

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



MAX-PLANCK-GESELLSCHAFT

## E-Mail-Server: rechtlich einwandfrei und technisch sicher

Rainer W. Gerling  
<http://www.mpg.de>

Erfahrungskreis Bayern 2003 1



MAX-PLANCK-GESELLSCHAFT

## Inhalt

- Rechtliche Bewertung eines E-Mail Servers
  - ◆ Rechtsrahmen
  - ◆ SPAM-Erkennung
  - ◆ Virenfilterung
- Technische Umsetzung
  - ◆ Verschlüsselung
    - ✦ PGP und S/MIME
    - ✦ Transportprotokolle
  - ◆ Virtuelle Poststellen und Verschlüsselung
  - ◆ Inhaltliche Kontrollen

Erfahrungskreis Bayern 2003 2

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## Telekommunikation

MAX-PLANCK-GESELLSCHAFT

- ❑ E-Mail ist ein Telekommunikationsdienst gemäß TKG!
- ❑ §85 TKG und §206 StGB regeln das **Fernmeldegeheimnis** (Artikel 10 GG).
- ❑ Die Telekommunikations-Datenschutzverordnung (TDSV) regelt die Verarbeitung der Verbindungsdaten im Detail.
- ❑ Besonderheiten (§16 TDSV)
  - ◆ Anrufbeantworter (Mailbox)
  - ◆ E-Mail-Server=> Nachrichtenübermittlungssystem mit Zwischenspeicherung

Erfa-Kreis Bayern 2003 3



## TKG § 3

MAX-PLANCK-GESELLSCHAFT

- ❑ "**Geschäftsmäßiges Erbringen von Telekommunikationsdiensten**" ist das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen **für Dritte** mit oder ohne Gewinnerzielungsabsicht.
- ❑ "**Telekommunikation**" ist der technische Vorgang des Aussendens, Übermittels und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen.

Erfa-Kreis Bayern 2003 4

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## Fernmeldegeheimnis im Arbeitsverhältnis

MAX-PLANCK-GESELLSCHAFT

- ❑ Hinweis Nr. 37 des Innenministeriums Baden-Württemberg verneint dies!  
(<http://www.rainer-gerling.de/hinweise>)
- ❑ „Damit werden z. B. auch Telekommunikationsnetze für geschlossene Benutzergruppen (Corporate Networks), über die möglicherweise in Zukunft erhebliche Teile der geschäftlichen Telekommunikation abgewickelt werden, vom Schutzbereich der Vorschrift umfaßt.“  
(aus der amtl. Begründung zum § 206 StGB; Entwurf zum Begleitgesetz zum TKG vom 4.8.1997, BT-Drs. 18/8453)

Erf-Kreis Bayern 2003 5



## Arbeitnehmerdatenschutz

(nach Bizer, DuD 2002)

MAX-PLANCK-GESELLSCHAFT

- ❑ Dienstliche Kommunikation
  - ◆ M1: Anwendung § 85 TKG (Fernmeldegeheimnis)
  - ◆ M2: Allg. PK-Recht und Verhältnismäßigkeitsprinzip
    - ◆ Förderung der Persönlichkeit der AN § 75 Abs. 2 BetrVG
    - ◆ Heimliche Überwachung in den Grenzen der Erforderlichkeit: § 89 Abs. 1 Satz 3 TKG i.V.m. TDSV
    - ◆ Löschung nach einem Tag § 6 Abs. 2 Satz 2 TDSV
    - ◆ „Zweck des Arbeitsvertrages“ § 28 Abs. 1 Satz 1 Nr. 1 BDSG
    - ◆ Freiwilligkeit der Einwilligung § 4e Abs. 1 Satz 1 BDSG
- ❑ Private Kommunikation
  - ◆ Anwendung § 85 TKG (Fernmeldegeheimnis)
    - ◆ Mitarbeiter ist zweifelsfrei Dritter

Erf-Kreis Bayern 2003 6

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



MAX-PLANCK-GESELLSCHAFT

## BetrVG-Grundlagen (§75 Abs. 2)

- ❑ Arbeitgeber und Betriebsrat haben die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Sie haben die Selbständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu fördern.

Erfar-Kreis Bayern 2003 7



MAX-PLANCK-GESELLSCHAFT

## Welche Nutzung?

- ❑ Arbeitsmittel für
  - ◆ dienstliche Nutzung
    - ✦ Fernmeldegeheimnis umstritten
  - ◆ persönliche Nutzung
    - ✦ Kommunikation mit dem Datenschutzbeauftragter
    - ✦ Kommunikation mit dem Betriebsrat
    - ✦ Kommunikation mit dem Betriebsarzt
  - ◆ private Nutzung
    - ✦ Abhören (§88 TKG, TKÜV, G-10, ...)
    - ✦ Fernmeldegeheimnis gilt definitiv

Erfar-Kreis Bayern 2003 8

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## Fernmeldegeheimnis

MAX-PLANCK-GESELLSCHAFT

### □ Stammdaten

- ◆ Name, Vorname, Anschrift, Bankverbindung

### □ nähere Umstände der Telekommunikation

- ◆ Rufnummern, Datum, Uhrzeit und Dauer einer Verbindung, übertragenes Datenvolumen

### □ Kommunikationsinhalte

- ◆ das gesprochene Wort, ausgetauschte Daten.
- ◆ Steuerdaten (§ 89 Abs. 3 Satz 2 TKG)
  - ◆ bei ISDN-Verbindungen zur Signalisierung ob Sprache oder Daten;
  - ◆ Port-Nummer bei TCP/IP Verbindungen

ErfA-Kreis Bayern 2003 9



## Stammdaten

MAX-PLANCK-GESELLSCHAFT

### □ Auskunft nach § 88 Abs. 6 TKG

### □ im Einzelfall auf Ersuchen an die zuständigen Stellen

- ◆ Verfolgung von Straftaten und Ordnungswidrigkeiten,
- ◆ zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung
- ◆ für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes

ErfA-Kreis Bayern 2003 10

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## nähere Umstände der Telekommunikation

MAX-PLANCK-GESELLSCHAFT

- ❑ betrieblichen Abwicklung seiner geschäftsmäßigen Telekommunikationsdienste
  - ◆ das Herstellen und Aufrechterhalten einer Telekommunikationsverbindung,
  - ◆ das ordnungsgemäße Ermitteln und den Nachweis der Entgelte
  - ◆ das Erkennen und Beseitigen von Störungen an Telekommunikationsanlagen,
  - ◆ das Aufklären sowie das Unterbinden von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes,
- ❑ auf schriftlichen Antrag eines Nutzers zum Zwecke
  - ◆ der Darstellung der Leistungsmerkmale (Einzelverbindungs nachweis) und
  - ◆ des Identifizierens von Anschlüssen (Fangschtaltung)
- ❑ Nach §§ 100g und 100h StPO Verbindungsdaten auch für die Zukunft (bis 31.12.2004 befristet)

ErfA-Kreis Bayern 2003 11



## Kommunikationsinhalte

MAX-PLANCK-GESELLSCHAFT

- ❑ Bei Missbrauchs bekämpfung Steuerdaten (§ 89 Abs. 3 Satz 2 TKG) mit Meldung an Regulierungsbehörde
- ❑ bei Störungsbehebung Aufschaltung auf Verbindung bei Signalisierung
- ❑ Für die Zukunft nach entsprechender Anordnung:
  - ◆ Nach §§ 100a, 100b StPO nur durch richterliche Anordnung
  - ◆ TKÜV
  - ◆ G10-Gesetz, BVerfSchG, BNDG, MADG

ErfA-Kreis Bayern 2003 12

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## Mailfilter

MAX-PLANCK-GESELLSCHAFT

- ❑ Werbe-E-Mail oder andere belästigender E-Mail (**SPAM**) wird vom Provider weg gefiltert!
- ❑ normale E-Mail erreicht den Empfänger nicht mehr (**name@hotmail.com**)
- ❑ §206 StGB: „*Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines ... Unternehmens unbefugt ... eine einem solchen Unternehmen zur Übermittlung anvertraute **Sendung unterdrückt.***“
- ❑ Zentrale Virenscanner und Inhaltsfilter??

ErfA-Kreis Bayern 2003 13



## Orientierungshilfe

[http://www.bfd.bund.de/information/DS-Konferenzen/oh\\_email.pdf](http://www.bfd.bund.de/information/DS-Konferenzen/oh_email.pdf)

MAX-PLANCK-GESELLSCHAFT

- ❑ Eine Protokollierung darf ohne Einwilligung erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.
- ❑ Private E-Mails sind wie private schriftliche Post zu behandeln. So sind eingehende private, aber fälschlich als Dienstpost behandelte E-Mails den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.

ErfA-Kreis Bayern 2003 14

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## BetrVG-Grundlagen (§87 Abs. 1)

MAX-PLANCK-GESELLSCHAFT

- Der Betriebsrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, in folgenden Angelegenheiten mitzubestimmen:
  1. Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb;
  - ...
  6. Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen;

ErfA-Kreis Bayern 2003 15



## EDV-Mitbestimmung R. Roßmann, DuD 26, 286 (2002)

MAX-PLANCK-GESELLSCHAFT

- Nach der gefestigten Rechtsprechung des Bundesarbeitsgerichts ist es für die Entstehung des Mitbestimmungsrechts entgegen dem Gesetzeswortlaut bereits ausreichend, wenn die technische Einrichtung zur Leistungs- und Verhaltenskontrolle **objektiv geeignet** ist. ... Da moderne Standardsoftwareprodukte in der Regel bereits vielfältige Auswertungs- und Protokollierungsmöglichkeiten bieten, ist die Eignung zur Verhaltens- und Leistungskontrolle im Sinne der Rechtsprechung beim Einsatz von EDV-Anwendungen im Arbeitsleben zumeist zu bejahen.

ErfA-Kreis Bayern 2003 16



# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## Regelungstatbestände

MAX-PLANCK-GESELLSCHAFT

- Private Nutzung
  - ◆ Ja oder Nein
- Verpflichtung zum Lesen der eMail
- Vertretungsregeln und Zugriff auf eMail
  - ◆ Zugriff bei Abwesenheit, Krankheit, Ausscheiden
- Verschlüsselung personenbezogener Daten
  - ◆ Recovery
- Protokollierung

ErfA-Kreis Bayern 2003 17



## Betriebsvereinbarung I

MAX-PLANCK-GESELLSCHAFT

- Wird die E-Mail verschlüsselt gespeichert, kann auf sie bei Verlust des Schlüssels nicht mehr zugegriffen werden, da private Schlüssel nicht rekonstruiert werden können. Wird eine E-Mail zu Dokumentationszwecken benötigt, muss sie unverschlüsselt archiviert werden.
- E-Mail mit personenbezogenen Daten darf innerhalb der X GmbH und an externe Stellen nur verschlüsselt versendet werden.

ErfA-Kreis Bayern 2003 18

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



MAX-PLANCK-GESELLSCHAFT

## Betriebsvereinbarung II

- ❑ Das Löschen von unerwünschter E-Mail (SPAM) geschieht nach vom Arbeitgeber zur Verfügung gestellten Regeln. Die Aktivierung dieser Regeln erfolgt durch den Mitarbeiter.
- ❑ Beschäftigte, die eine E-Mail-Kennung erhalten, müssen sicherstellen, daß dienstliche E-Mails auch bei Abwesenheit bearbeitet werden können.
  - ◆ Auto-Forward (Problem: private/persönliche E-Mail)
  - ◆ Auto-Reply (Offenbarung nach außen)

Erfahrungskreis Bayern 2003 19




MAX-PLANCK-GESELLSCHAFT

## Lösungen

- ❑ Virenscannen
  - ◆ Empfänger wird informiert und erhält E-Mail auf Wunsch/automatisch
  - ◆ Absender informieren??
- ❑ SPAM-Filter
  - ◆ Kennzeichnung der E-Mail zentral, aber Zustellung
  - ◆ Empfänger filtert auf Kennzeichen (eine Regel) oder auch nicht
- ❑ Blacklist
  - ◆ Vor dem „.“ (Punkt) im SMTP ablehnen
- ❑ Immer: Information über Details des Verfahrens

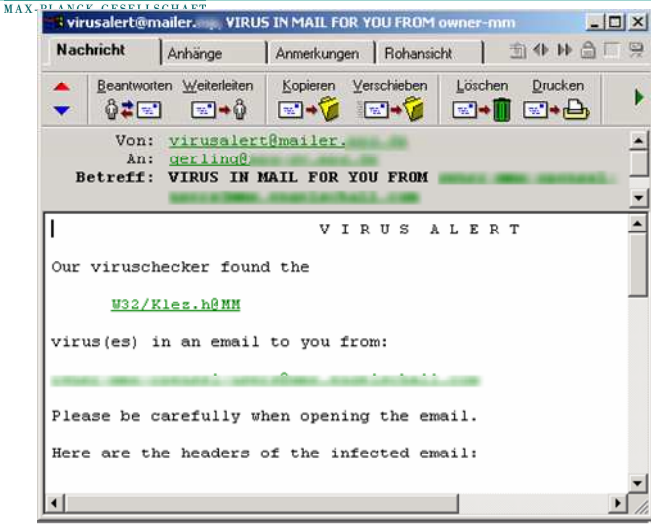
Erfahrungskreis Bayern 2003 20

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## Virenwarnung

---



MAX-PLANCK-GESELLSCHAFT

**Virusalert@mailero...** VIRUS IN MAIL FOR YOU FROM owner-mm

Nachricht | Anhänge | Anmerkungen | Rohansicht

Beantworten Weiterleiten Kopieren Verschieben Löschen Drucken

Von: virusalert@mailero...  
An: gerling@...  
Betreff: VIRUS IN MAIL FOR YOU FROM [redacted]

VIRUS ALERT

Our viruschecker found the

**W32/Klez.h@MM**

virus(es) in an email to you from:


[redacted]

Please be carefully when opening the email.

Here are the headers of the infected email:

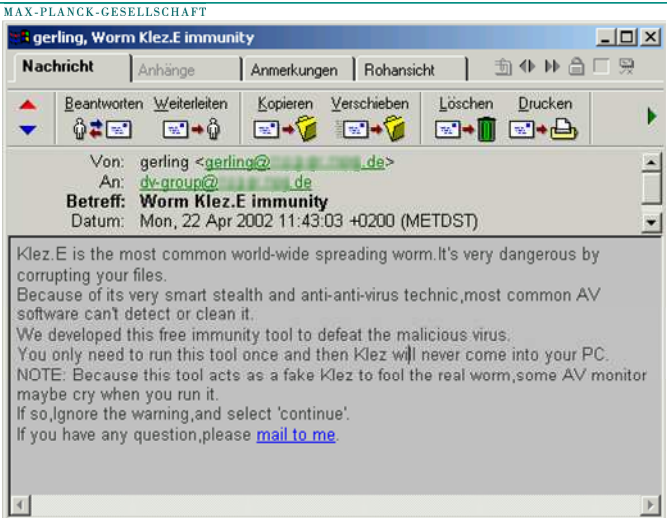
- Zeitlich verzögert Mail nachschicken
- Mit Passwort geZIPt
- Auf alle Fälle informieren
- Absender heute oft gefälscht

ErfA-Kreis Bayern 2003 21



## Bedrohung

---



MAX-PLANCK-GESELLSCHAFT

**gerling, Worm Klez.E immunity**

Nachricht | Anhänge | Anmerkungen | Rohansicht

Beantworten Weiterleiten Kopieren Verschieben Löschen Drucken

Von: gerling <gerling@...de>  
An: dv-group@...de  
Betreff: Worm Klez.E immunity  
Datum: Mon, 22 Apr 2002 11:43:03 +0200 (METDST)

Klez.E is the most common world-wide spreading worm. It's very dangerous by corrupting your files. Because of its very smart stealth and anti-anti-virus technic, most common AV software can't detect or clean it.

We developed this free immunity tool to defeat the malicious virus. You only need to run this tool once and then Klez will never come into your PC.

NOTE: Because this tool acts as a fake Klez to fool the real worm, some AV monitor maybe cry when you run it.


If so, ignore the warning, and select 'continue'.

If you have any question, please [mail to me](#).

- Klez.E
- Wurm
- Absender gefälscht
- Wie kriegt man den wirklichen Absender heraus?

ErfA-Kreis Bayern 2003 22

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## Mailserver

MAX-PLANCK-GESELLSCHAFT


- ❑ **Virens Scanner auf dem Mailserver**
  - ◆ **Betreff:**  
VIRUS IN MAIL FOR YOU FROM xxxxxx@planet.nl
  - ◆ **Header:**  
X-Virus-Scanned: (infected) by AMaViS perl-11+sophie

Viren-Abwehr aktivieren  Wenn EMail ein Virus enthält dann kopieren in Folder: ▼ Mail/unfug

- ❑ **SPAM Erkennung auf dem Mailserver**
  - ◆ **X-Spam-Status:** No, hits=18.3 required=5.0
  - ◆ **X-Spam-Level:** ++++++

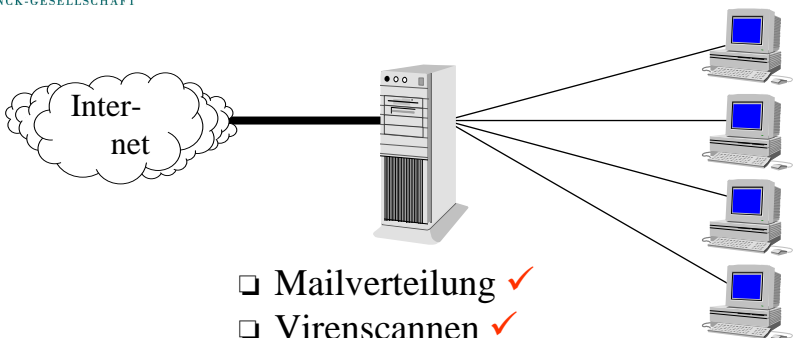
Spam-Abwehr aktivieren  Wenn **Score** einer EMail > 15 dann loeschen ▼

Wenn Score einer EMail > 6 dann kopieren in Folder: ▼ Mail/unfug



## Virtuelle Poststelle

MAX-PLANCK-GESELLSCHAFT



The diagram illustrates a virtual mailbox setup. On the left, a cloud labeled 'Inter-net' is connected to a central server rack. From the server, four lines radiate outwards to four separate desktop computer icons, representing clients accessing the mailbox.

- ❑ Mailverteilung ✓
- ❑ Virens Scanner ✓
- ❑ SPAM-Erkennung ✓
- ❑ Verschlüsselung

ErfA-Kreis Bayern 2003 24

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## Produkte

MAX-PLANCK-GESELLSCHAFT

- ❑ (GPGrelay)
  - ◆ GPGrelay läuft unter Windows (lokal)
- ❑ GEAM
  - ◆ GEAM läuft unter UNIX (Mailserve) und Windows PGP (und S/Mime)
- ❑ Utimaco SecurE-Mail Gateway
  - ◆ Eigenes OS
  - ◆ PGP, S/Mime und PrivateCrypto
- ❑ CryptoEx Gateway
  - ◆ „Selbstlernendes Gateway für E-Mail Sicherheit“
  - ◆ PGP und S/Mime

Erfa-Kreis Bayern 2003 25



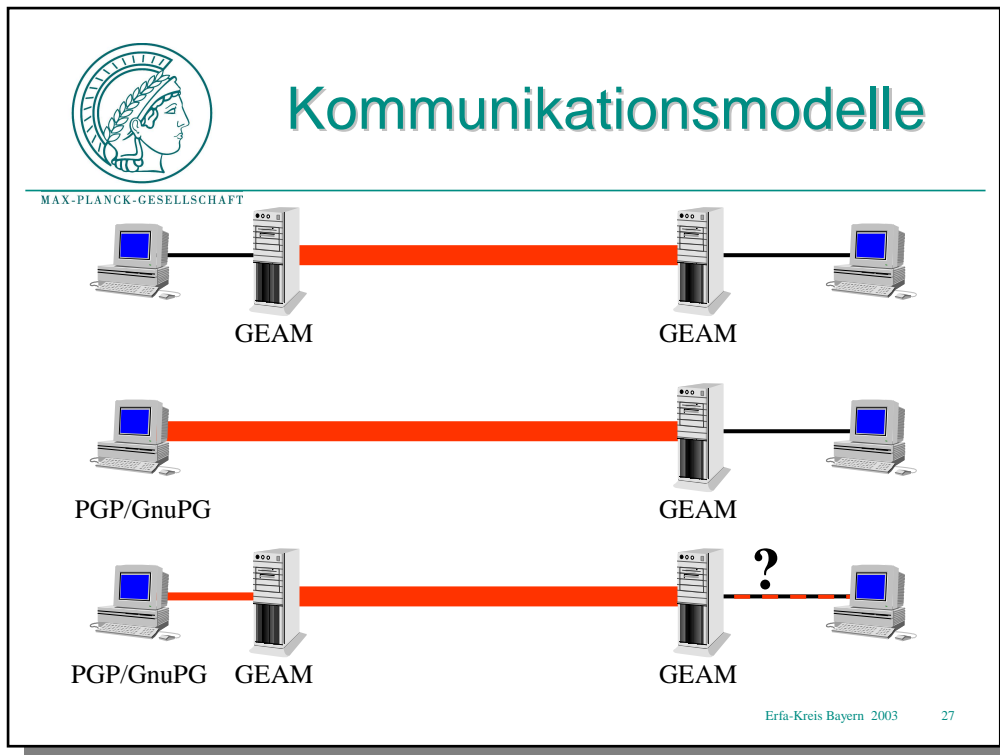
## Vorteile/Nachteile

MAX-PLANCK-GESELLSCHAFT

- ❑ Vorteile E-Mail-Verschlüsselungs-Proxy
  - ◆ Keine Anpassung des Mail-Klienten
  - ◆ Klient-Betriebssystem unabhängig
  - ◆ Vertretungsproblematik einfacher machbar
- ❑ Nachteile E-Mail-Verschlüsselungs-Proxy
  - ◆ Private Schlüssel auf dem Mail-Server
  - ◆ Kommunikation zum Mail-Server ungeschützt
  - ◆ Keine geschützte Individualkommunikation

Erfa-Kreis Bayern 2003 26

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



Das Diagramm zeigt die Probleme bei verschlüsselter E-Mail. Es enthält eine Liste von Punkten, die die Schwierigkeiten bei der Nutzung von E-Mail-Servern für verschlüsselte Kommunikation beschreiben.

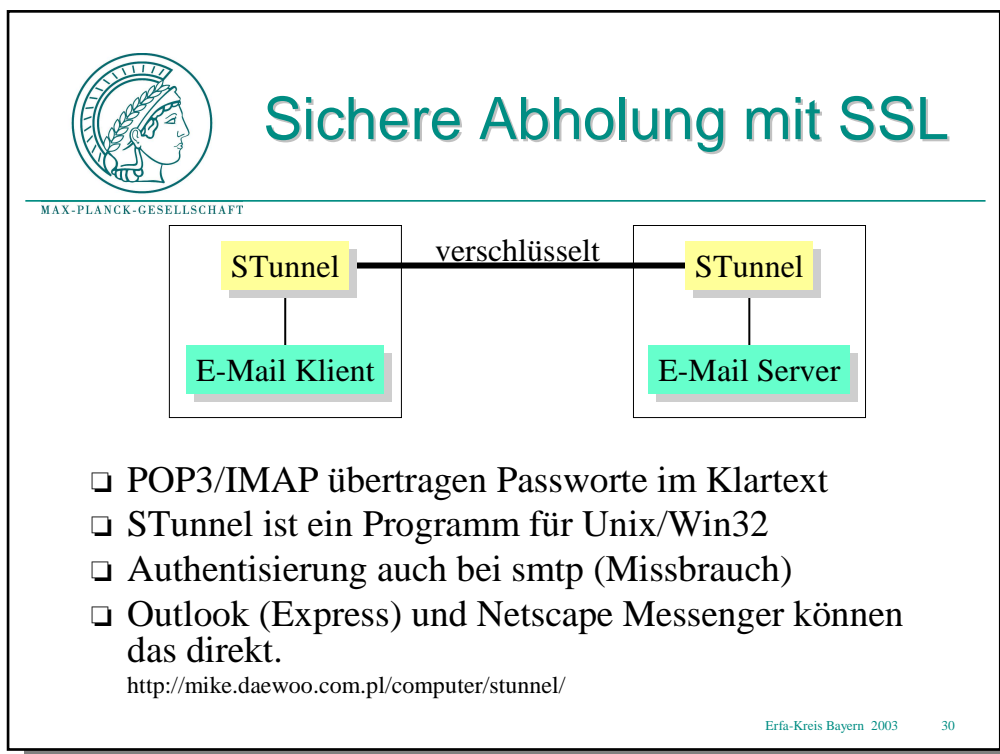
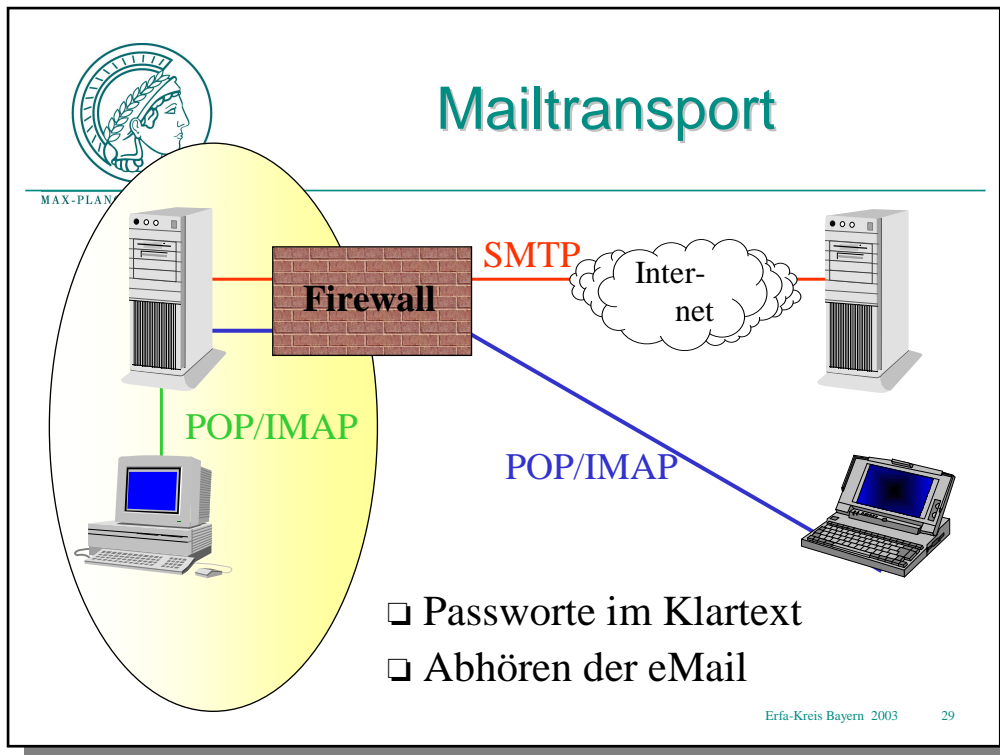
MAX-PLANCK-GESELLSCHAFT

Probleme


- ❑ Firmenpolicy: nur verschlüsselte E-Mail
- ❑ Aber Empfänger hat keinen öffentlichen Schlüssel ???
- ❑ Die Utimaco-Antwort:
  - ◆ Wird mit Zufallsschlüssel und PrivateCrypto verschlüsselt (uti-File für Windows)
  - ◆ Absender erhält Zufallsschlüssel per E-Mail damit er ihn dem Empfänger mitteilen kann

Erfa-Kreis Bayern 2003 28

# E-Mail-Server: rechtlich einwandfrei und technisch sicher



# E-Mail-Server: rechtlich einwandfrei und technisch sicher



## Outlook Express

---

- Outlook Express
  - ◆ pop3s (port 995)
  - ◆ imaps (port 993)
  - ◆ smtps (port 465)  
oder Port 25 mit starttls
- einfach anklicken

server.testnet.de Eigenschaften

Anschluss

Postausgangsserver (SMTP): 25 Standard

Dieser Server verwendet eine sichere Verbindung (SSL)

Postgangang (POP3): 995

Dieser Server verwendet eine sichere Verbindung (SSL)

Zeitlimit des Servers

Niedrig ———— Hoch 1 Minute

Senden

Nachrichten größer als 50 KB aufteilen

Zustellung


Kopie aller Nachrichten auf dem Server belassen

Vom Server nach 5 Tag(en) entfernen

Nach dem Löschen vom Server entfernen

OK Abbrechen Übernehmen

ErfA-Kreis Bayern 2003 31



## Ausblick

---

- Einführung von E-Mail ist mitbestimmt
- Das Fernmeldegeheimnis (oder ein vergleichbarer Schutz der Persönlichkeits-rechte) ist zu beachten
- Virenschutz und SPAM-Erkennung sind rechtlich einwandfrei machbar
- E-Mail Verschlüsselung ist unerlässlich und wird praktikabel
  - ◆ OpenPGP oder S/Mime zur Nachrichtenverschlüsselung
  - ◆ Transportverschlüsselung zum E-Mail-Server

ErfA-Kreis Bayern 2003 32