Antworten auf die häufigsten Fragen

Von Markus Will

Sinn der c’t-Krypto-Kampagne

? Bei Messen ist mir häufiger die c’t-Krypto-Kampagne aufgefallen. Was steckt dahinter?

! Die c’t-Krypto-Kampagne ist eine Initiative der c’t, die die Verschlüsselungsinfrastruktur stärken und Nutzern bei vertraulicher Kommunikation helfen soll. Seit 20 Jahren bietet c’t einen Verifizierungsservice für PGP/GPG-Schlüssel an, den Sie kostenlos in Anspruch nehmen können.

Der Inhalt einer unverschlüsselten E-Mail ist vor Blicken durch Dritte ähnlich schlecht geschützt wie eine Postkarte. Um dieses Manko zu beseitigen, programmierte der amerikanische Kryptoexperte Phil Zimmermann PGP (englisch „Pretty Good Privacy“, „ziemlich gute Privatsphäre“): eine Software, die E-Mails nach dem sogenannten Ende-zu-Ende-Prinzip verschlüsselt. Derartig verschlüsselte Mails können ausschließlich vom Verfasser und vom Empfänger gelesen werden, selbst Geheimdienste beißen sich die Zähne daran aus. GPG (auch GnuPG, „Gnu Privacy Guard“) wiederum ist ein Kryptografiesystem auf Open-Source-Basis, das sich wie PGP zum Ver- und Entschlüsseln von Daten eignet und elektronische Signaturen prüfen kann. GPG ist mit PGP kompatibel und weitgehend patentfrei.

PGP/GPG

? Wie sorgen PGP und GPG für mehr Sicherheit im Vergleich zu normalen Mails?

! Zentraler Bestandteil ist ein sogenanntes Schlüsselpaar (Code-Paar), welches aus einem öffentlichen Schlüssel (Public Key) und einem privaten Schlüssel (Private Key) besteht. Der private Schlüssel verbleibt beim Besitzer, ist passwortgeschützt und darf auf keinen Fall an Dritte weitergegeben werden. Der öffentliche Schlüssel hingegen wird weitergegeben, weil man nur mit ihm eine E-Mail für das angegebene Postfach verschlüsseln kann. Wenn als Beispiel Fred eine verschlüsselte Mail an Anna verschicken will, dann braucht er ihren öffentlichen Schlüssel. Damit verschlüsselt er die Nachricht und verschickt diese an Anna. Nur mit ihrem privaten Schlüssel kann sie den Inhalt dann entschlüsseln.

c’t-Signatur

? Ich habe mir einen öffentlichen Schlüssel generiert. Was hätte ich davon, ihn von c’t signieren zu lassen?

! Einen öffentlichen Key erstellt man unter Angabe der E-Mail-Adresse und eines Namens. Dabei kann aber auch ein falscher Name angegeben werden. Bei einem von uns zertifizierten Schlüssel hat der Empfänger die Sicherheit, dass sich der Absender uns gegenüber mit einem gültigen Dokument ausgewiesen hat. Der signierte Schlüssel sorgt also für Vertrauen und Glaubwürdigkeit.

Es gibt mehrere Möglichkeiten, eine Signierung von uns zu erhalten: Man kann sich bei uns am Messestand einen signierten Schlüssel generieren lassen. Das bieten wir auf Messen wie der CeBIT an. Außerdem können wir auch bereits bestehende Schlüssel signieren. Bei beiden Varianten muss man bei uns persönlich einen ausgefüllten Antrag auf Zertifizierung abgeben.

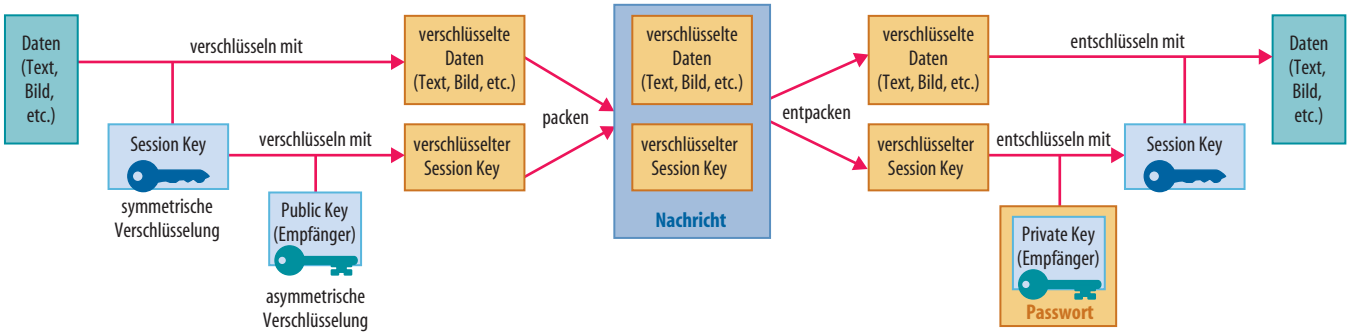
Alternativ kann man auch Anträge zu bestehenden Schlüsseln persönlich als Teilnehmer von Heise-Events abgeben. Zudem können Sie in unserem Verlagshaus (Heise Medien GmbH & Co. KG, Karl-Wiechert-Allee 10, 30625 Hannover) mittwochs von 16:30 bis 17:30 Uhr Ihren Antrag abgeben. In jedem Fall müssen Sie einen gültigen Personalausweis oder Reisepass mitbringen.

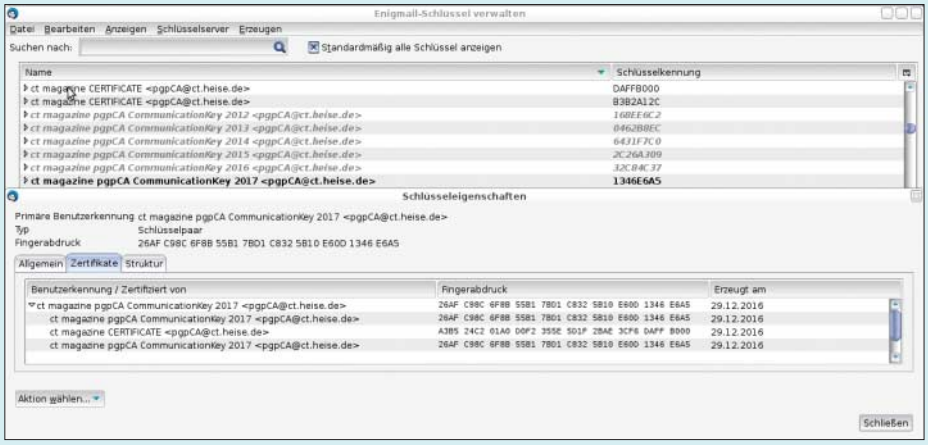
Programme für PGP/GPG

? Kann ich PGP/GPG-Verschlüsselung auch auf meinem Android-Handy nutzen?

PGP/GPG-Verschlüsselung

Detaillierter Ablauf einer Ende-zu-Ende-Kommunikation via PGP/GPG





Die Schlüsseleigenschaften: Der Fingerabdruck ist zentraler und unverkennbarer Bestandteil, da er sich nicht ändern lässt.

! Meist benötigt man für komfortables Verschlüsseln in einer Benutzeroberfläche zwei Komponenten: eine GPG-Installation sowie ein Plug-in für den Mail-Dienst. Unter Android hat sich die Kombination aus APG als Verschlüsselungstool und K-9 oder Kaiten als Mailprogramm bewährt. Wichtig: APG muss zuerst auf dem Smartphone installiert werden, da sonst das Mailprogramm nicht darauf zugreifen kann. Für Webmailer gibt es mittlerweile auch Lösungen: GPG lässt sich mit GMX und WEB.de über Firefox oder Chrome mithilfe des Plug-ins Mailvelope nutzen.

Bei Outlook unter Windows bietet sich GPG4Win an, für Thunderbird gibt es das Enigmail-Plug-in, welches unter GPG4Win funktioniert. In den meisten Linux-Distributionen ist GnuPG bereits vorinstalliert, für Apple Mail empfiehlt sich die GPG Suite.

Neue Mail-Adresse

? Ich habe kürzlich meinen E-Mail-Anbieter gewechselt. Kann ich den Schlüssel, der von c't zertifiziert wurde, auch mit meinem neuen Konto verwenden?

! Der alte Schlüssel kann um die zusätzliche Benutzerkennung der neuen Mail-Adresse erweitert werden. Es ist auch kein Problem, diese zur primären Adresse zu machen. Das von c't ausgestellte Zertifikat hat allerdings ausschließlich für die alte Mail-Adresse Gültigkeit. Wenn der Schlüssel für das neue Konto zertifiziert werden soll, muss also in jedem Fall ein neuer Antrag gestellt werden.

Passwort-Verlust

? Was passiert, wenn ich mein Passwort vergesse?

! Ohne den privaten Key lassen sich verschlüsselte Mails nicht mehr öffnen. Im schlechtesten Fall versauert der Schlüssel nicht nutzbar auf den PGP-Servern, da diese ein Löschen einzelner Schlüssel nicht vorsehen. Für genau den Fall empfiehlt sich ein Widerrufszertifikat (gpg –gen-revoke KeyID > MeinWiderrufszertifikat.txt), mit dem man einen Schlüssel auch ohne Passwort oder bei Verlust des geheimen Schlüssels für ungültig erklären kann.

Verschlüsselungszwang

? Muss ich zwangsläufig verschlüsselt mailen, wenn ich PGP/GPG installiert habe?

! Nein. Sie entscheiden selbst, ob Sie eine Nachricht verschlüsselt verschicken. Verschlüsselte Nachrichten haben nämlich auch Nachteile – beispielsweise kann man sie nicht über die Volltextsuche finden. Die Mail-Plug-ins erlauben es in der Regel, die Verschlüsselung je nach Wunsch an- und abzuschalten. Es ist sogar möglich, nur einen bestimmten Teil des Textes zu verschlüsseln. Auch Dateien auf Ihrer Festplatte können Sie mit PGP sichern.

Vorgehen nach Schlüssel-Erhalt

? Ich habe mir auf einer Messe einen Schlüssel erzeugen lassen. Was muss ich jetzt noch tun?

! Schicken Sie uns die Datei „an_pgpCA.asc“ per E-Mail an pgpca@heise.de. Bitte verfassen Sie die Mail als reine Textmail und kopieren Sie den Schlüsselblock in den Textteil – unsigniert und unverschlüsselt. Bitte achten Sie darauf, dass der Schlüsselblock keine Textumbrüche oder zusätzliche Leerzeilen enthält. Von welcher Adresse Sie die Mail versenden, spielt keine Rolle. Wir laden den öffentlichen Schlüssel auf unseren Server und versenden Überprüfungs-Mails an die Adressen aus dem Schlüssel. Etwas Geduld sollten Sie dabei haben: Die Bearbeitung der Zertifizierungsanträge kann einige Wochen in Anspruch nehmen.

Antrag per Mail

? Ich würde meinen Zertifizierungsantrag für einen Schlüssel gerne per Mail an die c't schicken. Geht das, wenn ich mit einem bereits zertifizierten PGP-Key unterschreibe?

! Wir pflegen bei der Zertifizierung eines Schlüssels einen sehr strengen Sicherheitsstandard. Aus diesem Grund nehmen wir ausschließlich eigenhändig abgegebene Anträge an. Selbst eine Mail mit bereits zertifiziertem PGP-Key erfüllt unsere Standards nicht, da der Schlüssel in der Zwischenzeit kompromittiert worden sein könnte. *(dahe@ct.de)* c't