Piratenpartei Deutschland
Landesverband Bayern

E-Mails verschlüsseln

Von der Erfindung des E-Vorhängeschlosses

PIRATEN PARTEI

30 Minuten theoretische Grundlagen
kleine Pause
60 Minuten Praxis

WLAN-Daten:
•SSID=Piratenpartei
•Passwort=geheim

Informationen:
•http://www.crypto-party.de/muenchen/

Denksportaufgabe:
•Gutes Passwort für den Verschlüsslungsschlüssel ausdenken
•Kennen Sie ihr E-Mail Passwort? Sie brauchen es später!

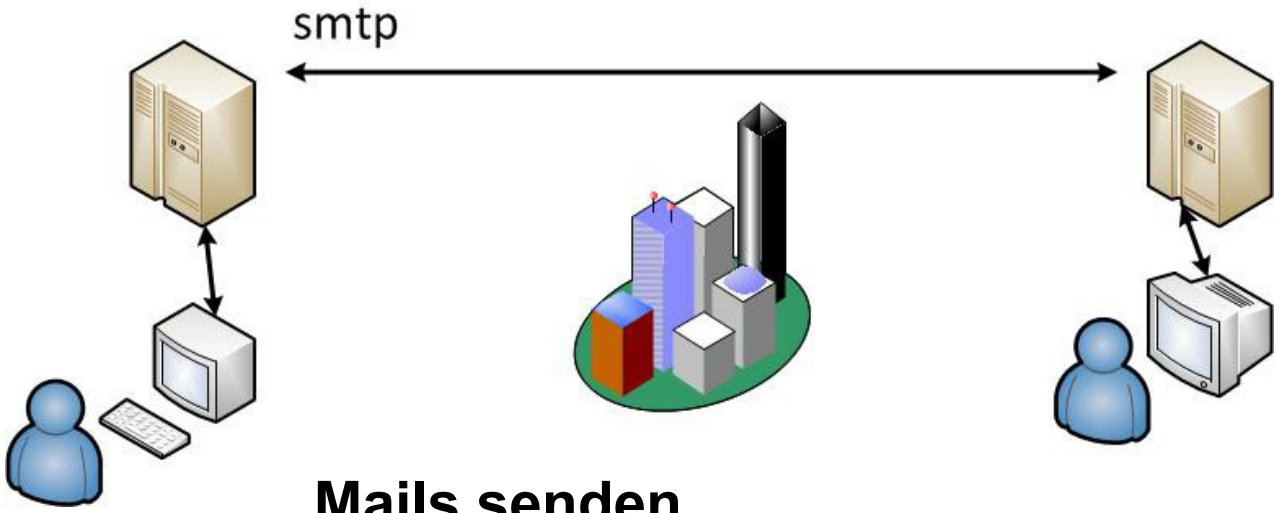
Grundlagen der E-Mail
- Mails senden
- 1. Mail nach Deutschland
- Mails senden und abholen
- Verschlüsselte Transportwege
- Mails im Zeitalter der Abhörschnittstellen
- Schwachpunkte aus Sicht der Vertraulichkeit

End-to-End-Verschlüsselung
- Symetrische Verschlüsselung
- Unsymetrische Verschlüsselung
- In 3-4 Schritten zur verschlüsselten Mail

Piratenpartei Deutschland
Landesverband Bayern

Grundlagen der E-Mail

PIRATEN PARTEI



Mails senden

- Mail senden (smtp)

1984 Erste E-Mail nach Deutschland (Uni Karlsruhe)

Received: Csnet-Sh.arpa by csnet-relay; 2 Aug 84 12:35 EDT
Date: Thu, 02 Aug 84 12:21:58 EDT
To: rotert%germany@csnet-relay.csnet
cc: zorn%germany@csnet-relay.csnet, cic%csnet-sh.arpa@csnet-relay.csnet, breeden%csnet-sh.arpa@csnet-relay.csnet
Subject: Willkomen in CSNET!
From: Laura Breeden breeden%csnet-sh.arpa@csnet-relay.csnet
Via: csnet-relay; 3 Aug 84 10:14-MET

Michael,

This is your official welcome to CSNET. We are glad to have you aboard. I gather that you and Dan were able to talk about some of the details of your implementation at the Paris conference. Dan also said you are interested in CSNET paraphernalia (like t-shirts). If I can come up with some stickers (abaout the only thing we have), I will send them.

I am going to send you some informational messages about using CSNET, including aboput formatting addresses, using the Name Server, and finding the way around the Internet. Please let us know if you have any questions.

Because some sites act as forwarders or have other internal concerns, we ask new sites to confirm that they are ready before we announce them up to the rest of CSNET. In your case, I would also like to include some information about DFN in the announcement (what hosts are on it, how to reach them via your host). From your recent message, it looks asthough your VAX is the only machine able to send and receive CSNET mail.

For the announcement I will also want to be sure that the information on the site sheet is correct and complete. We show the following for you:

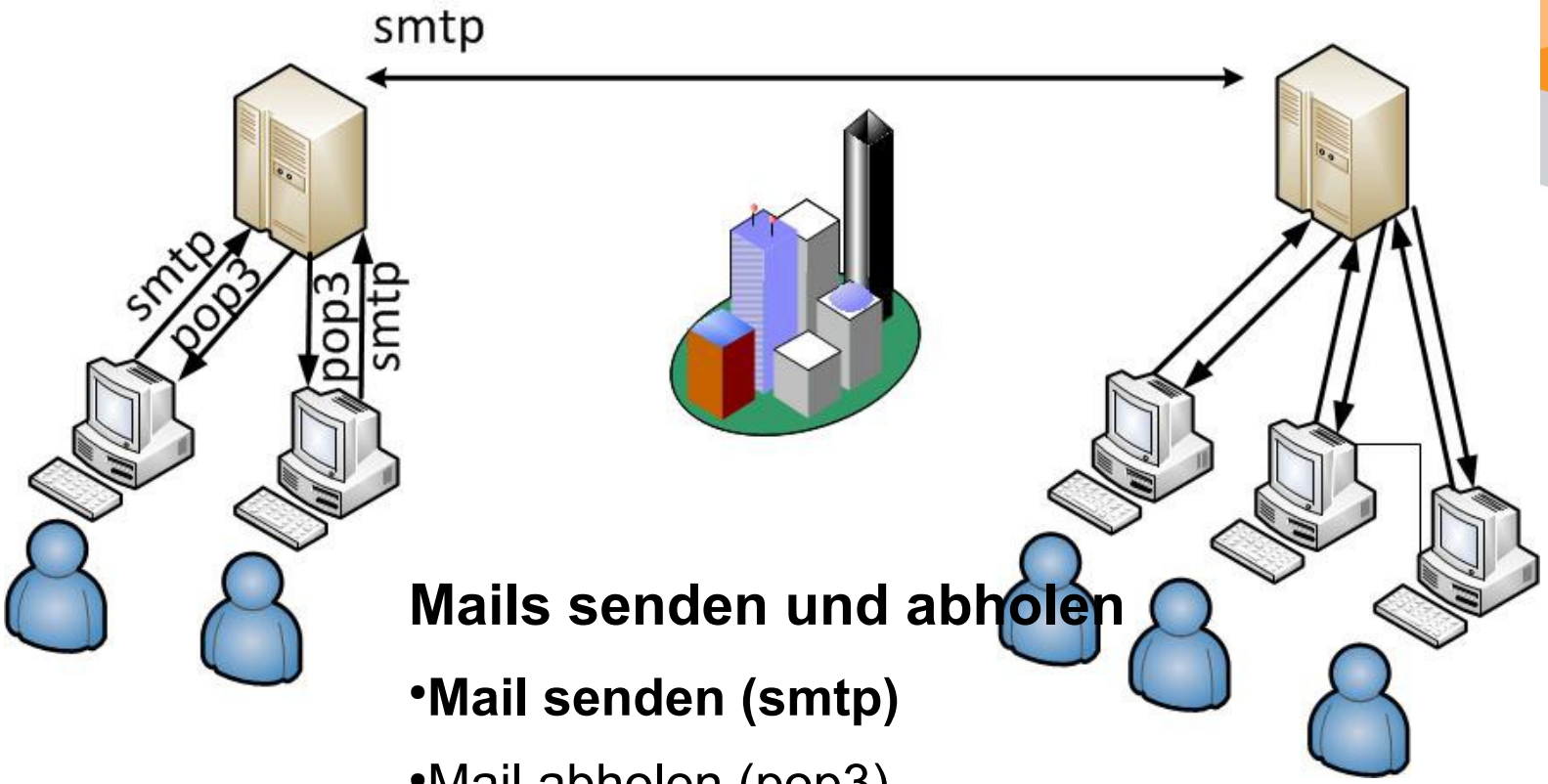
administrative liaison	W. Zorn (zorn@germany)
technical liaison	Michael Rotert (rotert@germany)
official name	germany
aliases	karlsruhe, uka, dfn

Let me know how you like to handle the announcement.

PIRATEN PARTEI

1984 POST OFFICE PROTOCOL (pop)

Piratenpartei Deutschland
Landesverband Bayern

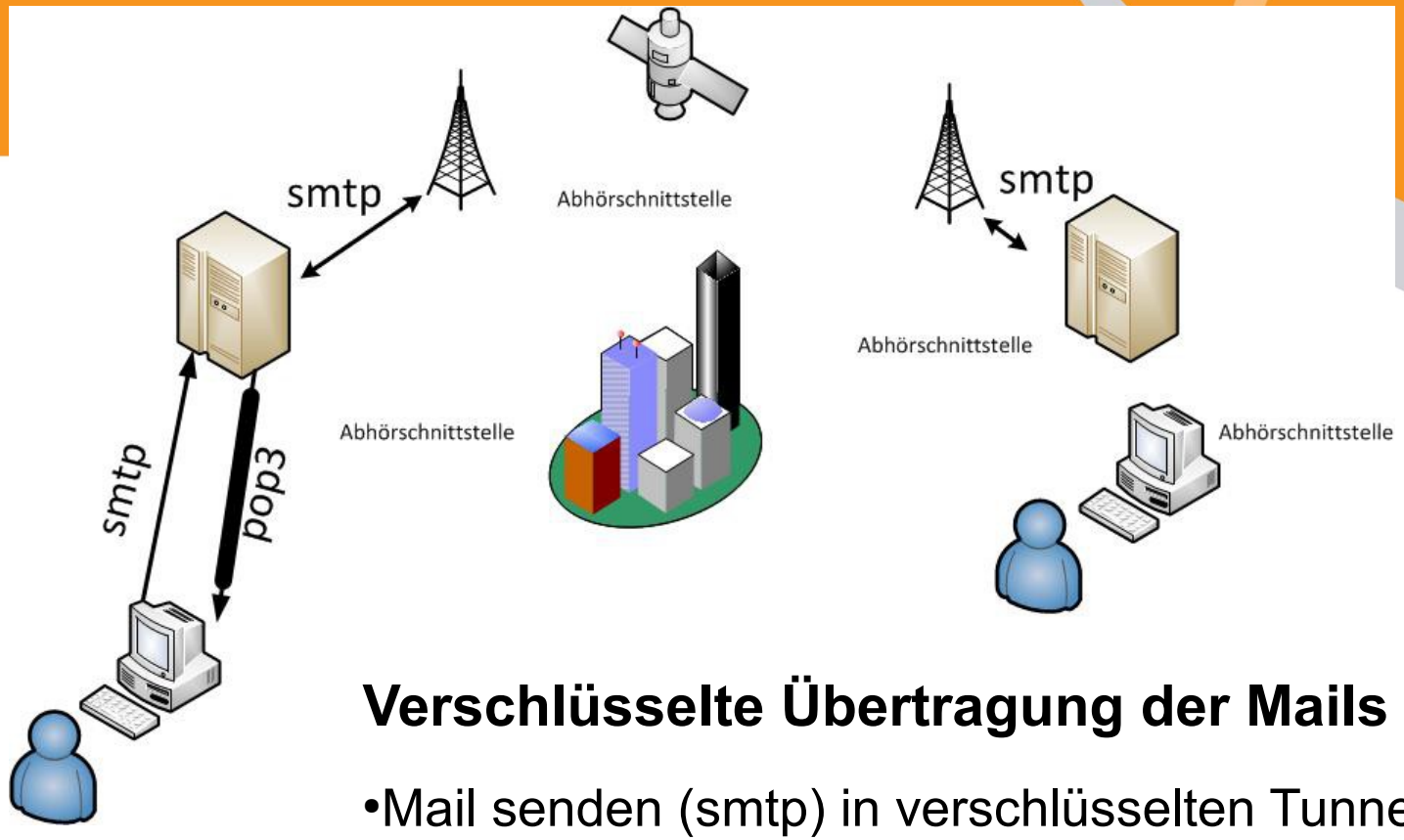


Mails senden und abholen

- **Mail senden (smtp)**
- Mail abholen (pop3)
- Mail abholen (imap)

PIRATEN PARTEI

1997 / 2002 / 2003 Verschlüsselte Transportwege (smtps / pop3s / imaps)

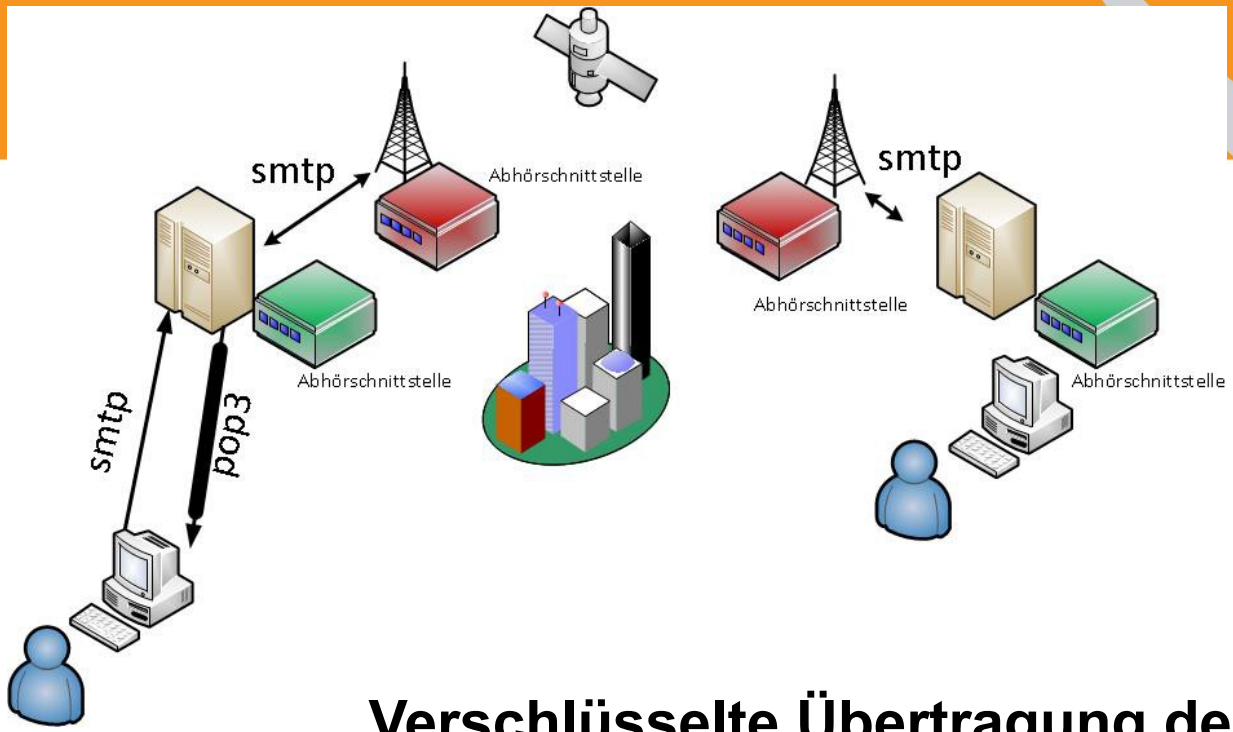


Verschlüsselte Übertragung der Mails

- Mail senden (smtp) in verschlüsselten Tunnel → smtps
- Mail abholen (pop3s) in verschlüsselten Tunnel → pop3s
- Mail abholen (imaps) in verschlüsselten Tunnel → imaps

PIRATEN PARTEI

1997 / 2002 / 2003 Verschlüsselte Transportwege (smtps / pop3s / imaps)



Verschlüsselte Übertragung der Mails

- Mail senden (smtp) in verschlüsselten Tunnel → smtps
- Mail abholen (pop3s) in verschlüsselten Tunnel → pop3s
- Mail abholen (imaps) in verschlüsselten Tunnel → imaps

PIRATEN PARTEI

Schwachpunkte:

- Mails liegen im Klartext auf dem PC (sent-Ordner)
- Mails liegen im Klartext auf beiden Mailservern
- Mails werden (vielleicht) im Klartext via smtp übertragen
- Mails liegen im Klartext auf dem PC (Inbox)

End-to-End-Verschlüsselung

TLS (Übertragungsweg):

- SSL
- htttps
- Pop3s
- smtps
- StartTLS

PGP (Inhalt):

- PGP (veraltet)
- GnuPG
- GPG4win

Schlüssel:

- Symetrische Schlüssel
- Unsymetrische Schlüssel (Schlüsselpaar)
  - Öffentliche Schlüssel
  - Private Schlüssel

Einfache symetrische Verschlüsslung:

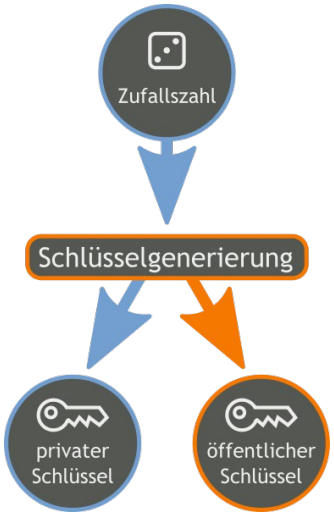
- rot13
- Triple-DES, RCA2, RCA4 und andere

Verarbeitungsstufen:

- Klartext
- Schlüssel (13 im Uhrzeigersinn)
- Verschlüsselter Text
- Schlüssel (13 gegen den Uhrzeigersinn)
- Klartext

unsymetrische Verschlüsselung:

- Ein Schlüsselpaar aus öffentlichem und privatem Schlüssel
- Entdeckt in den 70-er Jahren
- Extrem rechenaufwändig (seit ca. 2000 am PC beherrschbar)



öffentlicher Schlüssel

privater Schlüssel

Verarbeitungsstufen (Alice mailt an Bob)

- Öffentlichen Schlüssel (Vorhängeschloss) von Bob besorgen
- Mail mit Bobs öffentlichem Schlüssel verschlüsseln → smtp
- Mail mit Alice öffentlichem Schlüssel verschlüsseln → sent-Ordner
- Bob entschlüsselt mit seinem privaten Schlüssel

Wir misstrauen dem Transportweg

- Vertrauen in Betriebssystem
- Vertrauen in das Passwort
- Vertrauen in den Zufallsgenerator
- Vertrauen in Mathematik bzw. die Implementierung
- Vertrauen in den Schlüssel des Gegenübers

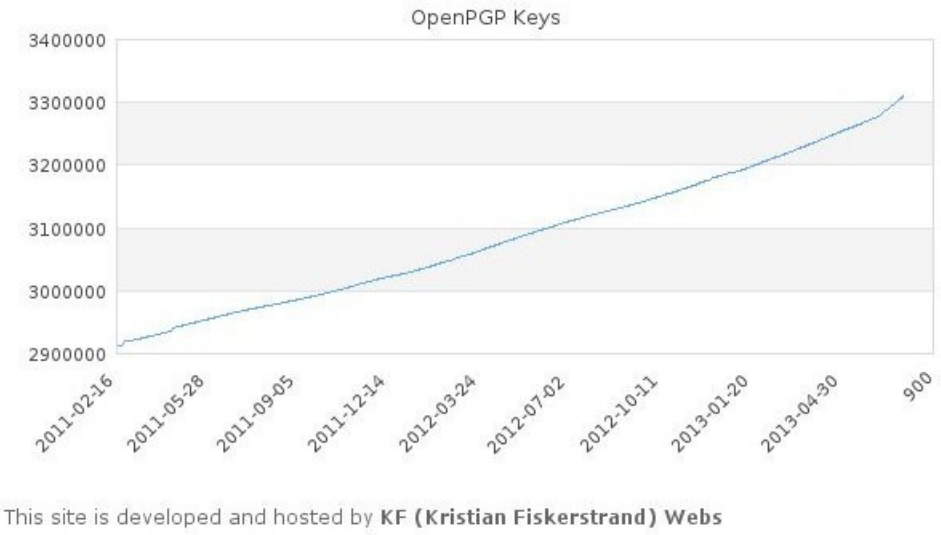
S/Mime vs. GnuPG

- Beide Methoden funktionieren
- Zentrale vs. dezentrale Strukturen
- Hier „Zertifikate“, dort „Schlüssel“
- Kosten für Zertifikate fallen (meist) an
- Zufriedenstellende kommerzielle Unterstützung vs. ???
- GnuPG unterstützt auch S/Mime ;-)

Was ist zu tun?

- Im Mailprogramm
  - Schlüsselpaar erzeugen (einmalig)
  - Öffentlichen Schlüssel hochladen (einmalig)
  - Öffentlichen Schlüssel für jeden Adressaten runterladen (je einmalig

- Alle öffentlichen Schlüssel auf Key-Server
- Eigener privater Schlüssel auf dem eigenen Rechner
  - Mit Passwort geschützt
  - Mit Ablaufdatum
  - Widerrufbar
  - Unterschreibbar



Programm	Betriebssysteme	Voraussetzung
Thunderbird Thunderbird to go (Windows)	Linux, *BSD, Mac OS X, Solaris,Windows	GnuPG Enigmail
Kmail (Kontact - KDE)	Linux, *BSD, Mac OS X, Solaris,Windows	GnuPG kgpg (Kleopatra)
Outlook (MS Office)	Windows (Linux)	GnuPG Gpg4win
Evolution (Gnome)	Windows XP, Linux, (Mac OS X)	GnuPG Seahorse
GPG[Mail]		

- Thunderbird (Mailprogramm vom Mozilla-Projekt)
- Enigmail (Plugin für den Komfort)
  - Schlüsselgenerierung
  - Schlüsselverwaltung (suchen und holen vom Keyserver)
  - Ver- und entschlüsseln
- Gpg4win (Verschlüsslungsalgorythmen)

- Schlüsselpaar erzeugen (Häckchen setzen)
- Öffentlichen Schlüssel auf Keyserver hochladen (OK klicken)
- In Mailprogramm einbinden

Piratenpartei Deutschland
Landesverband Bayern

- Thunderbird runterladen + installieren + konfigurieren
- Ggp4win runterladen + installieren
- Thunderbird starten und Enigmail als Plugin installieren
- „Jetzt neu starten“ klicken
- Auf „OpenPGP“ und „Einstellungen“ klicken

Positiv:

- Web-of-trust
- Dem Schlüssel ein Ablaufdatum geben
- Hybridverfahren → symetischer Schlüssel unsymetrisch geschickt
- Den Schlüssel widerrufen
- Mail signieren

Negativ:

- Kein Webmailer mehr
- Neben Bob und Alice gibt es auch Eve
- Absender, Empfänger und Betreff noch immer sichtbar
- Kein vorgelagerter Spam- oder Virenschutz

Fragen und Anmerkungen?