

Technische Grundlagen »Email«

Oder: Wo kann überall was schiefgehn?

Florian Streibelt

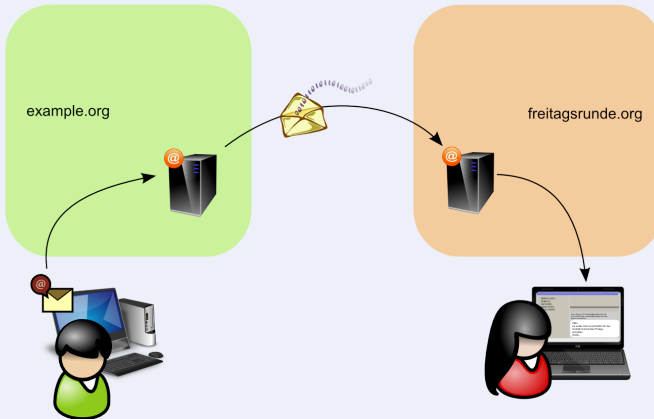
<florian@freitagsrunde.org>

Techtalk der Freitagsrunde, TU-Berlin

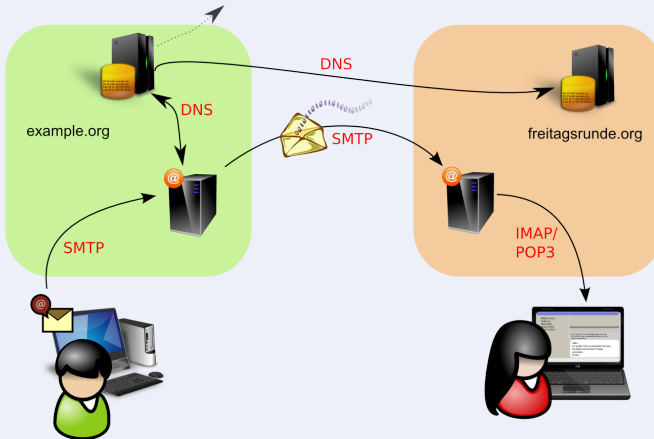
<http://freitagsrunde.org/>

29. April 2012

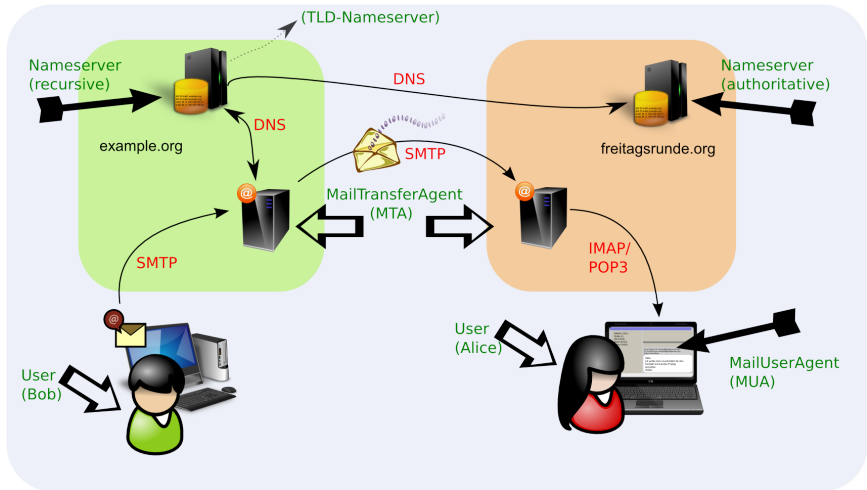
Email - abstraktes Problem



Email - Protokolle



Email - Nomenklatur



Alles klar?

- High-Level Überblick
- alles auf einmal ansehen ist zuviel
- wir hangeln uns von links nach rechts durch

Wer ist beteiligt?

Eine Reihe von Systemen spielen zusammen:

- Clients (MUA)
- Mailserver (MTA), evtl. Relays
- Nameserver aller Art
- Spezialfälle bei Antispam (später mehr)

Wie verstehen die sich?

Ausserdem eine ganze Reihe von Protokollen

- DNS
- SMTP
- LMTP
- IMAP
- POP3
- SIEVE

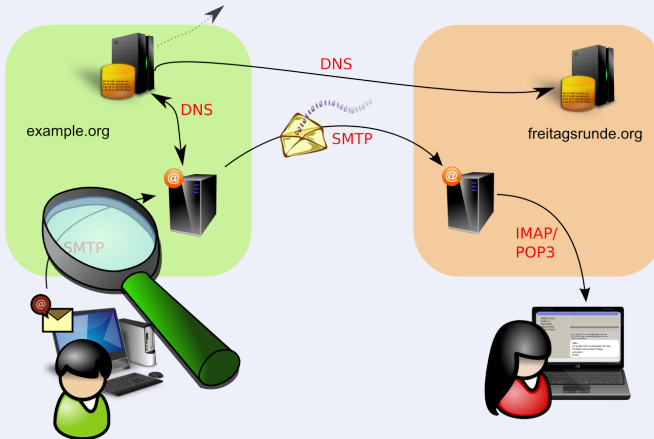
In Sonderfällen auch noch SQL, LDAP, NIS, YP, ...

Viele Fragen:

- ... und das funktioniert?
- ... wer blickt denn da noch durch?
- ... geht's noch komplizierter?

Antworten: Meistens funktioniert es irgendwie, Heinlein und Co. verdienen richtig Geld und ja, es geht noch viel komplizierter - spätestens bei den Layern > 8 (Gesetzliche Grundlagen).

Der erste Schritt



Erster Schritt: Der Benutzer klickt auf *Senden*.

- Protokoll: SMTP
- Kommunikationspartner: MUA und MTA
- Im Hintergrund laufen Authentifizierung, Verschlüsselung

- Simple Mail Transfer Protocol
- Eröffnet durch das Banner des Mailservers
- Der Client sagt HELO
- 3-4 Phasen: HELO,AUTH,ENVELOPE,DATA

Live Demo...

SMTP (Live Demo)

```
# nc localhost 25
220 flst61nb.lan.streibelt.net ESMTP Postfix (Debian)
HELO localhost
250 flst61nb.lan.streibelt.net
MAIL FROM: <florian@freitagsrunde.org>
250 2.1.0 Ok
RCPT TO: <florian.streibelt@TU-Berlin.de>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "Florian Streibelt" <florian@freitagsrunde.org>
To: "Florian Streibelt" <florian.streibelt@TU-Berlin.de>
Date: Thu, 19 Apr 2012 01:19:03 +0200
Subject: Test – Vortrag

Hallo ,
ich wollte nur mal testen!

.
250 2.0.0 Ok: queued as A1F85715A4
RSET
250 2.0.0 Ok
QUIT
221 2.0.0 Bye
```

Da fehlte doch jetzt was!

- keine Authentifizierung
- aber: genau so sprechen MTAs untereinander
- Wichtig: MAIL FROM != From:
- So funktioniert CC und BCC.
- Ausserdem: SPAM
- Verschlüsselung fehlte auch...

Ist ein extra Schritt nach dem HELO/EHLO:

- PLAIN / LOGIN
- verschlüsselt
- Challenge-Response Verfahren

Hinweis: Oft geht hier nur plain, da die Passwörter nicht im Klartext auf dem Server liegen, daher sollte die Verbindung SSL (oder TLS) nutzen!

Authentifizierung: PLAIN

```
220 mail.freitagrunde.org ESMTP Postfix (Debian/GNU)
EHLO flsnb
250-mail.freitagrunde.org
250-PIPELINING
250-SIZE 51200000
250-AUTH LOGIN PLAIN GSSAPI
250-AUTH=LOGIN PLAIN GSSAPI
AUTH LOGIN
334 VXNlcm5hbWU6
Zmxvcmlhbg==
334 UGFzc3dvcmQ6
c3RyZW5lGdlaGVpbSE=
235 2.7.0 Authentication successful
MAIL FROM: <florian@freitagrunde.org>
...
```

- Entweder SSL (Port 465, 587) oder TLS (port 25).
- SSL: transparent, Ende zu Ende, Protokollunabhängig
- TLS: zunächst Unverschlüsselt, dann Wechsel (STARTTLS)

Verschlüsselung: TLS vs. SSL

```
# nc mail.tu-berlin.de 25
220 mail.tu-berlin.de - ESMTP (exim-4.75/mailfrontend-4)
    ready at Thu, 19 Apr 2012 02:12:37 +0200
EHLO flsnb
250-mail.tu-berlin.de Hello 91-65-94-101-dynip.superkabel.de [91.65.94.101]
250-SIZE 157286400
250-8BITMIME
250-PIPELINING
250-STARTTLS
250 HELP
STARTTLS
220 TLS go ahead
```

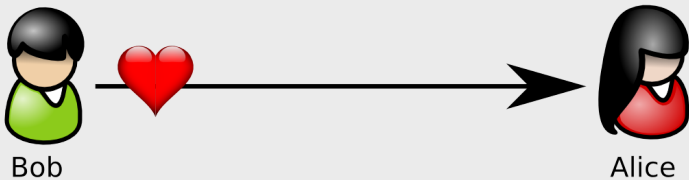
Ab hier weiter wie SSL

```
# openssl s_client -host mail.tu-berlin.de -port 465
```

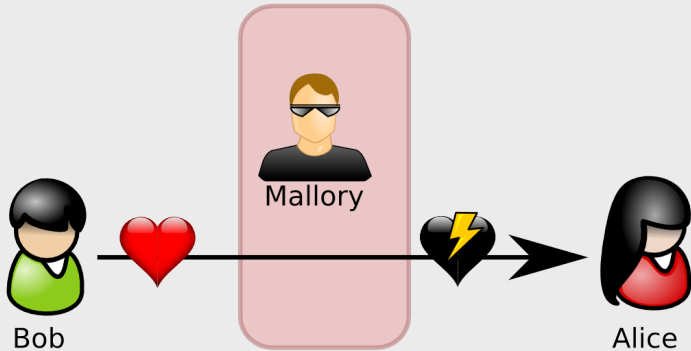
Was möchte ich erreichen?

- Authentizität
- Vertraulichkeit
- Integrität

Alice and Bob...

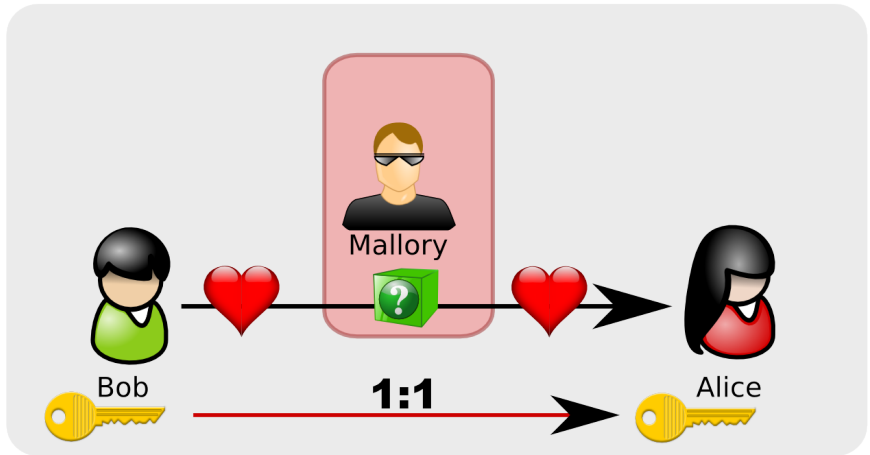


Message Manipulation

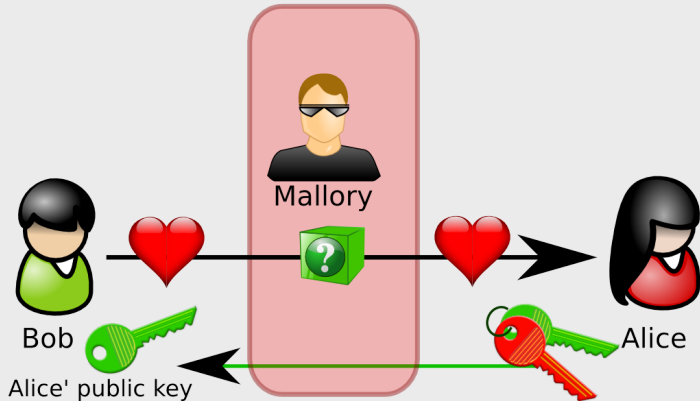


- Symetrische Verschlüsselung
- Asymetrische Verschlüsselung
- Signaturen
- CAs

Symmetrisch



Asymmetrisch



Symetrische Verschlüsselung

- geteilter Schlüssel
- Schlüsselverteilungsproblem
- hoher Aufwand

Asymetrische Verschlüsselung

- Schlüssel besteht aus zwei Teilen
- Öffentlicher und Privater Schlüssel
- Öffentlicher Schlüssel zum Verschlüsseln
- Privater Schlüssel zum Entschlüsseln
- Privater Schlüssel zum Signieren

$decrypt(encrypt(clear, pubkey), privkey) == clear$

- Asymmetrisches Kryptoverfahren
- Hashalgorithmus
- das zusammen ergibt Signaturen
- Hashwert mit **privatem** Schlüssel verschlüsselt
- Jeder prüft mit dem öffentlichen Schlüssel.
- Zertifikat ist signierter öffentlicher Schlüssel

Certification Authority: Mitspieler



Certification Authority

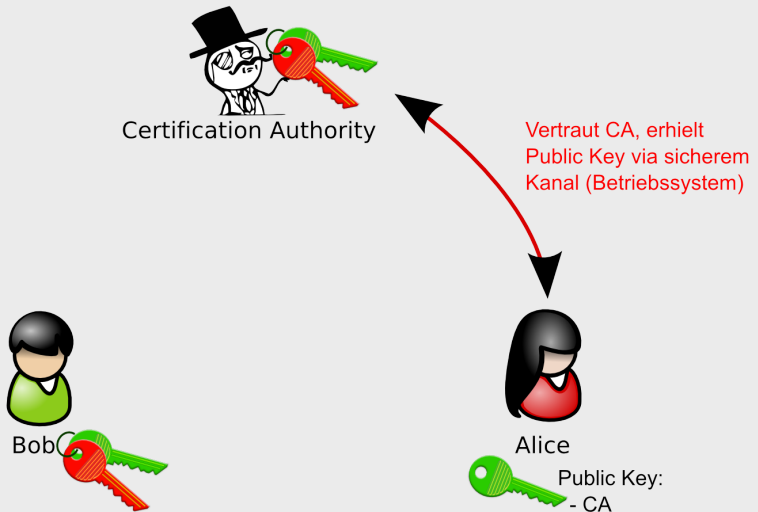


Bob

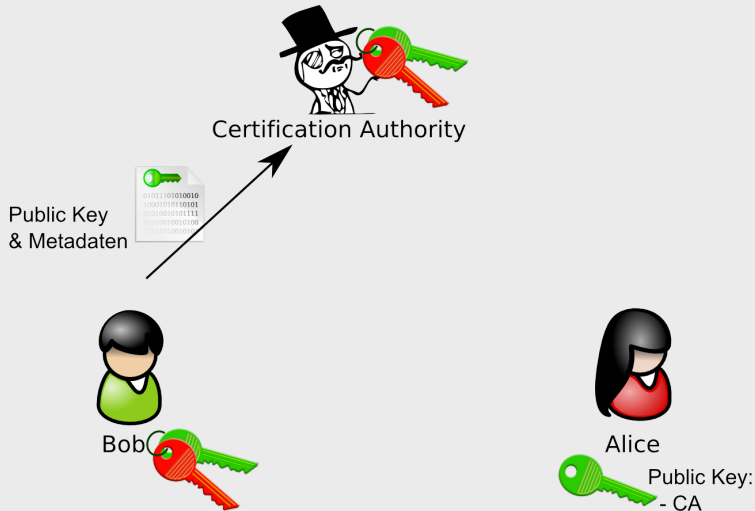


Alice

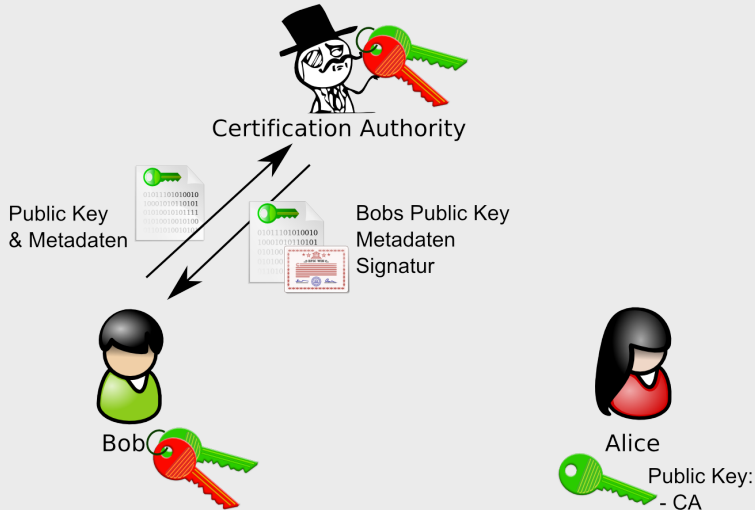
Certification Authority: Alice vertraut CA



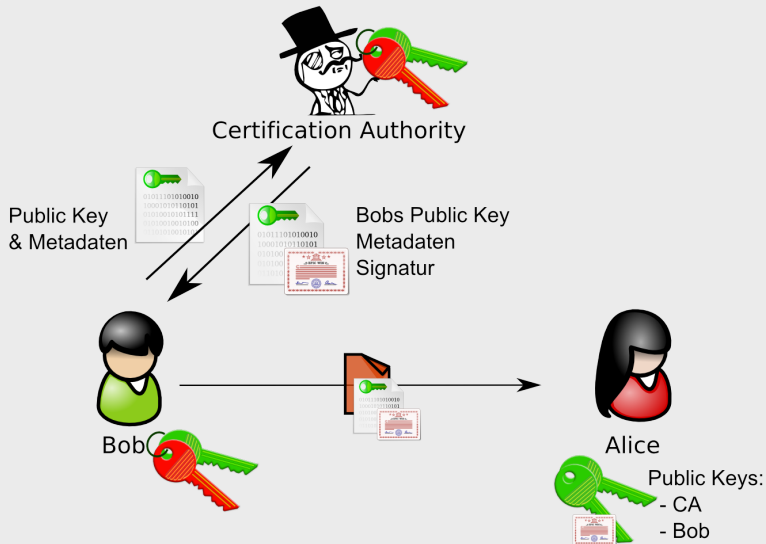
Certification Authority: Bobs Key an CA



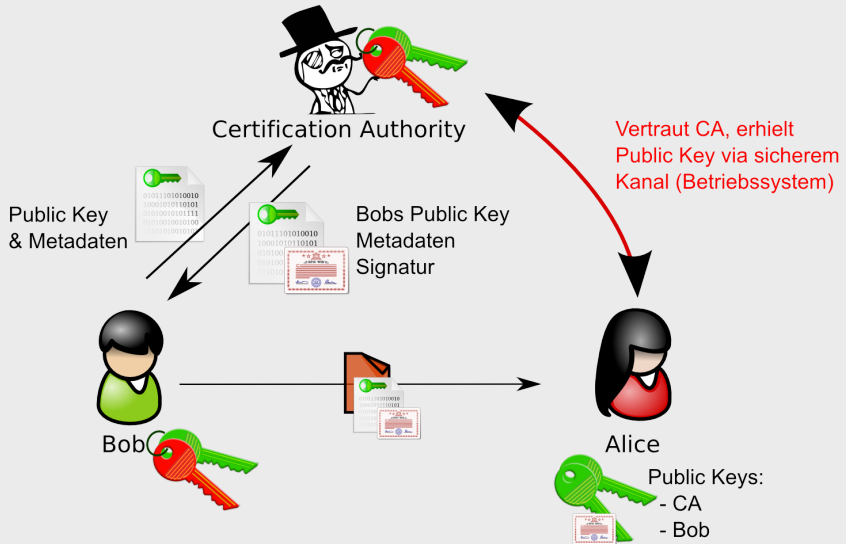
Certification Authority: Key wird signiert



Certification Authority: Bob versendet...



Certification Authority: Alice prüft Signaturen



- vertrauenswürdige Stelle
- signiert öffentliche Schlüssel mit ihrem privatem Schlüssel
- alle vertrauen diesem Schlüssel der CA
- alle so signierten Schlüssel sind nun auch gültig
- ergibt Hierarchie, Baumstruktur

- MTA transportiert E-Mail
- Jetzt neu: Spamfilter, Crypto, Archivierung, ...
- Admin-Stuff: Policies, Begrenzung
- Zentrales Element: Mailqueue

- Ist der Absender berechtigt?
- lokaler Empfänger?
- Relay für den Empfänger?
- Relay für den Absender?
- Oft: Existiert der Empfänger?
- Manchmal: Existiert der Absender?

Wie sieht eigentlich eine valide Emailadresse aus?

- Username, Domainpart
- Aber auch: Extension via +
- Multiple @ z.B. bei UUCP
- Kommentare erlaubt
- Es gibt eine Regex...

Exkurs: Regex zum Email verifizieren

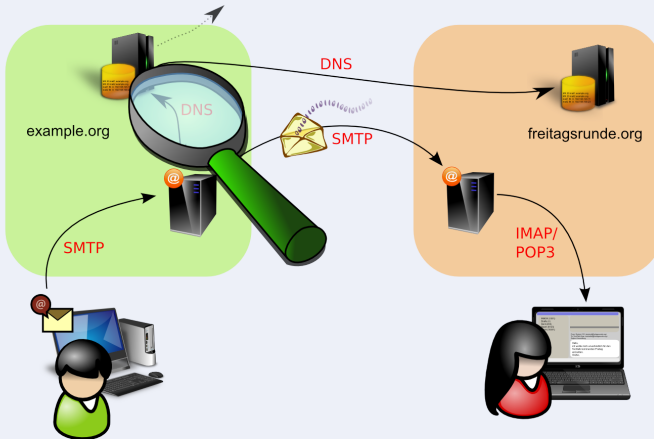
Quelle:

<http://www.ex-parrot.com/pdw/Mail-RFC822-Address.html>

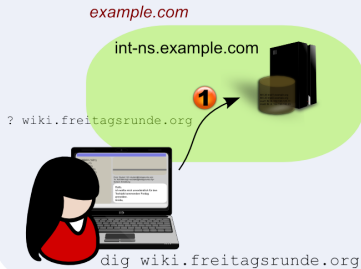
[illegible]

- Lokal: In die Mailbox des Users oder an lokalen Prozess
- Relay: Weiterleiten, nur wohin?
- Feste transports oder den Empfänger fragen!
- Moment: Empfänger fragen? Aber wer ist das?
- Lösung: Informationen sind im DNS hinterlegt

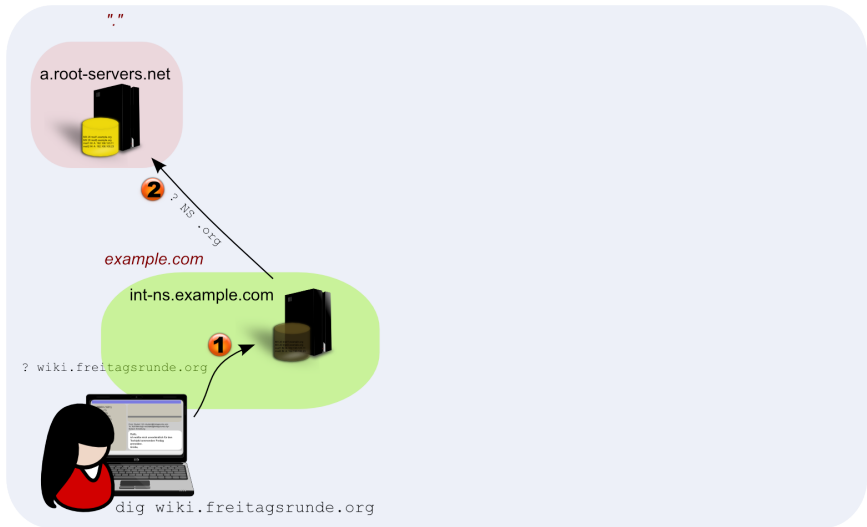
Der zweite Schritt: DNS



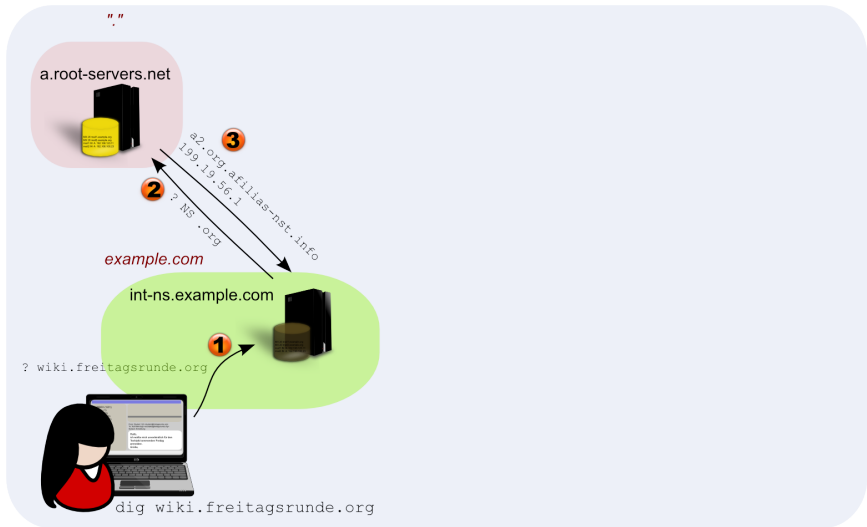
- Hierarchisches System mit Baumstruktur
- Oberste Ebene: Rootserver (weltweit verteilt)
- Lokaler DNS handelt sich durch die Struktur
- Rootserver (TLD), Registry für Domain, DNS des Ziels



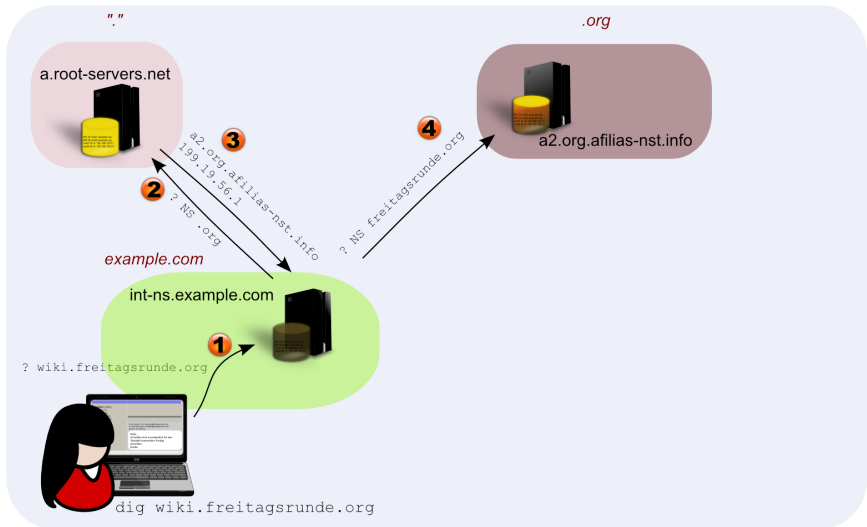
Exkurs: DNS



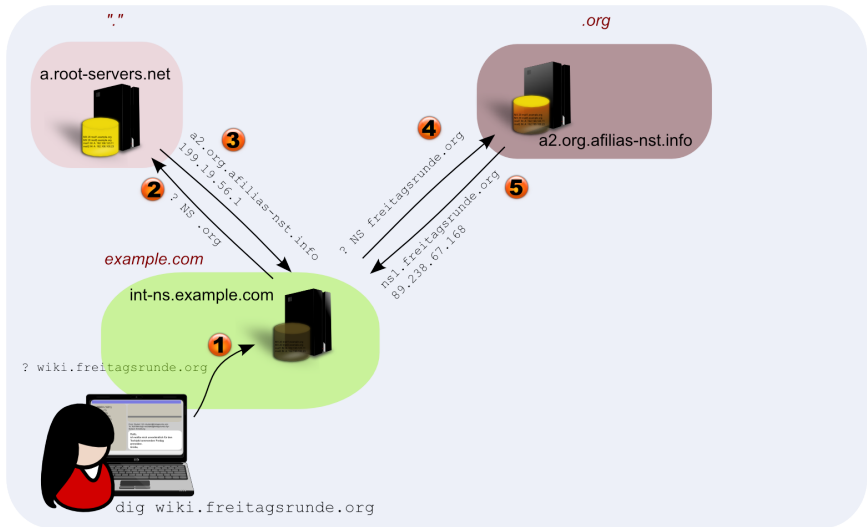
Exkurs: DNS



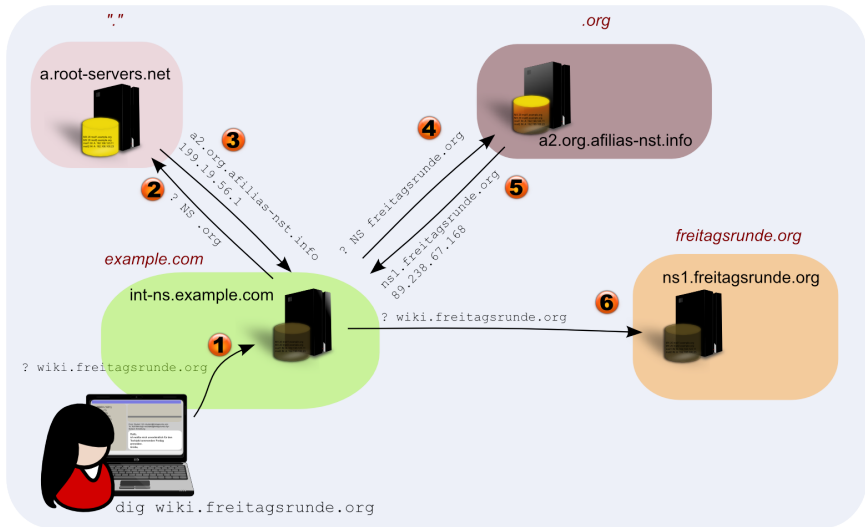
Exkurs: DNS



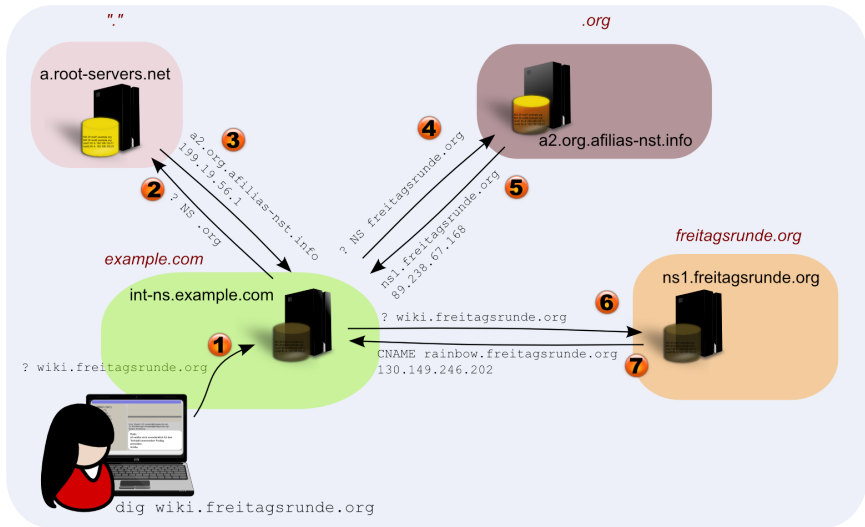
Exkurs: DNS



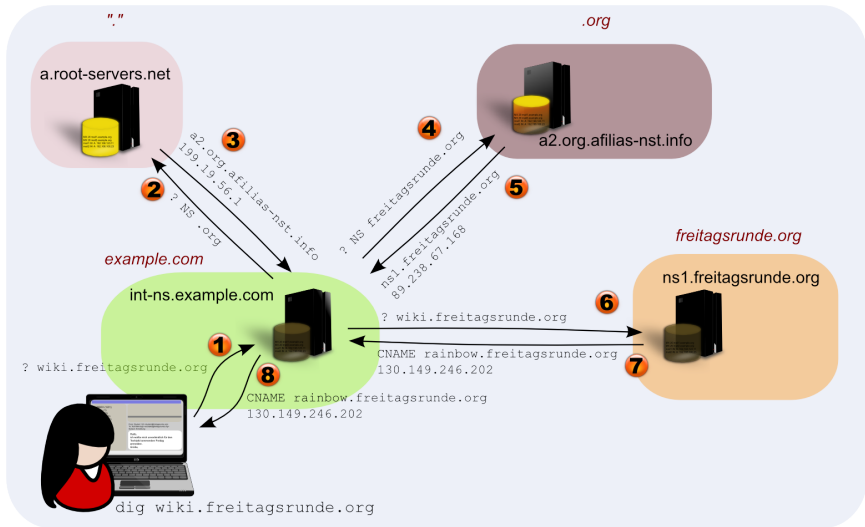
Exkurs: DNS



Exkurs: DNS



Exkurs: DNS



Es existieren viele verschiedene Resource-Record Typen, die wichtigsten:

- A, AAAA für Ipv4 und IPv6 Adressen
- PTR für Reverse-Lookups
- NS für Nameserver
- CNAME (Canonical Name) als Verweis
- SRV für Services
- TXT für Texteinträge
- MX für Mailserver

Exkurs: DNS - Zone

```
$ORIGIN .
$TTL 21600      ; 6 hours
streibelt.de    IN SOA  ns01.streibelt.net. hostmaster.streibelt.net. (
                        2012032002 ; serial
                        21600      ; refresh (6 hours)
                        2700       ; retry (45 minutes)
                        1814400    ; expire (3 weeks)
                        600        ; minimum (10 minutes)
                        )
                        NS        ns01.streibelt.net.
                        NS        ns04.f-streibelt.de.
                        MX        50 mx01.streibelt.net.
                        MX        50 mx02.streibelt.net.
                        TXT       "v=spf1 a mx ~all" "google-site-verification=OC...vBEi8"
                        A         85.214.205.237
                        AAAA      2a01:238:42e2:3b00:7549:af5c:51b8:9dab

$ORIGIN _tcp.streibelt.de.
_imap          SRV        0 0 0 .
_imaps         SRV        0 1 993 mx02.streibelt.net.
_pop3          SRV        0 0 0 .
_pop3s         SRV        10 1 995 mx02.streibelt.net.

$ORIGIN streibelt.de.
www            CNAME      streibelt.de.
```

Exkurs: DNS - Zone (1)

```
$ORIGIN .
$TTL 21600          ; 6 hours
streibelt.de IN SOA ns01.streibelt.net. \
                    hostmaster.streibelt.net. (
                    2012032002 ; serial
                    21600      ; refresh (6 hours)
                    2700       ; retry (45 minutes)
                    1814400    ; expire (3 weeks)
                    600        ; minimum (10 minutes)
                    )
NS      ns01.streibelt.net.
NS      ns04.f-streibelt.de.

MX      50 mx01.streibelt.net.
MX      50 mx02.streibelt.net.
```

Exkurs: DNS - Zone (2)

```
MX      50 mx01.streibelt.net.
MX      50 mx02.streibelt.net.
TXT     "v=spf1 a mx ~all" \
        "google-site-verification=OC...vBEi8"

A       85.214.205.237
AAAA    2a01:238:42e2:3b00:7549:af5c:51b8:9dab
```

```
$ORIGIN _tcp.streibelt.de.
_imap    SRV      0 0 0 .
_imaps   SRV      0 1 993 mx02.streibelt.net.
_pop3    SRV      0 0 0 .
_pop3s   SRV      10 1 995 mx02.streibelt.net.
```

```
$ORIGIN streibelt.de.
www      CNAME    streibelt.de.
```

Exkurs: DNS - dig (Livedemo)

```
$ dig streibelt.de
```

```
; <<>> DiG 9.4.1-P1 <<>> streibelt.de
;; global options:  printcmd
;; Got answer:
;; -->>HEADER<<-- opcode: QUERY, status: NOERROR, id: 9350
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 2

;; QUESTION SECTION:
;streibelt.de. IN A

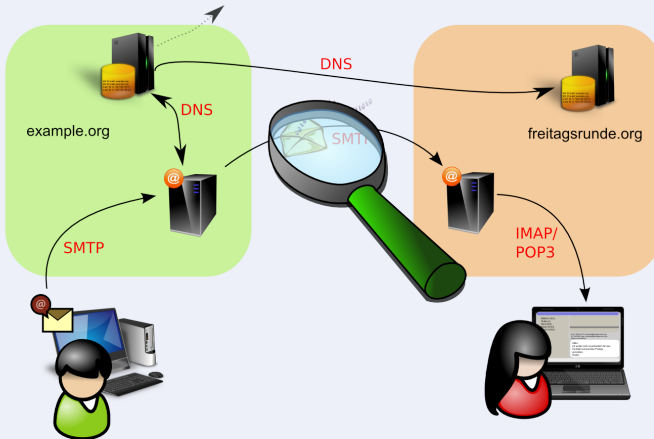
;; ANSWER SECTION:
streibelt.de. 21600 IN A 85.214.205.237

;; AUTHORITY SECTION:
streibelt.de. 21600 IN NS nsb2.schlundtech.de.
streibelt.de. 21600 IN NS ns01.streibelt.net.
streibelt.de. 21600 IN NS ns04.f-streibelt.de.

;; ADDITIONAL SECTION:
nsb2.schlundtech.de. 119 IN A 217.160.113.52
nsb2.schlundtech.de. 119 IN A 83.169.55.12

;; Query time: 11 msec
;; SERVER: 217.11.48.200#53(217.11.48.200)
;; WHEN: Thu Apr 19 18:18:31 2012
;; MSG SIZE rcvd: 172
```

Der dritte Schritt: Transport



zweiter Hop: MTA zu MTA (Header)

- Mailheader ist voller Informationen
- Jeder Hop fügt (u.a.) Received-Zeilen ein
- Oft: Authentifizierter User
- Mailclient, Virens Scanner, etc
- von unten nach oben lesen
- kann auch manipuliert werden
- Stichwort: DKIM

Exkurs: Mailheader

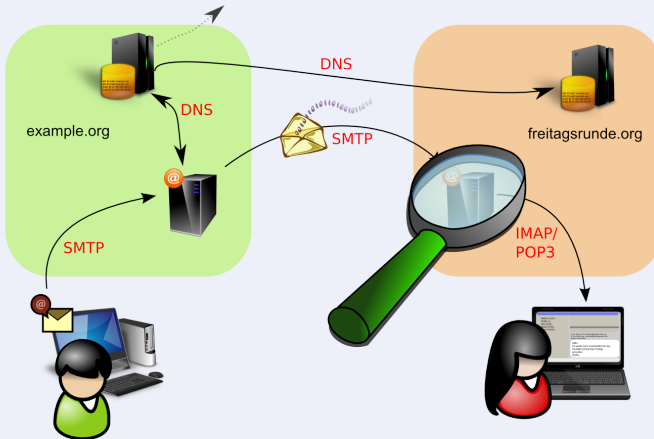
Return-Path: <florian@freitagsrunde.org>
Received: from mx02.streibelt.net ([89.238.67.167])
by mail.tu-berlin.de (exim-4.75/mailfrontend-4) with esmtps [TLSv1:AES256-SHA:256]
for <florian.streibelt@TU-Berlin.de>
id 1SKe9j-0005MS-Bq; Thu, 19 Apr 2012 01:19:23 +0200
Received: from flst61nb.lan.streibelt.net (Remote IP hidden)
(using TLSv1 with cipher ADH-AES256-SHA (256/256 bits))
(No client certificate requested)
(Sender was authenticated on mx02)
by mx02.streibelt.net (Postfix) with ESMTP id 3CC31413AC
for <florian.streibelt@TU-Berlin.de>; Thu, 19 Apr 2012 01:19:23 +0200 (CEST)
Received: from localhost [127.0.0.1]
by flst61nb.lan.streibelt.net (Postfix) with SMTP id A1F85715A4
for <florian.streibelt@TU-Berlin.de>; Thu, 19 Apr 2012 01:18:20 +0200 (CEST)
From: "Florian Streibelt" <florian@freitagsrunde.org>
To: "Florian Streibelt" <florian.streibelt@TU-Berlin.de>
Date: Thu, 19 Apr 2012 01:19:03 +0200
Subject: Test - Vortrag
Message-Id: <20120418231830.A1F85715A4@flst61nb.lan.streibelt.net>

Hallo,
ich wollte nur mal testen!

Wichtige Header

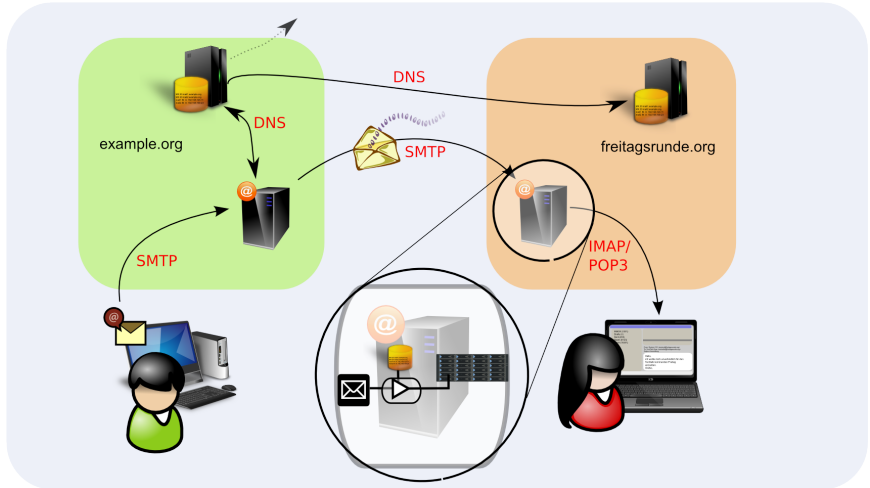
- From, To, Subject, Date
- Received
- Delivered-To, X-Original-To
- Message-ID, In-Reply-To, References

Der vierte Schritt: Ziel-MTA



- Relay/Proxy für internen Server
- Lokale Zustellung in Mailboxen
- Virtuelle Domains, User in Datenbanken
- 'Mailboxserver' (Cyrus, Dovecot, ...)

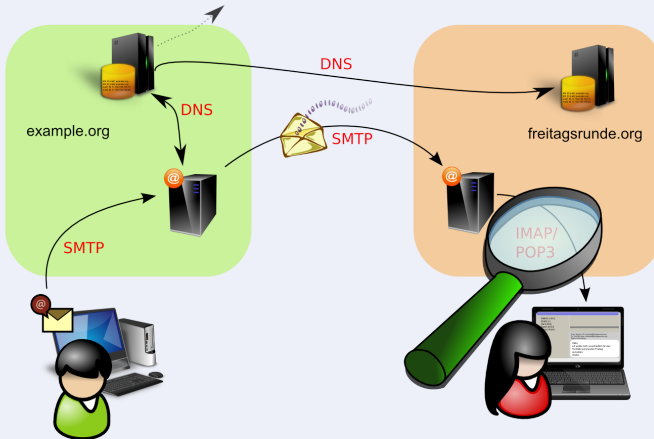
Der fünfte Schritt: Lokale Zustellung



Ziel-MTA - Beispiel Virtuelles Setup

- Valide Emailadressen in Datenbank
- Übergabe an lokalen Delivery-Agent (LDA)
- LMTP oder Pipe/Fifo
- Zuordnung von Adresse zu Mailbox
- Speichern der Emails in Maildir/Mbox
- Serverbasierte Filter (SIEVE)

Der sechste Schritt: Mail Retrieval



- lokaler Zugriff (PINE, Mutt, ...)
- POP3 - Post Office Protocol
- IMAP - Internet Message Access Protocol
- Webmail - nutzt auch nur pop/imap

- unterstützt keine Ordnerstrukturen
- Email wird normalerweise gelöscht
- relativ simpel

- Ordner mit Unterordnern erlaubt
- geteilte Ordner möglich
- Email bleibt i.d.R. auf dem Server
- Suchoperationen auf dem Server
- unterstützt Metainformationen (gelesen, wichtig, ...)

Exkurs: POP3 (1)

```
$ telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK Dovecot ready.
USER florian
+OK
PASS ccccccccc
+OK Logged in.
LIST
+OK 1936 messages:
1 3580
2 1770
3 982
[...]
1936 2383
.
RETR 3
```

Exkurs: POP3 (2)

RETR 3

+OK 982 octets

Return-Path: <bounce@freitagsrunde.org>

X-Original-To: root

Delivered-To: florian@freitagsrunde.org

Received: by mail.freitagsrunde.org (Postfix, from userid 0)
id 25CFE118471D; Wed, 14 Mar 2012 03:16:02 +0100 (CET)

From: root (Cron Daemon)

To: root

Subject: Cron <root@stan> test -x /usr/sbin/run-crons && /usr/sbin/run-crons

X-Cron-Env: <SHELL=/bin/bash>

[...]

Message-Id: <20120314021603.25CFE118471D@mail.freitagsrunde.org>

Date: Wed, 14 Mar 2012 03:11:42 +0100 (CET)

>>Hier koennte Ihre Werbung stehen...<<

.

RSET

+OK

QUIT

+OK Logging out.

Connection closed by foreign host.

Exkurs: IMAP (1)

```
$ telnet localhost 143
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE
  IDLE NAMESPACE STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
1 LOGIN florian xxxxxxxxx
1 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE
  IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS MULTIAPPEND
  UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1
  CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH
  LIST-STATUS SEARCH=FUZZY SPECIAL=USE NAMESPACE QUOTA] Logged in
```

Exkurs: IMAP (2)

2 SELECT INBOX

```
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft Junk NonJunk
    $label1 $label3 $label2 $Forwarded $MDNSent $label4 redirected)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft
    Junk NonJunk $label1 $label3 $label2 $Forwarded $MDNSent $label4
    redirected \*)] Flags permitted.
* 1938 EXISTS
* 0 RECENT
* OK [UNSEEN 1] First unseen.
* OK [UIDVALIDITY 1229720409] UIDs valid
* OK [UIDNEXT 26774] Predicted next UID
* OK [HIGHESTMODSEQ 45880] Highest
2 OK [READ-WRITE] Select completed.
```

Exkurs: IMAP (3)

3 FETCH 5 full

```
* 5 FETCH (FLAGS (NonJunk $label1) INTERNALDATE "14-Mar-2012 12:36:43 +0100"
RFC822.SIZE 982 ENVELOPE ("Wed, 14 Mar 2012 03:11:42 +0100 (CET)"
"Cron <root@stan> test -x /usr/sbin/run-crons && /usr/sbin/run-crons
" (("Cron Daemon" NIL "root" "MISSING_DOMAIN")) (("Cron Daemon" NIL "root"
"MISSING_DOMAIN")) (("Cron Daemon" NIL "root" "MISSING_DOMAIN"))
((NIL NIL "root" "MISSING_DOMAIN")) NIL NIL NIL
"<20120314021603.25CFE118471D@mail.freitagsrunde.org>")
BODY ("text" "plain" ("charset" "us-ascii") NIL NIL "7bit" 349 2))
3 OK Fetch completed.
```

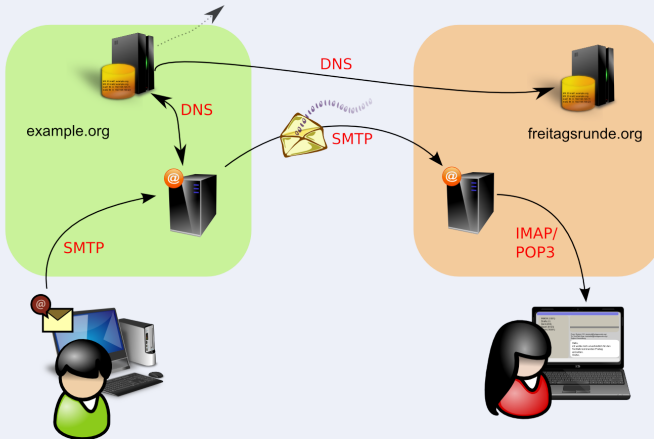
4 LOGOUT

* BYE Logging out

4 OK Logout completed.

Connection closed by foreign host.

Email - Die Übersicht



Offene Fragen?

Bis hierher Fragen?

Weitere Themen:

- SPAM
- Mailinglisten
- Freitagsrunden-Setup

- Bis 90% SPAM werden gemessen
- je früher Ablehnen, desto besser
- statische Regeln,
- heute oft auch per RBL
- Abfrage über DNS-Protokoll
- Filter in zweiter Linie
- Ressourcen sparen!
- Greylisting kaum wirksam

SPAM: Strenge Regeln

- HELO-checks
- Timing- und Protokollanalyse
- Blacklists für bestimmte Hosts
- Whitelists für eigene Hosts
- eigene Domain im From ablehnen
- Bitte: keine Filter für abuse/postmaster

SPAM: Quellen regulieren

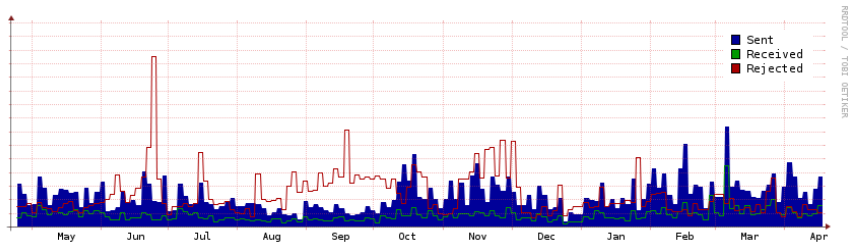
- SPF - via TXT-Records
- IN TXT "v=spf1 a mx all"
- DKIM
- Digitale Signatur von Headerteilen

- Datenbank mit bekannten Spammern
- täglich neu generiert
- Abfrage mit Namen des MTA per DNS
- Ergebnis: z.B. kein Eintrag oder 127.0.0.1
- eig. Missbrauch von DNS, klappt aber hervorragend
- z.B. <http://www.dnsbl.manitu.net/>
- Beim Benutzen: Nie als einzige Quelle! Scoring!

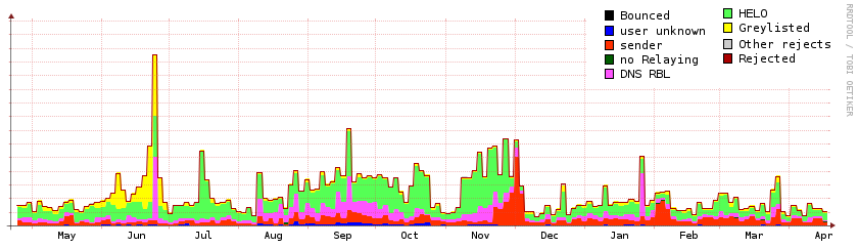
SPAM: Greylisting

- Greylisting nutzt kaum noch
- Zuviele geknackte Rechner
- kippen bei echten MTAs ein
- Idee: beim Ersten Versuch ablehnen
- echter Mailserver versucht wieder
- Leider nicht alle!

SPAM: Durchsatz/Reject



SPAM: Gründe für Reject



- Bsp.: Mailman
- Envelope-From: Eindeutig pro Liste
- From: Der eigentliche Absender
- RCPT-TO einfach wiederholen pro Empfänger
- Header zeigen 'Bulkmail' an
- Wichtig: daher keine Vacationmsg, normalerweise

- Eigener Techtalk, nur kurz:
- Port 25 ist zu
- Mailfilter der tubit für uns inakzeptabel
- externe Server nehmen E-mails an
- Weiterleitung über abweichenden Port (SMTP)
- Ausgehend wegen Antispam der tubit/IRB über dieselben Server
- TU-Interne mail macht also Rundreise

Dank an:

- das Publikum für die Geduld und die Fragen!
- Methyltheobromin und Guaranin in H_2O

Bildnachweise:

- Einzelbilder von [Openclipart.org](https://openclipart.org/)