AUSSPÄHUNG VON BERUFSGEHEIMNISTRÄGERN IN ZEITEN DIGITALER ÜBERWACHUNG

Jürgen Fricke, procube systementwicklung
http://procube.com,
fricke@procube.com

„Wie die Schnecke, die ihr Haus immerzu bei sich trägt, so müssen die Beschäftigten in der schönen neuen flüchtigmodernen Welt ihr jeweils persönliches Panoptikum selbst hervorbringen und auf dem eigenen Buckel mitschleppen.“

Zygmunt Baumann

Situation

Alle beteiligen sich Tag für Tag am allgemeinen Daten-Striptease. Ob über das Internet, *sichere* Computernetzwerke, *billige* Clouds oder *günstige* weltweit verfügbare Bildtelefonie. Auch die allgegenwärtigen Smartphones erzeugen oftmals unabsichtlich zahlreiche Datenspuren im Netz.

Wer wertet das aus, und (wie) können wir uns dagegen schützen?

Schlagzeilen

Historiker Foschepoth über US-Überwachung
"Die NSA darf in Deutschland alles machen"
SZ-online, 9.7.2013

Anders als die grüne Bewegung haben wir keine Robben
CONSTANCE KURZ, DATENSCHÜTZERIN

Kritik an Überwachung von Journalisten
Niedersachsens Verfassungsschutz sammelte Daten von Neonazi-Expertin Röpke / SPD und Grüne fordern Aufklärung

FR, 20.9.2013

weitere Schlagzeilen

Verfassung instandsetzten
Dokumentation: Überwachungsstaat Bundesrepublik Deutschland?
Historische Grundlagen und Notwendige Konsequenzen.
Vortrag von Josef Foschepoth

junge Welt, 3.9.2013

Kanzlerin Merkel verspricht:
"Alle Materialien aus dem Kanzleramt und vom BND werden dem NSAUA zugeliefert"

netzpolitik.org, 15.5.2015

GOOGLE, Macht und Missbrauch

SZ, 2.9,2013

online: Googles Datenmacht zahlt sich aus

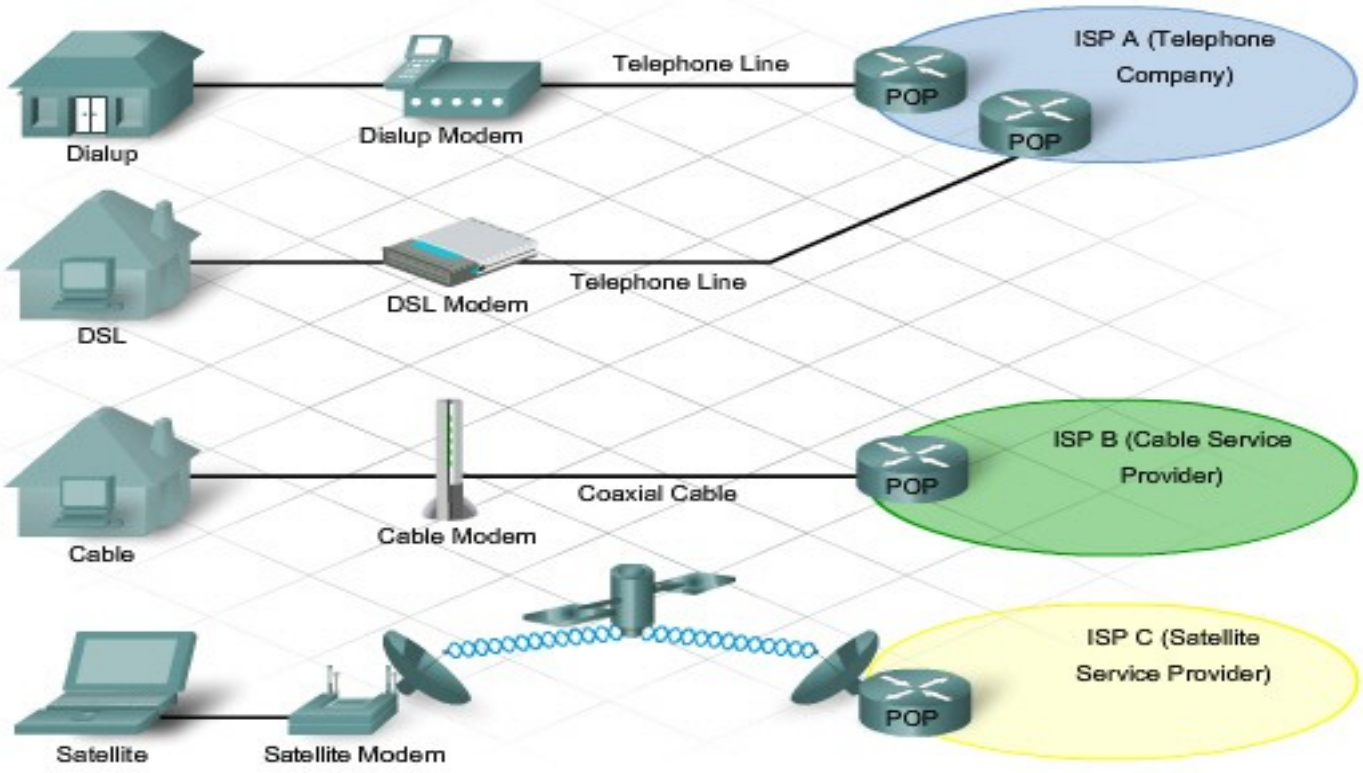
Authentizität

Das Authentifizieren von elektronischen Daten ist ein weiterer bedeutsamer Punkt. Wie zuvor erwähnt, ist es möglich, die Absenderadresse und den Inhalt einer E-Mail zu fälschen.
Für unsere Korrespondenz, den Austausch von Dokumenten und das Abwickeln von Geschäftsvorgängen über das Internet ist es wichtig, den Absender eindeutig zu identifizieren und dass die Integrität der Daten überprüfbar ist. Auch das Leserecht ist zu kontrollieren.

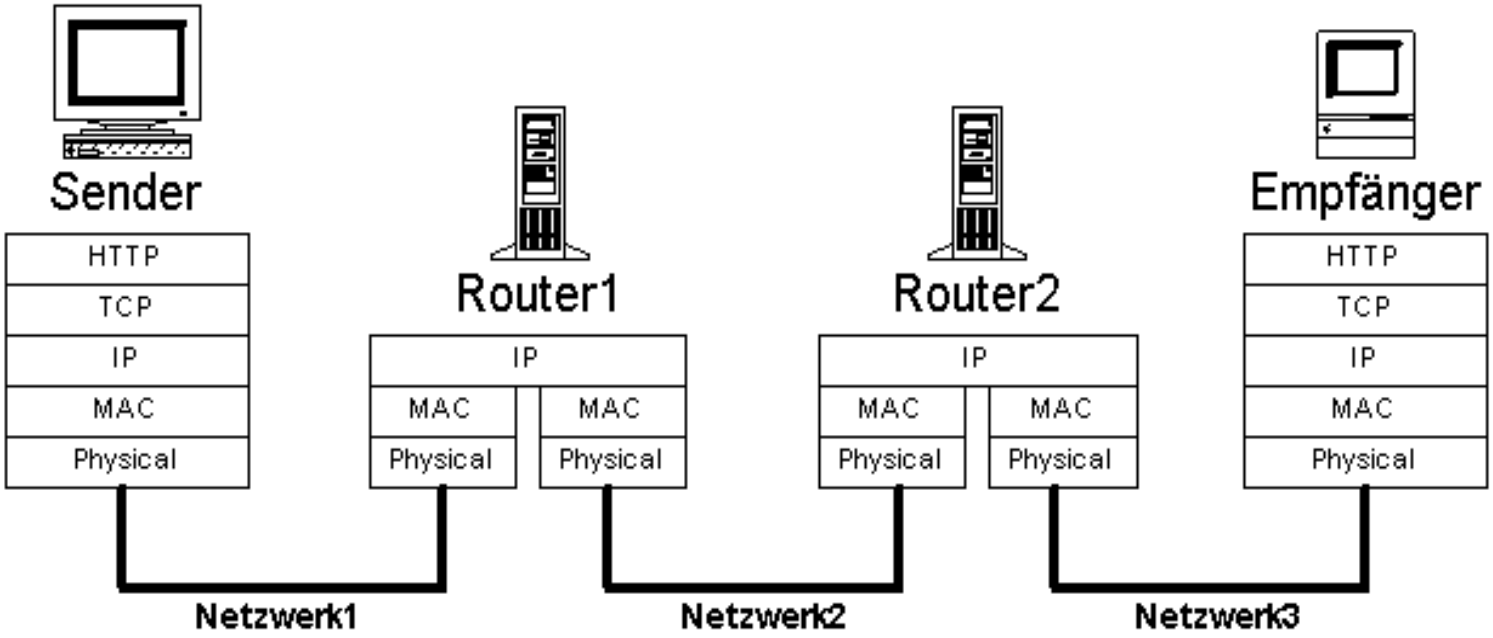
Ihre Daten - Unsere Kommunikation?

Wenn Dokumente via E-Mail unverschlüsselt übermittelt werden, ist deren Inhalt weniger vertraulich als der einer mit Bleistift beschriebenen Postkarte.
Administratoren Ihres Mail-Relays wie auch EDV-Beauftragte des Empfängers können ohne Weiteres Ihre E-Mails lesen, abfangen oder verändern. Auf ihrem Weg zum Empfänger durchlaufen E-Mails häufig etliche Router und Rechner.
Weltweit schnorcheln übergriffige Institutionen massiv Daten aus unserer Kommunikation.

Verbindungen im Büro (LAN)



IP-Routing



Die Notation der IPv4-Adressen besteht aus vier Zahlen, die Werte von 0 bis 255 annehmen können und mit einem Punkt getrennt werden, beispielsweise 10.0.70.42. Technisch gesehen ist die Adresse eine 32-stellige (IPv4) oder 128-stellige (IPv6) Binärzahl.

IP-Adressen

Eine IP-Adresse ist eine Adresse in Computernetzen, die – wie das Internet – auf dem Internetprotokoll (IP) basiert. Sie wird Geräten zugewiesen, die an das Netz angebunden sind, und macht die Geräte so adressierbar und damit erreichbar. Die IP-Adresse kann einen einzelnen Empfänger oder eine Gruppe von Empfängern bezeichnen (Multicast, Broadcast). Umgekehrt können einem Computer mehrere IP-Adressen zugeordnet sein.

Übermittlungswahrheit

Beispiel:

Geschäftspartner erstellen täglich zahlreiche Belege, die elektronisch dargestellt und einmal pro Woche im Stapel verarbeitet werden. Diese Dokumente werden wie vereinbart und üblich in Postscript erstellt. Man vertraut seit Langem auf die Partnerschaft und die hier kurz umrissene alltägliche kaufmännische Praxis.

Preisfrage

Es fällt niemandem auf, dass *während* der Übertragung einer der zahlreichen Belege gefälscht wurde.
Alle Datensichtgeräte stellen den vereinbarten Kaufpreis mit 15.317,45 € scheinbar korrekt dar. Mit einer Ausnahme: Bei einem der Beteiligten wird das Dokument verfälscht dargestellt.

Fehlerkultur?

Das Opfer, ein verlässlicher Mitarbeiter mit Prokura, erkennt auch auf *seinem* Ausdruck 16.317,45 € und zahlt diesen Betrag.

In diesem Beispiel wurden Dokumente gezielt *während* der Übertragung verfälscht. Ein mehrfaches Ausnutzen dieser technischen Lücke verursacht hier beträchtlichen Schaden für die beteiligten Geschäftspartner.

Bis zur Aufklärung wird das Vertrauen der Geschäftspartner belastet.

Five Eyes - Cyberpolizei?

Die Situation ist vergleichbar mit einem Hühnerstall auf diesen passen ausgerechnet fünf Füchse auf. Das ist für ein Kartell oder Oligopol nur logisch, oder?

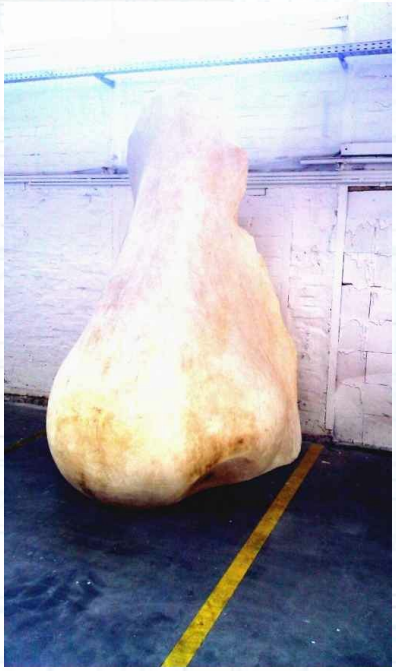
Ergibt sich daraus warum es auf uns nur *natürlich* wirkt, wenn ab und an ein Huhn *verschwindet?*

Visualisierte Verkehrsdaten

Es gibt zahlreiche Instrumente für das Beobachten und Auswerten von Verkehrsdaten.

Siehe bitte lfd. Visualisierung

zur Darstellung des Netzwerkdatenverkehrs auf dem Test-PC.



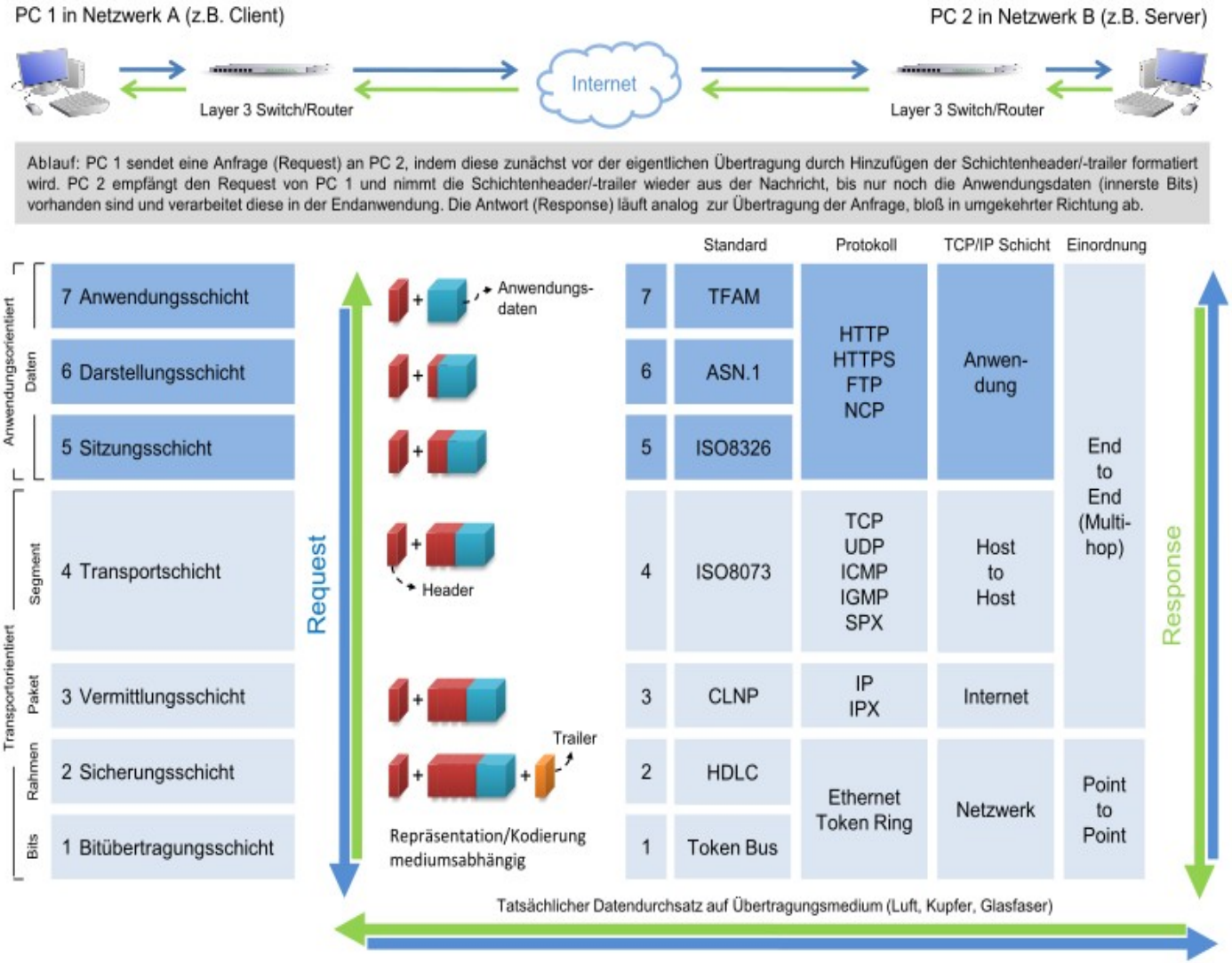
Klartext oder was ist WYSIWYG?

Klartext – beinahe nichts ausser Klartext ?

Was wir im Kabel tatsächlich übertragen und was sehen wir auf dem Bildschirm?

Desktop-Software stellt Ihre Daten auf Ihrem Datensichtgerät dar. Diese Daten entsprechen nicht den übermittelten oder vorgehaltenen Daten. Sie wurden aufbereitet. D.h. Daten werden verarbeitet bevor diese wie gewohnt lesbar dargestellt sind.

Kommunikation im OSI-7-Schicht-Modell (Open Systems Interconnection Reference Model)



Warum Kryptographie?

Angewandte Kryptographie gewährleistet

- Vertraulichkeit

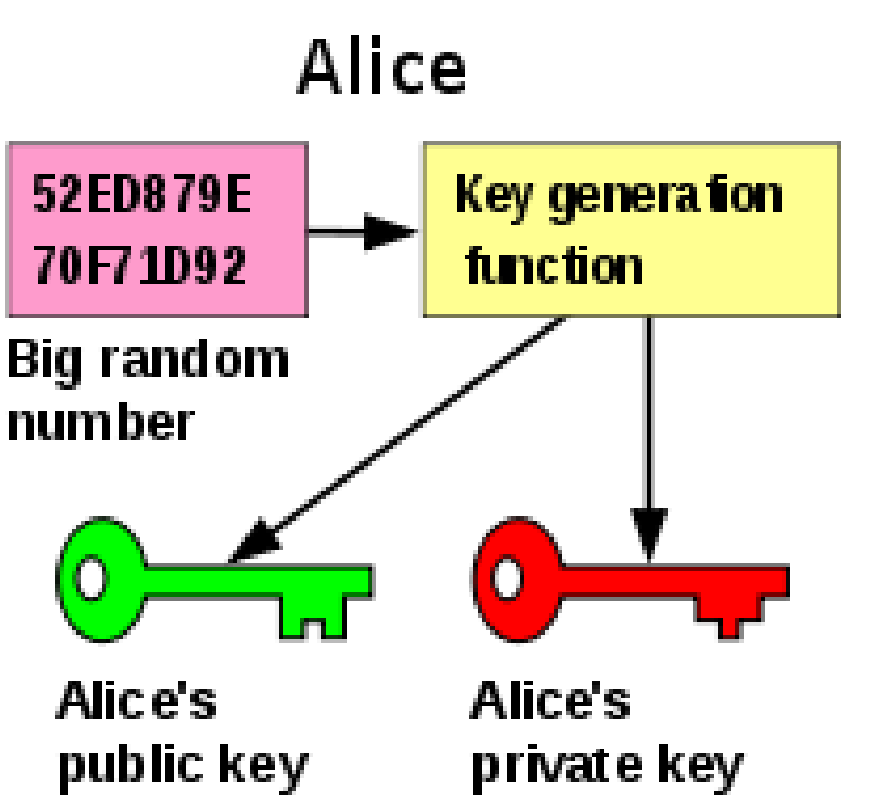
- Integrität und

- Authentizität

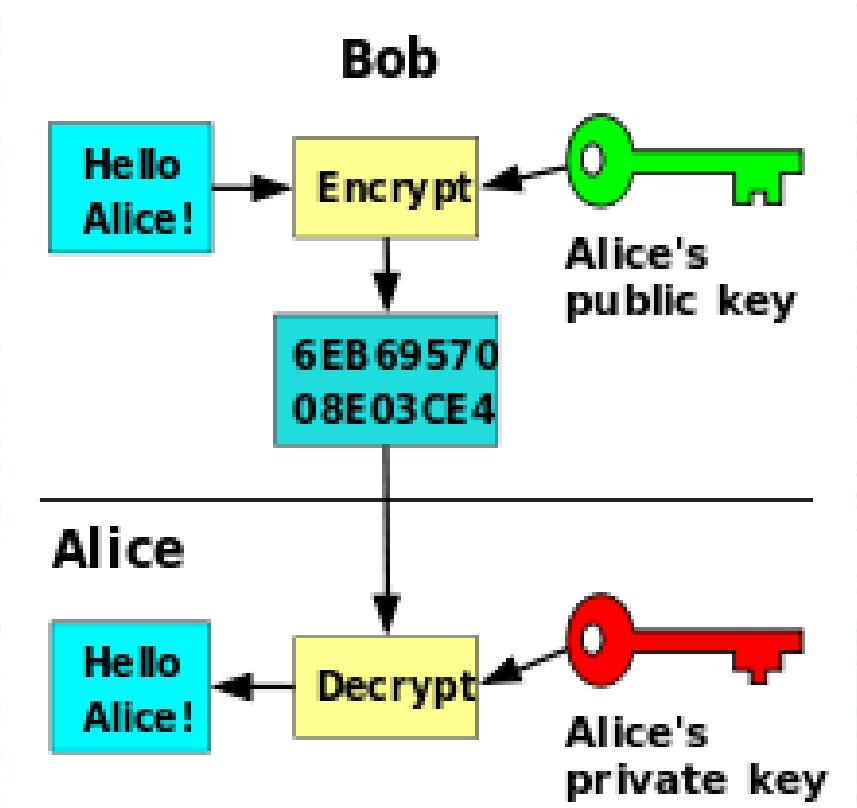
Digitaler *Briefumschlag* & Signatur

Die einzige Möglichkeit, um Vertraulichkeit, Integrität und Authentizität von elektronischen Dokumenten zu gewährleisten, ist die Benutzung wirkungsvoller kryptographischer Verfahren, wie sie bei GnuPG Anwendung finden. Durch Verschlüsselung erreichen Sie, dass Ihre Daten nur von den Personen gelesen werden können, denen Sie ein Leserecht gewähren. E-Mails werden quasi in einem *blickdichten Briefumschlag* übertragen und ggf. signiert.

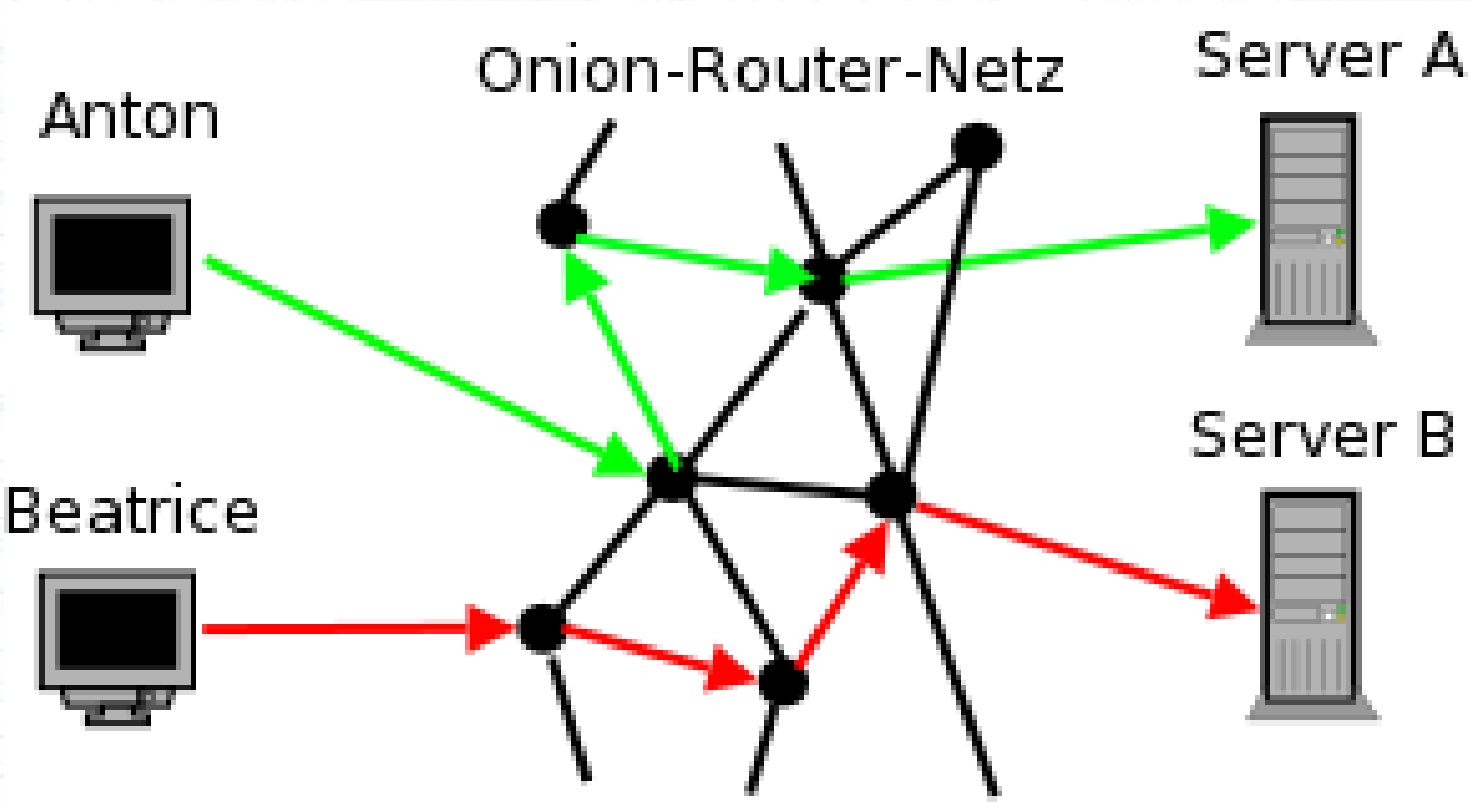
Asymetrische Verschlüsslung



Chiffrieren und Dechiffrieren



Anonym surfen - Das Tor-Netzwerk



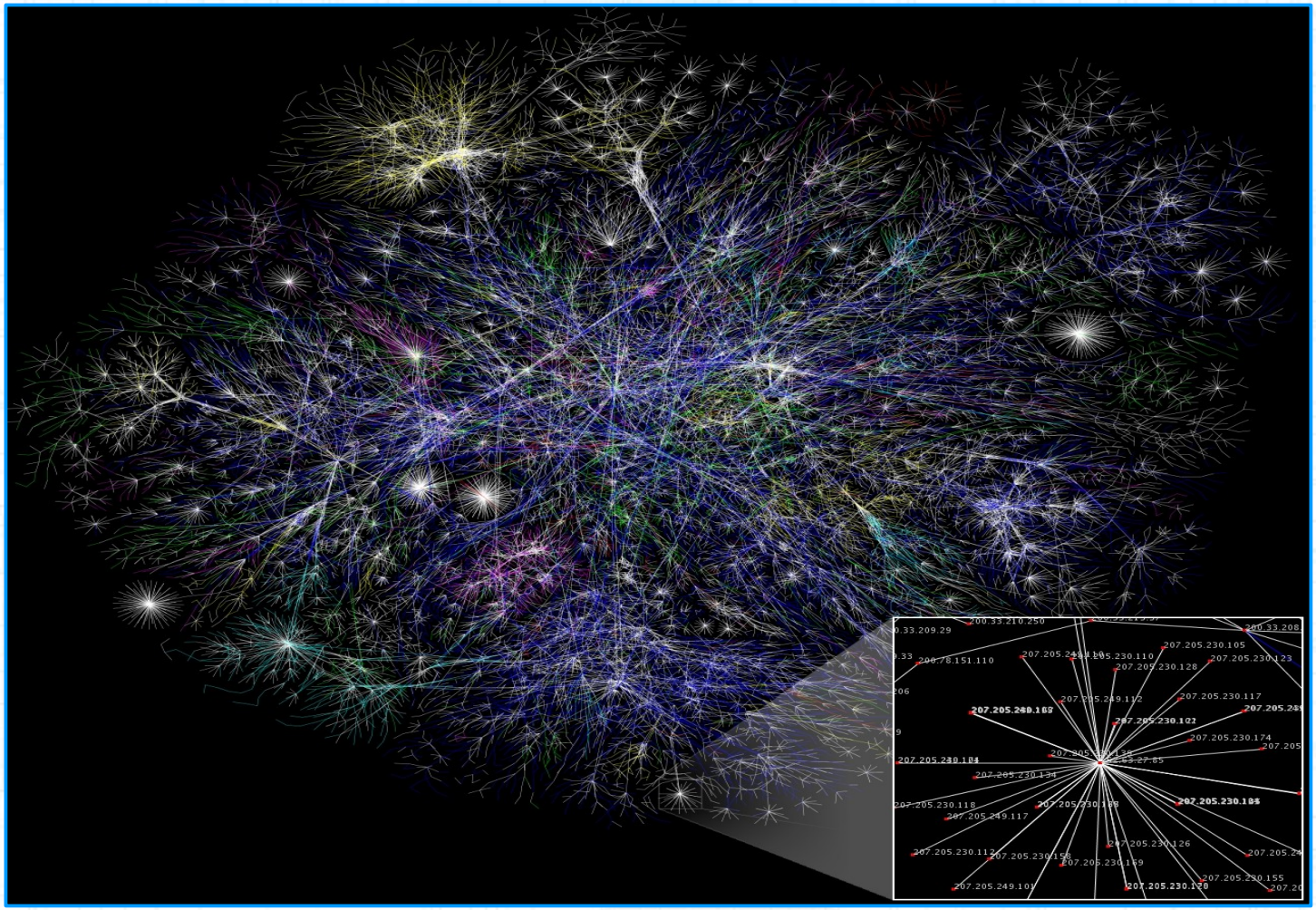
IP-Adressen und ihre Verwendung

Die IP-Adresse wird verwendet, um Daten von ihrem Absender zum vorgesehenen Empfänger transportieren zu können. Ähnlich der Postanschrift auf einem Briefumschlag werden Datenpakete mit einer IP-Adresse versehen, die den Empfänger eindeutig identifiziert. Aufgrund dieser Adresse können die „Poststellen“, die Router, entscheiden, in welche Richtung das Paket weitertransportiert werden soll. Im Gegensatz zu Postadressen sind IP-Adressen nicht an einen bestimmten Ort gebunden.

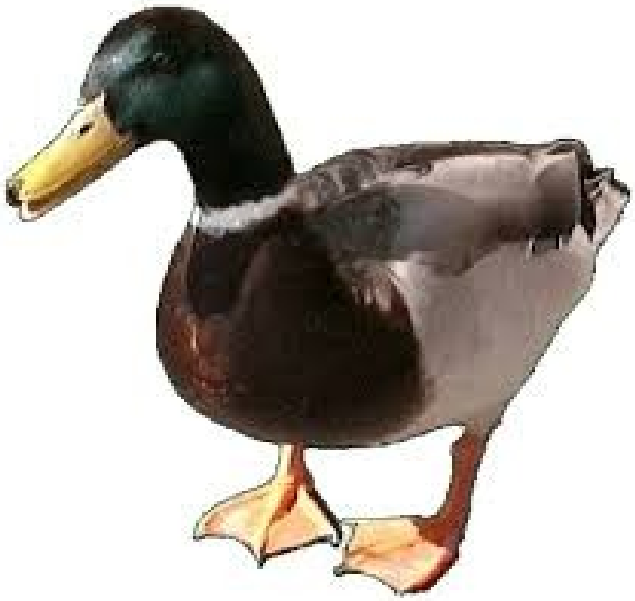
Das OSI-Modell

Das OSI-Modell, englisch Open Systems Interconnection Model, ist ein Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur. Es wird seit 1983 von der International Telecommunication Union und seit 1984 auch von der International Organization for Standardization als Standard veröffentlicht.
Seine Entwicklung begann im Jahr 1977.

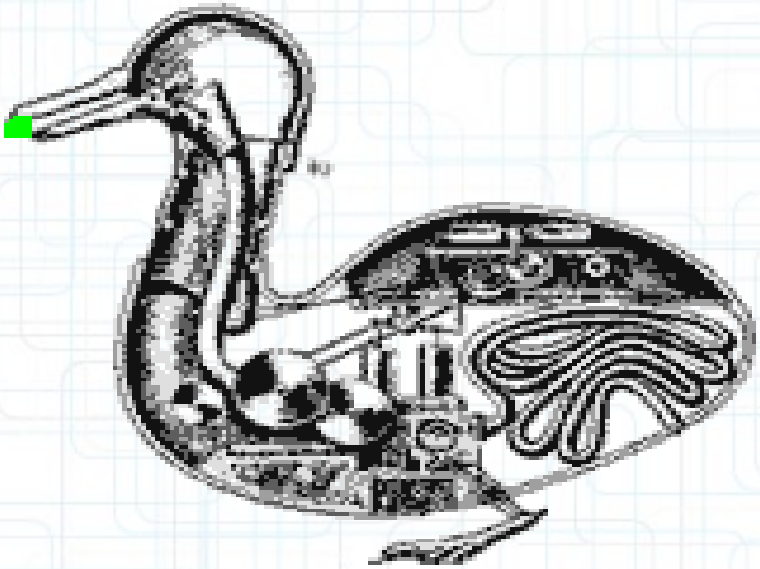
Das Netz, eine komplexe Sache



Alles Lebendige ist komplexer …



… als vereinfachende Darstellungen!



Praxis:

Voraussetzungen für Enigmail OpenPGP

Neben Thunderbird und einer passenden Enigmail-Version benötigen Sie nur noch die OpenPGP Verschlüsselungs-Software GnuPG Version 1.4.11 oder neuer. Die aktuellen Versionen für Windows enthalten inzwischen auch ein Installationsprogramm, das die Einrichtung der Software relativ einfach macht.

GnuPG

Praxis: Installation

1. Installieren Sie Thunderbird
2. Installieren Sie GnuPG
3. Installieren Sie Enigmail in Thunderbird über den Add-ons-Manager

Praxis:

Thunderbird Installation

1. Herunterladen der aktuellen Version über
   http://thunderbird-mail.de/wiki/Herunterladen

2. z. B: C:\Programme\Thunderbird

GnuPG

Praxis:

GNUPG installieren

1. Bezug der aktuellen Software via http://gnupg.org/download/
2. Die Software in ein Verzeichnis Ihrer Wahl installieren

   z. B: C:\Programme\GNUPG\

Hinweis

Verwenden Sie unter Windows nur GnuPG ab Version 1.4.x

Praxis:

Empfangen chiffrierter E-Mails

Um eine Mail zu lesen, die verschlüsselt/signiert ist, klicken Sie auf die Schaltfläche „Entschlüsseln“ in der Symbolleiste:

Damit wird die E-Mail entschlüsselt und/oder die enthaltene Signatur verifiziert. Wenn Sie eine signierte E-Mail bekommen haben und deren Unterschrift überprüfen möchten, benötigen Sie den öffentlichen Schlüssel des Absenders.

Im Bereich der Kopfzeilen der angezeigten Mail haben Sie nun, je nachdem ob die E-Mail signiert und/oder verschlüsselt war,bis zu zwei Symbole: einen Briefumschlag und ein Vorhängeschloss.

Praxis:

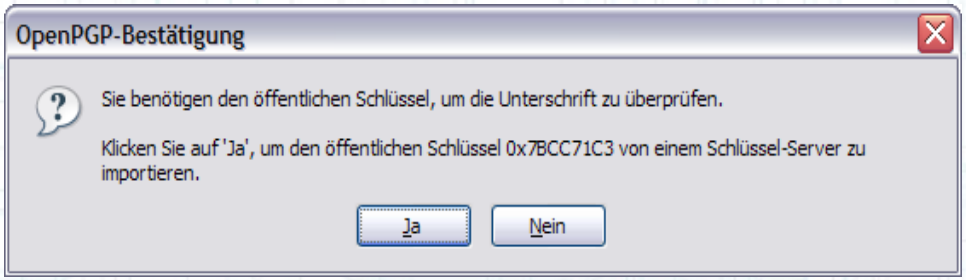
Prüfen der Signatur

Ein Linksklick auf den Briefumschlag oder das Vorhängeschloss zeigt die OpenPGP-Sicherheitsinformationen zu der erhaltenen E-Mail an:

Praxis:

Schlüssel vom Keyserver importieren

Wenn Sie nicht im Besitz des öffentlichen Schlüssels sind, weist Enigmail Sie mit einem Dialog darauf hin:



Mit einem Klick auf „Ja“ bringt Enigmail dann den folgenden Dialog:

Praxis:

Schlüssel unbekannt?

Falls erforderlich, können Sie den gewünschten Schlüssel-Server auswählen und dann mit einem Klick auf „O. k.“ veranlassen, dass Enigmail den Schlüssel auf einem Schlüssel-server sucht.

Wenn der Schlüssel auf dem Schlüsselserver verfügbar ist, importiert Enigmail diesen in Ihren Schlüsselbund. Sie erhalten dann noch eine etwas kryptisch aussehende Meldung, in der aufgelistet wird, welche(r) Schlüssel importiert wurde(n).

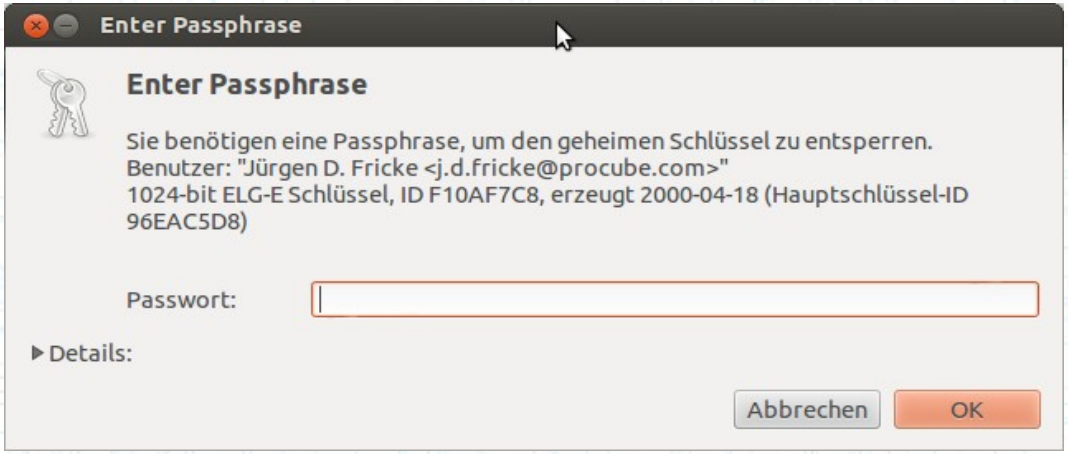
Beachte!

Sollte der Schlüssel nicht auf dem Schlüssel-server gefunden werden, so informiert Enigmail Sie auch darüber. Fordern Sie dann den Schlüssel direkt vom E-Mail-Partner an.

Praxis:

Passphrase eingeben

Wurde die Nachricht nicht nur signiert, sondern auch verschlüsselt, fordert Enigmail Sie zur Eingabe der Passphrase auf:



Klartext :-)

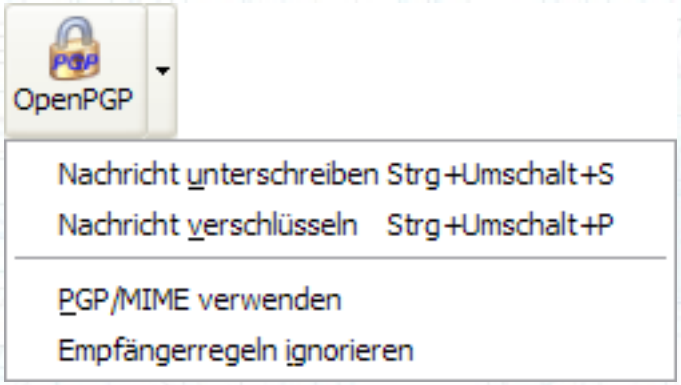
Die chiffrierte Nachricht wird dann lesbar als Klartext dargestellt.

Praxis:

Verfassen chiffrierter E-Mails

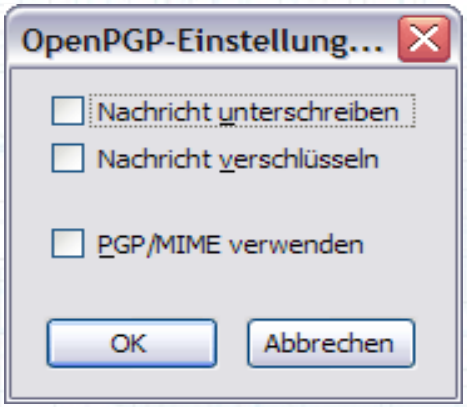
Um eine E-Mail zu signieren und/oder zu verschlüsseln, gehen Sie folgendermaßen vor:

Starten Sie Thunderbird und verfassen Sie wie gewohnt eine neue Nachricht. Anschließend klicken Sie in der Funktionen-Symbolleiste des „Verfassen“-Fensters auf den kleinen Pfeil an der OpenPGP-Schaltfläche und wählen die gewünschte Option aus:



Praxis:

Verfassen chiffrierter E-Mails



Wählen Sie „Nachricht unterschreiben“, um die Nachricht zu signieren.

Wählen Sie „Nachricht verschlüsseln“, um die Nachricht zu verschlüsseln.

Wählen Sie „PGP/MIME verwenden“, um die Nachricht mit Hilfe von PGP/MIME zu signieren/verschlüsseln. Leider wird dies noch nicht von allen PGP-fähigen Programmen unterstützt.

Wählen Sie „Empfängerregeln ignorieren“, um evtl. konfigurierte Empfängerregeln nicht auszuführen. Das ist insbesondere dann interessant, wenn Sie die E-Mail an mehrere Empfänger senden.

Praxis: Verfassen chiffrierter E-Mails

Unten im „Verfassen“-Fenster sehen Sie einen kleinen Stift und ein Schloss. Durch Anklicken wird die E-Mail entweder signiert (Stift) und/oder verschlüsselt (Schloss).

Sobald Sie die E-Mail fertig geschrieben und die OpenPGP-Optionen ausgewählt haben, können Sie wie gewohnt die Nachricht absenden. Ggf. wird erneut ein Passwort verlangt.

Hinweis PGP/Mime

Wenn Sie Nachrichten in HTML schreiben oder möchten, dass der Anhang auch verschlüsselt wird, sollten Sie unbedingt PGP/MIME verwenden!

GnuPG

Weiterführende Literatur und NGOs

Verein für Bürgerrechte und Datenschutz:
Digital Courage e.V. http://digitalcourage.de/

Offenes Netzwerk und Non-Profit-Organisation für Anonymität im Internet:
http://www.torproject.org

Vereine die Weiterbildung und Aufklärung unterstützen:
Zwiebelfreunde e.V., http://zwiebelfreunde.de

Initiative gegen Totalüberwachung e.V.
http://gegen-totalueberwachung.de

Kurzbeschreibung und Bestellung PrivacyDongle:
http://foebud.org/privacydongle-2013-anonymes-surfen-im-internet
https://www.bsi.bund.de/cln_174/ContentBSI/Themen/ProdukteTools/

Mehr zur GNUPG card via http://g10code.com

Laientaugliche Darstellung für anonymes Surfen und
Verschlüsselung von E-Mails:
Jörg Schieb, Mirko Müller
PC konkret - Meine Daten schützen
Stiftung Warentest, 12,90 €
ISBN 978-3-937880-62-4

Vielen Dank für Ihre Aufmerksamkeit