TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik | Institut Systemarchitektur | Professur Rechnernetze

WS 2016/2017
LV Rechnernetzpraxis

10. Verzeichnisdienste
(Directory Services)

Dr. rer.nat. D. Gütter

Mail: Dietbert.Guetter@tu-dresden.de
WWW: http://www.guetter-web.de/education/rnp.htm

10.01.2017

Verzeichnisdienste - Beispiele

OSI **X.500**, ursprünglich ITU-Empfehlung (CCITT)

- Standardisierter, weltweiter Verzeichnisdienst
- X.500 … X.518: Informationsmodell, Dienstbeschreibung, Protokolle, …
- X.509: Sicherheitsaspekte

LDAP (Lightweight Directory Access Protocol)

- vereinfachte Variante des X.500 Directory Access Protocol (DAP)
  Realisierung über TCP/IP
- DeFacto-Standard für Zugriff auf Verzeichnisdienste

UDDI (Universal Description, Discovery an Integration)

- Verzeichnisdienst für Web Services

DNS (Domain Name System)

- Verzeichnisdienst des Internet

Verzeichnisdienste - Definition

Reale Objekte

Personen, Organisationen, Rechner, Prozesse, Dateisysteme, Mailboxen etc.

Logische Objekte

Interessierende Informationen hierzu, gespeichert als Einträge

Namen

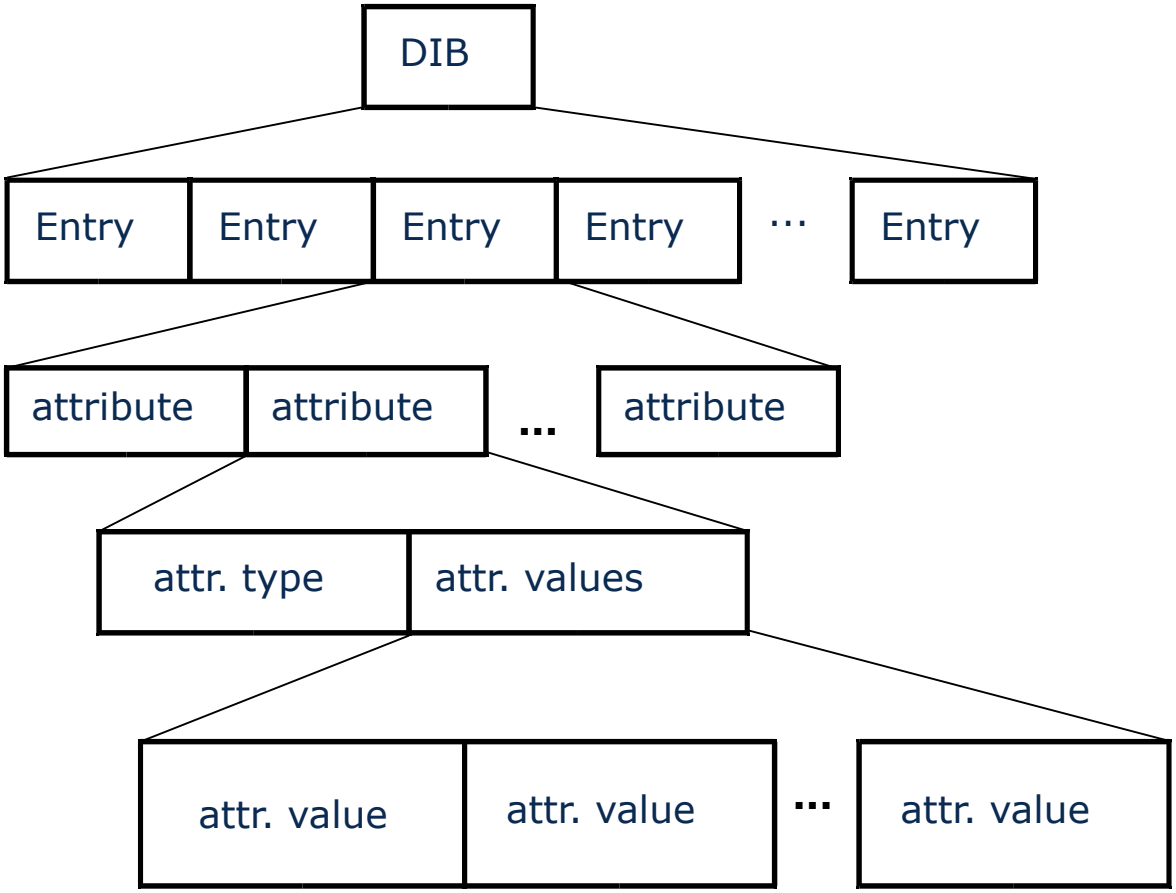
Benutzerfreundliche, systemunabhängige Bezeichner für Objekte,
lange Gültigkeitsdauer

Adressen

Objektbezeichner mit Lokationsangabe, ungeeignet für menschliche Benutzer
Änderungen unterworfen, topologieabhängig
(Beispiel: Internet-IP-Adressen)

⇒**Verzeichnisdienst:**
Zuordnung von Attributen zu einem Objekt,
z.B. Adresse zu einem Computer

DIB - Directory Information Base



DIT - Directory Information Tree

Speicherung der Einträge als Baumknoten

- Wurzelknoten ohne Elternknoten
- alle anderen Knoten haben genau 1 Elternknoten
- Knoten haben 0 bis n Kindknoten
- Jeder Knoten hat einen eindeutigen Namen

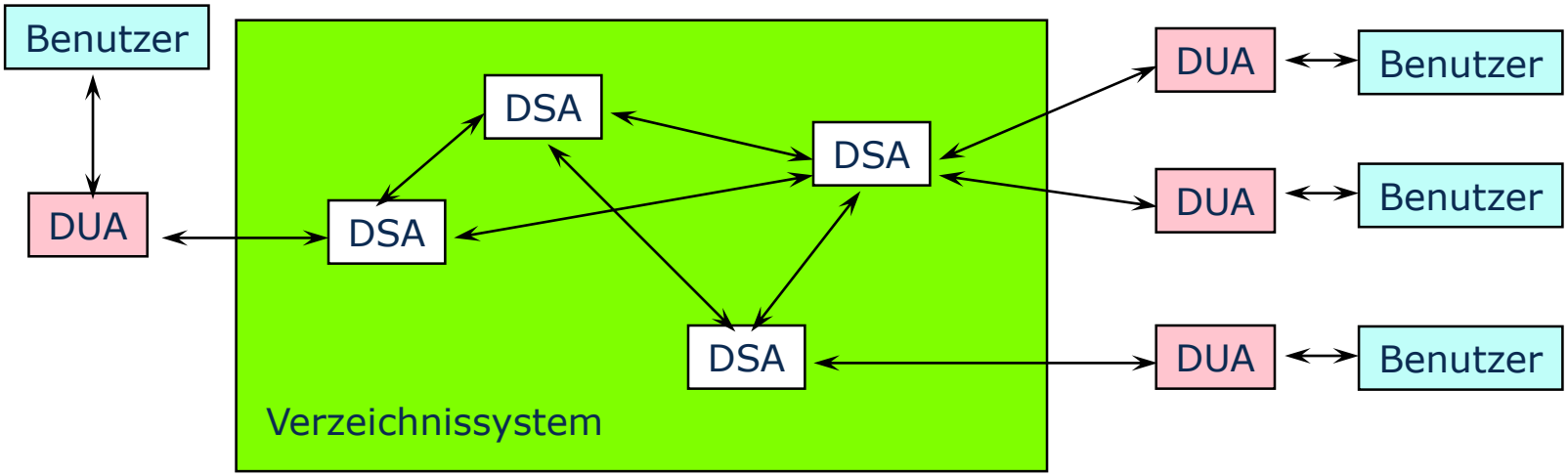
  RDN (Relative Distinguished Name)
  DN (Distinguished Name)

- Beschreibung der Attribute durch Klassen
- Vererbung

  Übernehmen/Ergänzen von Attributen
  bei Definition spezialisierter Klassen

X.500 Verteilte Architektur

DUA Directory User Agent
DSA Directory System Agent, Server von X.500



Informationstypen

- Originator (Initiator einer Anfrage)
- Operation Progress (Anfrage nach Operationsfortschritt)
- Trace Information (Weg eines Auftrages)

X. 500 Directory Service

Abfrageoperationen

- Yellow Pages Attribute => Namen, z.B: Firmenart => Firma_X
- White Pages Namen => Attribute, z.B. Firma_X => Adresse)

Änderungsoperationen

- Hinzufügen und Entfernen von Einträgen
- Verwaltung des Verzeichnisses

Verteilte Realisierung, Verteilung des großen Datenvolumens

- hohe Lokalität der Zugriffe
- optional auch Replikation => schnellere Verfügbarkeit

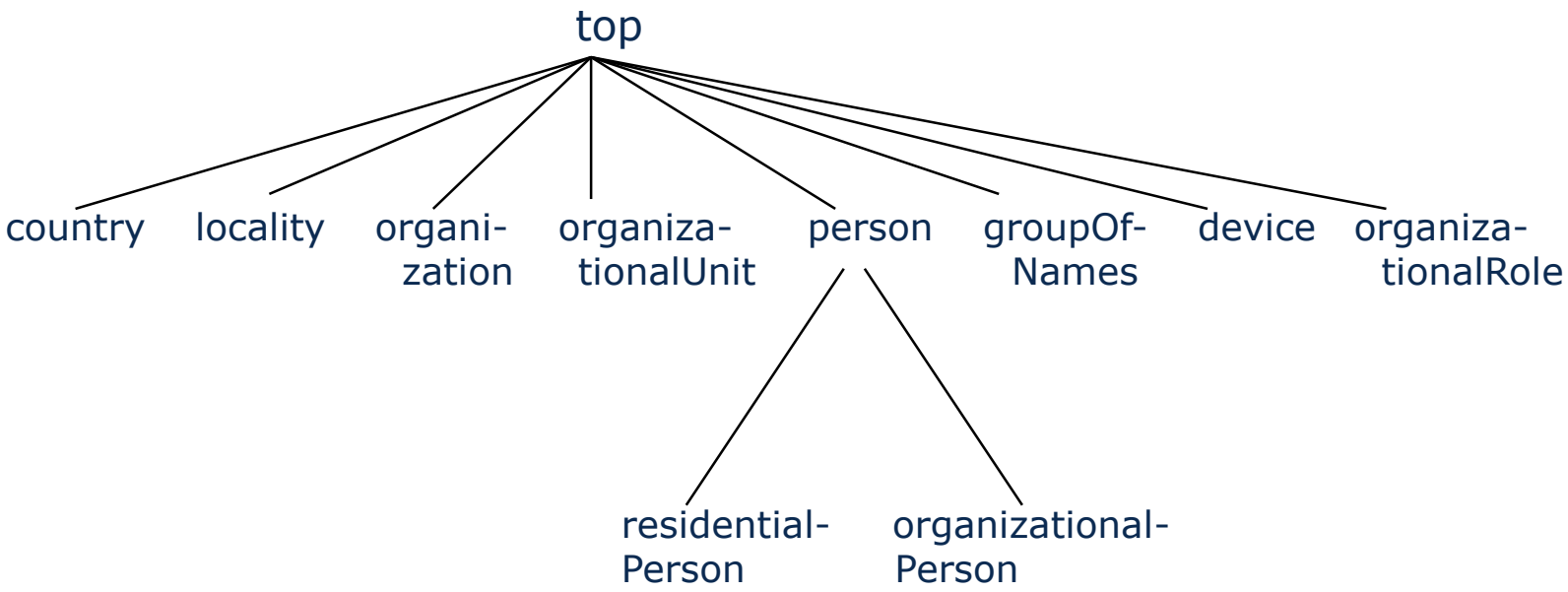
- keine ständige Konsistenz (z.B. bei Replikaten),
  sondern Konvergenz zu konsistentem Zustand (ggf. mit oberer Zeitschranke)

Eingliederung existierender Daten (z.B. aus einer separaten Datenbank)

X. 500 Objektklassen

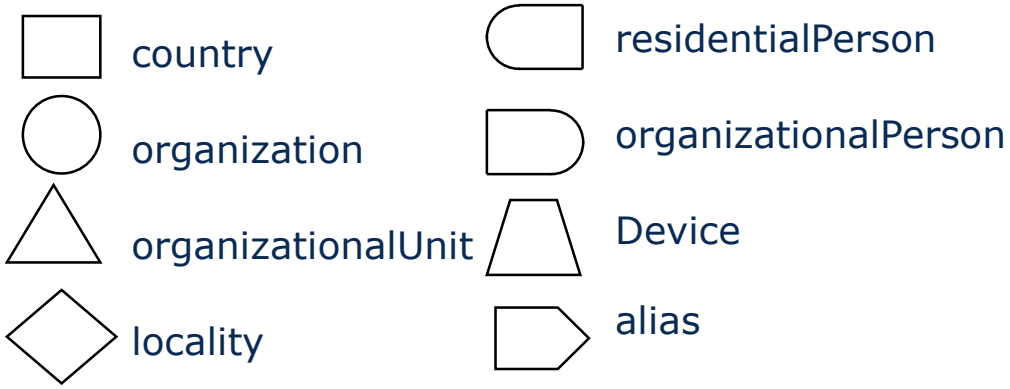
Beschreibung
der zwingend notwendigen und optionalen Attribute durch Klassen

Vererbung
Übernehmen und Ergänzen von Attributen bei Definition spezialisierter Klassen



X.500 Namensraum hierarchisch, Baumstruktur

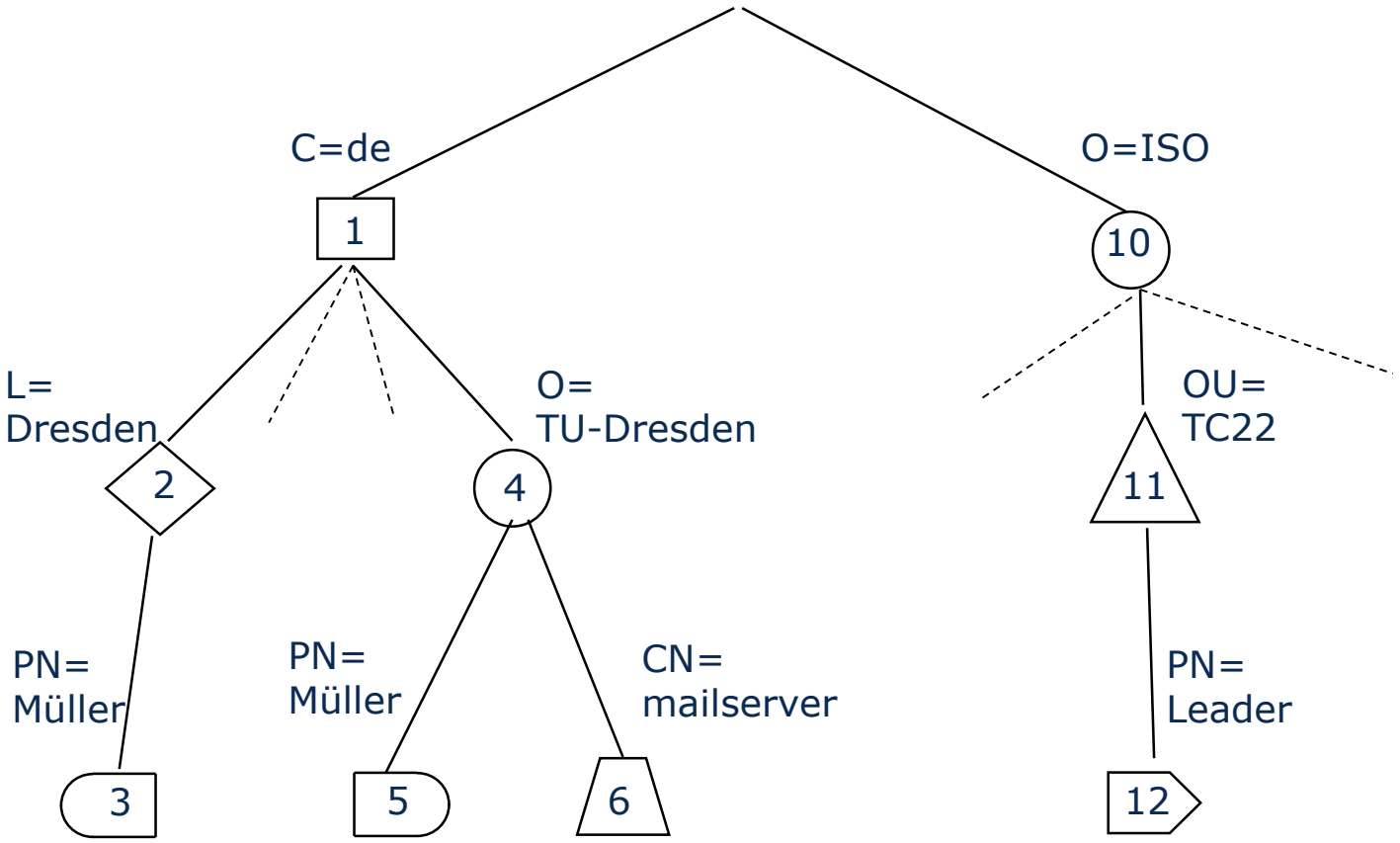
- Mehrere logische Objekte für ein reales Objekt möglich,
  z.B. Herr Müller privat/dienstlich
- Vordefinierte (evtl. mehrwertige) Attribute als Namenskomponenten / Typisierung



C	countryName
O	organizationName
OU	org.UnitName
L	localityName
CN	commonName
PN	privateName

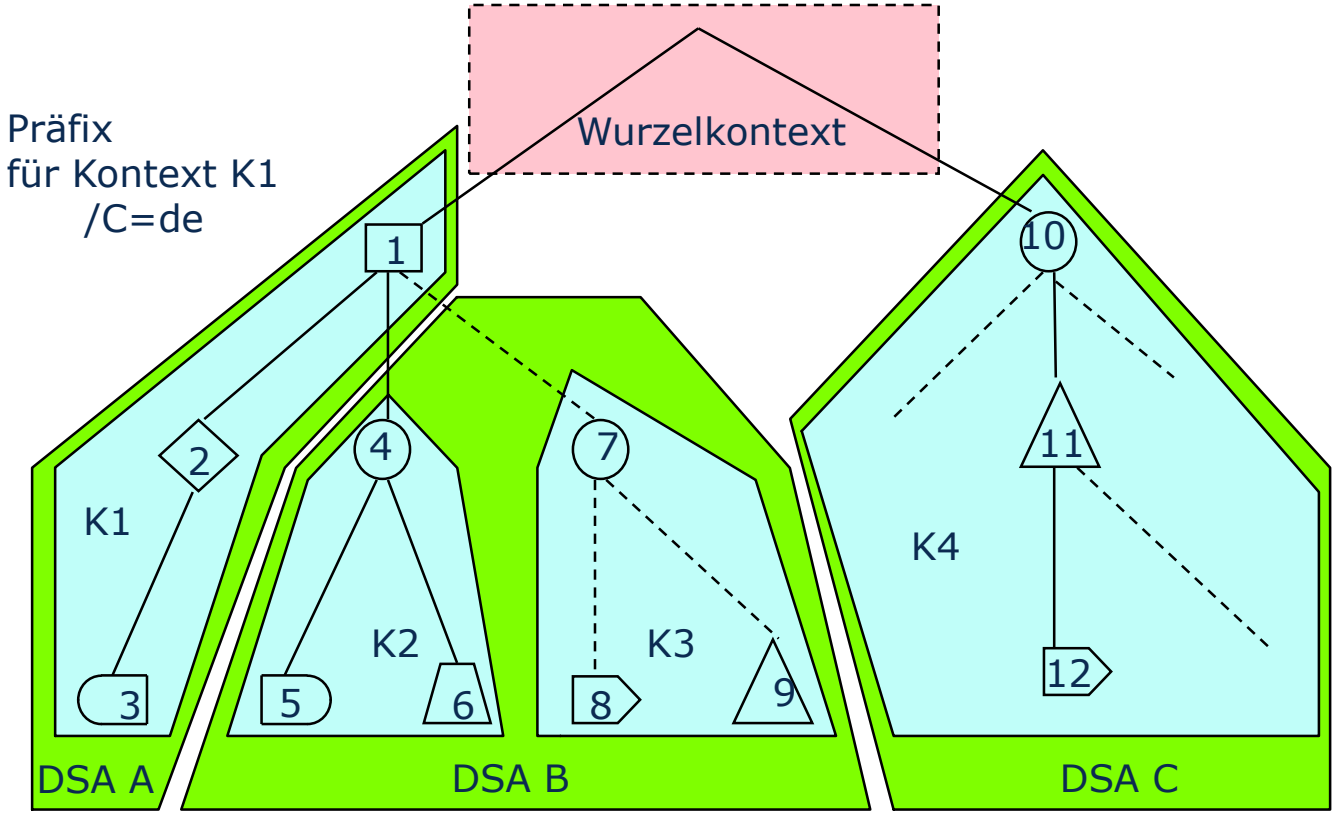
- RDN = Relative Distinguished Name, z.B. "PN = Müller"
- Beispielnamen für eine Person
  - C=de/L=Dresden/PN=Müller
  - C=de/O=TU-Dresden/OU=Informatik/PN=Müller
  - O=ISO/OU=TC22/PN=Leader

X.500 DIT Beispiel



DIT - Partitionierung in Kontexte K (Teilbäume)

- Kontextpräfix: Name des Wurzeleintrages, Wurzelkontext mit leerem Präfix
- Kontexte werden DSAs zugeordnet
- Verzeigerung der Kontexte, Querreferenzen und kontextinterne Referenzen

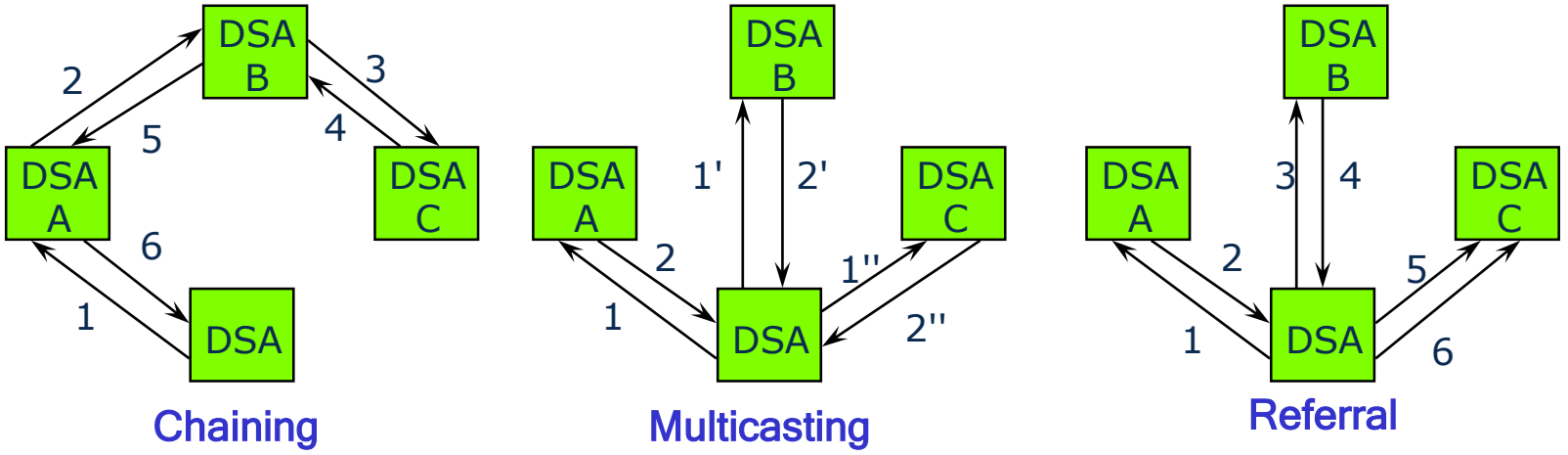


Operationelle Verteilung

Ziel: Bearbeitung eines Benutzerauftrages verteilt über mehrere DSAs

Phasen der Bearbeitung

- Namensauflösung (bis lokaler Eintrag gefunden)
- Evaluation (Durchführung lokaler Operationen, z.B. Search)
- Resultatausgabe (Sammeln und Rücksenden an Auftraggeber)



Weiterleitung über Referenzen zwischen DSA entsprechend Baumstruktur	Gleichzeitige Weiterleitung an mehrere DSA	DSA beantwortet Anfrage mit Referenz auf anderen DSA

X.509v3 – hierarchische Zertifikation

RFC 5280 – IETF Profil von X.509v3

Zertifikat = Datei (vom Typ „.CER“, „.CRT“, „“.PEM“, …)

Struktur eines Zertifikats

- Version
- Seriennummer
- Algorithmen-ID
- Aussteller
- Gültigkeit von … bis …
- Subject
- Subject Public Key Info
  Public-Key-Algorithmus
  Subject Public Key
- Eindeutige ID des Ausstellers (optional)
- Eindeutige ID des Inhabers (optional)
- Erweiterungen …

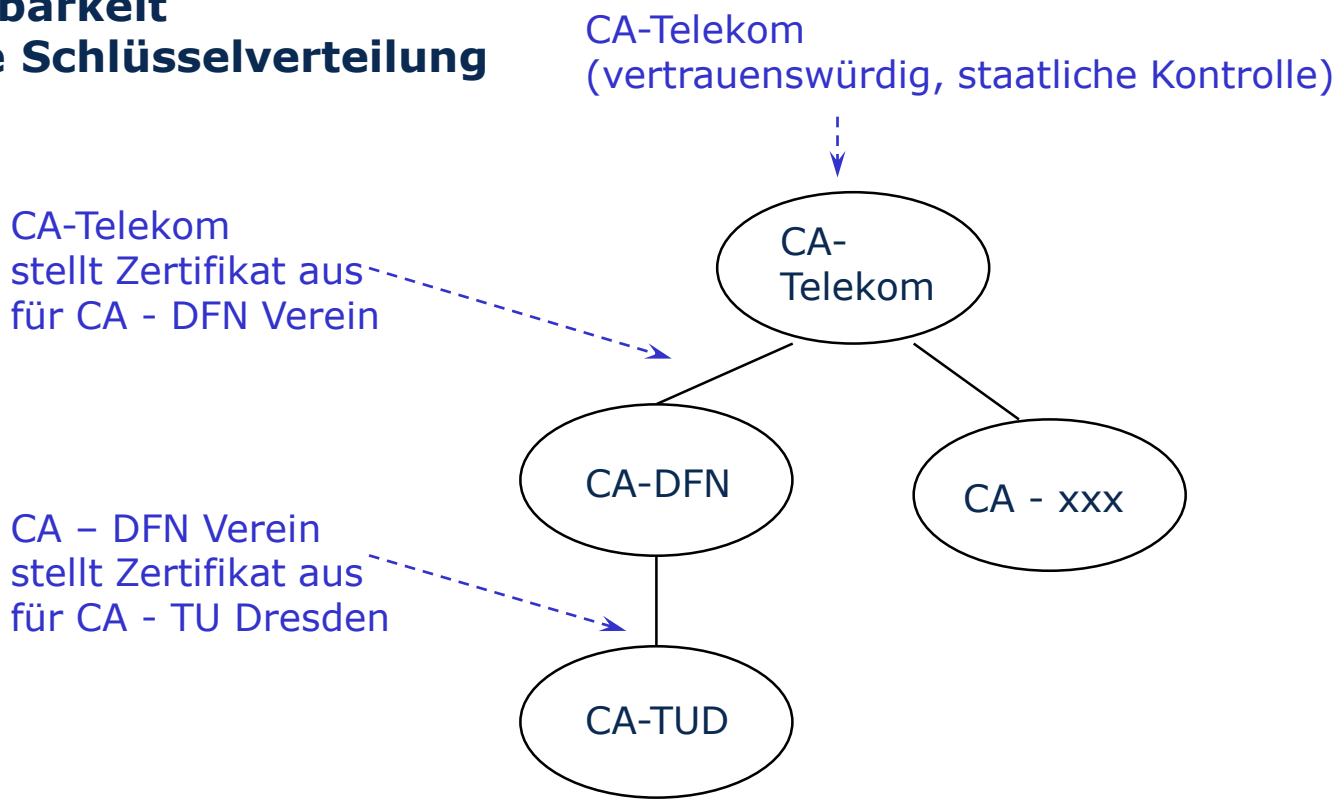
Zertifikat-Signaturalgorithmus
Zertifikat-Signatur

X.509v3 – hierarchische Zertifikation

Zertifikate werden signiert durch eine vertrauenswürdige Zertifizierungstelle (CA bzw. Certificate Authority),

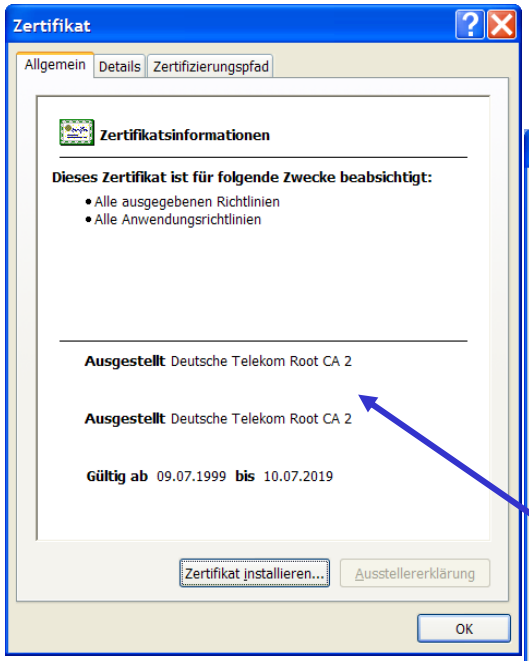
CA–Hierarchie

➔Skalierbarkeit
➔ leichte Schlüsselverteilung

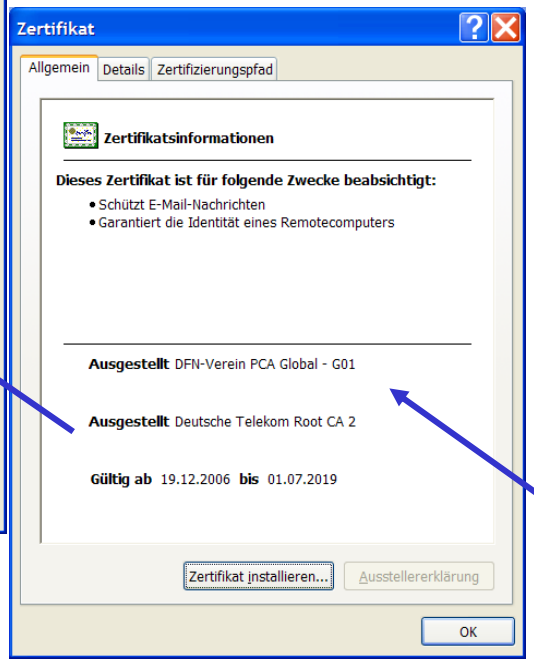


X.509v3 Beispiel für hierarchische Zertifikate

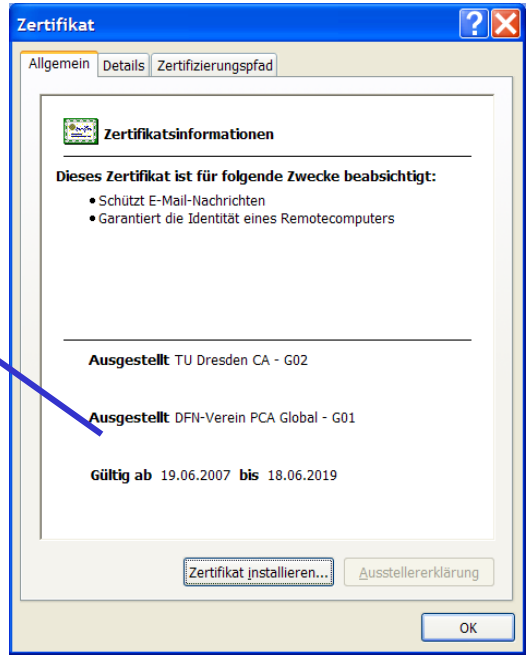
Deutsche Telekom Root CA 2



DFN-Verein PCA Global - G01



TU Dresden CA – G02



X.509v3 Beispiel Zertifikat „TU Dresden CA – G02“

```
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIECpckLTANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJE
RTETMBEGA1UEChMKREZOLVZlcmVpbjEQMA4GA1UECxMHREZOLVBLSTEkMCIGA1UE
AxMbREZOLVZlcmVpbiBQQ0EgR2xvYmFsIC0gRzAxMB4XDTA3MDYxOTA5NDkxOFoX
DTE5MDYxODAwMDAwMFowgYUxCzAJBgNVBAYTAkRFMSgwJgYDVQQKEx9UZWNobmlz
Y2hlIFVuaXZlcnNpdGFldCBEcmVzZGVuMQwwCgYDVQQLEwNaSUgxHDAaBgNVBAMT
E1RVIERyZXNkZW4gQ0EgLSBHMDIxIDAeBgkqhkiG9w0BCQEWEXBraUB0dS1kcmVz
ZGVuLmRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwQ4ek/NE9uzQ
J/dQemELBDQVk/yxH2xj2oDs4TNcNQo8dyAgopWAoCXiD0JgWU/UWpccRds9jhgz
3EU7qnGhT5ILXRmsNQRRCF/pBntyLc9hpWiiz50AR8HKfjg4/DnYLw+MGamJL7I2
g8dXJNrKRx1cSxIf+8m3sSS939c2rajyZCtnybjnnlM9yKe+LD6oSp90AOUOROCV
B5b4d5eEwxa25hCDJ7Uaqyfi2htiQkNhvYXxFL8XqN2a+svPCHRvnex26flyZGWK
Dnp1SLZvc/mrc6PjQcXZlvJw9NMSQBudsUEsDeB0fqrY9AnJzLY+Nc17+rpdhO5b
Ubm6jTN7JwIDAQABo4IBszCCAa8wEgYDVR0TAQH/BAgwBgEB/wIBATALBgNVHQ8E
BAMCAQYwHQYDVR0OBBYEFMUrU5MXg8n1RkLtQ2rftoCmR/LgMB8GA1UdIwQYMBaA
FEm3xs/oPR9/6kR7Eyn38QpwPt5kMBwGA1UdEQQVMBOBEXBraUB0dS1kcmVzZGVu
LmRlMIGIBgNVHR8EgYAwfjA9oDugOYY3aHR0cDovL2NkcDEucGNhLmRmbi5kZS9n
bG9iYWwtcm9vdC1jYS9wdWIvY3JsL2NhY3JsLmNybDA9oDugOYY3aHR0cDovL2Nk
cDIucGNhLmRmbi5kZS9nbG9iYWwtcm9vdC1jYS9wdWIvY3JsL2NhY3JsLmNybDCB
ogYIKwYBBQUHAQEEgZUwgZIwRwYIKwYBBQUHMAKGO2h0dHA6Ly9jZHAxLnBjYS5k
Zm4uZGUvZ2xvYmFsLXJvb3QtY2EvcHViL2NhY2VydC9jYWNlcnQuY3J0MEcGCCsG
AQUFBzAChjtodHRwOi8vY2RwMi5wY2EuZGZuLmRlL2dsb2JhbC1yb290LWNhL3B1
Yi9jYWNlcnQvY2FjZXJ0LmNydDANBgkqhkiG9w0BAQUFAAOCAQEA2KD/xG/6ZPPI
t2t1bZGxjOu+qi8ZEsBHFMW3umQpXbClmN8cV7KkYkrfTD/QE8FV0S+Foymqf1q9
zJXwMo5wXAvhqPDUuMcjca7F7oCq5mPJqrA0+Yd1tuQTn6377j8ubm4ukGUxhCTy
2EilQmogUtC0b/AOZtycNc6Miq+9NO8Juo09ylGHsf420bhCC57v6WuXROAav2XT
tvzHEULhrSEv57kRxthTK5fE19w/OpPtzRG+NDtFAdv2dPrVlDhwh+b7j1DTCmk3
CfktV1zNsc86VPdcqlO0CBSA1L+XXPBel03DgEzErSd8PDcpwZ+KPBYrRLYBxcwb
zKkxSPuylA==
-----END CERTIFICATE-----
```

X.509v3 entschlüsseltes, kommentiertes Zertifikat

Version	V3
Seriennummer	0a 97 24 2d
Signaturalgorithmus	sha1RSA
Aussteller	CN = DFN-Verein PCA Global - G01OU = DFN-PKIO = DFN-VereinC = DE
Gültig ab	Dienstag, 19. Juni 2007 10:49:18
Gültig bis	Dienstag, 18. Juni 2019 01:00:00
Antragsteller	E = pki@tu-dresden.deCN = TU Dresden CA - G02OU = ZIHO = Technische Universitaet DresdenC = DE
Öffentlicher Schlüssel	30 82 01 0a 02 82 01 01 00 c1 0e 1e 93 f3 44 f6 ec d0 27 f7 50 7a 61 0b 04 34 15 93 fc b1 1f 6c 63 da 80 ec e1 33 5c 35 0a 3c 77 20 20 a2 95 80 a0 25 e2 0f 42 60 59 4f d4 5a 97 1c 45 db 3d 8e 18 33 dc 45 3b aa 71 a1 4f 92 0b 5d 19 ac 35 04 51 08 5f e9 06 7b 72 2d cf 61 a5 68 a2 cf 9d 00 47 c1 ca 7e 38 38 fc 39 d8 2f 0f 8c 19 a9 89 2f b2 36 83 c7 57 24 da ca 47 1d 5c 4b 12 1f fb c9 b7 b1 24 bd df d7 36 ad a8 f2 64 2b 67 c9 b8 e7 9e 53 3d c8 a7 be 2c 3e a8 4a 9f 74 00 e5 0e 44 e0 95 07 96 f8 77 97 84 c3 16 b6 e6 10 83 27 b5 1a ab 27 e2 da 1b 62 42 43 61 bd 85 f1 14 bf 17 a8 dd 9a fa cb cf 08 74 6f 9d ec 76 e9 f9 72 64 65 8a 0e 7a 75 48 b6 6f 73 f9 ab 73 a3 e3 41 c5 d9 96 f2 70 f4 d3 12 40 1b 9d b1 41 2c 0d e0 74 7e aa d8 f4 09 c9 cc b6 3e 35 cd 7b fa ba 5d
Schlüsselverwendung	Zertifikatssignatur, Offline Signieren der Zertifikatssperrliste, Signieren der Zertifikatssperrliste (06)
Schlüsselkennung des ...	c5 2b 53 93 17 83 c9 f5 46 42 ed 43 6a df b6 80 a6 47 f2 e0
Stellenschlüsselkennung	Schlüsselkennung=49 b7 c6 cf e8 3d 1f 7f ea 44 7b 13 29 f7 f1 0a 70 3e de 64
Alternativer Antragsteller	RFC822-Name=pki@tu-dresden.de
Sperrlistenverteilungspunkt	[1]Sperrlisten-Verteilungspunkt Name des Verteilungspunktes: Vollst. Name: URL=http://cdp1.pca.dfn.de/global-root-ca/pub/crl/cacrl.crl [2]Sperrlisten-Verteilungspunkt Name des Verteilungspunktes: Vollst. Name: URL=http://cdp2.pca.dfn.de/global-root-ca/pub/crl/cacrl.crl
Zugriff auf Stelleninformation	[1]Stelleninformationszugriff Zugriffsmethode=Zertifizierungsstellenaussteller (1.3.6.1.5.5.7.48.2) Alternativer Name: URL=http://cdp1.pca.dfn.de/global-root-ca/pub/cacert/cacert.crt [2]Stelleninformationszugriff Zugriffsmethode=Zertifizierungsstellenaussteller (1.3.6.1.5.5.7.48.2) Alternativer Name: URL=http://cdp2.pca.dfn.de/global-root-ca/pub/cacert/cacert.crt
Basiseinschränkungen	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=1
Fingerabdruckalgorithmus	sha1
Fingerabdruck	1e 0e 9f 57 3c a1 b5 89 68 c3 33 f8 a3 8c d2 f4 ec a2 5d 52

LDAP (Lightweight Directory Access Protocol)

- RFC 1487, 4511

  deFacto-Standard für den Zugriff auf Verzeichnisdienste
  offener Standard (ermöglicht Herstellerunabhängigkeit)

  breite Herstellerunterstützung
  s. IBM-Redbook (http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf)

- Nutzung für Adreßbücher, Nutzerverwaltung, Authentifizierung

- Vereinfachte Variante des X.500 Directory Access Protocol (DAP)

  objektorientierte Datenmodellierung
  Skalierbarkeit durch Verteilung
  Ausfallsicherheit durch Replikation
  hohe Sicherheit durch Zugriffskontrolle und Authentifizierung

- **Realisierung über TCP/IP**

LDAP IETF-Standards

- Informationsmodell
- Namensraum
- Netzwerkprotokoll (Client-Server)

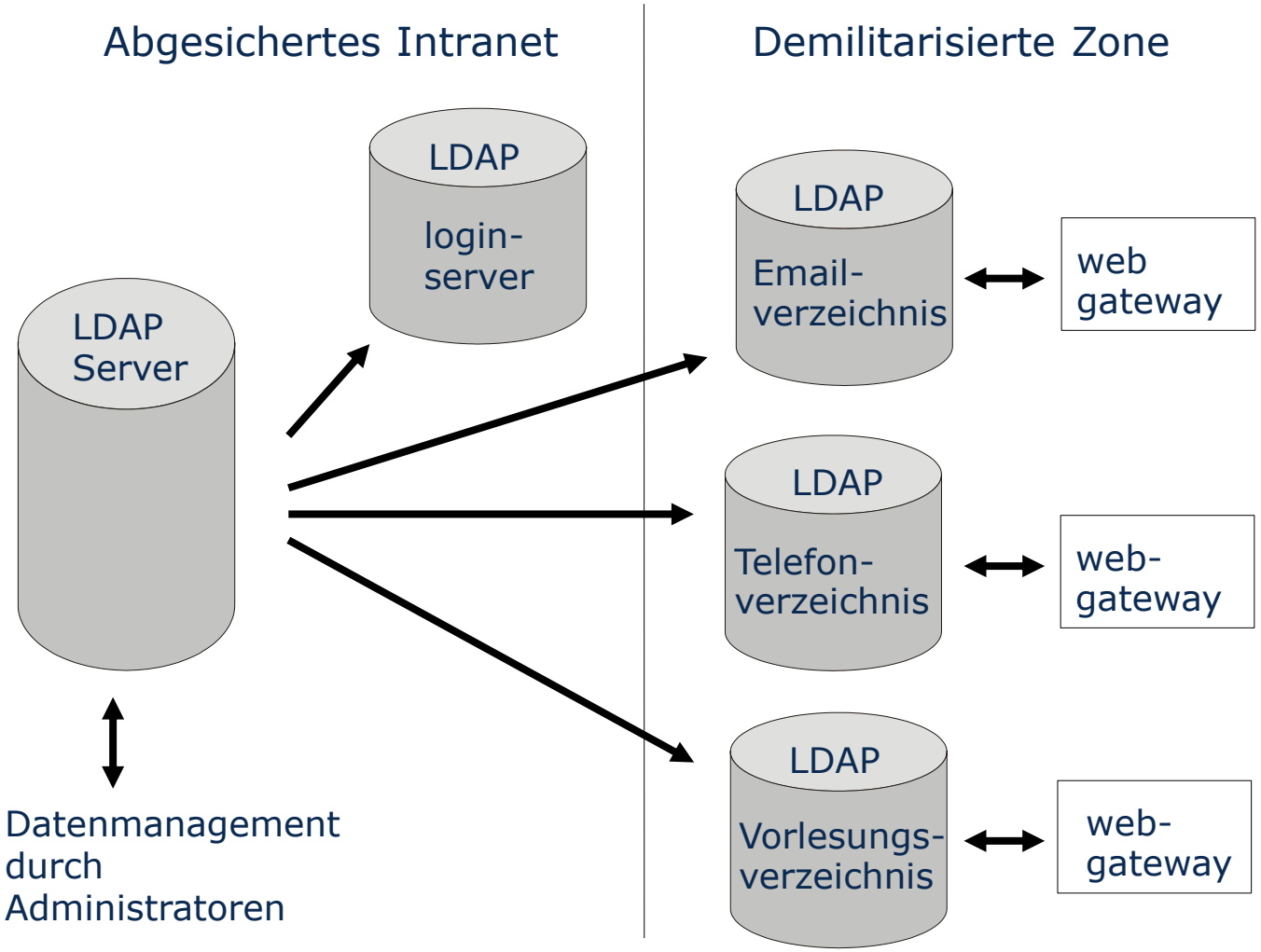
Authentifizierung:	bind, unbind, abandon
Abfragen:	search, compare
Manipulationen:	add, delete, modify, modifyDN

- Authentifizierungs- und Verschlüsselungsmechanismen
- Datenaustauschformat (LDIF)
- APIs für C und Java
- Referierungsmodell (Referral)

LDAP – Implementierungen

- Front-End für heterogene Directory Server
  - MS Active Directory
  - IBM Secure Way
  - SUN One Directory Server
  - Novell Directory Service (NDS): eDirectory
  - Netscape Directory Service
  - Open LDAP http://www.openldap.org/
- Clients
  - Mailagenten für E-Mailrecherche
  - Browser (LDAP-URL)
  - Verschlüsselungssoftware (PGP, S/MIME)
- Standardimplementierungsbestandteil
  - IMAP, SMTP Authentification
  - Apache Webserver

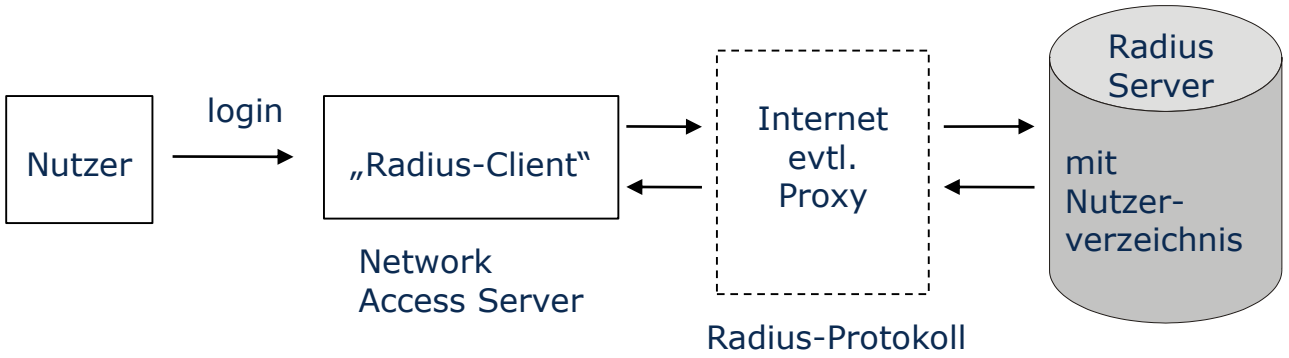
Beispiel LDAP-Nutzung



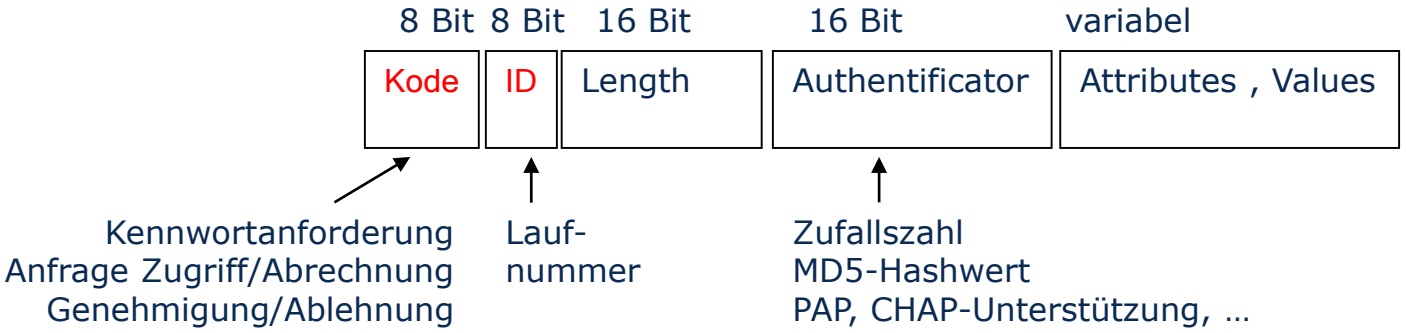
Radius (Remote Authentication and Dial-In User Service)

UDP-basiertes Protokoll zur Sicherung von

- Authentifizierung — Login, …
- Autorisierung — Zugriffsrechte, …
- Abrechnung — Nutzungsdauer, …



Nachrichtenformat



Domain Name System (DNS)

RFC 1034, 1035
Verzeichnisdienst zur Verwaltung des Internet-Namensraumes

Replizierte Datenbanken

Organisation der Namensvergabe durch ICANN
(Internet Corporation Assigned Names and Numbers); www.icann.org
bzw. durch beauftragte Unternehmen

Namensraum - hierarchische Baumstruktur

• root		
• top level domain	z.B.	de
• domain		tu-dresden
• sub level domain		inf
• host name		mephisto

Schreibweise von rechts nach links, getrennt durch „.“

mephisto.inf.tu-dresden.de

DNS – Domänenstruktur

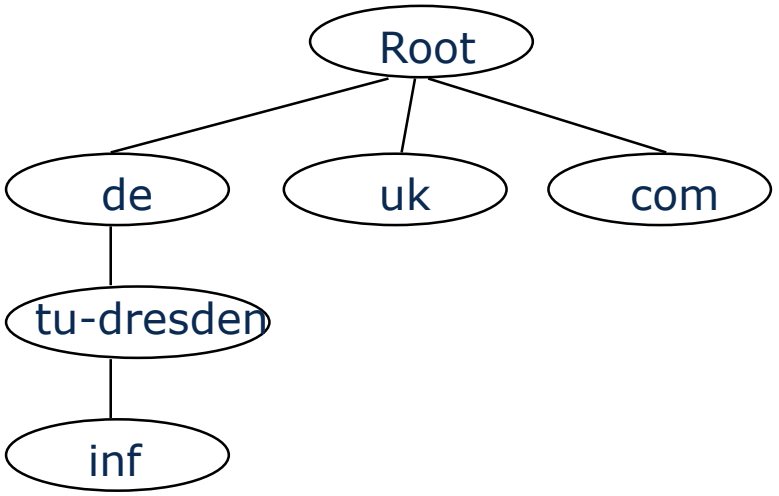
Vergabe der top-level-domain-Namen durch ICANN

applikationsoriente Namen

traditionell (US-orientiert):	com, firm, edu, gov, mil, net, org, tv
neu:	biz, info, pro, name, aero, museum, coop

Staaten-Identifikationen

de, uk, de, fr, nl, cz, pl, eu, ua



Vergabe der domain-Namen
und der sub-level-domain-Namen

durch untergeordnete
NIC (Network Information Center)
z.B. DENIC

DNS - Serverhierarchie

- Namensverwaltung
  durch schrittweisen Abstieg in einer Serverhierarchie,

  sog. **Root-Server** (s. www.root-servers.org)
  kennen die zuständigen Nameserver der top-level.domains
  diese die zuständigen Nameserver der Domänen, …

- DNS-Server besitzen Referenzen (IP-Adressen) auf die Root-Server
  und mindestens auf einen Nameserver der übergeordneten Ebene

- „Zone of Authority", eigenständig verwalteter Teil des Namensraumes
  kann rekursiv weiter unterteilt werden (Unterzonen)

  Zonen besitzen
  einen Primär- und mindestens einen Sekundär-DNS-Server

- jeder Nameserver verwaltet die DNS-Informationen für seine Zone
  d.h er kennt alle Mitglieder der Zone,
  einschließlich der Nameserver der Unterzonen

DNS – Root Server

13 Root Server, weltweit verteilt

name	org	city	type	url
a	InterNIC	Herndon,VA, US	com	http://www.internic.org
b	ISI	Marina del Rey,CA, U	edu	http://www.isi.edu/
c	PSInet	Herndon,VA, US	com	http://www.psi.net/
d	UMD	College Park,MD, US	edu	http://www.umd.edu/
e	NASA	Mt View, CA, US	usg	http://www.nasa.gov/
f	ISC	Palo Alto, CA, US	com	http://www.isc.org/
g	DISA	Vienna, VA, US	usg	http://nic.mil/
h	ARL	Aberdeen, MD, US	usg	http://www.arl.mil/
i	NORDUnet	Stockholm, SE	int	http://www.nordu.net/
j	(TBD)	(colo w/ A)	()	http://www.iana.org/
k	RIPE	London, UK	int	http://www.ripe.net/
l	(TBD)	(colo w/ B)	()	http://www.iana.org/
m	WIDE	Tokyo, JP	int	http://www.wide.ad.jp/

DNS – Root Server

RFC 1035

DNS - Anfrageauflösung

- DNS-Server
  Applikation über UDP (Anfragen/Antworten) bzw. TCP (lange Transfers)
  jeweils Port 53

- Anfrage durch DNS-Client

  Auflösung durch lokale Verwaltungsdatei „hosts“ (nur in Spezialfällen)
  sonst durch Anfrage bei einem Default-DNS-Server

- Resolver

  Nameserverprozeß, der keine Namensverwaltung betreibt
  → Anfrageweiterleitung

- Reaktion der DNS-Server

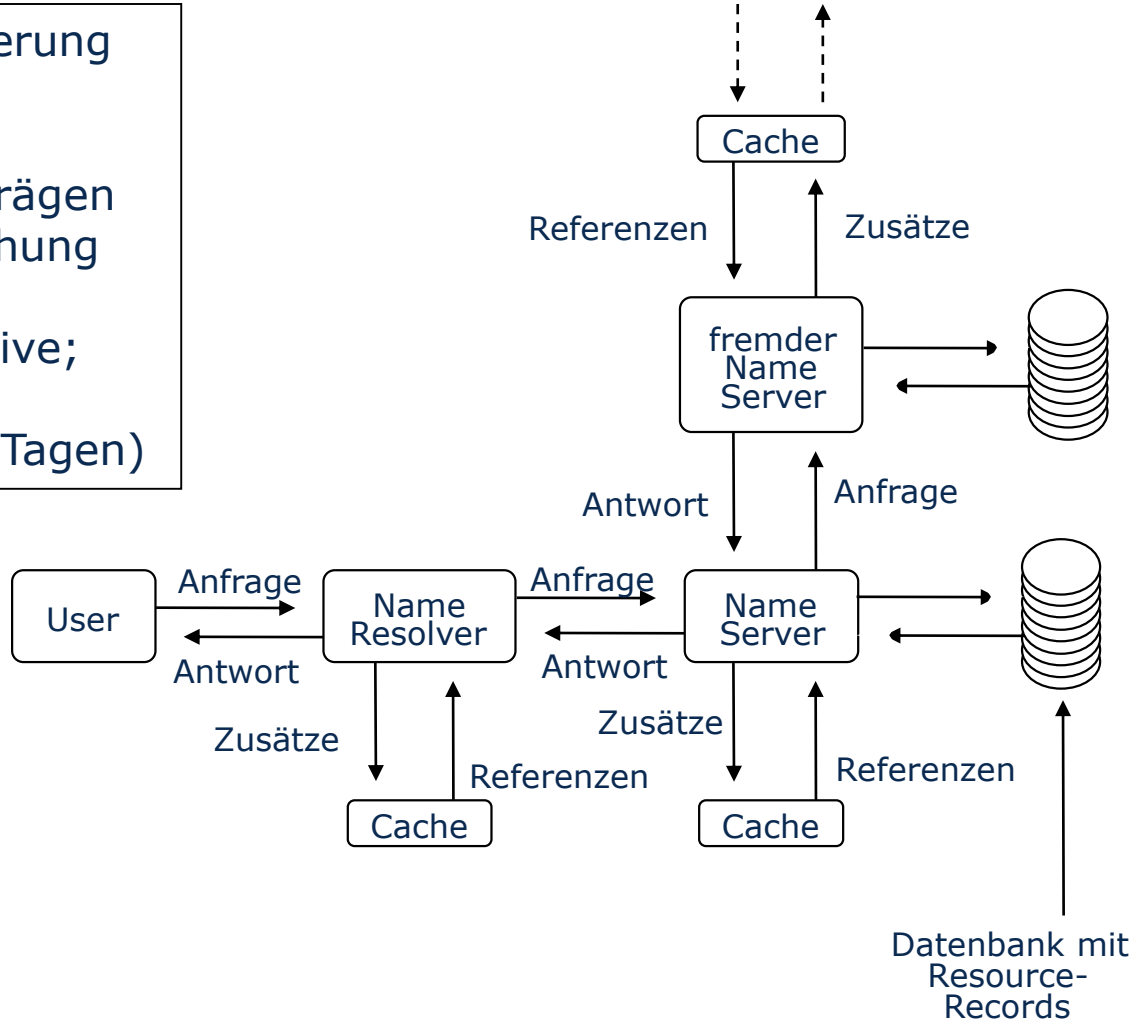
  Antwort „authoritative“, falls er den angefragten Namensraum verwaltet, sonst
  Antwort „non authoritative“ nach Anfrage bei autorisiertem Server

DNS – Abfrage

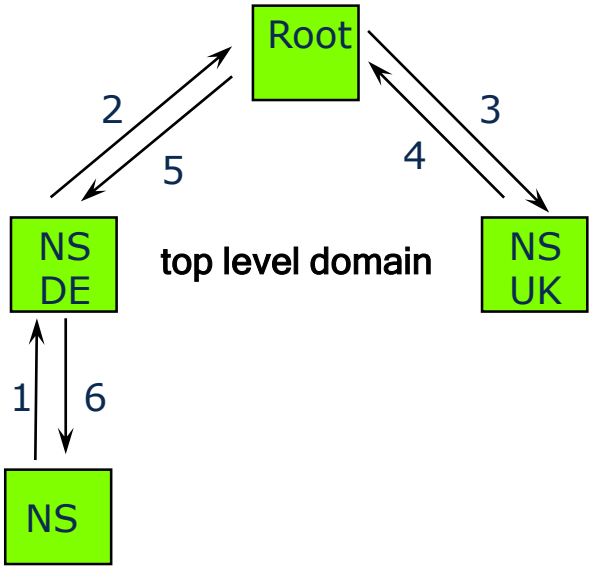
Effizienzverbesserung

Caching
von Namenseinträgen
mit Zeitüberwachung

(TTL – Time to Live;
Bereich
von Minuten bis Tagen)

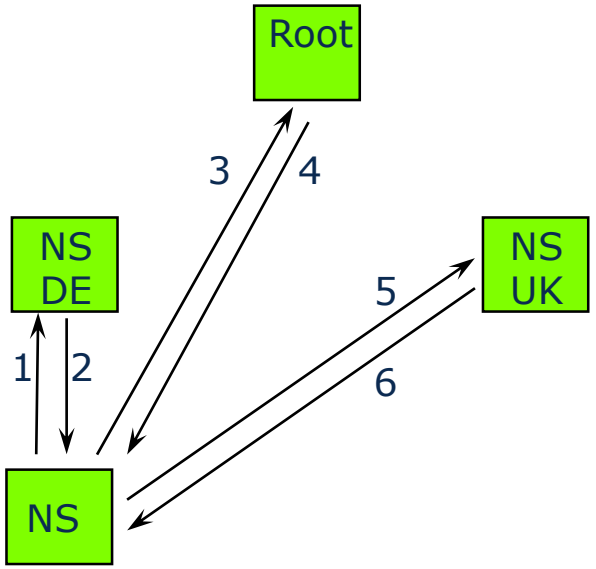


DNS – rekursive und iterative Anfrageauflösung



Rekursive Anfrage

nach domain
„vodafone.uk"



iterative Anfrage

nach domain
„vodafone.uk"

Kombination der Auflösung möglich, meist
Client rekursiv, Nameserver iterativ

DNS - Nachrichtenformat

Zuordnung

Antwort-Anfrage über laufende Nummer

Query-ID	Flags, Opcode, Rcode
Anzahl der Fragen	Anzahl der Antworten
Anzahl der Quellen	Anzahl der Zusätze
Frageabschnitt	
Antwortabschnitt	
Quellenabschnitt	
Zusatzinformationsabschnitt	

Frageabschnitt

- Domänenname
- Art (verlangte Information)
- Klasse (anfragendes Protokoll)

Quellenabschnitt

- Format wie Antwortabschnitt
- kennzeichnet DNS-Server, der die Information geliefert hat

Antwortabschnitt

- Domäne, Art, Klasse (s.o.)
- max. Cache-Dauer
- Datenlänge
- Daten

Zusatzinformationsfeld

- weitere Informationen zum zum Anfragenamen
- z.B. bei MX-Type Mailserver-IP-Adresse

DNS – RR (Resource Records)

Art	Inhalt
A	**Adreß-Record** Zusammenhang Name → 32-Bit-IP-Adresse
CNAME	Eigentlicher Name eines Alias
HINFO	Information zum Host (CPU, Betriebssystem)
MINFO	Informationen über Mailbox oder Mail-Liste
MX	Name eines Mailserver der Domäne
NS	Name des DNS-Servers der Domäne
PTR	Umkehrung Adreß-Record: IP-Adresse → Name
SOA	mehrere Felder zur Namensvergabehierarchie
WKS	Well Known Services (Liste Dienstangebot, z.B SMTP, …)
TXT	beliebige ASCII-Zeichenkette

RR-Felder

Typ, Name (owner), Resource Data (RDATA), Time To Live (TTL)

DNS Spoofing

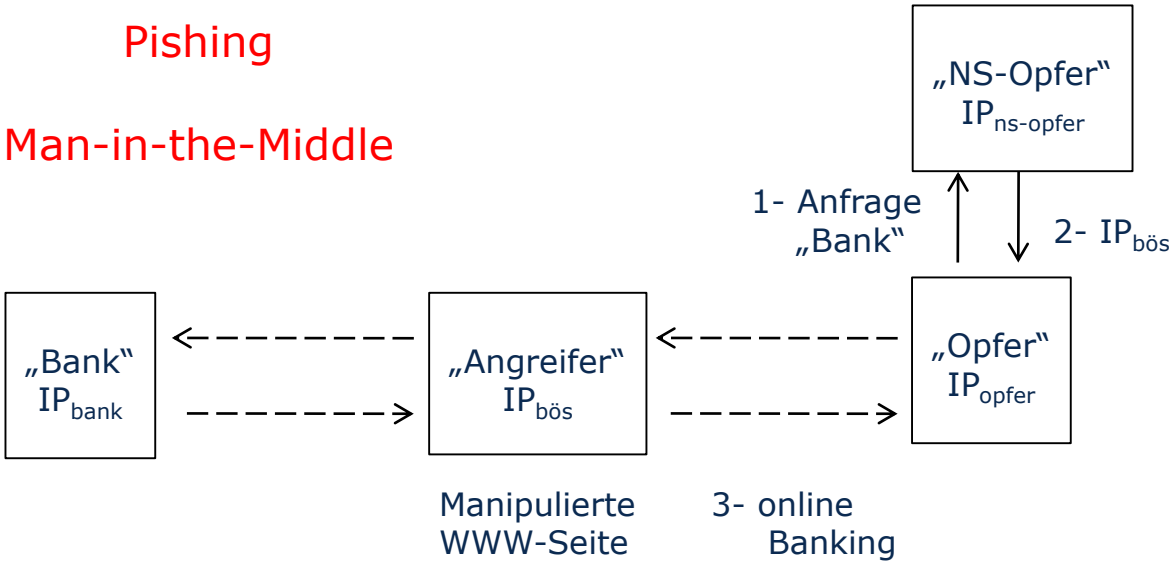
Spoofing Manipulation der Zuordnung “Name” – “IP-Adresse”

DNS ist gegenwärtig nicht sicher !

z.B. Umlenkung der WWW-Seite einer Bank

Pishing

Man-in-the-Middle



DNS Spoofing

- "Angreifer" schickt Anfrage "Angreifer" an "NS-Opfer"
  →Query-ID
- "Angreifer" schickt Anfrage "Bank" an "NS-Opfer"
  und bereitet manipulierte Antwort vor
- "NS-Opfer" fragt iterativ den zuständigen Server "NS-Bank"

  "Angreifer" schickt (mit manipulierter Absenderadresse "NS-Bank")
  Antwort mit falscher Zuordnung, aber richtiger Query-ID !!

  "NS-Bank" antwortet etwas später
  mit richtiger Zuordnung, aber veralteter Query-ID

  → richtige Antwort wird verworfen
- NS-Opfer antwortet zukünftig mit falscher Zuordnung

Ausweg

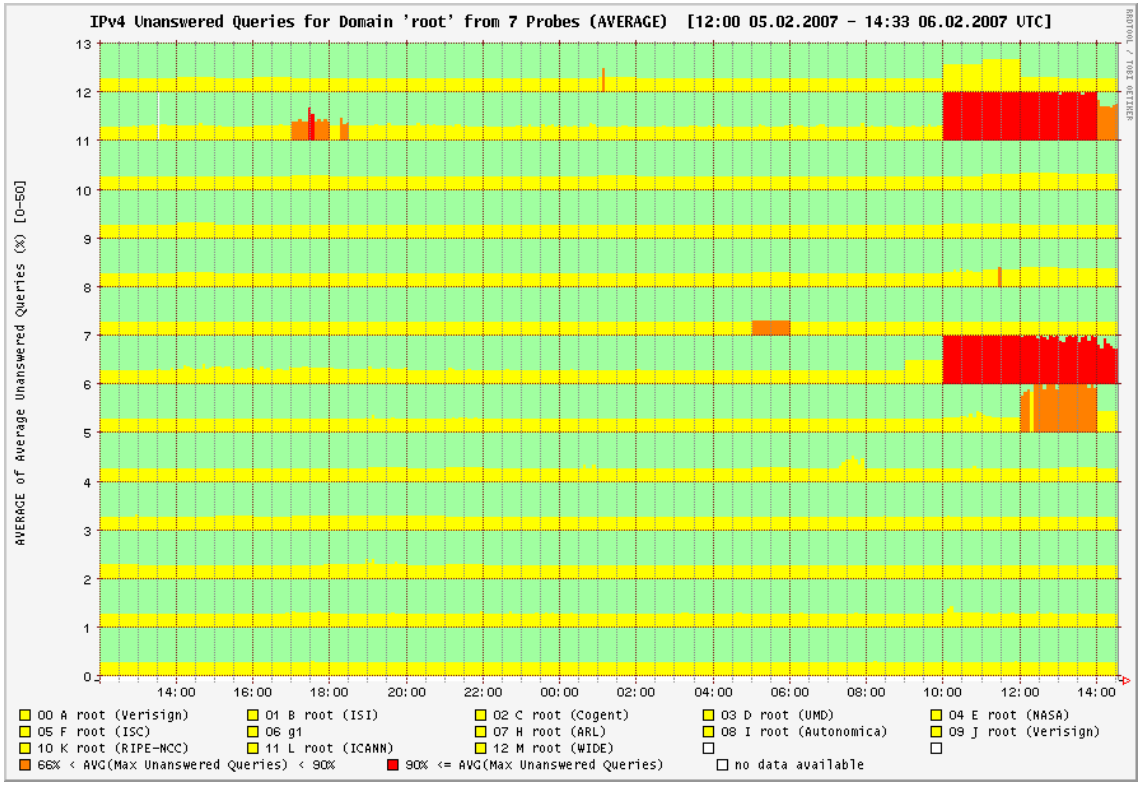
Signierung der Antworten, problematisch wegen Zeitaufwand

DDoS - Attacks (Distributed Denial of Service)

Attacke auf alle 13 Root-Server am 5.2.2007

http://dnsmon.ripe.net/dns-servmon/domain/plot?domain=root;tstart=1170676800;tstop=1170772430;af=ipv4f

→ z.Tl. Totalausfall (Anzahl nichtbeantworteter Anfragen > 90%)



L (ICANN)

G (DoD)

IPv6 - Umstellungsprobleme

RFC 1035

- Beschränkung von DNS-Nachrichten (per UDP) auf 512 byte
- IPv6 evtl. unvollständige Antworten, Sendewiederholungen, …

RFC 2671

Verbesserung