email de'luxe

Features, die nicht jeder hat

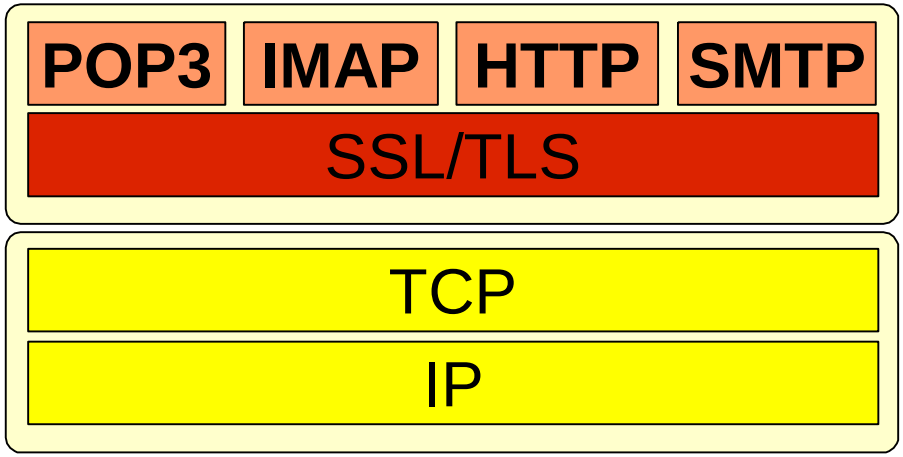
SSL & Cyrus & Sieve

Jörg Kinzebach <joerg@duck.franken.de>

SSL

SSL
"Secure Socket Layer"
v 3.0 seit 1995

TLS
"Transport Layer Security"
v 1.0 1996-1999



Cyrus POP3/IMAP Server

der Carnegie Mellon University

- IMAP4
- POP3

- Access Control Lists
- Spool-File pro Mail
- Administration via IMAP
- Unterstützung für Quota auf Mailbox
- SSL/TLS
- Unterstützung von SASL
  "Simple Authentication and Security Layer"
  (RFC2222)

Sieve

RFC 3028 "Sieve: A Mail Filtering Language"

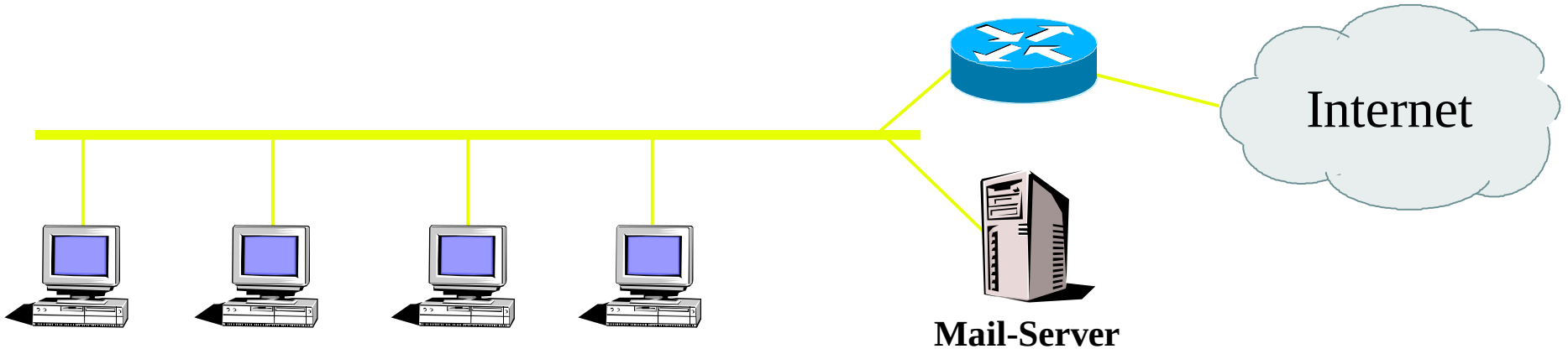
Filtern von Mail bei der Auslieferung an den lokalen User.

- standardisierte Filtersprache
- Regeln pro Nutzer
- durch Nutzer selbst veränderbar

Features,
die nicht jeder hat

Anforderungen an das Mailsystem und
Lösungen für benötigte Features.

08/15 Office



- nur lokale Clients
- "schneller" Zugriff auf Server
- Nutzer immer am gleichen PC
- geringes Mailaufkommen

➡ Einfacher Mailserver mit POP3-Daemon

POP3

Post Office Protocol Version 3

seit 1988 – Nachfolger von POP & POP2

typische POP3-Session:

- Client authentisiert sich bei POP3 Server
- Client transferiert bei Bedarf Mail von Server zu lokalem Speicher
- Client sollte nach erfolgreicher Übertragung Mail von Server löschen
- Client beendet die Verbindung zum Server
- Nutzer arbeitet lokal mit den heruntergeladenen Mails

Vorteile von POP3:

- kein Filesharing Protokoll nötig um Mail von Server auf Client zu transferieren
- einfaches Protokoll, einfach zu implementieren
- große Anzahl von Mailclients mit POP3-Unterstützung

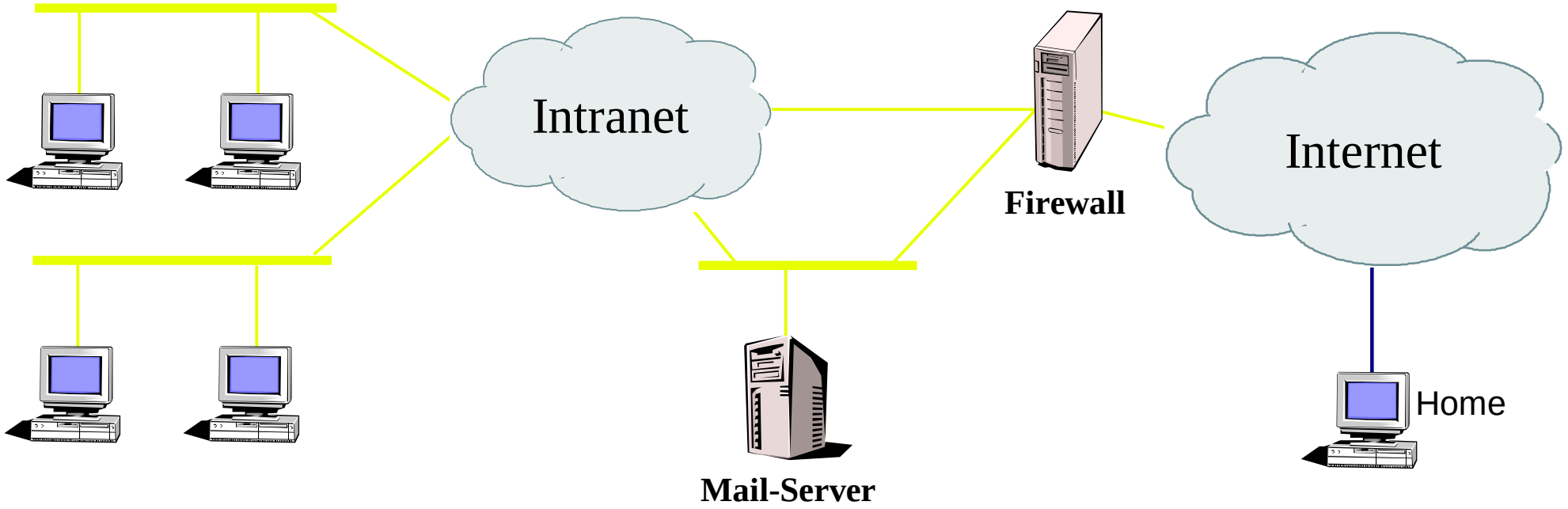
POP3

Nachteile von POP3:

- nur "offline" Modus unterstützt
- die Arbeit mit Mails muß lokal erfolgen
- keine Veränderung der Mails auf dem Server möglich
- potentiell große Downloads
- Client muß regelmäßig nachfragen um von neuen Mails zu erfahren
- keine zeitgleichen Zugriffe auf Mailbox von verschiedenen Workstations

email de'luxe

"High Profile"-Office oder ISP



- Mailabruf von wechselnden Netzen
- Benachrichtigung über neue Mails
- zentrale Archivierung von Mails
- große Mengen an Mails
- Mailversand von wechselnden Netzen
- Sichere Übertragung von Kennworten und Mails (Abruf und Versand)

IMAP4

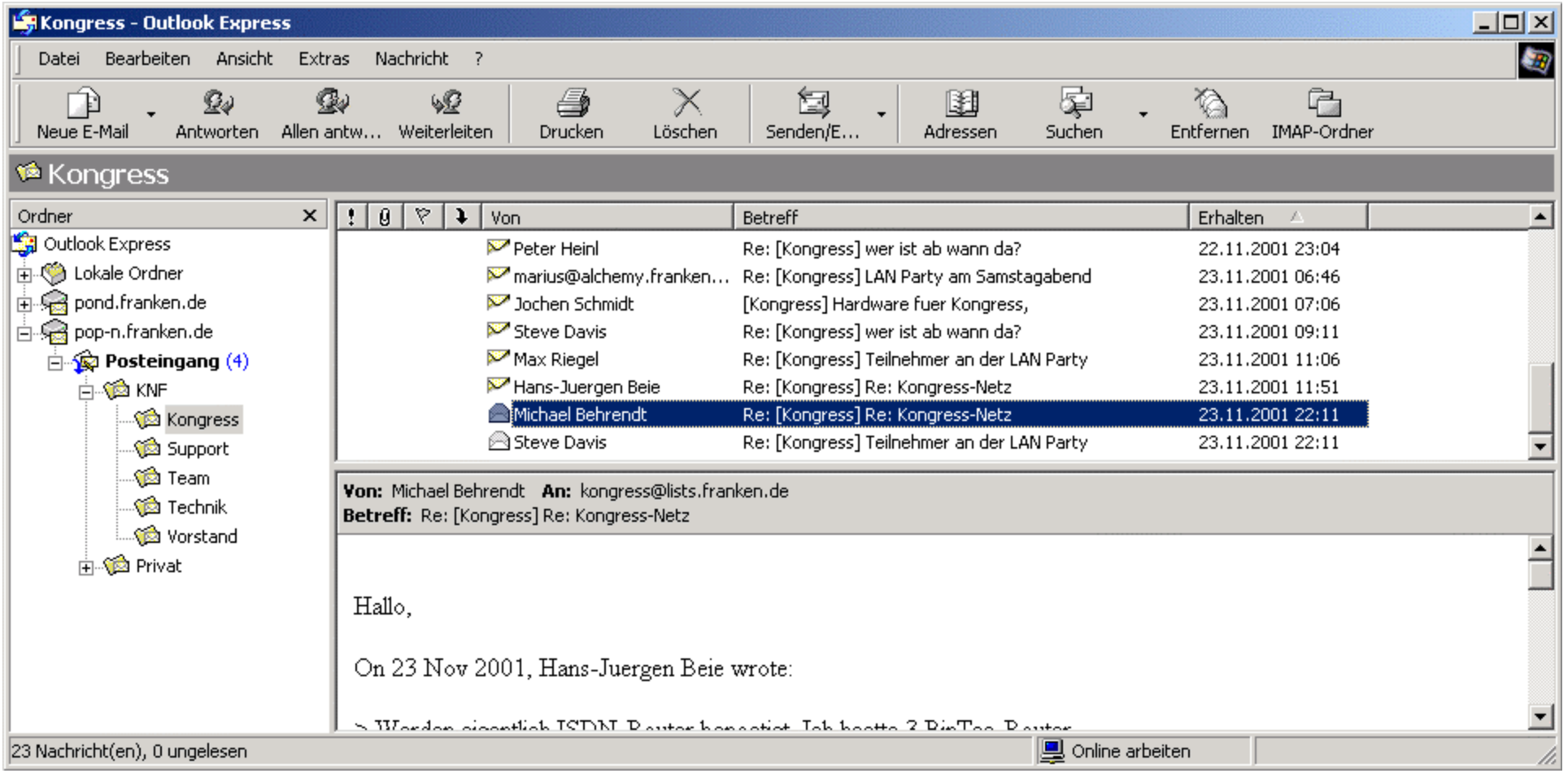
Internet Mail Access Protocol

- 1986 entwickelt an der Standford University
- Message-Flags können auf Server gespeichert/geändert werden
  (z.B. "read", "unread", "answered")
- "online", "offline" und "disconnected" Benutzung
- Übertragung von Teilen einer Nachricht möglich (z.B. "nur Header" oder bei MIME-codierten Attachements)
- paralleler Zugriff auf Mailbox von mehreren Clients
- Unterverzeichnisse auf Server
- Zugriffsrechte auf Server erlauben "sharen" von Foldern
- Suchoperationen können vom Server durchgeführt werden

email de'luxe

Folder auf IMAP-Server

Archivierung der Mails in Foldern auf IMAP-Server



IMAP4

Probleme von IMAP4 im Vergleich zu POP3:

- komplizierteres Protokoll
- von weniger Mailprogrammen unterstützt
- wenn Mail auf dem Server archiviert wird, benötigt dieser mehr Festplattenkapazität
- größere Last (CPU/IO) auf Mailserver

POP3/IMAP-Implementationen

einfache Daemon verwenden das UNIX mbox-Format

- Bei Abruf einer einzelnen Nachricht muß das komplette File mit allen Mails nach der angefragten durchsucht werden
- Beim Löschen einer Mail muß nahezu das gesamte Spoolfile aller Mails umkopiert werden

POP3/IMAP Daemon mit Maildir

- jede Mail wird in einem einzelnen File abgelegt, daruch ist ein geziehlter Zugriff möglich sowie Löschen ohne Zwischenspeicher

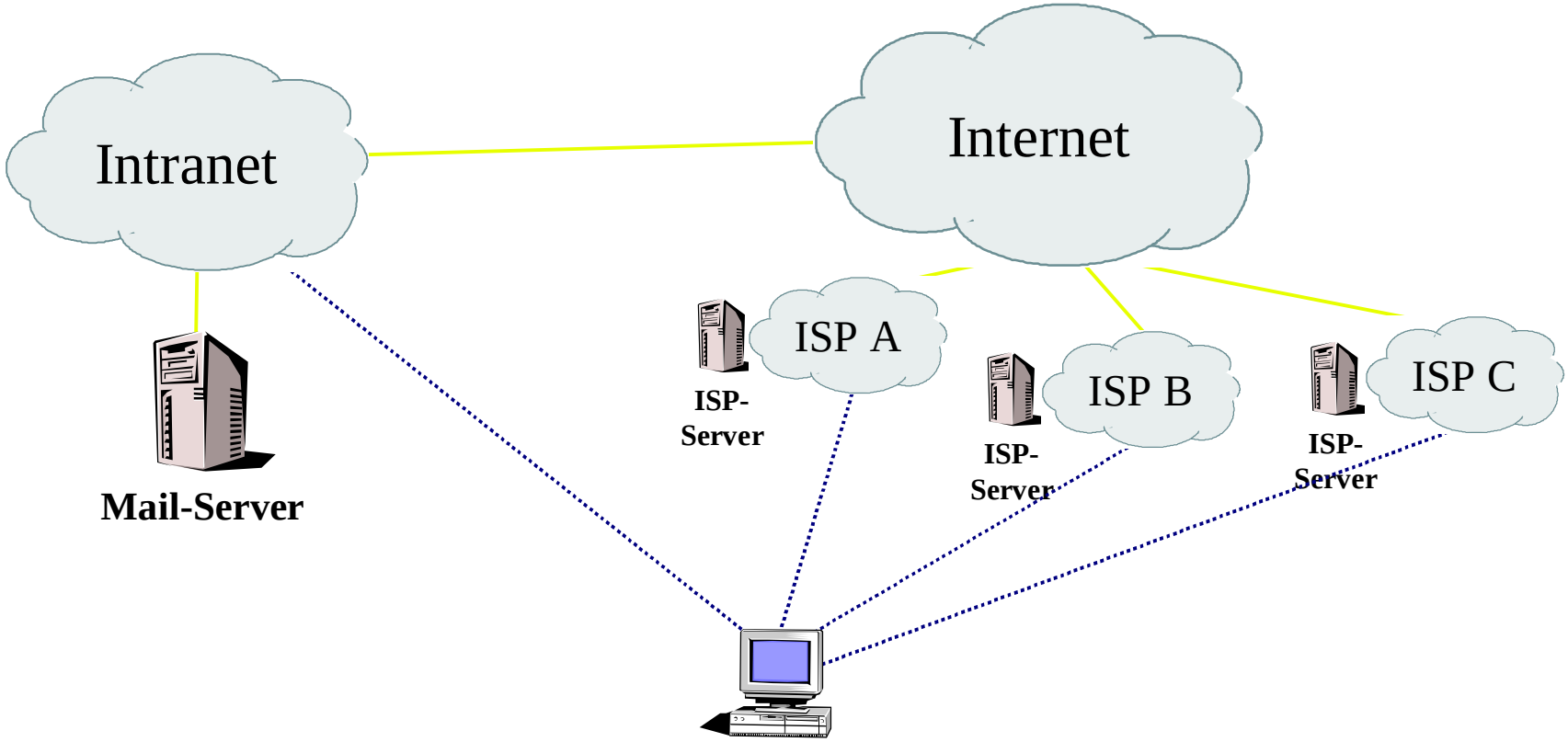
Cyrus

- eigener Daten-Store mit Index

email de'luxe

send mail

Mail von wechselnden Orten (mobil) versenden



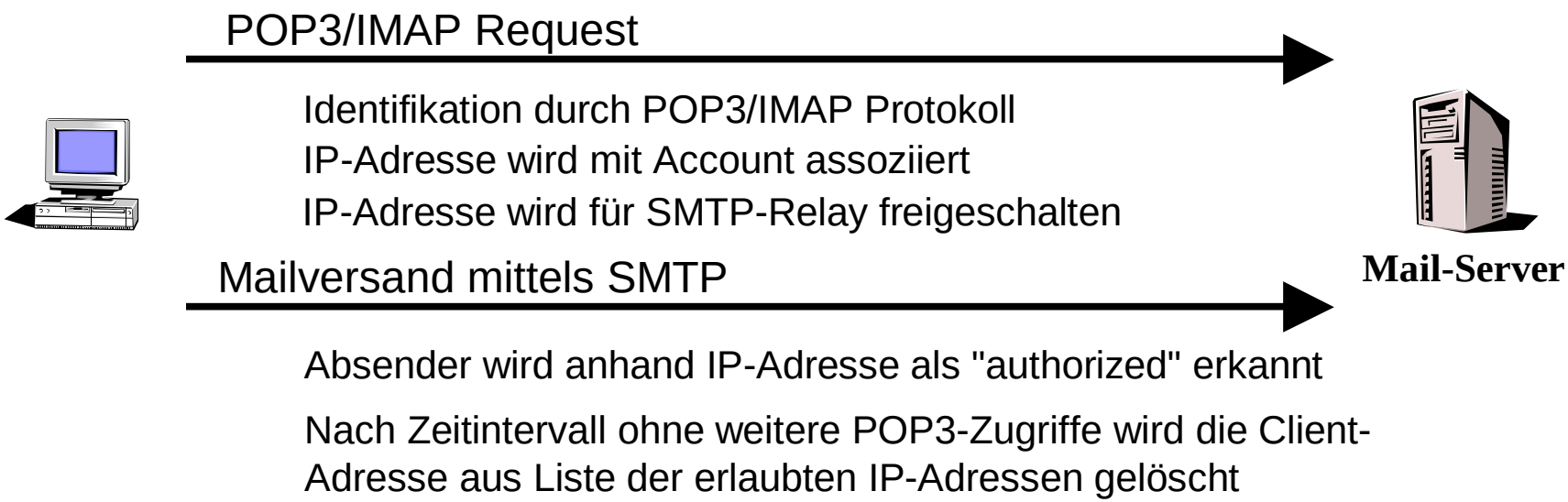
- Relay Restrictions
- Erzwungene Absender-Adressen
- Security

send mail

Versand von Mails über gleichbleibend konfigurierten Mailserver

☞ Identifizierung des Clients nötig um "Relaying" zu erlauben

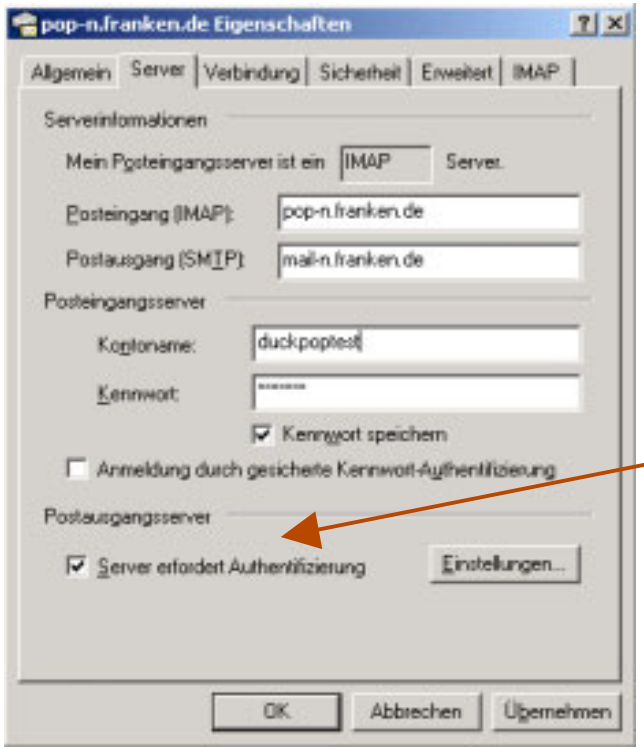
- From: - Adresse ☞ von jedermann Fälschbar
- POP before SMTP (z.B. DRAC "Dynamic Relay Authorization Control")



- Verknüpfung von POP3/IMAP-Server mit SMTP-Server nötig
- SMTP-Server erfährt nicht den genauen Zeitpunkt, zu dem die bisher dem Account zugehörige IP-Adresse an einen neuen User vergeben wird.

send mail

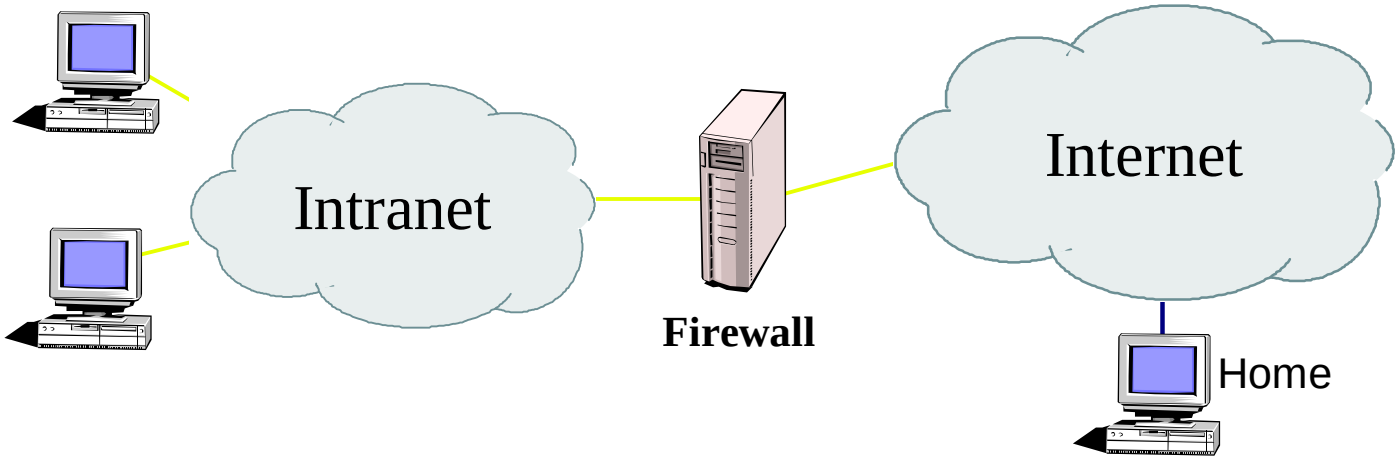
- SMTP AUTH
  - RFC 2554 ("SMTP Service Extension for Authentication") basiert auf SASL
  - Server signalisiert dem Client daß er Authentisierung unterstützen würde
  - Client sendet optional die Identifikationsdaten



SMTP-Auth bei Outlook-Express

Sicherheit

- sicherer Empfang von Mails
- sicherer Versand von Mails

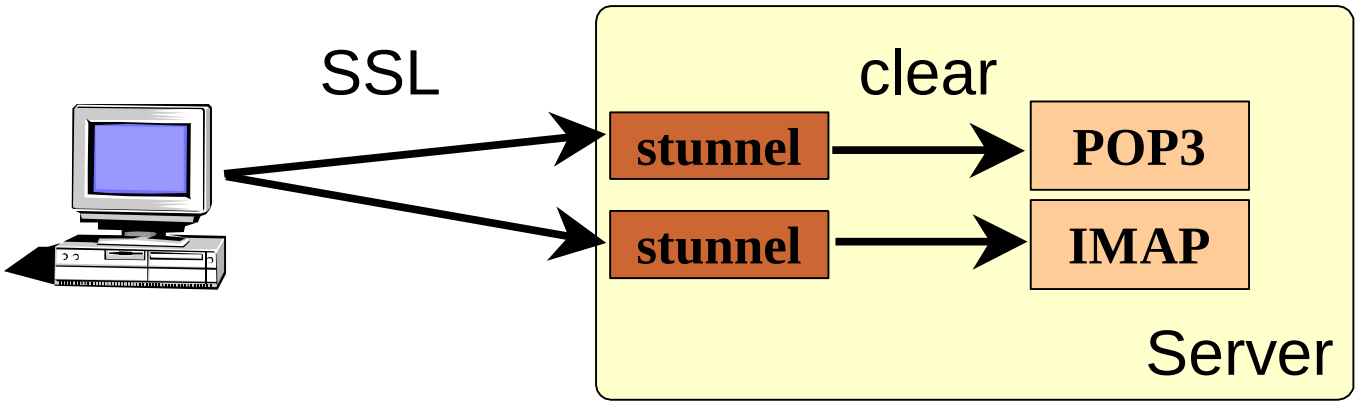


- Bei über das Intranet versandten Mails ist die Firmen-interne Übertragung "sicher".
- Mitarbeiter mit externem Zugang verschicken hingegen über unsicheres Medium

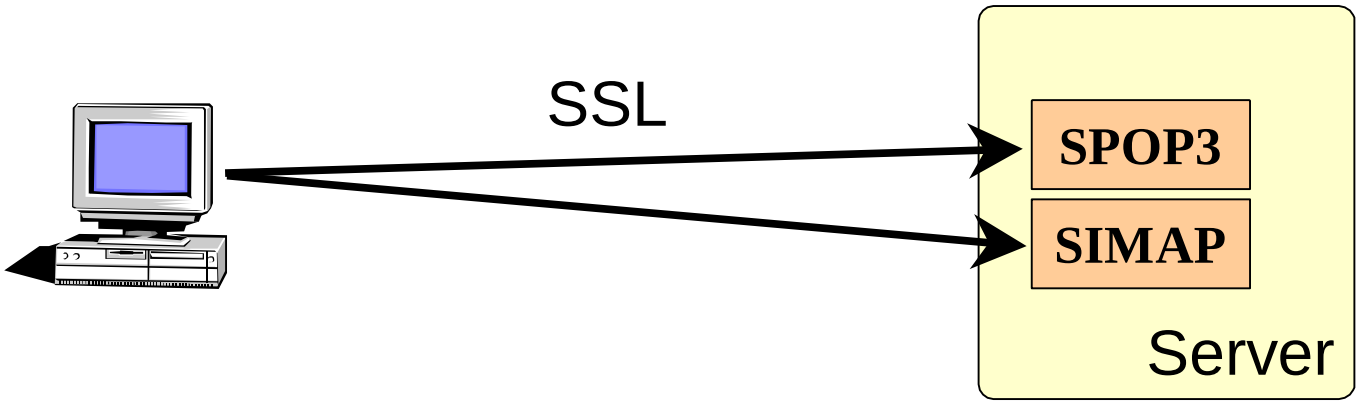
Sicherer Empfang

Mailabruf

- Vorschalten eines SSL-Wrappers



- Integration von SSL in das Server-Programm



Sicheres Versenden

Mailversand via SMTP und TLS

RFC 2487
"SMTP Service Extension for Secure SMTP over TLS"

- Server signalisiert dem Client die Bereitschaft über TLS zu kommunizieren
- Client muß TLS Handshake anfordern
- Verschlüsselung der gesamten Kommunikation zwischen Client und Server

email de'luxe

Sieve

Mailfilterung auf Server für Nutzer

- automatisches Entfernen von nervigen Status-Mails
- selektive Mailweiterleitung
- automatisierte Verteilung von Mails in Ordner

Sieve-Filter

- Aufgrund von
  - From
  - To
  - Subject
  - Größe der Mail
  - beliebige Einträge im Mail-Header

email de'luxe

Sieve

- Ergebnisse von Filtern
  - Ignorieren
  - Zurückweisen
  - Weiterleiten
  - Abspeichern
  - In Ordner abspeichern

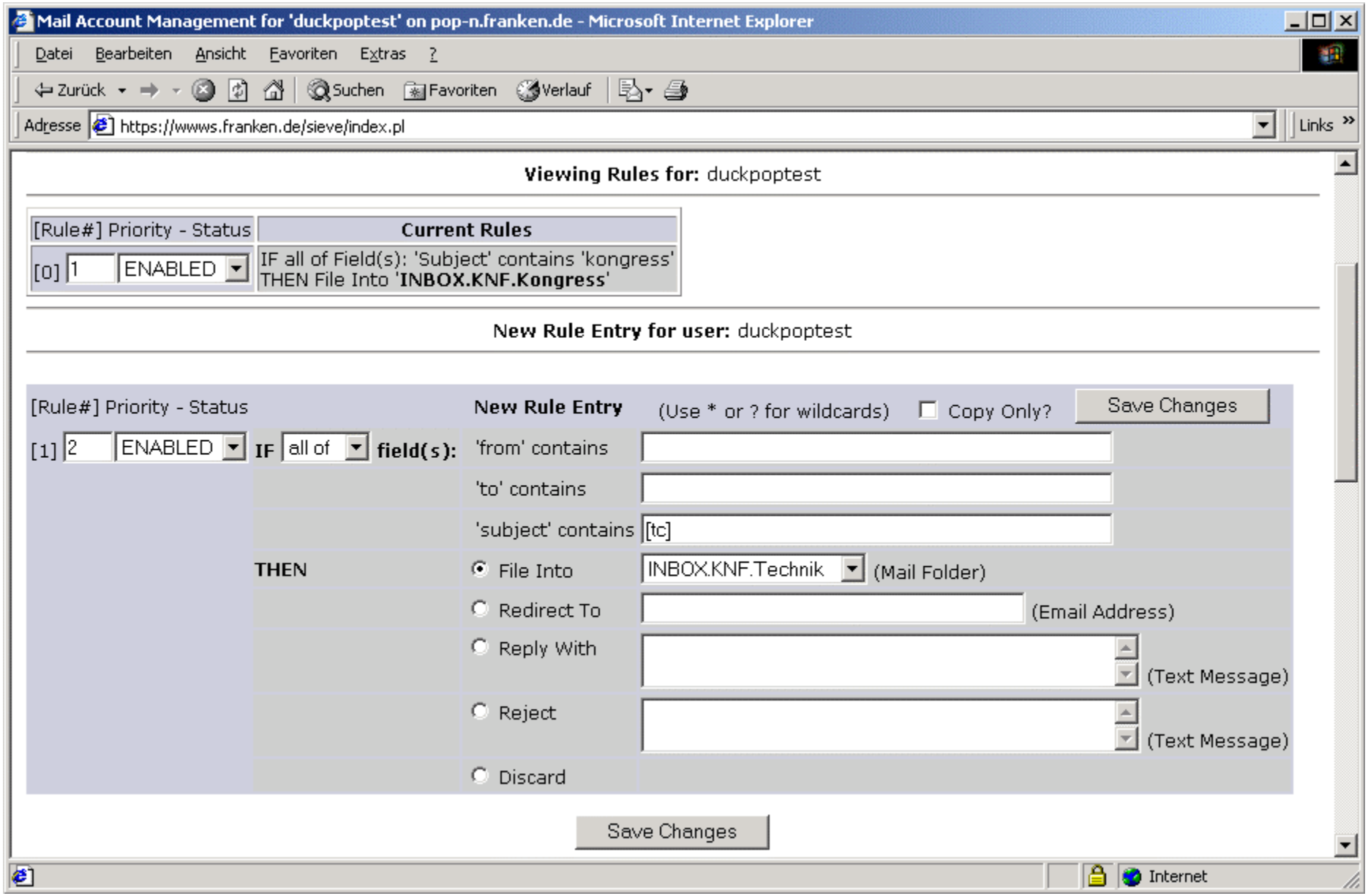
Sieve

Beispiel Sieve-Skript:

```
require ["fileinto"];

if allof (header :contains "subject" "urgent") {
     redirect "joerg@i250.de";
}

if allof (header :contains "subject" "kongress") {
     fileinto "INBOX.KNF.Kongress";
}

elsif allof (header :contains "subject" "[tc]") {
     fileinto "INBOX.KNF.Technik";
}

elsif allof (header :contains "subject" "ADV:") {
     discard ;
}

else {
     keep;
}
```

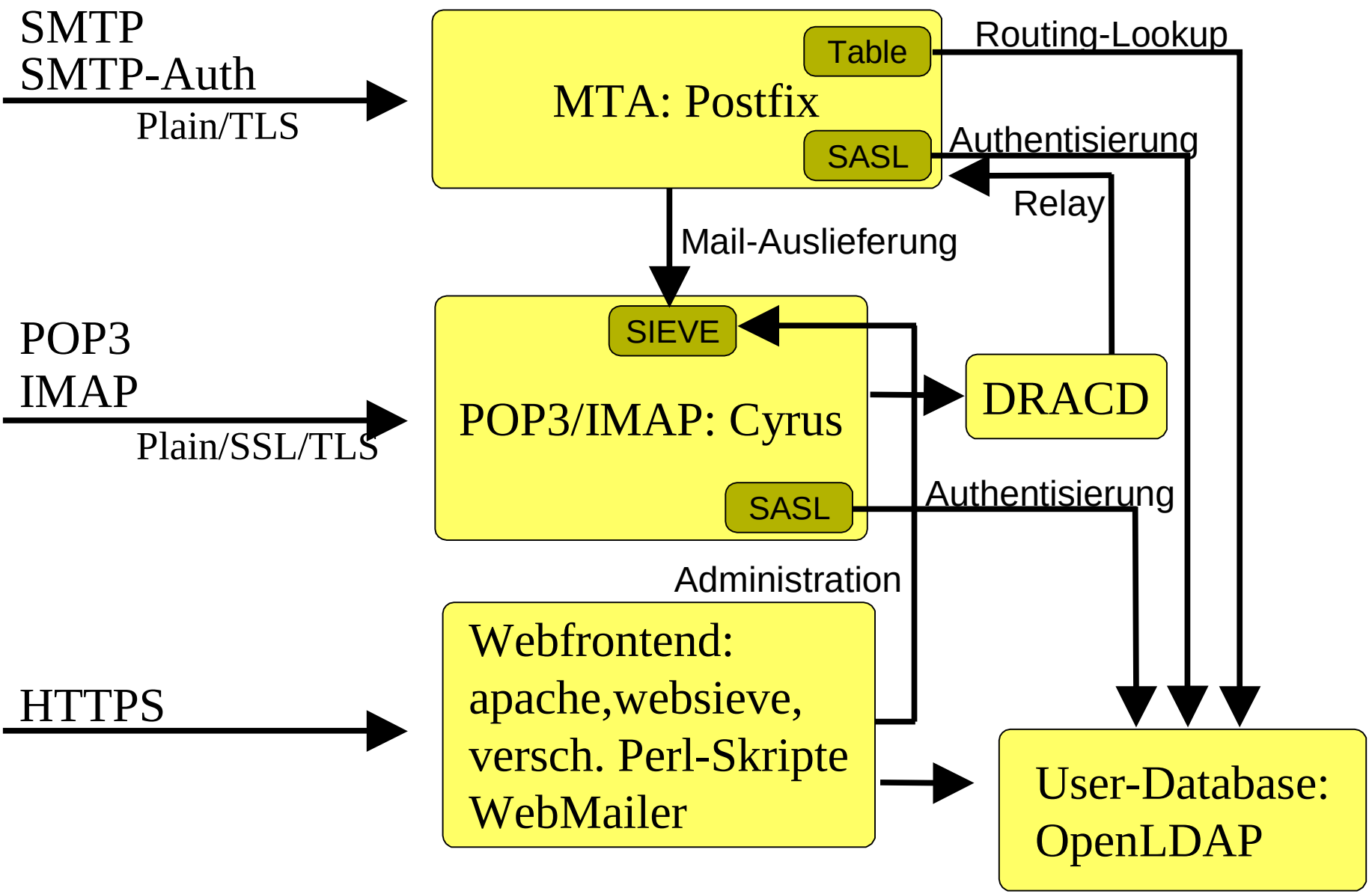
Sieve

Webfrontend zur Verwaltung von Filter-Regeln: WebSieve



email de'luxe

Systemübersicht



email de'luxe

Clients

Clients für Zugriff auf IMAP4-Server via SSL

- Microsoft Outlook Express 5.X
- Netscape Communicator 4.X
- Eudora 5.X
- Mulberry
- Communigate
- Pine
- mutt

email de'luxe

Features

- Mobiler Zugang zu Mail
  - keine Anpassung der Maileinstellungen bei Netz oder Dialup-Providerwechsel
- Sicherer Zugang zu Mail
  - Keine Übertragung von Kenntwörtern im Klartext
  - Sicherheit vor Sniffer beim Abruf von Mails
  - "Interne" Mails auch von außen Sicher einlieferbar
- Archivierung
  - Mailarchiv von überall aus zugreifbar
  - Automatisierte Sortierung in Unterordner

Links

- IMAP Allgemein
  - http://www.imap.org/
- Cyrus
  - http://asg.web.cmu.edu/cyrus/
- Sieve
  - http://www.ietf.org/rfc/rfc3028.txt (Sieve: A Mail Filtering Language)
  - http://www.cyrusoft.com/sieve/
  - http://sourceforge.net/projects/websieve
- Authentication
  - http://mail.cc.umanitoba.ca/drac/ (POP before SMTP)
  - http://www.ietf.org/rfc/rfc2554.txt (SMTP Service Extension for Authentication)
- SSL/TLS
  - http://www.ietf.org/rfc/rfc2246.txt (TLS)
  - http://www.ietf.org/rfc/rfc2487.txt (SMTP Service Extension for Secure SMTP over TLS)
- SASL
  - http://www.ietf.org/rfc/rfc2222.txt (Simple Authentication and Security Layer)
  - http://asg.web.cmu.edu/sasl/

SSL & Cyrus & Sieve

Happy mailing!