

Verschlüsselte E-Mail-Kommunikation unter Linux

Florian Knodt <adlerweb@adlerweb.info>



Verschlüsselte E-Mail-Kommunikation unter Linux



Warum Verschlüsseln?

- Unverschlüsselte Verbindungen können von vielen Stellen abgefangen und manipuliert werden
 - Internetprovider, Netzbetreiber
 - Geheimdienste
 - Automatische Auswertung?
 - Der PC hat immer recht
 - Benutzer im selben Netzwerk
 - Ich könnte in der Nähe sein ;)

Demo: Mails mitlesen per Wireshark

SSL/TLS Benutzen!

- SSL/TLS verschlüsselt die Verbindung zwischen PC und Server
- Inhalt und Metadaten
- Zertifikat prüfen
- Zwischen/am Server unverschlüsselt

The image shows two overlapping windows from a Windows operating system. The foreground window is titled "Server-Einstellungen" (Server Settings) and displays the following information:

- Serverart: IMAP
- Server: mail.yotaweb.de
- Benutzername: (empty field)
- Sicherheit und Authentifizierung: **SSL/TLS** (highlighted with a red box)
- Authentifizierungsmethode: Passwort
- Server-Einstellungen: Beim Starten auf neue Nachrichten prüfen

The background window is titled "Zertifikat-Ansicht: 'mail.google.com'" (Certificate View: 'mail.google.com') and shows the following details:

- Verwendung: SSL-Server-Zertifikat
- Ausgestellt für:
 - Allgemeiner Name (CN): mail.google.com
 - Organisation (O): Google Inc
 - Organisationseinheit (OU): <kein Teil des Zertifikats>
 - Seriennummer: 31:BB:90:90:00:01:00:00:90:3A
- Ausgestellt von:
 - Allgemeiner Name (CN): Google Internet Authority
 - Organisation (O): Google Inc
 - Organisationseinheit (OU): <kein Teil des Zertifikats>
- Validität:
 - Ausgestellt am: 02.07.2013
 - Läuft ab am: 01.11.2013
- Fingerabdrücke:
 - SHA1-Fingerabdruck: 17:C8:BE:59:77:C8:C7:3D:85:FC:5B:68:BF:67:65:E3:C1:D8:BF:43
 - MD5-Fingerabdruck: 8D:36:99:45:34:73:82:C4:DB:04:F3:51:80:B9:E4:AC

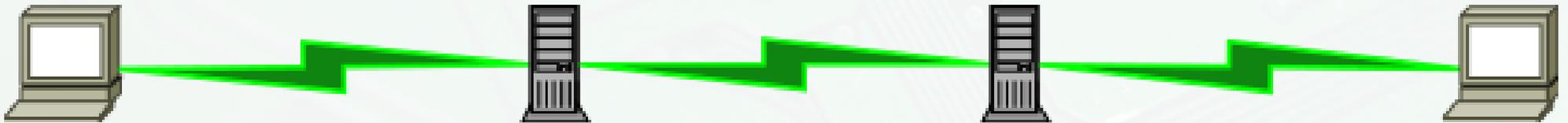
Below the windows, a browser address bar shows a secure connection: <https://mail.google.com> with a lock icon.



Demo: Mails am Server abfangen

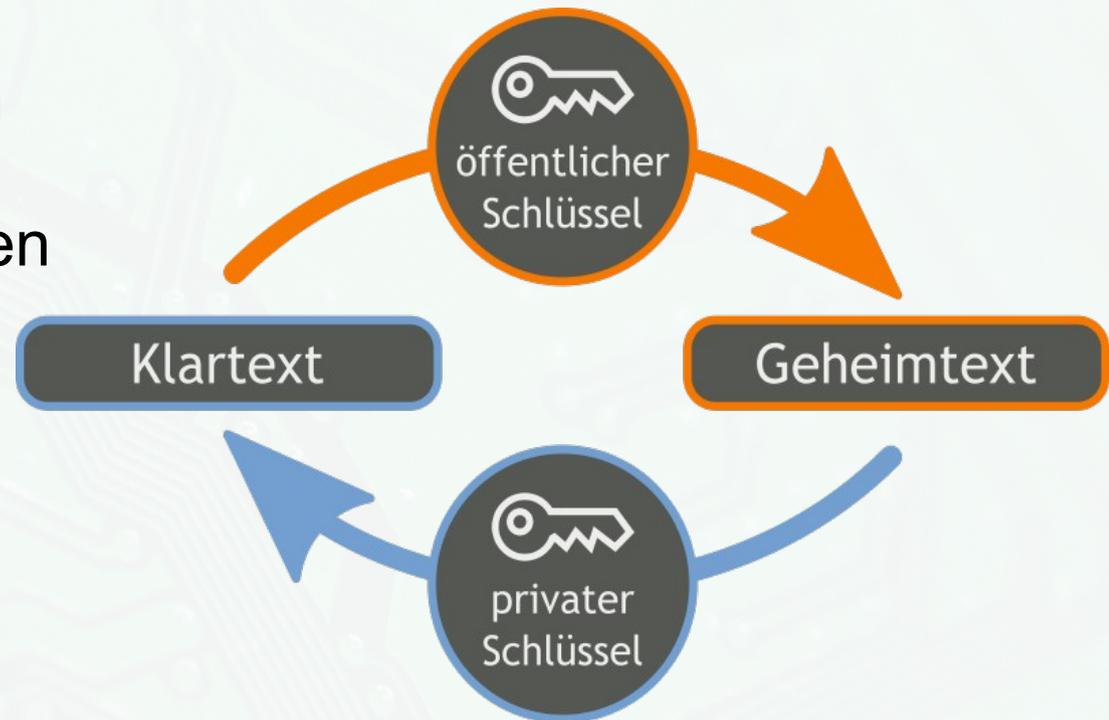
Inhaltsverschlüsselung

- Mailinhalt wird zwischen den Kommunikationspartnern verschlüsselt
- Sender und Empfänger müssen sich bereits kennen
 - Keyserver lockern diese Einschränkung



Asymmetrische Kryptografie

- Nicht wie bei symmetrischen Verfahren ein Passwort
- Schlüssel besteht aus 2 Teilen
 - Öffentlicher Schlüssel:
Nur verschlüsseln
 - Privater Schlüssel:
Nur entschlüsseln



Standard 1: S/MIME

- Auf X.509 aufbauend
 - Hierarchische Struktur; Zentrale Zertifizierungsstellen
 - Freie Anbieter haben nur wenig Prüfung
 - Gute Prüfung gegen Geld
- Wird von fast allen Mailclients direkt unterstützt
- z.T. auch als Browser-Plugin für Webmail

Standard 2: PGP



- Basiert auf einem dezentralen WOT
 - Vertrauen muss „erarbeitet“ werden
- Freie Implementierung: GnuPG / GPG
- Für die meisten Mailsysteme als Plugin verfügbar
- Für Firefox und Chrome als Plugin verfügbar
- GPG ist nicht auf E-Mail beschränkt

Demo: PGP mit Thunderbird und Enigmail

Demo: PGP im Browser

Was bleibt

- Inhalt Ende-zu-Ende verschlüsselt
- Metadaten nur teilweise verschlüsselt
 - ~~Vorratsdatenspeicherung~~ Mindestspeicherfrist greift weiterhin!

...und der Rest?

- Webseiten
 - HTTPS nutzen
 - Tor & Co kann bedingt anonymisieren
- Chat
 - z.B. Pidgin mit OTR, Xabber oder Gibberbot auf Android
- Social Media
 - Dezentralen Systemen wie statusNET und Diaspora die Daumen drücken

Fragen?

- ...werden auch verschlüsselt entgegen genommen:

f.knodt@yotaweb.de GPG 0x3DF6966D