

Design und Realisierung von E-Business- und Internet-Anwendungen

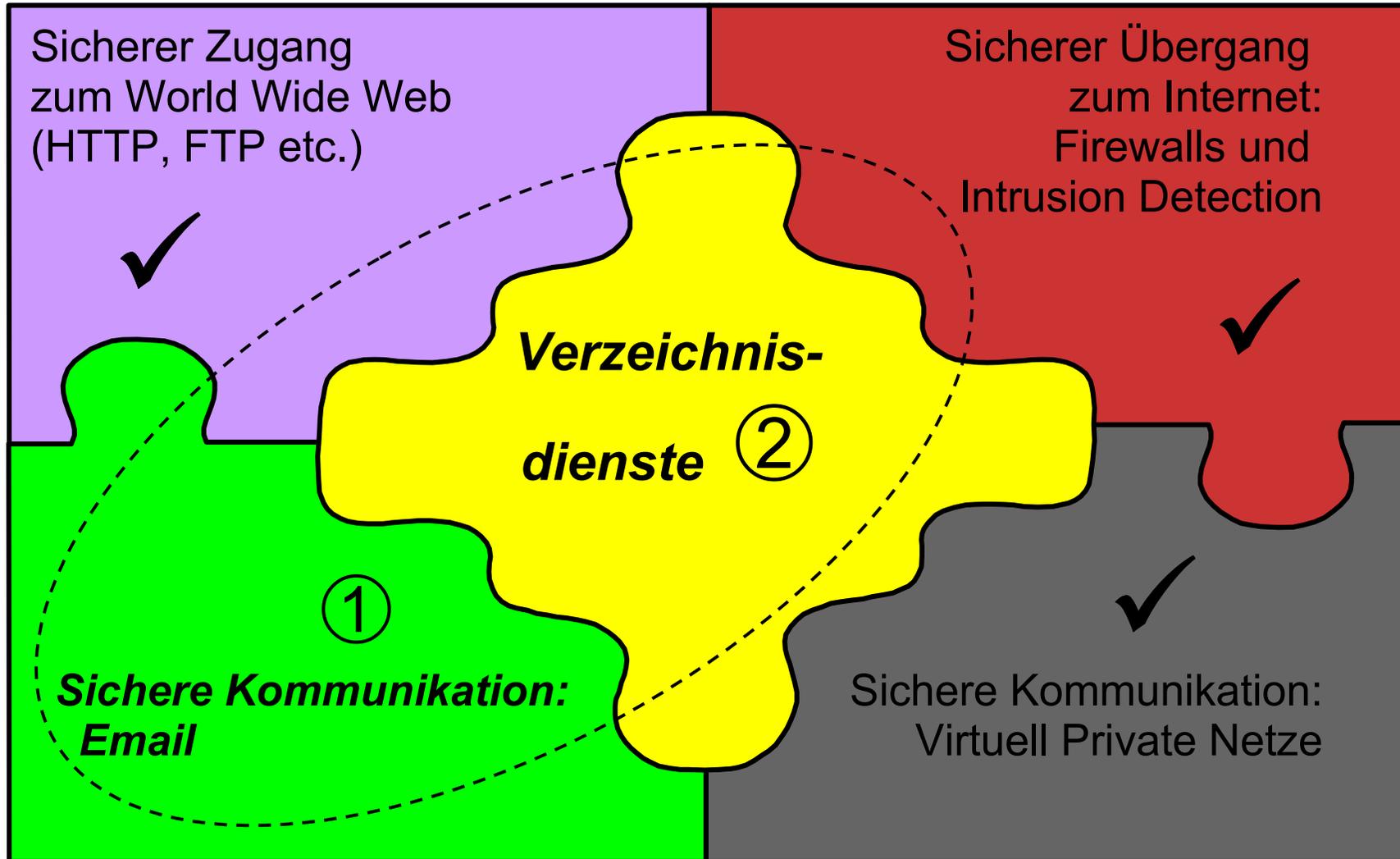
„Email- und Verzeichnisdienste“

Dr. Stephen Heilbronner et al.
Prof. Dr. Heinz-Gerd Hegering

SoSe 2006

Wg. ECTS Credits
bitte ggf. bei
hegering@lrz.de
melden

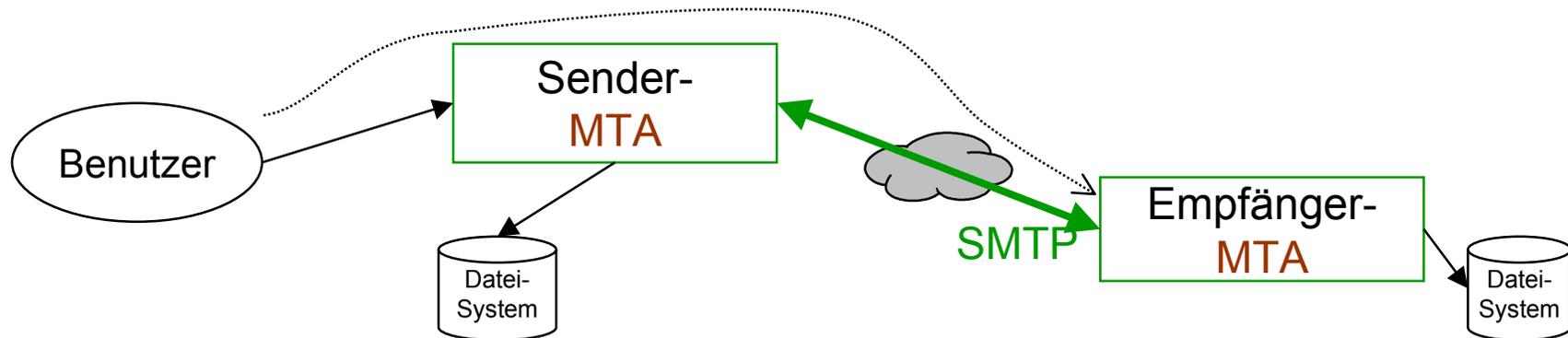
Vorherige Themen aus „Grundlagen“



Email-Relaying

Simple Mail Transfer Protocol (SMTP)

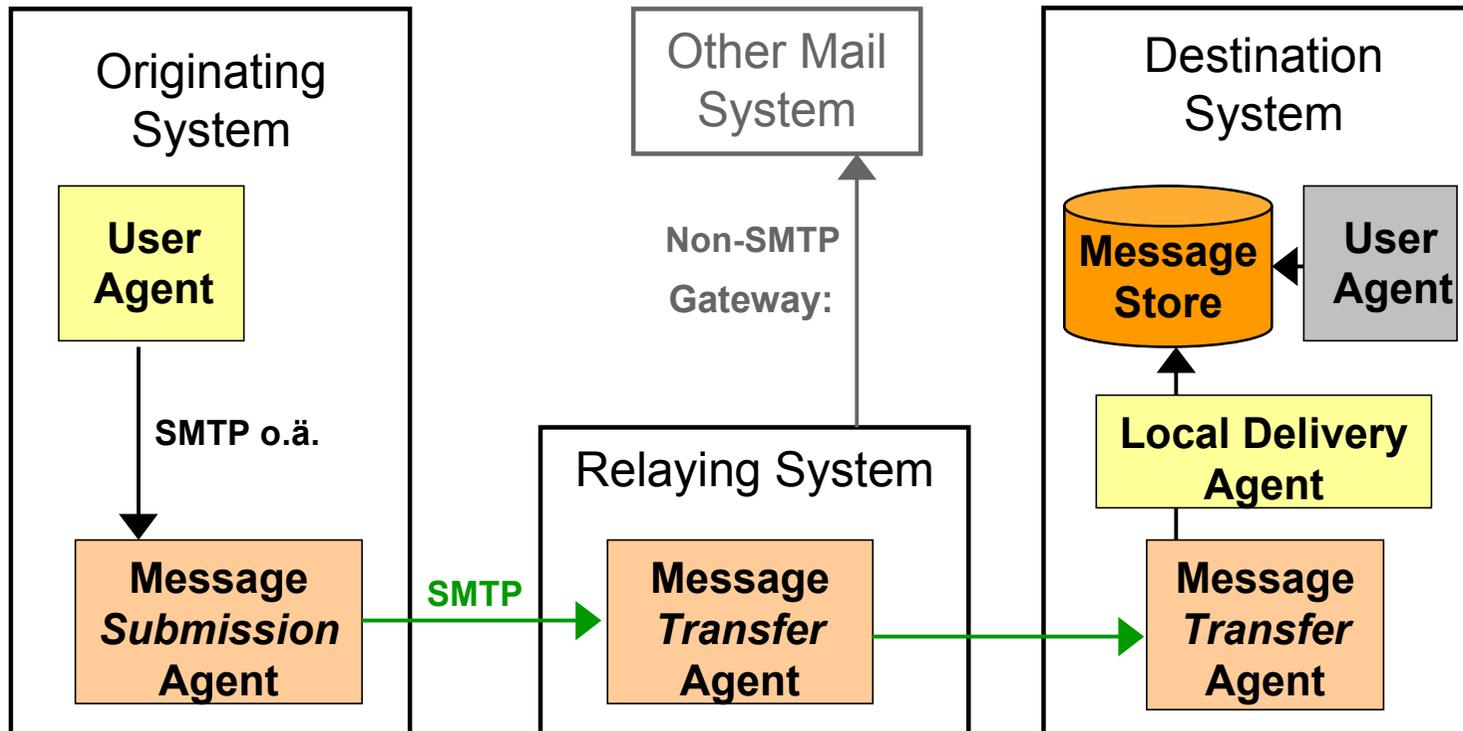
- Standard für den Transport von Email über IP-Netze (IETF RFC 2821/2822)
- Ursprüngliche Grund-Idee (Architektur):



- Neuere Features des SMTP:
 - Sender kann Wünsche über Zustellungsversuche äußern (Fax, SMS)
 - Aushandlung einer Authentifizierung/Verschlüsselung (TLS)

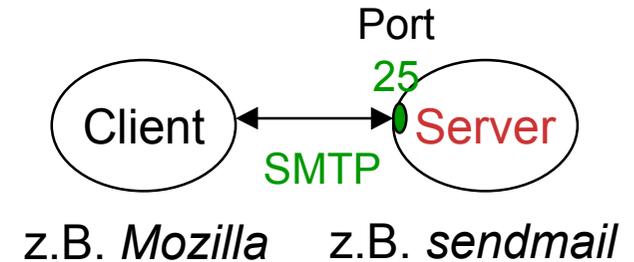
Email-Relaying SMTP: Aktuelle Architektur

- User Agent
- Message Submission Agent
- Message Transfer Agent
- Local Delivery Agent



Dienst: Email-Relaying

SMTP: Protokollablauf



Client aus „wonderland“: Socket => `mailhub.dobbs.com 25`

220 mailhub.dobbs.com **ESMTP Sendmail**

HELO mailout.wonderland.com

250 Hello mailout.wonderland.com[62.156.196.227]

MAIL FROM: <alice@wonderland.com>

250 OK

RCPT TO: <bob@dobbs.com>

250 OK

DATA

354 Start mail input; Keep going; end with <CRLF>.<CRLF>

From: "Alice" <alice@wonderland.com>

To: "Bob" <bob@dobbs.org>

Subject: Have you seen my white rabbit?

Content-Type: text

I'm most concerned. I fear that he may have fallen down a hole.

Alice

.

250 OK - Message accepted

Selber probieren!
„telnet mail-server 25“

Dienst: Email-Relaying

SMTP: Bestimmung des „nächsten“ MTA (Relay)

- Erforderliche Abbildung:
 - Ziel-Domäne → zuständiges Relay bzw. Destination Host
- Implementiert durch:
 - Verzeichnisdienst DNS
 - Lookup des *MX-Record* als spezielle DNS-Anfrage

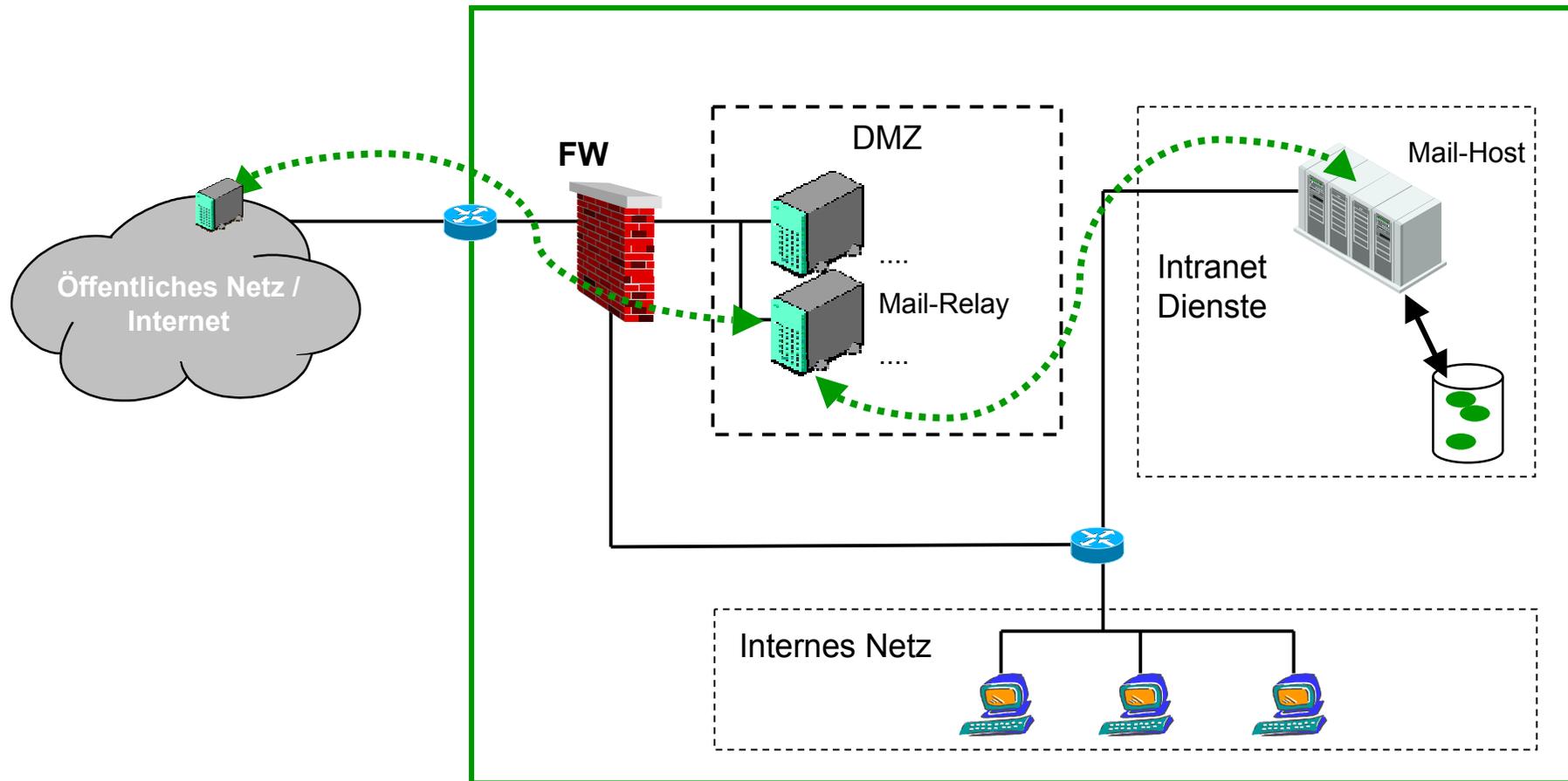
Ziel-Domäne → „Wer ist Mail-Exchange?“

```
~ # dig dobbs.com mx
...
;; ANSWER SECTION:
dobbs.com. 1D IN MX 10 mailhub.dobbs.com.
dobbs.com. 1D IN MX 100 mailrelay1.dobbs.com.
...

;; ADDITIONAL SECTION:
mailhub.dobbs.com. IN A 129.187.214.135
mailrelay1.dobbs.com. IN A 129.187.254.101
...
```

Dienst: Email-Relaying

Email-Relay am Internet-Übergang



Dienst: Email-Relaying

SMTP: Ausfallsicherheit „by Design“

- Mehrfache MX-Records
 - Vorhergehendes Relay probiert nach Prioritäten alle weiteren Relays (MX-Einträge) durch
- Bei Ausfall „Stauung“ auf dem jeweils vorhergehenden Relay

```
mailout:/# mailq
                /var/spool/mqueue (1 request)
----Q-ID----  --Size--  -Q-Time-----  -----Sender/Recipient-----
f4FJg5019876    0      May 15 21:42  heilbron@muclab.de /
                                   stephen.heilbronner@bmw.de
(host map: lookup (t-systems.de): deferred)
```

- Timeout nach mehreren Tagen
(z.B. 5 mit jeweils periodischem Feedback an Absender)

Dienst: Email-Relaying

Email-Relay: Designkriterien

■ Auslegung statisch

- Größe Hintergrundspeicher:
 - Anzahl NICHT-zustellbarer Emails * Größe
 - 100 * 150 KB => 15 MB
- Größe Hauptspeicher: praktisch irrelevant!

■ Auslegung dynamisch

- Prozessorleistung: real immer irrelevant (außer bei GMX 😊)
- (Anzahl/sec) * Größe * Verarbeitungs-Komplexität

Vernachlässigbar,
aber die Zusatzdienste
nicht vergessen

Dienst: Email-Relaying

4 typische Angriffsszenarien auf sichere Email

- Unerwünschte Inhalte (Content Filtering)
 - Viren etc.
- Anti-Relaying / Anti-Spamming
 - Email von unerwünschten Absendern
- Anti-Spoofing
 - Email mit vorgetäuschten Absendern
- Abhören
 - Verschlüsselung

Dienst: Email-Relaying

Exkurs: Email-Policy !

- Rechtslage für private Email-Nutzung in betrieblichem Umfeld ist komplex
- Aufstellung einer betrieblichen Email-Policy unbedingt erforderlich:
 - Verbot privater Nutzung oder nicht ?
 - „Content-Scanning“ erlaubt oder nicht
 - Behandlung von „problematischer“ Email:
 - Warnung an Empfänger/Absender
 - CC: an Postmaster ?
 - Modifikation der Email
 - Verschieben in Quarantäne-Bereich bis auf Weiteres
- Getroffene Maßnahmen sollten immer mit BR vereinbart sein, ankündigt und dokumentiert werden.

Dienst: Email-Relaying

Sicherheit: Content Filtering

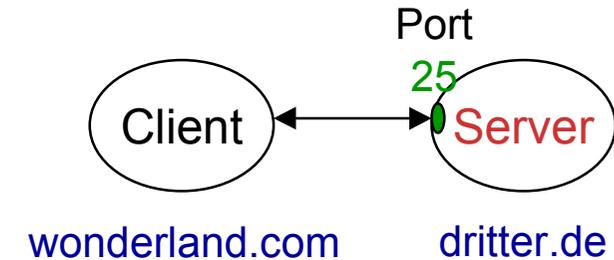
- Prinzip:
 - Bestimmung des Attachment-Typs
 - Mustererkennung in Attachment-Inhalten

- Behandlung erkannter Viren
 - Kennzeichnung des Attachments
 - Löschen des Attachments
 - Email in „Quarantäne“-Bereich verschieben
 - Benachrichtigung interner Absender bzw. Empfänger

- CC an Administrator problematisch (siehe oben)...

Dienst: Email-Relaying

Sicherheit: Anti-Relaying



■ Erkennung

- Absender und Empfänger gehören nicht zum „Einzugsbereich“ des Relays

```
# telnet mailhub.dritter.de 25
R: 220 mailhub.dritter.de ESMTP Sendmail
S: HELO mail.wonderland.com
R: 250 Hello mail.wonderland.com [62.157.196.227]
S: MAIL FROM:<alice@wonderland.com>
R: 250 OK
S: RCPT TO:<bob@dobbs.com>
R: 550 bob@dobbs.com... Relaying denied
S: QUIT
R: 221 mailhub.dritter.de closing connection
```

■ Behandlung

- Ablehnung
- oder: Verzögerung („Spam-Trap“) !!

Dienst: Email-Relaying

Sicherheit: Anti-Spamming

- Unsolicited Bulk Email (UBE) / Unsolicited Commercial Email
 - Massenhaft versandte, vom Empfänger „unerwartete“ Email

- Teilweise verhindert durch
 - *Anti-Relaying* => keine Weiterleitung an Dritte
 - *Anti-Spamming* => keine Annahme aus „typischen Spam-Quellen“ (Spam-Domains)
 - DNS-basiertes System für derartige Infos: *mail-abuse.org*
 - 1.) MTA befragt DNS nach Informationen:
 - www.cyberspam.com.db.mail-abuse.org ?
 - 127.0.0.2.db.mail-abuse.org ?
 - 2.) Antwort bestimmt dann Verhalten des MTA

Dienst: Email-Relaying

Sicherheit: Anti-Spoofing

- Vortäuschen eines (internen) Absenders
- Maßnahmen

- Überprüfung der Absender auf „Sinnhaftigkeit“
- kryptologisch sichere Authentisierung

```
# telnet mailhub.dobbs.com 25
R: 220 mailhub.dobbs.com ESMTP Sendmail
S: HELO xyz.irgendwas.de
R: 250 Hello xyz.irgendwas.de [62.157.196.227]
S: MAIL FROM:<alice@dobbs.com>
R: 250 OK
S: RCPT TO:<bob@dobbs.com>
R: 250 Rcpt OK
S: DATA
R: 354 Enter mail, go ahead
S: From: Susan <susan@dobbs.com>
S: To: Bob <bob@dobbs.com>
S:
S: I think you should be fired!
S: .
R: 250 2.0.0 Message accepted for delivery
S: QUIT
R: 221 mailhub.dritter.de closing connection
```

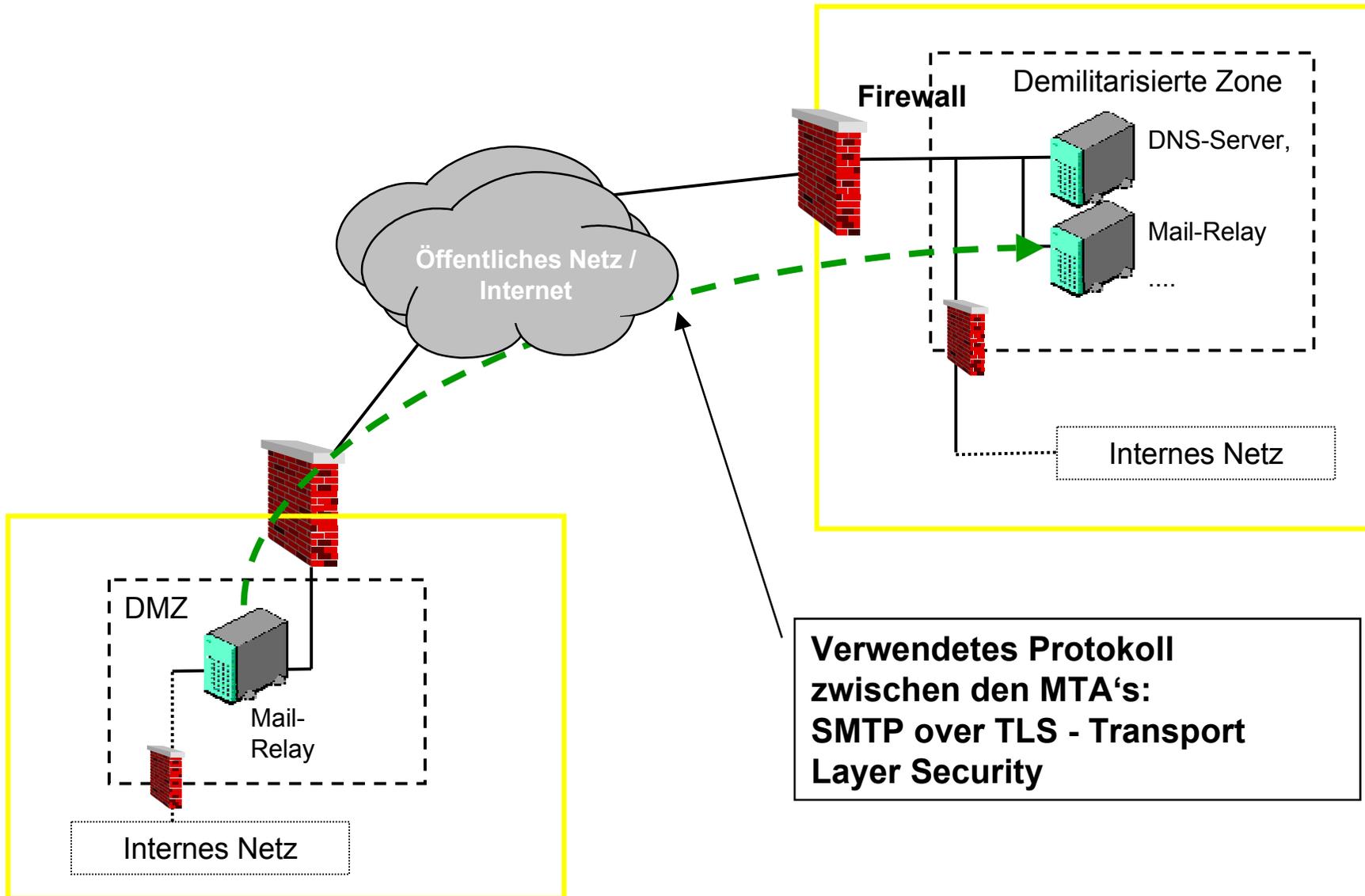
Dienst: Email-Relaying

Sicherheit: Verschlüsselung (1)

- Ende-zu-Ende Verschlüsselung von Email verfügbar, z.B.:
 - PGP
 - S/MIME
- Warum wird sie praktisch kaum eingesetzt ?
 - Authentifizierung unsicher
 - Problem: Zertifikatsverteilung (Public-Key-Infrastruktur) ...
- Probleme der Ende-zu-Ende-Verschlüsselung
 - Software „kompliziert“, Nutzen/Schaden für „normalen“ User nicht erkennbar
 - Analyse der Inhalte (Viren!) dann komplex/unmöglich...
 - Archivierung der Unternehmens-Email (Key-Escrow) komplex
- Was braucht ein Unternehmen zumindest ?
 - Verschlüsselung/Authentifizierung eigentlich nur bei angreifbaren Strecken notwendig (d.h. beim Transfer übers Internet)

Dienst: Email-Relaying

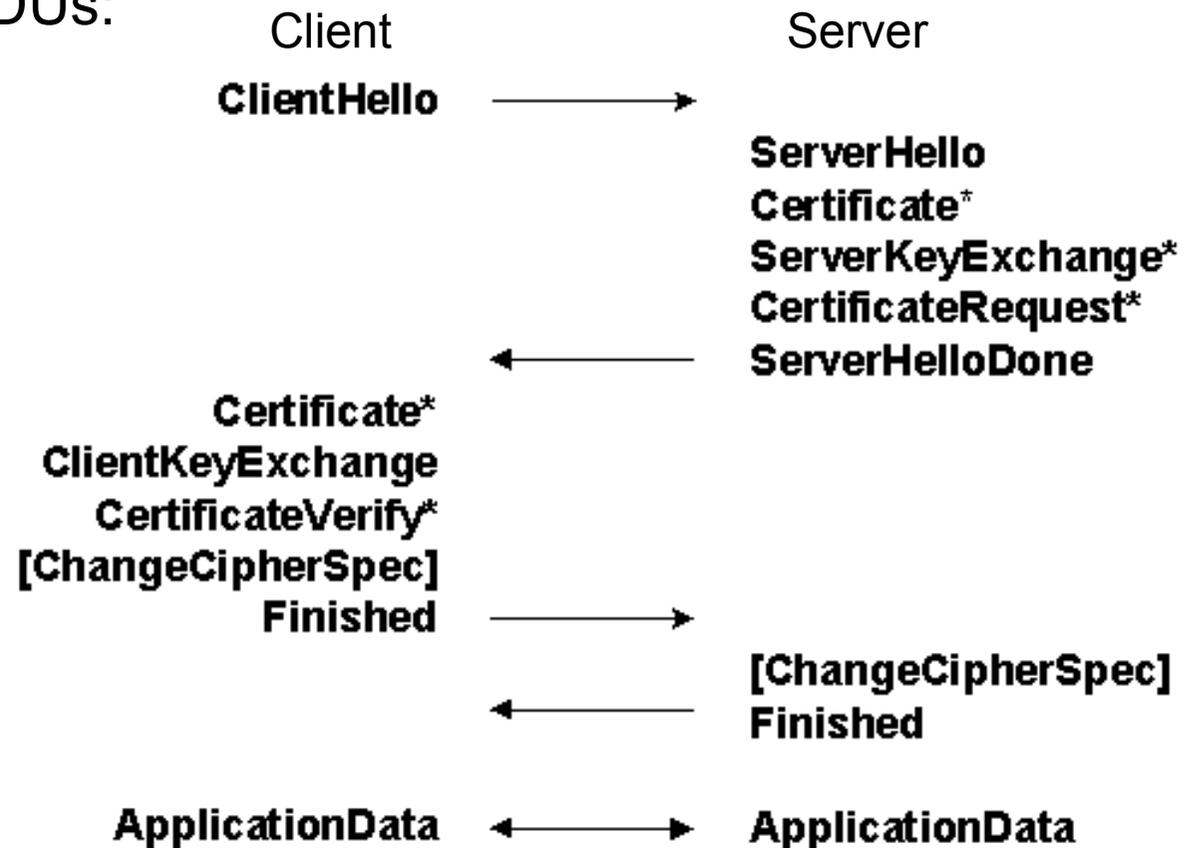
Email: Abschnittsweise Verschlüsselung



Dienst: Email-Relaying

Exkurs: Transport Layer Security (TLS)

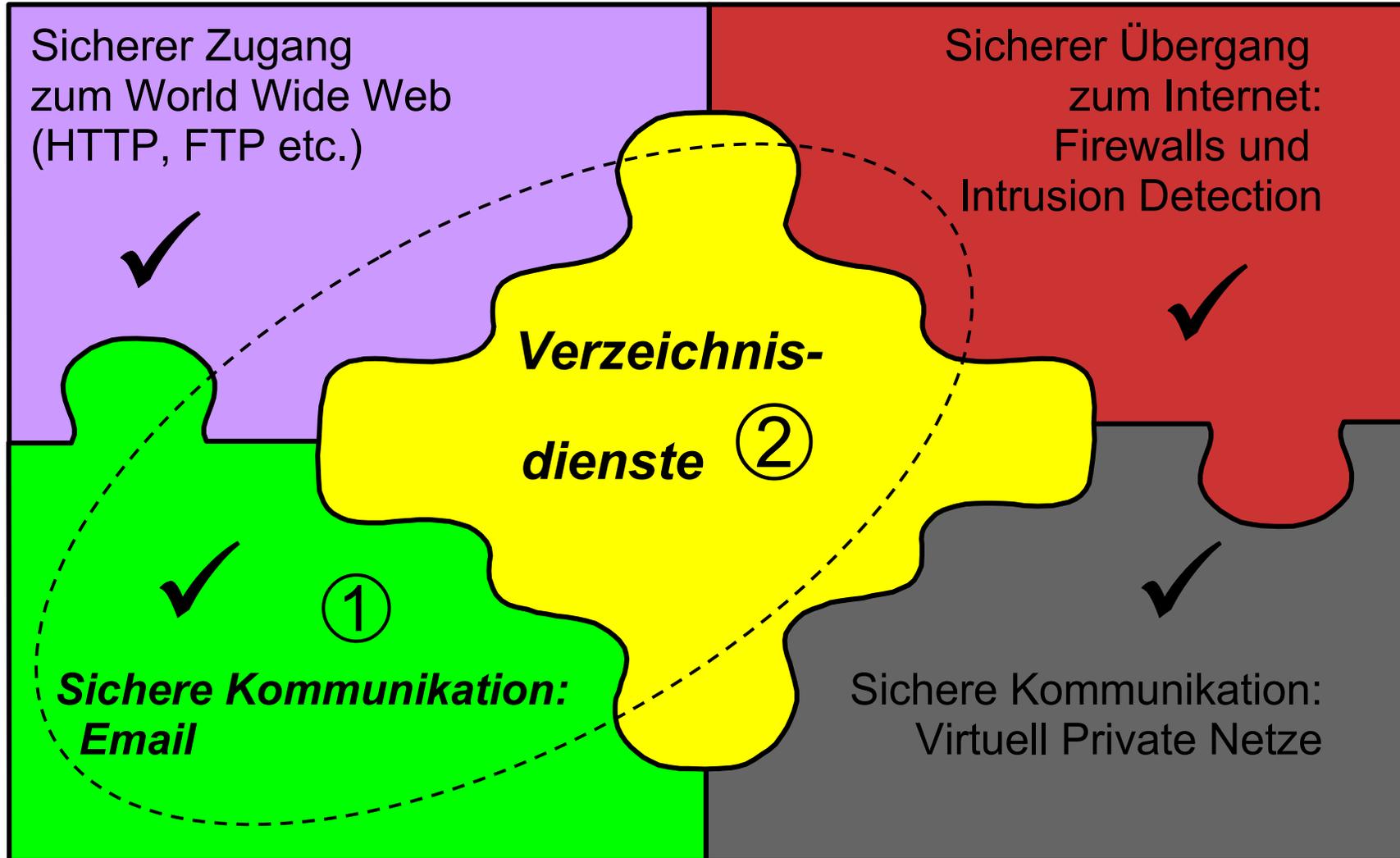
- Verschieden einsetzbar (z.B. für SMTP, HTTP, IMAP)
- Standard nach RFC 2246
- Ausgetauschte PDUs:



Dienst: Email-Relaying

Ende

Vorherige Themen aus „Grundlagen“



Dienst: Verzeichnis Einsatzgebiete

- A Directory is like a database...
 - you can put information in, and later retrieve it.
...but it is *specialized*. Some typical characteristics are...
 - designed for **reading** more than writing
 - offers a **static view** of the data
 - simple **updates** without transactions

- Netz (Schicht 3) - Endsysteme
 - Bestimmung von Eigenschaften / Lokalisierung
 - Domain Name *System* (DNS)

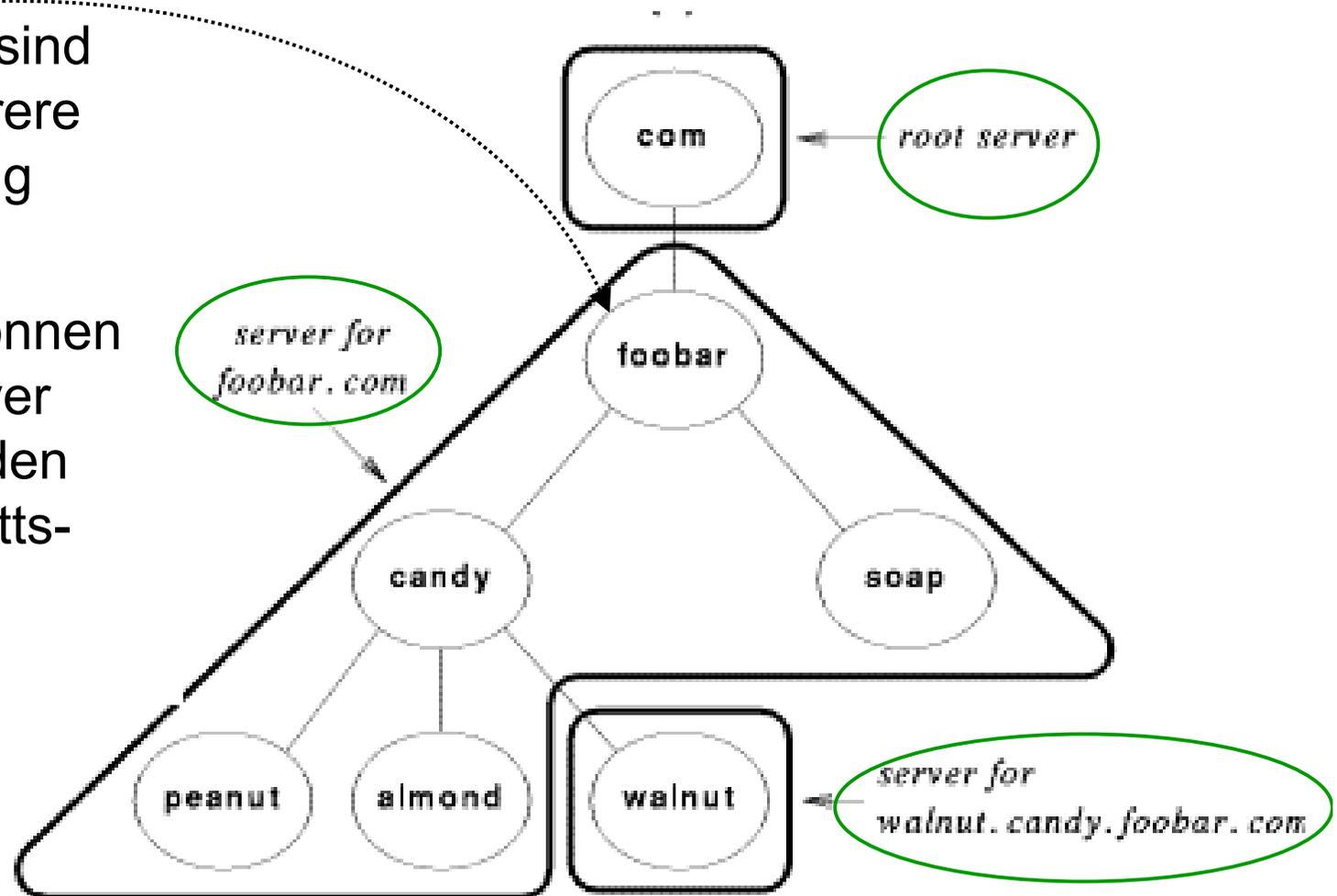
- Anwendung (Schicht 7)
 - Verwaltung von Objekteigenschaften
 - Lightweight Directory Access Protocol (LDAP)

Dienst: Verzeichnis

DNS: Architektur

- **DNS-Server** sind für 1 oder mehrere Zonen zuständig

- Subzonen können an andere Server „delegiert“ werden (auch ausschnittsweise)



Dienst: Verzeichnis DNS-Operationen

- Durchführung verschiedener „Abbildungen“
 - Name → IP-Adresse (A)
 - IP-Adresse → Name (PTR)
 - Name → Mailhost (MX)
 - Zone → Zoneninformation (SOA)
 - Name → Textuelle Information (TXT)
 - Zone → Public Key (KEY)
- Auflistung von Zonen und Einträgen
 - meist nur an explizit autorisierte Systeme zugelassen
- Aktualisierung von Einträgen (Dynamic DNS)
 - Unterstützung Systeme mit wechselnden IP-Adressen, z.B. mobile Systeme

Dienst: Verzeichnis

DNS: Betriebsaspekte

- Basis-Element der Internet-Infrastruktur
 - Hohe Verfügbarkeit
 - Schneller Zugriff
- Verbesserung durch
 - Caching Server
 - Cache für bereits abgefragte Information bis zu einem Timeout
 - Secondary Server
 - ebenfalls zuständig für eine Zone
 - befragt regelmäßig den Primary Server nach neuer Information, oder
 - nach einem NOTIFY

Dienst: Verzeichnis

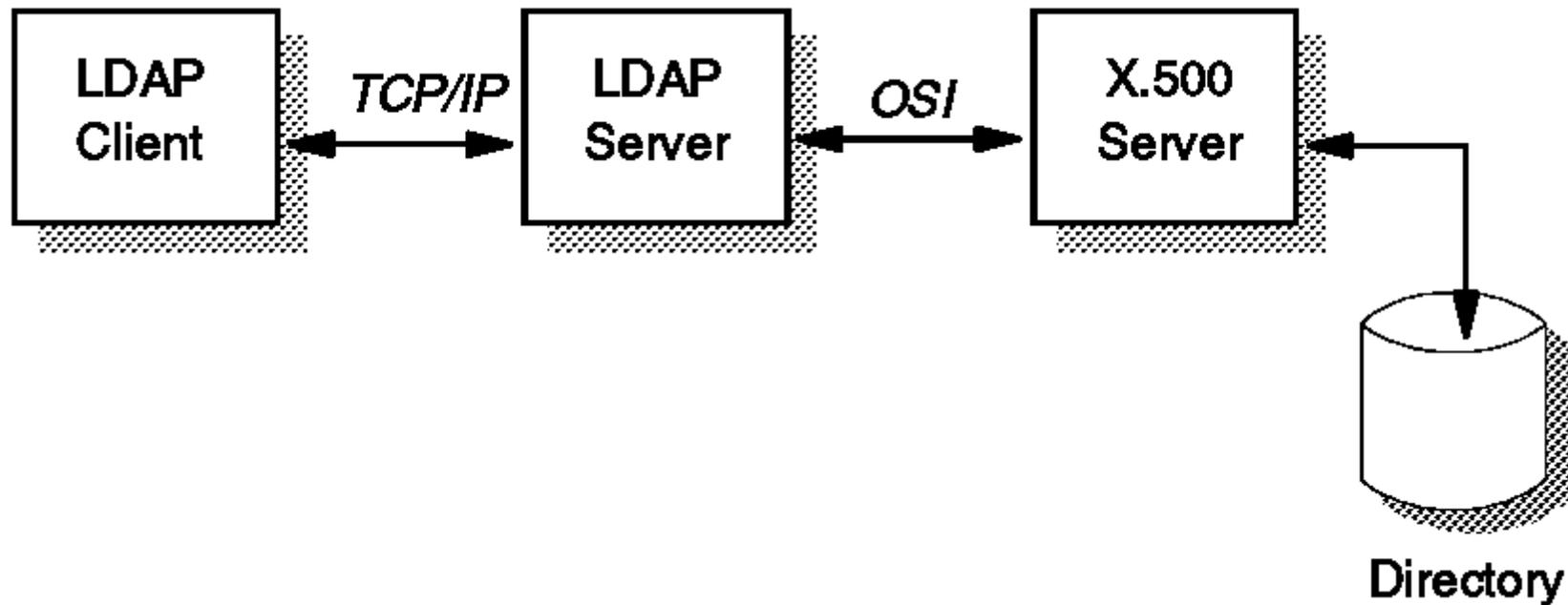
Lightweight Directory Access Protocol (LDAP)

- Kommunikationsprotokoll für komplexere Verzeichnisse
- Informationsmodell für Syntax und (teilweise) Semantik der gespeicherten Information
- Strukturierung der Information durch Namensräume
- im Entstehen: ein **verteiltes** Betriebsmodell zur Beschreibung und Referenzierung der Daten
- Protokoll und Informationsmodell sind erweiterbar
- aber nicht:
 - Speichermodell
 - Programmierschnittstelle (anderer Standard...)
 - Implementierungsbeschreibung

Dienst: Verzeichnis

LDAP-Architektur

- Abgeleitet auf dem OSI-Standard X.500
- Vereinfachtes Zugriffsprotokoll für Clients



Dienst: Verzeichnis

LDAP - Zugriff und Operationen

- Transportprotokoll: TCP
- Verbindungsaufbau
 - authentifiziert oder anonym
 - eventuell verschlüsselt
- Verzeichnisoperationen:
 - Search: Und-verknüpfte Bedingungen auf Verzeichnisausschnitt
 - Read: ein Eintrag,
 - Add, Update, Move, Compare
- Informationsmodell (entspricht X.501)
 - Das Verzeichnis (Directory Information Tree - DIT) ist ein Baum
 - Eintrag identifiziert durch *Distinguished Name* (DN):
 - Sequenz von RDNs, wie in typischen Dateisystemen ...

Dienst: Verzeichnis

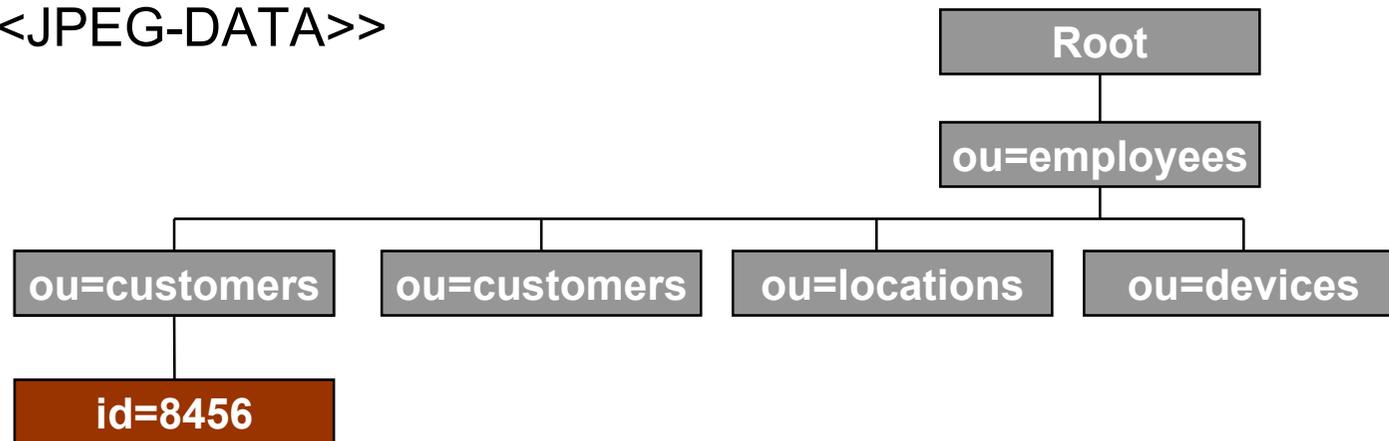
LDAP - Informationsmodell

■ Entry (Eintrag):

cn: Robert Seagal
cn: Bob Seagal
nr: 8456
mail: bob@dobbs.com
telephoneNumber: 54754-369
telephoneNumber: 54754-484
roomNumber: 3996
picture: <<JPEG-DATA>>

■ Distinguished Name:

id=8456
ou=employees



Dienst: Verzeichnis

LDAP: Wozu wird es verwendet?

- Benutzer authentifizieren
 - Speicherung von Passwort-Information (gesichert durch Einwegverschlüsselung)
- Benutzer autorisieren
 - Anwendungsspezifische Rechte im Verzeichnis speichern
 - „Wer darf wohin surfen?“
- Verteilte Aktualisierung
 - Jeder Eintrag/Baumabschnitt kann eigene Zugriffsrechte haben
- Physische Ressourcen verwalten
 - IT-Managementsysteme (z.B. Element Manager) können Informationen über Switches, Hubs und Firewalls zugriffsgesichert bereitstellen

Das wärs für heute ...

- Auch die Folien von heute kommen auf die Web-Seite der Vorlesung
- Ende der Grundlagen
- Wie geht's weiter ?

Virtuell private Netze

auf der Basis standardisierter Protokolle

- Für (fast) Alles:
IBM Red Book: *“TCP/IP Tutorial and Technical Overview“*
 - <http://publib.boulder.ibm.com:/cgi-bin/bookmgr/bookmgr.cmd/BOOKS/EZ306201>
- LDAP
 - <http://www.Idapman.org/>
- IMAP
 - <http://www.washington.edu/imap/>