Encryption by Default

pretty Easy privacy

Hartmut Goebel
Diplom-Informatiker, CISSP, CSSLP
ISO 27001 Lead Implementer

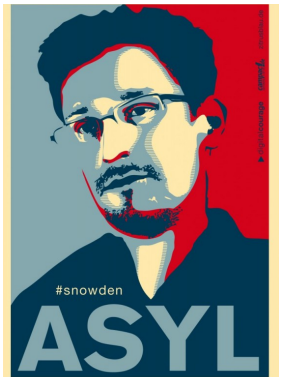
Zur Person: Hartmut Goebel

- Berater für IT-Security in komplexen Umgebungen
- Berät seit 2003 Banken, mittelständische Unternehmen und Konzerne beim Management von IT-Sicherheit
- „Datenschutz“ seit ca. 1985

- Diplom-Informatiker, CISSP, CSSLP, ISO 27001 Lead Implementer
- Fachautor und -Redner
- Blog: www.goebel-consult.de/blog
- Kolumne: www.cissp-gefluester.de

digitalcourage

- Gegründet 1987
- Bürgerrechte, Datenschutz
- BigBrotherAward seit 2000
- Technikaffin, doch Demokratie soll nicht „verdatet und verkauft“ werden
- klären auf und mischen uns in Politik ein
- Verfassungsklage gegen Vorratsdatenspeicherung
- 1.000.000 für Snowden



Goebel CONSULT

Agenda

- Welche Anforderungen wir an Kommunikation stellen und wie es heute aussieht
- Weshalb S/MIME und PGP kein Durchbruch gelingt und weshalb De-Mail und „Volksverschlüsselung“ Totgeburten sind
- Was p≡p besser macht und weshalb Digitalcourage überzeugt ist, dass es Erfolg haben wird

Welche Anforderungen wir an Kommunikation stellen und wie es heute aussieht

Weshalb „vertraulich“ kommunizieren

- geht niemanden etwa an
  - persönlichen Situation
  - politischer Meinungsäußerungen
- Journalisten
- Wistleblower
- Wirtschaftsspionage

- deswegen Post- und Fernmelde Geheimnis
  - Schutzrechte der Bürger gegenüber dem Staat

Anforderungen an Technische Mittel

Damit es sinnvoll ist

- Ende-zu-Ende verschlüsselt
- pseudonym
- anonym
- abstreitbar
- dezentral
- mehrere Identitäten

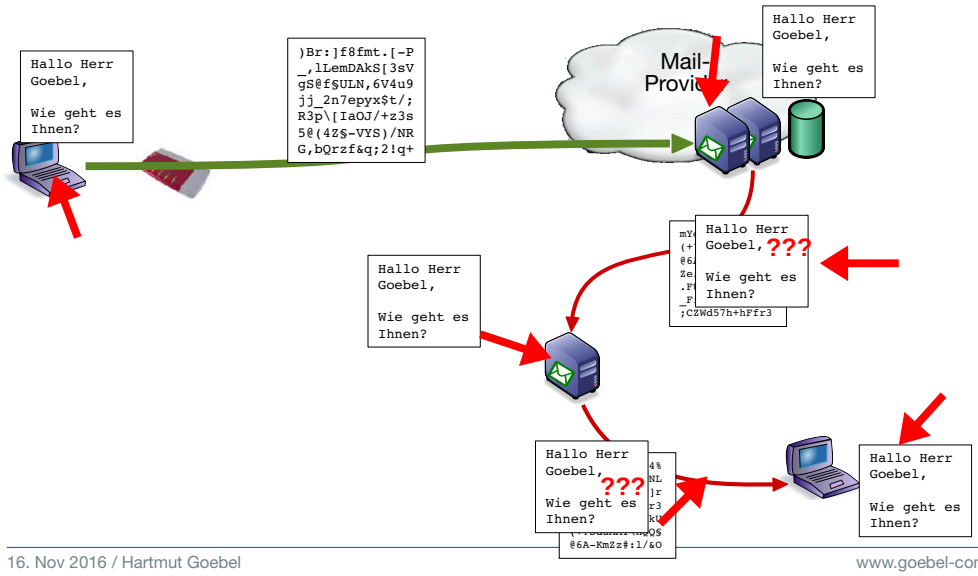
Damit es genutzt wird

- bequem
- per default
- nie im Weg
- billig

Eine ganz normale Mail

```
From: Hartmut Goebel <h.goebel@goebel-consult.de>
Subject: Informationen zum Projekt - Vertraulich
To: Hartmut Goebel <h.goebel@goebel-consult.de>
Organization: Goebel Consult
Date: Mon, 7 Nov 2016 13:58:04 +0100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101
 Thunderbird/38.3.0
Message-ID: <58207A5C.2020100@goebel-consult.de>
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit

Sehr geehrter Herr Goebel,

anbei bekommen Sie die Informationen zu unserem Projekt. Beachten Sie
bitte, dass die Informationen vertraulich sind.

--
SchÃ¶nen GruÃŸ
Hartmut Goebel

Blog: http://www.goebel-consult.de/blog/totgeburt-volksverschlusselung
```

So wird eine Mail „verschlüsselt“ übertragen – TLS/SSL



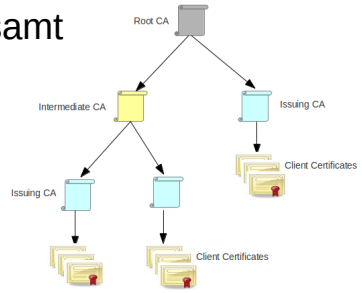
Weshalb S/MIME und PGP kein Durchbruch gelingt und weshalb De-Mail und „Volksverschlüsselung“ Totgeburten sind

Goebel CONSULT

Ausflug
Wie wird „Vertrauen“ hergestellt?

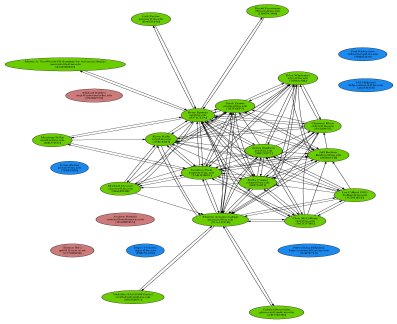
Zertifizierungsstelle

Passamt



Web of Trust

Bring Deine Freundinnen mit



3. Konzept:

Trust on first use

Goebel CONSULT

S/MIME

pseudonym	ja
anonym	teilweise
dezentral	nein: Zertifizierungsstelle nötig
mehrere Identitäten	ja
bequem	ja: In jedem Mailprogramm eingebaut nein: Es ist umständlich, sich Zertifikate zu besorgen nein: Man muss die Zertifikate regelmäßig erneuern nein: Wo bekomme ich die Zertifikate der anderen her?
per Default	nein: man muss sich Zertifikate besorgen nein: muss ausdrücklich aktiviert werden
nie im Weg	teilweise
billig	„Daten sind das neue Öl“

PGP / GPG

pseudonym	ja
anonym	ja
dezentral	ja
mehrere Identitäten	ja
bequem	nein: In vielen Mailprogrammen „aufgepfropft“ nein: Beim Einrichten werden viele Fragen gestellt, die die Nutzer nicht beantworten können. nein: Handling der Schlüssel (wenn gemäß Lehrbuch) aufwändig und umständlich nein: Wo bekomme ich die Schlüssel der anderen her? nein: viele Fragen, viele Optionen
per Default	nein: „Vertrauen Sie diesem Schlüssel?“ nein: muss ausdrücklich aktiviert werden
nie im Weg	teilweise
billig	kostenlos

Volksverschlüsselung

pseudonym	nein: Identifikation mit Ausweis, Post-Ident oder Telekom-Kundennummer (sic!) nein: Ausgestellt auf alle Vornamen
anonym	nein
dezentral	nein: nur ein Anbieter
mehrere Identitäten	nein
bequem	nein: Hat alle Probleme von S/MIME nein: Identifikation durch Ausweis nötig nein: die meisten Mailprogramme kennen die Zertifizierungsstelle nicht
per Default	nein: man muss sich Zertifikate besorgen nein: muss ausdrücklich aktiviert werden
nie im Weg	teilweise
billig	Privat kostenlos, für Firmen wohl nicht erhältlich

DE-mail

pseudonym	nein – Identifizierte Benutzer sind ausdrückliches Ziel
anonym	nein
dezentral	nein
mehrere Identitäten	nein
bequem	nein: Zugriff immer per Webbrowser
per Default	nein: Ende-zu-Ende Verschlüsselung ist aufgepfropft
nie im Weg	nein: nicht in Arbeitsabläufe integriert
billig	?

Allen gemeinsam

pseudonym	
anonym	
dezentral	
mehrere Identitäten	
bequem	nein: Zertifikate oder Schlüssel zwischen Geräten synchronisieren ist umständlich, bei den eingesammelten Zertifikaten sogar sehr
per Default	
nie im Weg	
billig	

Was p≡p besser macht und weshalb Digitalcourage überzeugt ist, dass es Erfolg haben wird

Konzept von p≡p

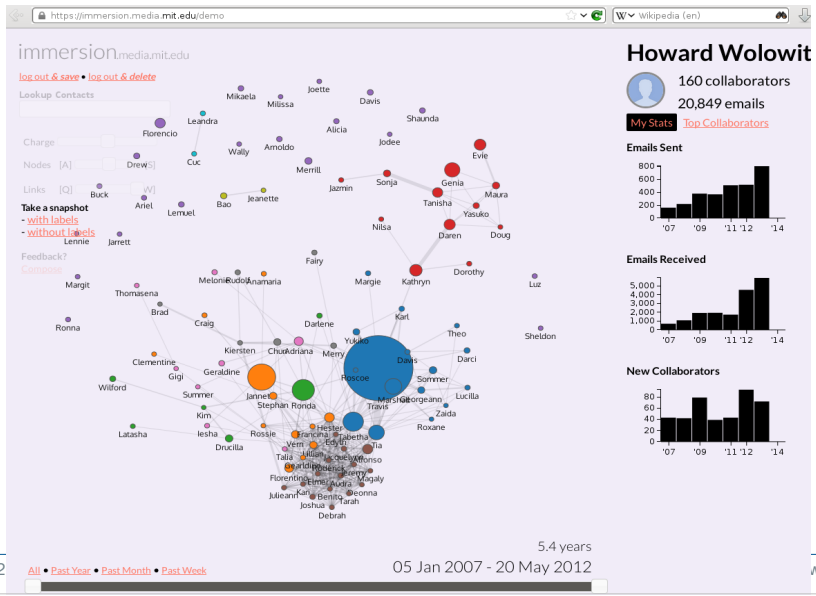
- Benutzt bewährte Technik: GPG
- Stellt keine Fragen
- Der eigenen Schlüssel
  - erstelle automatisch Schlüssel
    - mit den richtigen Parametern
    - für jede E-Mail-Adresse eine
  - schickt eigenen Schlüssel immer mit (konfigurierbar)
- Die Schlüssel der anderen
  - sammelt alle Schlüssel ein
  - holt sie automatisch vom Key-Server (konfigurierbar)
- verschlüsselt wann immer es kann
  - benutzt automatisch was geht
  - aber: verschickt Nachricht immer
- Vertrauen
  - „trust on first use“
    - „vertraut“ jedem fremden Schlüssel erst einmal
  - Einfacher Farbcode
    - grau, gelb, grün, rot
  - Trustwords
- Zusatz-Feature: Schlüssel-Synchronisation

Workflow (2 p≡p users)

Eine verschlüsselte Mail

```
From: Hartmut Goebel <h.goebel@goebel-consult.de>
Subject: Informationen zum Projekt - Vertraulich
To: Hartmut Goebel <h.goebel@goebel-consult.de>
Organization: Goebel Consult
Date: Mon, 7 Nov 2016 13:59:27 +0100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101
 Thunderbird/38.3.0
Message-ID: <58207A2F.4010107@goebel-consult.de>
MIME-Version: 1.0
Content-Type: application/pkcs7-mime; name="smime.p7m"; smime-type=enveloped-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message

MIAGCSqGSIb3DQEHA6CAMIACAQAxggGdMIIBmQIBADCBgDB5MRAwDgYDVQQKEwdSb290IENB
MR4wHAYDVQQLExVodHRwOi8vd3d3LmNhY2VydC5vcmcxIjAgBgNVBAMTGUNBIENlcnQgU2ln
bmluZyBBdXRob3JpdHkxITAfBgkqhkiG9w0BCQEWEnN1cHBvcnRAY2FjZXJ0Lm9yZwIDEmHI
MA0GCSqGSIb3DQEBAQUABIIBAA8FM1Smf9jeqF0mVFcm93havgQTH7zFMDJMyHqwrvU7290J
G+VkBzAAYEnG9d4KcM43uiYj0ow5E0M8r1ZaRVrYiQagyp3HYru+N52FOVGJAGpyvhTEFATF
mSxev+B/o1WDKhD6ojgBc2YPaNCo1+GAbW3ljdj14Os3KByBwIPXy0SBg9eLYcI8Wvh9Ybdz
2DErPPIP8BbO6HVxxDXsig8F6aNdYnbRB5QxA/z4BqGdaunC2nPou3kqITGZibGylL6e35sB
a6RwkWObknID9CaTxkAOcv8ODknS0uSG3HK8swoZdRs8PmfXy2lS8tshHStgQocy5Xl9DmW7
O5JQnGcwgAYJKoZIhvcNAQcBMBQGCCqGSIb3DQMHBAgSizrSBmfk6qCABIIRWJqsxtpPQib6
oBtfFRZvaml Z4SmttCV+UI7uV7BeHw5tqW43/m5u8ndE0VipmpkzA9tr5l8rCud+BL0lB3qc
DD7u1N48bkNMefT2ciO82aGuKoqiPysv934yHRt/fQ3mR3ZiKaY3a0v1bVi58+B3MmgfPUxF
.....
```

„Nur Meta-Daten“



p≡p gegen „Meta“-Daten

- Betreff wandert in den Body
- Andere Übertragungswege
  - Weg von SMTP
  - OTR über GNUnet
  - …

Was p≡p kann – für Privatleute und Unternehmen.

- Privat
  - p≡p verschlüsselt alle Ihre E-Mails, wann immer es geht
  - auf allen Ihren Geräten
  - kostenlos
    - Ausser Sie benutzen Outlook, ein iPhone oder bevorzugen es, Google Geld in den Rachen zu werfen
- Unternehmen
  - Konfiguration via GPO (nur Outlook)
  - Verschlüsseln mit zusätzlichen Schlüsseln
  - Escrow-Server
  - Verschlüsselte Mails auf dem Server

p≡p bekommen

GNU/Linux

- Thunderbird & Enigmail installieren

Windows

- Thunderbird & Enigmail
  - Thunderbird herunterladen
  - Enigmail innerhalb Thunderbird installieren (kostenlos)
- Outlook
  - https://pep.digitalcourage.de

Mobil

- Android
  - F-droid (kostenlos)
  - Google Play Store
- iPhone
  - Apple Phone Store

digitalcourage

Verschlüsselung ist nicht alles

- Berücksichtigen Sie auch unsere anderen Tipps
  - https://digitalcourage.de/selbstverteidigung
  - Auch als freundlicher Adventskalender
- Werden Sie Mitglied

Goebel CONSULT

Noch Fragen?

Goebel Consult

www.goebel-consult.de

h.goebel@goebel-consult.de

CISSP®

CSSLP®

ISO/IEC 27001 Lead Implementer

Selbstverteidigung: E-mail (1)

- Erzwingen Sie TLS/SSL
- Benutzen Sie ein sicheres E-Mail-Postfach
  - Besser kleine, europäische Provider lokale Provider
    - Ab 10.000 Kunden Abhörschnittstelle Pflicht
  - Posteo, mailbox.org, mykolab.com, uberspace.de, Bürgernetze, Individual Network (IN)
  - Sicherheit von Maildiensten, c't 4/2014, Seite 86
    - jpberlin.de, mykolab.com, posteo.de, privatedemail.net
    - Selbst testen: heise.de/-1932806
- Wenn Sie eine eigene Domain haben, verwenden Sie diese auch als E-Mail-Adresse.

Selbstverteidigung: E-mail (2)

- Verwalten Sie Ihre Mails nicht im Browser
  - sonst Mailen = Surfen
  - Mails bleiben zunächst auf dem eigenen Rechner
  - [Verschlüsselung nur so sicher möglich]
  - Mailprogramm: Thunderbird
    - Plattform-unabhängig, erweiterbar
    - Freie Software

Selbstverteidigung: E-mail (3)
Statt E-Mails nach außen weiterleiten

- Outlook-Web-Access o.ä.
- Smartphone mit Verbindung zur Firma – am besten über einen sogenannten VPN-Tunnel.

PGP-Verschlüsselung bei web.de/GMX

- Scheint technisch okay

Aber

- Plugin im Browser = Mails im Browser
- Noch immer web.de/GMX
- Geschlossene Gesellschaft

➡ Besser Thunderbird + Enigmail
➡ Noch besser p≡p – pretty Easy privacy