Peer Heinlein <p.heinlein@heinlein-support.de>

„Post Snowden“

E-Mail-Security 2017

Peer Heinlein <p.heinlein@heinlein-support.de>

„Erst entschlüsseln Sie die PGP-Mail und dann laden sie den Inhalt auf Dropbox hoch.“

(Logan CIJ Symposium 2016 Berlin)

Peer Heinlein <p.heinlein@heinlein-support.de>

Geht's um E-Mail-Security...

- Heinlein Support GmbH / Peer Heinlein
  - Linux Security Consultant seit 1995
  - Spezialist für Mailserver und Anti-Spam/Anti-Virus seit 1992
  - Diplom-Jurist / Prädikatsexamen
  - Kunden:
    - ISPs > 100.000 Kunden (EWEtel, Strato)
    - Universitäten, Forschungseinrichtungen
    - diverse Landesrechenzentren (ITDZ, Stuttgart, Baden-Franken, Thüringen)
    - Div. politische Instititionen und Stiftungen
    - Spezialfälle >> n-Millionen Mails/Tag (XING, StudiVZ)
  - Heinlein Support GmbH: 28 Mitarbeiter mit Sitz in Berlin

E-MAIL

IST

TOT.

(Und dann kamen welche, die haben das einfach nicht gewusst.)

4 Mrd. Accounts in 2015!

	2011	2012	2013	2014	2015
Worldwide Email Accounts (M)	**3,146**	**3,375**	**3,606**	**3,843**	**4,087**
Corporate Email Accounts	**788**	**850**	**918**	**991**	**1,070**
% Corporate Email Accounts	*25%*	*25%*	*25%*	*26%*	*26%*
Consumer Email Accounts	**2,358**	**2,525**	**2,688**	**2,852**	**3,017**
% Consumer Email Accounts	*75%*	*75%*	*75%*	*74%*	*74%*

Corporate vs. Consumer Email Accounts, 2011–2015

Quelle: Ridacti Group

Peer Heinlein <p.heinlein@heinlein-support.de>

Social media didn't kill email

where US citizens start their online day

Sources

EmailStatCenter.com ReadWriteWeb.com PewInternet ccloop.com CampaignMonitor Office Blogs The Radicati Group, Inc. Skype LinkedIn Microsoft Wrike

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail 1995:

Mach Spam-/Virenschutz!

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail 2005:

Mach Spam-/Virenschutz!
Mach TLS!

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail 2015:

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail 2015:

Peer Heinlein <p.heinlein@heinlein-support.de>

Teil I:
Wer macht derzeit was?

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail made in Germany

Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail made in Germany: Was machen die?

- Regelt, daß EMIG-Teilnehmer untereinander SSL einsetzen müssen.
  - Hätten Sie einfach so SSL aktiviert, wäre das auch der Fall. :-)
- Stellt per hardcoded Policy sicher, daß SSL eingehalten wird.
  - Würde DANE/DNSSEC auch machen
  - EMIG enstand vor DANE.
  - Fordert kein DNSSEC – wäre per MX-Record-Injection angreifbar.
- Zeigt dem User an, daß die Mail per SSL an einen EMIG-Partner versendet wird
  - EMIG verschweigt, daß auch Mail an andere ISPs genauso sicher per SSL rausgehen.
  - Anbieter wie mailbox.org zeigen bei jedem Empfänger den SSL-Status an und stellen SSL-Versand sicher :-)

E-Mail made in Germany

E-MAIL MADE IN GERMANY
Eine Initiative von GMX, Telekom und WEB.DE

Start | Verschlüsselung | Datenverarbeitung | Kennzeichnung | De-Mail | Outlook Add-In | Teilnehmer | Jetzt wechseln!

TEILNEHMER

GMX · Telekom · WEB.DE · freenet · 1&1 · STRATO · HORNETSECURITY · TÜVRheinland

Weitere Unternehmen werden zertifiziert und geprüft durch:

E-Mail made in Germany ist eine Initiative von GMX, Telekom und WEB.DE.

Unsere Initiative ist offen für weitere Partner, die bereit sind, sich unter ihrer E-Mail-Domain dauerhaft zur Einhaltung unserer Sicherheitsregeln zu verpflichten.

Bei Interesse wenden Sie sich bitte an:
teilnehmer@e-mail-made-in-germany.de

Impressum | Presse

Eine Initiative von GMX · WEB.DE · Telekom

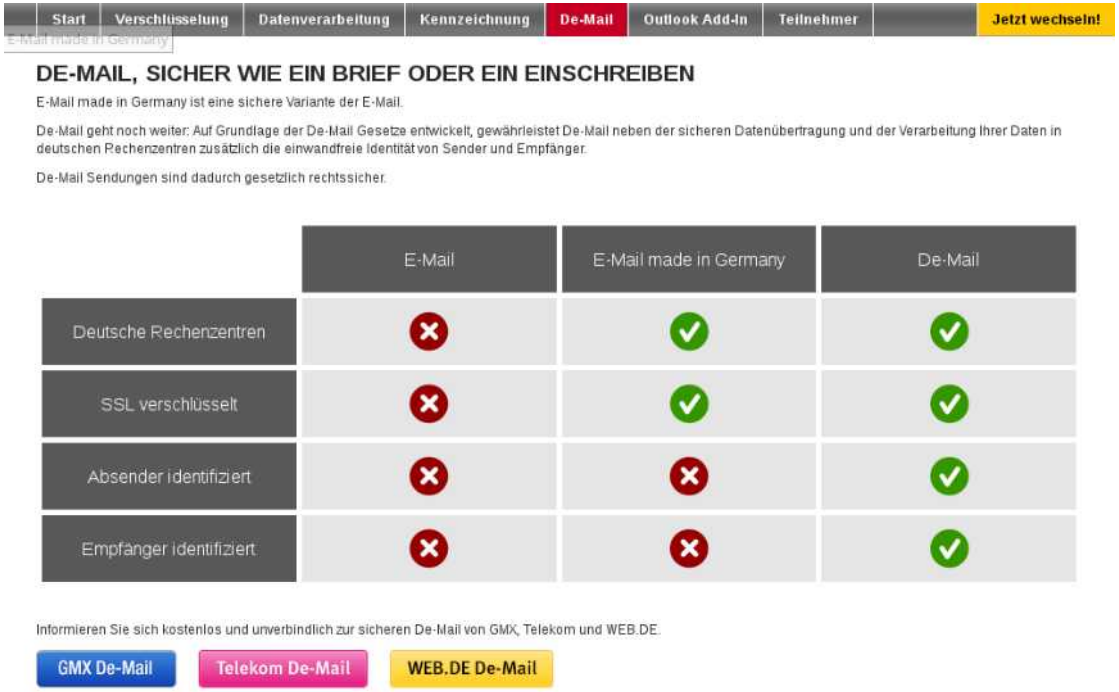
Peer Heinlein <p.heinlein@heinlein-support.de>

E-Mail made in Germany: Wer macht mit?

- Weiterhin nur sehr beschränkter Teilnehmerkreis
  - GMX, web.de, T-Online, freenet, 1&1, Strato, Hornet Security, Mediabeam
  - Ca. 30 Partner in Umsetzung (Versicherung, Großversender)
- Kostspielige Zertifizierung durch TÜV Rheinland notwendig

E-Mail made in Germany:

- Wird massiv als Werbe-/Marketingmaßnahme genutzt, insb. zum Vorteil der „Erfinder“ GMX, web.de, T-Online
  - Leitet auch Werbung zu DE-Mail ab.



Peer Heinlein <p.heinlein@heinlein-support.de>

BSI: Technische Richtlinie „Sicherer E-Mail-Transport“ TR-03108

Peer Heinlein <p.heinlein@heinlein-support.de>

TR Sicherer E-Mail-Transport

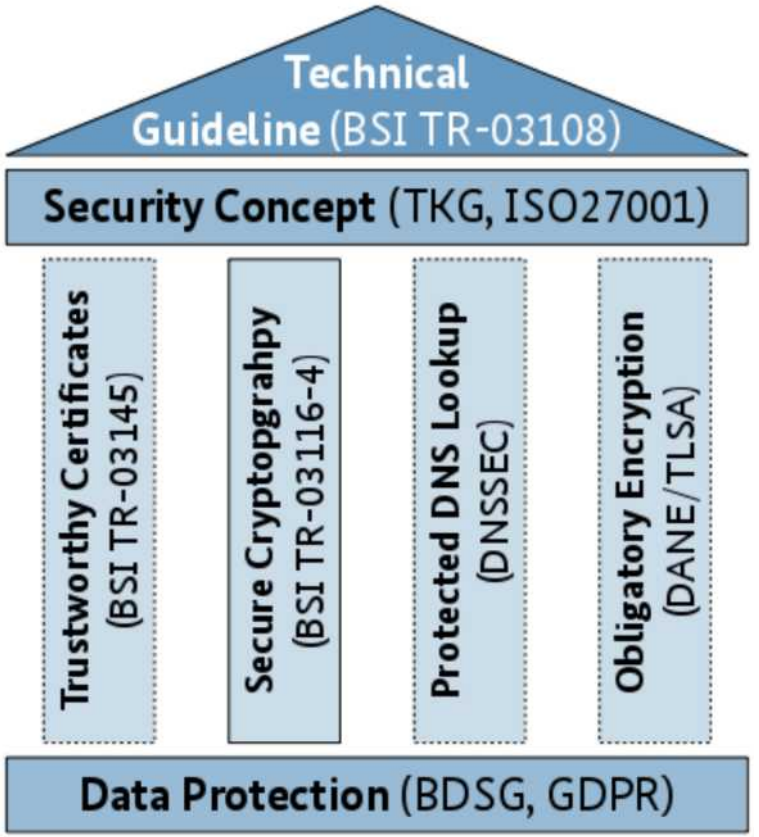
- Mitte 2015 startete das BSI die Erarbeitung der Technischen Richtlinie „Sicherer E-Mail-Transport“ (BSI TR-03108)
  - BSI entwickelte Entwurf
  - Arbeitsgruppensitzungen mit Providern und Mail-Experten
  - 12. April 2016 abschließendes Treffen der Arbeitsgruppe
    - [12.4.: DNSSEC wird von Anfang an verpflichtend.]
    - [16.4.: web.de führt DNSSEC ein.]

- Endgültige Fassung am 20.5.2016
  - Bislang kaum Zertifizierungen nach TR-03108
  - Erste Zertifizierung hätte m.M.n. nicht erteilt werden dürfen, Spezifikation wurde grob nicht eingehalten.

Peer Heinlein <p.heinlein@heinlein-support.de>

Das definiert die TR:

- Nutzung „guter“ CAs für SSL
- Verwendung sicherer Ciphers
- DNSSEC
- DANE/TLS
- Aufklärung der Nutzer durch Anzeige?
- Nachweis eines Sicherheitskonzepts nach TKG (eh vorhanden) oder ISO27001.



- „EMIG + DANE + Besseres SSL = TR-03108“

Peer Heinlein <p.heinlein@heinlein-support.de>

TR-Zertifizierung als Anreiz zum Mitmachen

- Provider können sich nach der TR zertifizieren lassen
  - Genauer Ablauf und Kosten noch unklar
- TR-Zertifizierung darf zu Werbezwecken als Auszeichnung genutzt werden!
- Auch Providern aus dem Ausland soll die TR-Zertifzierung offen stehen
  - (Darum: RZ Deutschland und BDSG oder vergleichbar)
- Internationale Aufmerksamkeit für TR E-Mail erwünscht
  - BSI tritt damit auf Konferenzen im In- und Ausland auf

Peer Heinlein <p.heinlein@heinlein-support.de>

Die Volksverschlüsselung („VV“)

Peer Heinlein <p.heinlein@heinlein-support.de>

Volksverschlüsselung („VV“)

- Zentrale S/MIME-Zertifizierungsstelle des Fraunhofer Instituts
  - S/MIME hat anders als PGP eine zentrale Zertifizierungsstelle!
  - Telekom ist Volksverschlüsselungspartner, aber am Ende kann sich jeder Nutzer jedes Providers ein Zertifikat holen
- Software/App richtet alle Komponenten ein und erzeugt Schlüssel – Fraunhofer stellt Schlüssel-Server
  - Derzeit: Windows. Geplant: MacOSX, Linux, iOS, Android
- Schlüssel & Betrieb für Private kostenlos, aber ggf. Kosten zur Identitätsprüfung

Peer Heinlein <p.heinlein@heinlein-support.de>

Volksverschlüsselung („VV“)

- Das leisten die Fraunhofer-Beiträge zur Volksverschlüsselung:
  - Zertifizierungsstelle für Schlüsselbeglaubigung
  - Verzeichnisdienst, um Schlüssel abrufen zu können
  - Sperrdienst für verloren gegangene Schlüssel
  - Aufbau und kontinuierliche Pflege einer kostenlosen Infrastruktur zur flächendeckenden Ausrollung von Schlüsseln
  - Benutzerfreundliche Software für Windows
  - Versionen für Mac OS X, Linux, iOS und Android sind geplant

Peer Heinlein <p.heinlein@heinlein-support.de>

Volksverschlüsselung: Keine anonyme Nutzung

- Zertifikate sind Class-3-Zertifikate!
- D.h. Identität des Inhabers ist eindeutig feststellbar
  - Keine anonyme Nutzung wie bei PGP möglich!
  - Derzeit: Registrierung ggf. unter Nutzung der Personalausweisenummer.
  - Später auch PostIdent & Co geplant.

heinlein

Post-Snowden Mail-Security 2017
[SLAC 2017]
Peer Heinlein <p.heinlein@heinlein-support.de>

Vertrauenswürdige Verteilung von Verschlüsselungs-Schlüsseln („VVV“)

Peer Heinlein <p.heinlein@heinlein-support.de>

Vertrauenswürdige Verteilung von Verschlüsselungs-Schlüsseln („VVV“)

- Konsortium von Fraunhofer SIT, Provet/Uni-Kassel, ULD, DesignLab der UdK Berlin und mailbox.org
  - Projektlaufzeit: Ab jetzt bis Ende 2017
  - Gefördert vom Bundesministerium für Bildung und Forschung (BMBF)

ULD provet Projektgruppe verfassungsverträgliche Technikgestaltung
Fraunhofer SIT
mailbox.org damit Privates privat bleibt
Design Research Lab

Peer Heinlein <p.heinlein@heinlein-support.de>

VVV: Unsere Aufgabe

- Entwickelt Standards zum Austausch von User-Schlüsseln zwischen Providern (weiter)
  - Entwickelt auch Plugins und Softwarekomponenten
  - Unterstützung für PGP und ggf. auch S/MIME
- Die Projektpartner untersuchen die wissenschaftlichen und technischen Aspekte des Schlüsseltauschs:
  - Usability
  - Rechtsfragen
  - Datenschutzfragen
  - uvam.
- mailbox.org übernimmt Praxis- und Enduser-Tests

Peer Heinlein <p.heinlein@heinlein-support.de>

Transport E-Mail-Security („TES“)

Peer Heinlein <p.heinlein@heinlein-support.de>

TES: Transport E-Mail Security

- Konsortium initial gegründet von

- TES ist ausdrücklich offen für alle anderen Provider und sucht aktiv europa- und weltweit Kooperationen mit den „großen“ Providern.
  - Gut ein Dutzend Treffen in Europa und aller Welt im letzten Jahr
  - Sehr positive internationale Resonanz der großen Player

Das macht TES

- TES-Mitglieder stellen nach einem bestimmten Verfahren PGP-Keys ihrer User zur Verfügung
  - Key im DNS über OPENPGPKEY oder Referenz auf HKP-Keyserver noch offen
  - Problem: Bislang kann jeder beliebig für alle Mailadressen Keys erzeugen.
  - TES reduziert das notwendige „Vertrauen“ in die Richtigkeit des Schlüssels wenigstens auf den Provider des Nutzers herunter
    - Ja, der Provider könnte für seinen Nutzer falsche Schlüssel herausgeben.
    - Aber eben nur noch dessen Provider und nicht jeder x-beliebige.
- Bestimmte DNS-Records zeigen an, ob TES für eine einzelne Domain nutzbar ist und über welchen TES-Provider die Keys abgewickelt werden.
  - mailbox.org arbeitet daran, dass TES und VVV kompatibel sind.

TES: Keys für User ohne Keys

- TES regelt auch, daß Provider für ihre User selbst PGP-Schlüssel erzeugen sollen, wenn diese noch keine Keys haben.
  - Aber dann – und nur dann – kann der Absender die Mail nicht nur mit SSL, sondern auch mit PGP verschlüsselt lossenden.
  - Ja, dann hat der Provider den Private Key.
  - Ohne TES würde die Mail im Klartext versandt werden.
  - Der Provider kann dem User die Mail transparent decodieren und anzeigen.
  - Die Mail ist auf dem Transportweg nachhaltig und konträr zu SSL geschützt, für den Endanwender ist das aber transparent und ohne Aufwand nutzbar.
  - „Fortgeschrittene User“ können eigene PGP-Keys nutzen und können eigene Schlüssel nutzen bzw. den Private Key selbst verwalten
  - („alles kann, nichts muß“).

Peer Heinlein <p.heinlein@heinlein-support.de>

Teil II:
Verschlüsseln im Alltag

Peer Heinlein <p.heinlein@heinlein-support.de>

PGP im Webmailer:

Wie macht man das?

Peer Heinlein <p.heinlein@heinlein-support.de>

Mailvelope:

Es lebe des Browser-Plugin

Peer Heinlein <p.heinlein@heinlein-support.de>

Mailvelope: Nicht immer alltagstauglich

- Mailvelope ist Browser-Plugin, muß explizit auf dem Nutzer-Rechner installiert sein.
  - Probleme im Urlaub / beim Kunden / bei Freunden / im Internet-Cafe.
  - Wenn das erste mal unterwegs der Zugriff auf wichtige Mails scheitert oder Urlaub ansteht läßt die Begeisterung für PGP schlagartig nach.
  - Was mache ich denn, wenn ich unterwegs an meine Mails muß?! Mailvelope im spanischen Internet-Cafe installieren?!

„Private-Keys sind nur auf dem privaten Rechner wirklich sicher“.

- Sind sie das?
- Auf einem privaten Rechner / Handy vertraue ich…
  - Dem Betriebssystem
  - Der Web-/Mailapplikation
  - Allen installierten Plugins
  - Den von mir besuchten Webseiten
  - Den Virenprogrammierern, die mich infiziert haben
  - Meinem Virenschutzprogramm
- Auf dem Handy auch noch:
  - Google/Apple
  - Allen beiläufig installierten Apps
  - Der Handy-Hardware (Samsung, LG uvam.)
- Puh. Ganz schön viele Leute.

Peer Heinlein <p.heinlein@heinlein-support.de>

Kann Mailvelope sicher sein?

- Mailvelope auf nicht-vertrauenswürdigen Rechnern würde Private Key sofort komplett kompromittieren.
  - Welcher Windows-Rechner / welches Android / welches iPhone ist denn nun vertrauenswürdig?
- Mailvelope speichert Private Key im Browser-Filestorage
  - Gut erreichbar für Browser, alle Plugins, Webseiten, Drive-By-Viren uvam.
  - Wir haben Viren „in the wild“ beobachtet, die gezielt die Private Keys von Mailvelope-Installationen abgreifen!
  - Keys können sogar über XSS-Angriffe geklaut werden!
  - Wieso hinterfragt das eigentlich niemand?
- JavaScript bietet nach Experten-Meinung keine vertrauenswürdige Umgebung für sichere Cryptographie und damit für Mailvelope

Peer Heinlein <p.heinlein@heinlein-support.de>

Mailvelope bei GMX & web.de

- PGP-Verschlüsselung von GMX & web.de basiert auf vorpaketierten erweiterten Mailvelope-Installationen.
  - Macht nix, die Presse hat‘s gefeiert wie Neu.
  - Private Schlüssel lagern mit einer Passphrase des Users geschützt auf dem Server des Providers
  - Mailvelope kann diesen Schlüsselcontainer herunterladen, lokal decodieren und verwenden. Schick!

Peer Heinlein <p.heinlein@heinlein-support.de>

Der Guard:

PGP mal serverseitig

Peer Heinlein <p.heinlein@heinlein-support.de>

Der Guard: Überall-PGP serverseitig

- Mailbox.org und Open-Xchange haben den „Guard“ entwickelt
  - Keys liegen mit Passphrase des Users auf dem Server (wie Mailvelope)
- Ver-/Entschlüsselung und Signierung findet komplett im Server statt nachdem der User seinen Schlüssel aktiviert hat
  - Schlüssel des Users ist zur Laufzeit immer mit einem dem Provider unbekannten Session-Key codiert.
  - Schlüssel wird nie auf den unsicheren Client (Desktop-PC, Browser, Android, iPhone) kompromittiert
- Jederzeit voller Zugriff auch von nicht-vertrauenswürdigen PCs
  - Worst Case: Konkrete Mail bekannt, aber Schlüssel bleibt unerreichbar!

Peer Heinlein <p.heinlein@heinlein-support.de>

Wem vertraue ich beim Guard?

- Auch beim Guard muß man jemandem vertrauen:
  - Der Server-Hardware
  - Dem Linux-OS
  - Den Programmierern des Guard

- Gretchenfrage:

  Welcher Computer ist gefährdeter? Server oder Desktop/Handy?

Peer Heinlein <p.heinlein@heinlein-support.de>

Guard und Mailvelope schließen sich nicht aus!

- Aber wem das alles nicht gefällt: Der Guard ist ein Angebot.
  - Alles ist weiterhin möglich.
- Der User kann auch weiterhin Mailvelope nutzen. Das ist ein Browserplugin, das geht prinzipiell „immer“.
  - Unabhängig davon interagiert Guard auch direkt mit Mailvelope, beispielsweise zum Schlüsselaustausch.
- Wir zwingen keinen zum Guard und unterstützen Mailvelope explizit.
  - (Aber wir warnen davor)

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

PGP-Keys sicher verteilen:

Das kann doch nicht so schwer sein?

Peer Heinlein <p.heinlein@heinlein-support.de>

HKP-Server

Der klassische Key-Server

Peer Heinlein <p.heinlein@heinlein-support.de>

PGP-Keys verteilen: HKP

- HKP-Server sind die klassischen „Key-Server“, wie man sie von den PGP-Schlüsselsuchen her kennt
  - HKP = HTTP Keyserver-Protokoll (HTTP 1.0 auf speziellen Ports)
- HKP-Server verteilen einfach nur Schlüssel. Sonst nichts.
  - Problem: Jeder kann einen Key-Server betreiben
  - Jeder kann einen Key mit beliebigen IDs/Mailadressen erzeugen!
  - Welcher Key ist vertrauenswürdig?
  - Was ist, wenn es mehrere Schlüssel bzw. widersprüchliche Schlüssel auf verschiedenen Servern gibt?
- gpg kann Keys von HKP-Servern fetchen!

DNS-Referenzen zum HKP-Server

- Über DNS TXT-Records kann abgefragt werden, welche HKP-Server für eine Domain genutzt werden sollen („PKA“)
  - PKA = Public Key Association
  - Jeder Mailadresse hat einen Eintrag
  - Localpart des Usernamens dabei im Klartext
  - Record verweist auf ID des Keys
- Vorteil: HKP-Server können auch mehrere Zertifikate und Revokes managen
  - HKP-Server können auch abgelaufene Keys vorhalten um später noch Signaturen prüfen zu können.
- DNSSEC nicht vorgeschrieben, könnte kompromittiert sein.
  - Aber es hindert uns ja keiner, das heute mit DNSSEC zu betreiben.

Peer Heinlein <p.heinlein@heinlein-support.de>

OpenPGP Web Key Service (WKS)

Peer Heinlein <p.heinlein@heinlein-support.de>

GnuPG schafft Fakten mit WKS

- Parallel zu VVV entstand Draft "OpenPGP Web Key Service"
  - https://tools.ietf.org/id/draft-koch-openpgp-webkey-service-04.txt
- WKD und VVV sind sehr ähnlich
  - 11.09.2016 GnuPG Version 2.1.14: erste Version mit WKS-Unterstützung
  - 28.07.2017 ab GnuPG Version 2.0.: ist WKD per Default eingeschaltet
  - Große Nutzerbasis -> gnupg, gpg4win,enigmail!
- Mailbox.org arbeitet an Unterstützung von WKS im Guard
  - SRV-RR wurde in den WKD-Draft aufgenommen

- Unterschiede VVV und WKS:
  - Schlüsselformat: HKP=ASCII WKD=Binär
  - eindeutiges User-/Schlüssel-Mapping: HKP=Mailadresse, WKD=LocalPart-Hash

Peer Heinlein <p.heinlein@heinlein-support.de>

PGPKEY:

Es lebe das DNS.

Peer Heinlein <p.heinlein@heinlein-support.de>

DANE/OPENPGPKEY: Die Keys direkt im DNS

- Ein RFC-Draft regelt, daß PGP-Keys als BLOB im DNS-Record der Maildomain veröffentlicht werden können
  - Mailadressen werden über einen Hash eingetragen
  - DNSSEC/DANE sichern
  - Problem: Groß-/Kleinschreibung der Mailadressen im DNS-Hash unklar!
  - Problem: Handhabbarkeit im DNS für ISPs > 1 Mio User?
  - Problem: Revoke-Zertifikate?
  - Problem: Prüfung von Signaturen nachdem Keys abgelaufen sind?
- DNS-Provider könnte Schlüssel seines Users manipulieren
  - Trust ggü. Provider weiterhin notwendig
- gpg kann Keys aus dem DNS fetchen!
  - DANE/DNSSEC schützt das alles.

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Das war mein Best-Of der Mailthemen 2016/2017.

Mehr gerne im persönlichen Gespräch.

(oder per Mail...)

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.

Peer Heinlein

Mail: p.heinlein@heinlein-support.de

Telefon: 030/40 50 51 – 42

- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

Post-Snowden Mail-Security 2017
[SLAC 2017]
Peer Heinlein <p.heinlein@heinlein-support.de>

Ja, diese Folien stehen auch als PDF im Netz...
http://www.heinlein-support.de/vortrag

Peer Heinlein <p.heinlein@heinlein-support.de>

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Peer Heinlein <p.heinlein@heinlein-support.de>

Wir suchen:
Admins, Consultants, Trainer!

Wir bieten:
Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

http://www.heinlein-support.de/jobs

Peer Heinlein <p.heinlein@heinlein-support.de>

Und nun...

- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Und viel Erfolg an der Tastatur...

Bis bald.

Peer Heinlein <p.heinlein@heinlein-support.de>

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln in Training und Schulung die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN ELEMENTS

Hard- und Software-Appliances für Archivierung, IMAP und Anti-Spam und speziell für den Serverbetrieb konzipierte Software rund ums Thema E-Mail.