# Sicherheitsaspekte in Active Directory


Dr. Ralf Schneider
DFN–Projekt AMBIX
Zentrum für Datenverarbeitung
Universität Tübingen
ambix-d@mail500.uni-tuebingen.de


5. März 1998

# Grundlagen X.500

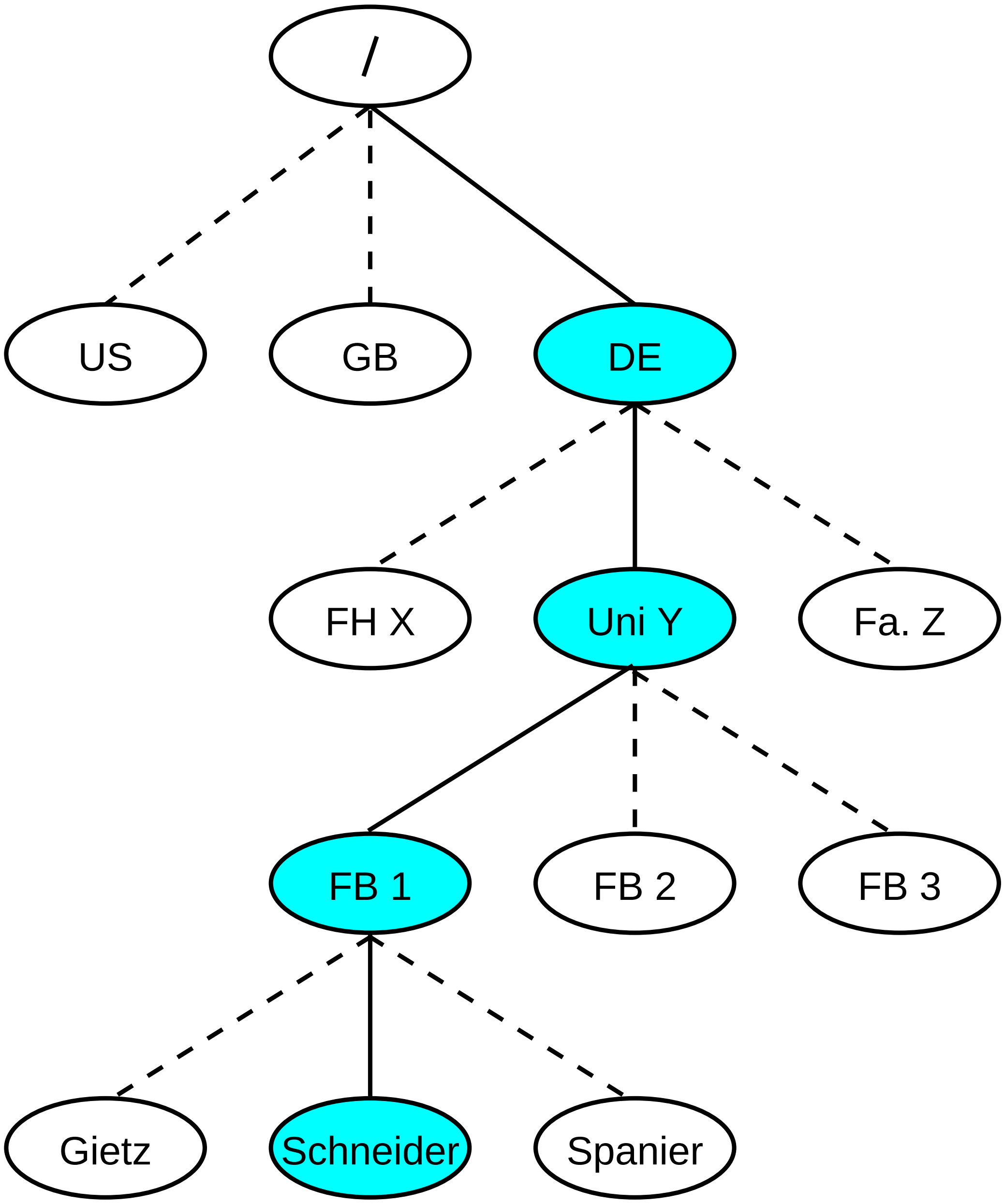
- international standardisierte Datenbank (ITU und ISO)
- hierarchisch strukturiert *(Directory Information Tree = DIT)*
- weltweit verteilbar auf *Directory System Agents* (DSAs)
- weltweit gleichartiger Zugriff mit *Directory User Agents* (DUAs)
- Protokolle zur Kommunikation:

  DUA ⇔ DSA:
  - *Directory Access Protocol* (DAP)

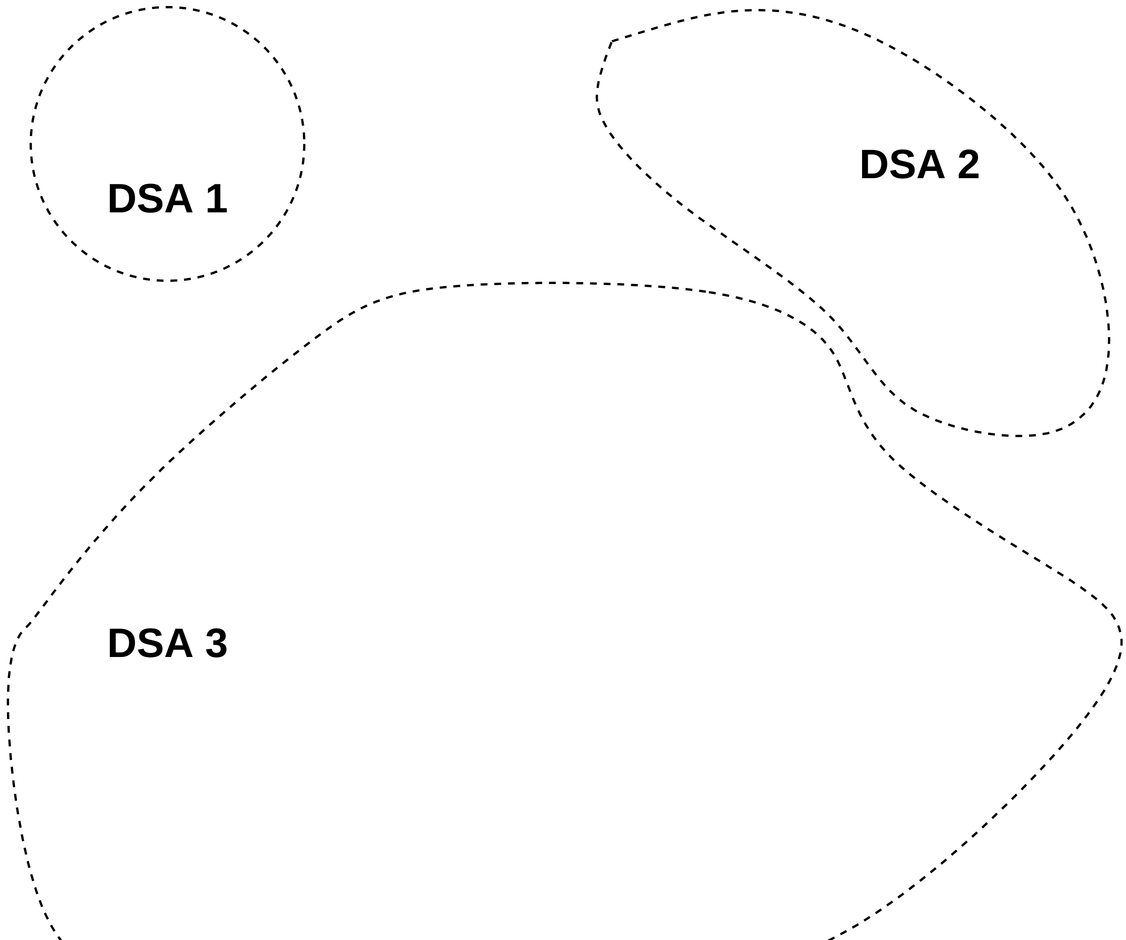
  DSA ⇔ DSA:
  - *Directory System Protocol* (DSP)
  - *Directory Operational Binding Management Protocol* (DOP)
  - *Directory Information Shadowing Protocol* (DSP)

  DUA ⇔ DSA:
  - *Lightweight Directory Access Protocol* (LDAP)
- Mechanismen zur Replikation
- Mechanismen zur Authentifizierung und Zugriffskontrolle

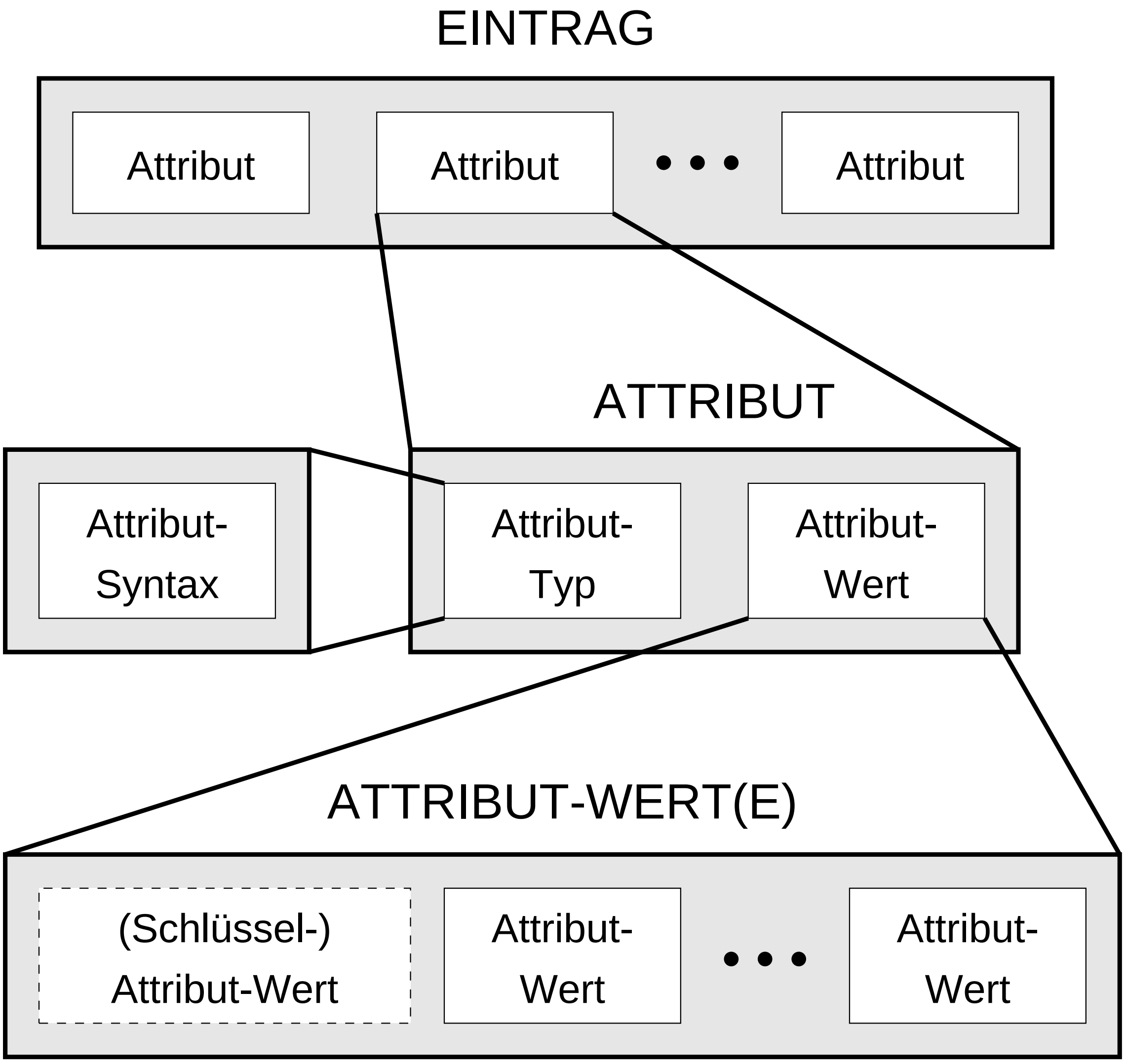
# DIT



# DIT



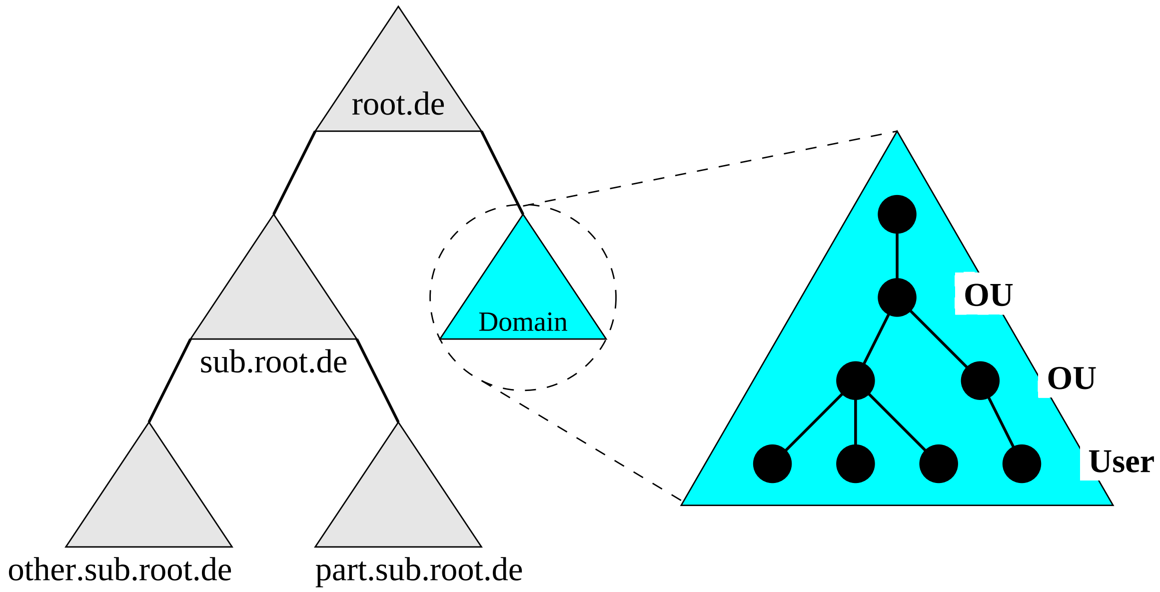
# Struktur eines Eintrags

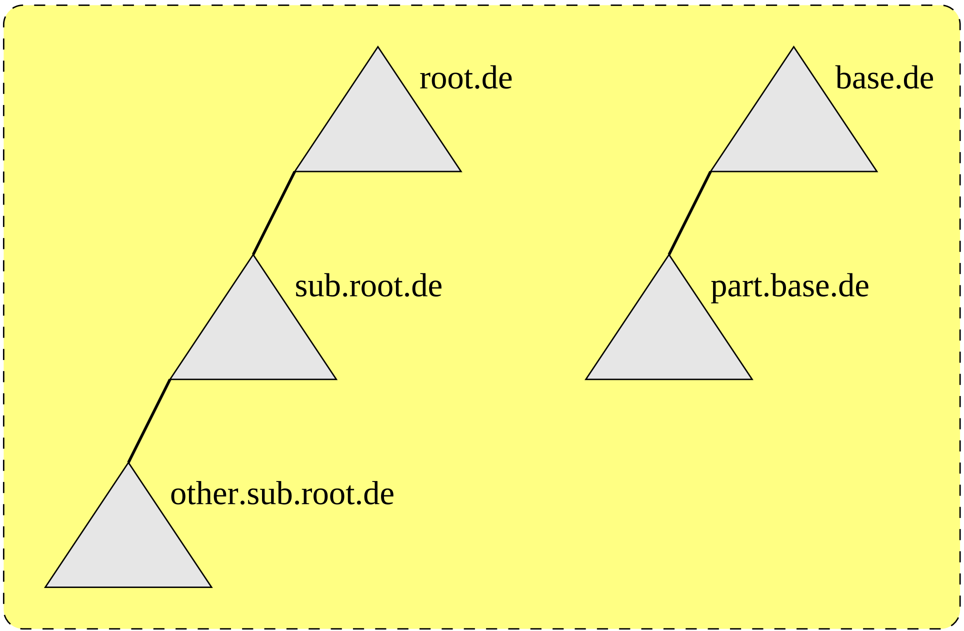


# Namen


| DIT | RDN | DN |
|---|---|---|
| / | | |
| DE | c=DE | c=DE |
| Uni Y | o=Uni Y | c=DE, o=Uni Y |
| FB 1 | ou=FB 1 | c=DE, o=Uni Y<br>ou=FB 1 |
| Schneider | cn=Schneider | c=DE, o=Uni Y<br>ou=FB 1, cn=Schneider |

# (Domain) Tree, Forest



# Features von Active Directory

- hierarchischer Namensraum
- DNS–Integration, Dynamic–DNS
- Namen
  - DN
  - *User Principal Name* (UPN)
  - *Object Globally Unique Identifier* (GUID)
  - HTTP URLs
  - LDAP URLs
  - *Universal Naming Convention* (UNC)
- Replikation
- *Global Catalog* (GC)

# Zugang zu Active Directory

Unterstütze Protokolle:

- LDAP v2 und LDAP v3
- MAPI–RPC

Nicht Unterstütze Protokolle:

- alle X.500 Protokolle!

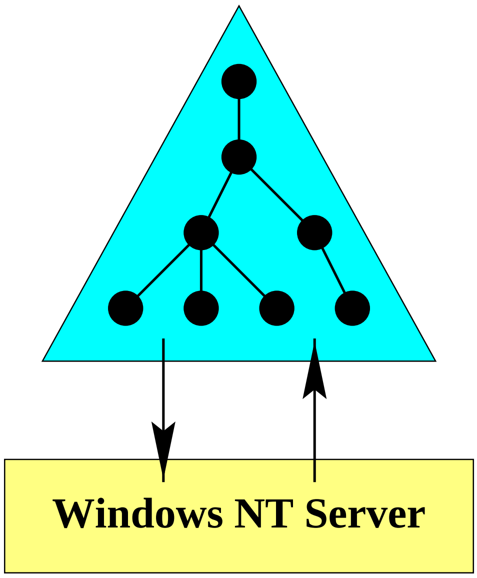
  DAP, DSP, DISP, DOP

APIs:

- *Active Directory Service Interface* (ADSI)
- LDAP C API
- *Windows Messaging* API (MAPI)

# Zusammenhang AD und Sicherheit

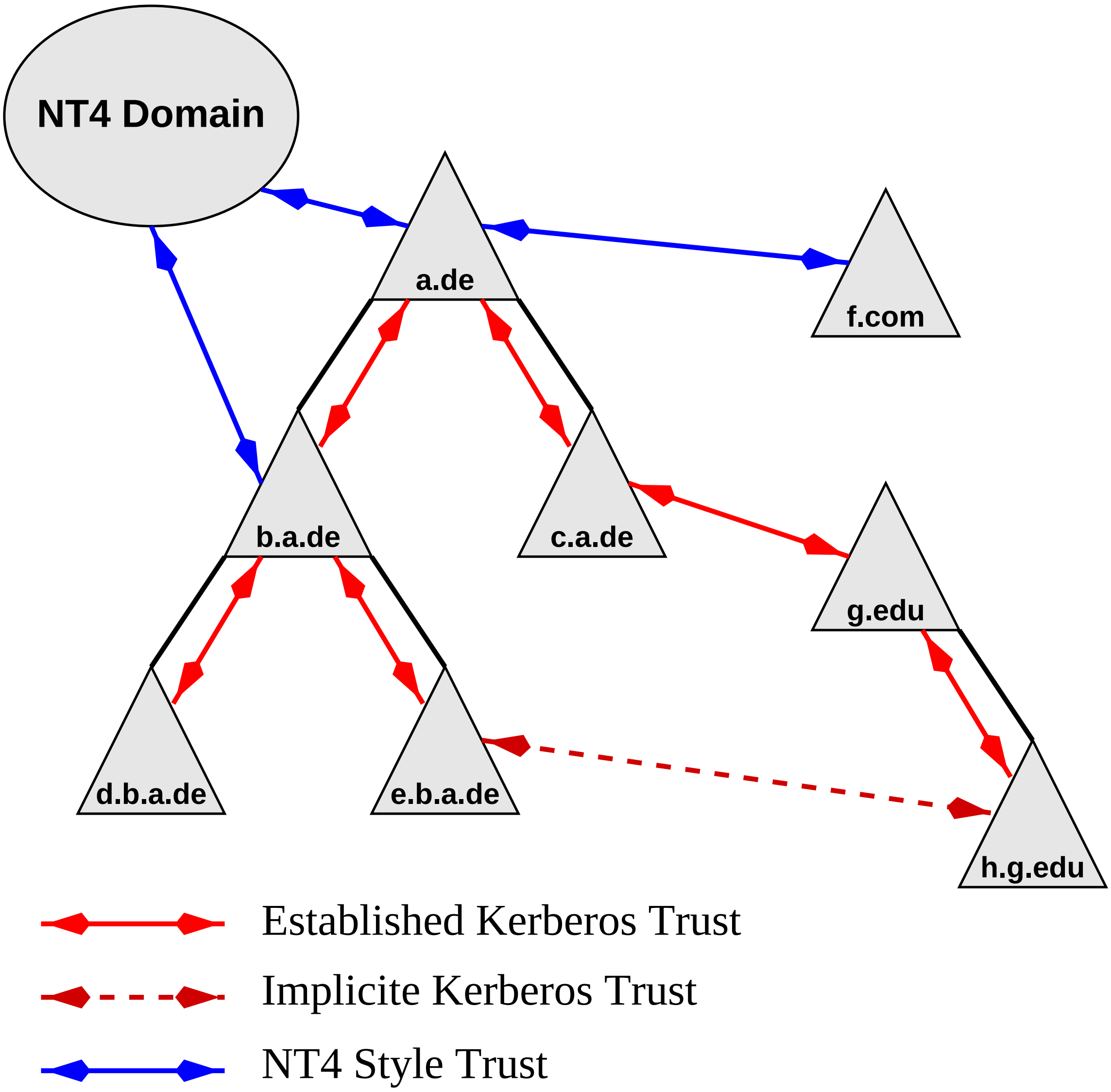
- Active Directory speichert
  - Sicherheits–Policy
  - Informationen über Benutzer und Ressourcen
  - Trust–Informationen
- Betriebssystem implementiert
  - Sicherheitsmodell für alle Einträge



# Zugriffsrechte

- *Access Control Lists* (ACLs) regeln Zugriff auf Einträge
- Definition/Gültigkeit von ACLs (Wer? Welche? Worauf?)
  - Rechte: ◇ *Create* ◇ *Modify* ◇ *Read* ◇ *Search* ◇ . . .
  - Gültig: ◇ Eintrag ◇ Gruppe von Attributen<br>◇ einzelne Attribute
- Voreinstellung: Schreiben/Lesen Eintrag
- statische Vererbung der ACLs
- Delegation: Zugriffsrechte für OU oder *Container*
  - Ändern von Attributen des *Containers*
  - Anlegen, Ändern, Löschen von Einträgen im *Container*
  - Ändern von Attributen in Einträgen

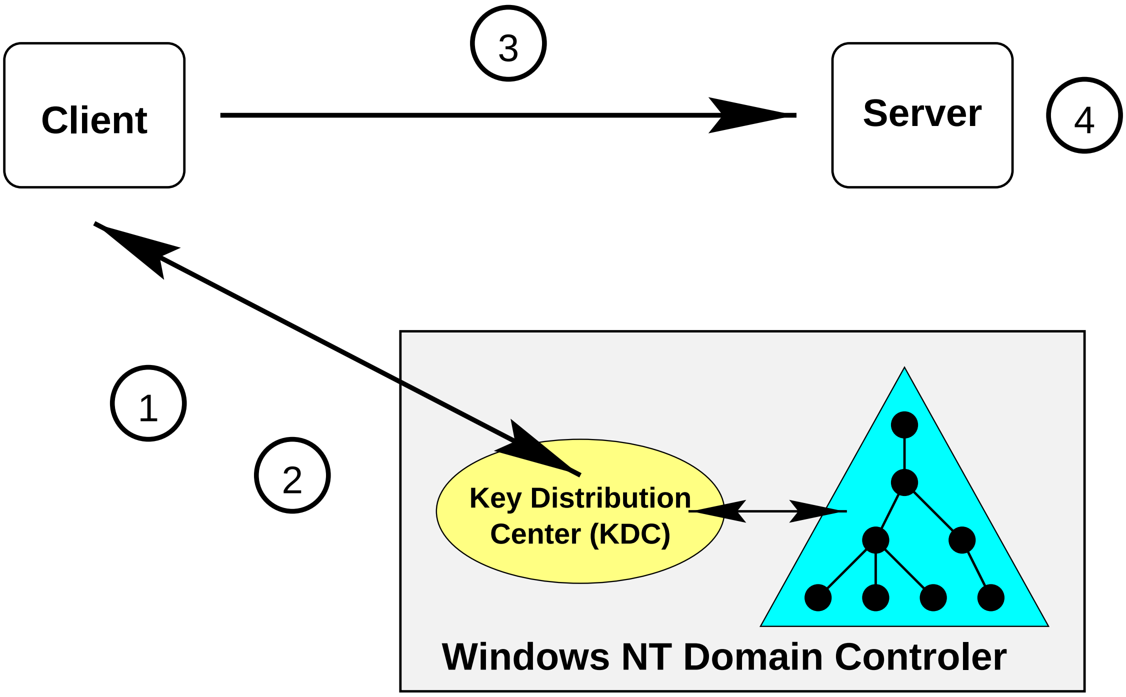
# Sicherheitsbeziehungen



# Sicherheitsprotokolle

- Windows NT *Lan Manager* (NTLM)
  - *Remote File Access*
  - *Secure* RPC
- Kerberos Version 5
  - Ersatz für NTLM
  - Erweiterung für *Public Keys*
- *Distributed Password Authentication* (DPA)
  - MSN, CompuServe
  - mehrere Server, ein Passwort
- *Public Key Crypto Systems* (PKCSs)
  - *Secure Socket Layer* (SSL) 3.0
  - X509v3

# Kerberos Authentifizierung

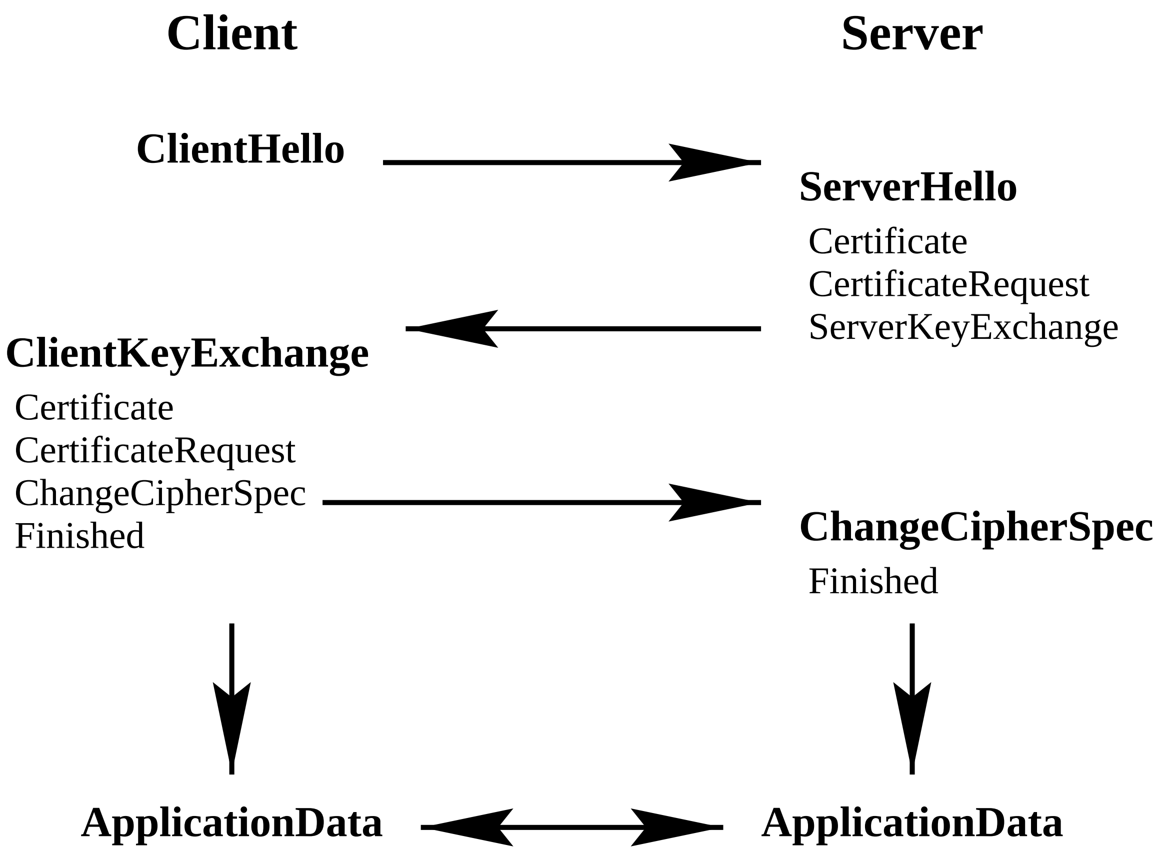



1. Anmeldung beim KDC
2. Anforderung Sitzungs–Ticket für Server
3. Client übermittelt Sitzungs–Ticket an Server
4. Server überprüft Sitzungs–Ticket

# PKCS

- Client Authentifizierung mit SSL 3.0
  - Verifikation Signatur ⇒ *Certification Authority* (CA)
  - Zertifikatinformationen ⇒ Windows NT Account
- Authentifizierung „externer Benutzer“
  - Verifikation Zertifikat ⇒ CA
  - *Subject Name* (X.509–Zertifikat) ⇒ Windows NT Account
- *Microsoft Certificate Server*
  - Bearbeitung Zertifikate–Anfragen
  - Erstellung von Zertifikaten (X.509)
  - Management von Zertifikaten und *Certificate Revocation Lists* (CRLs)
- Crypto API
  - Zertifikat– und CRL–Management
  - Zertifikaterstellung, –austausch, –verifikation
  - Digitale Signaturen, Verifikation, Verschlüsselung

# SSL 3.0 Handshake



# Kontakt

E–Mail: ambix-d@mail500.uni-tuebingen.de

URL: http://ambix.uni-tuebingen.de/