LDAP und Kerberos

Folien unter http://ca.tu-berlin.de/docs/pdf/LDAP-Vortrag.pdf

LDAP: Agenda

- Was ist LDAP?
- LDAP Strukturen / Datenmodell
- LDAP Operationen
- LDAP Anwendungen
- tubIT LDAP Server

Was ist LDAP?

LDAP ist die Abkürzung für:
Ligthweigth Directory Access Protocol

Aktuell

- LDAP ist ein Synonym für ein verteiltes Verzeichnis mit zugehörigem Netzwerkprotoll, dass den Zugriff auf die Daten regelt.
- aktuelle Version: LDAPv3 (RFC 3377). Sie erlaubt Erweiterungen durch den Betreiber.

Historie

- Abgeleitet aus X.500. X.500 definiert ein objektorientiertes Datenmodell.
- das ***Directory Access Protocol (DAP)*** regelt den Zugriff auf die Daten.
- hat sich nicht als Standard etabliert:
  zu komplex, baut auf dem ISO Protokoll Stack auf.

LDAP Strukturen / Datenmodell

LDAP Datenmodell:

- LDAP Informationsmodell
  - Einträge, Attribute, Objektklassen, Schema

- LDAP Namensraum, Directory Information Tree (DIT)
  - Aufbau des Distinguished Name (DN)

Was kann gespeichert werden?

- Alphanumerische Daten
  Namen, Adressen, Telefonnummern ...
- Binärdaten
  Fotos, Grafiken, X.509 Zertifikate ...
- Zeiger auf andere Daten
  Innerhalb des DIT, Zeiger auf externe Daten, URI, Dateinamen ...
- Durch eigene Schemata beliebig erweiterbar.

Das LDAP Informationsmodell:

- Informationen werden in LDAP logisch als ***Einträge*** in einem Baum, dem ***Directory Information Tree (DIT)*** dargestellt.
- Jeder Eintrag besitzt einen eindeutigen ***Distinguished Name***.
- Jeder Eintrag gehört zu (mindestens) einer ***Objektklasse***.
- Objektklassen werden durch ihre ***Attribute*** definiert.
- Ein Attribut besitzt einen ***Typ*** und einen oder mehrere Werte.
- Die Definitionen der Objektklassen und Attributtypen ergeben das ***Schema***.

LDAP Strukturen / Informationsmodell: Einträge

Einträge:

Distinguished Name
Attribut-1 Wert
Attribut-2 Wert
Attribut-2 Wert
Attribut-3 Wert

Beispiel für einen Eintrag mit drei Attributen und DN

```
dn: cn=Peter Pan, o=TUB, ou=tubIT, c=de
objectclass: person
cn: Peter Pan
gn: Peter
```

LDAP Strukturen / Informationsmodell: Attribute

Attribute:

- Attribute sind die konstituierenden Bestandteile eines Eintrags
- Attribute sind 'Typ: Wert' Paare (in LDIF Notation)

```
dn: cn=Peter Pan, o=tubIT, dc=tu-berlin, dc=de
objectclass: person
cn: Peter Pan
gn: Peter
gn: John
```

Der Teil vor dem Doppelpunkt gibt den Typ, der dahinter den Wert des Attributs an. Die Objektklasse legt fest, welche Attribute in einem Eintrag vorhanden sein dürfen oder müssen. Der DN ist kein Attribut!

LDAP Strukturen / Informationsmodell: Attribute

Attributtypen:

Ein Attributtyp wird durch folgende Komponenten definiert

- Name
- Object Identifier (OID)
- Syntax
- Matching rules
- Vererbung

LDAP Strukturen / Informationsmodell: Attribute

Name:

- String bestehend aus Buchstaben, Zahlen, Bindestrichen (-)und Semikula (;).
- keine Unterscheidung zwischen Groß- und Kleinschreibung für Attributnamen (sehr wohl aber für Attributwerte!).
- Beispiele:
  - locality
  - displayName
  - telephoneNumber

LDAP Strukturen / Informationsmodell: Attribute

Object Identifier (OID):

Eine durch Punkte strukturierte Zahl (analog zu IP-Adressen), die weltweit eindeutig ist, z.B.:

`1.3.6.1.4.1.1466.115.121.1.15`

OIDs werden von der Internet *Assigned Numbers Autority (IANA)* vergeben.

LDAP Strukturen / Informationsmodell: Attribute

Syntax:

Die Syntax eines Attributs legt fest, wie Daten behandelt werden.
Beispiele:

- Directory String – Syntax für druckbare, UTF-8 kodierte Unicode Strings, ohne Berücksichtigung von Groß- und Kleinschreibung
- Telephone Number – String der eine Telefonnummer darstellt. Nichtnumerische Zeichen werden bei Suchvorgängen ignoriert.
- Syntax Definitionen werden durch OIDs referenziert.

LDAP Strukturen / Informationsmodell: Attribute

Matching rules:

Die Vergleichsregeln beziehen sich auf die Werte eines Attributs

- Equality
- Substring
- Ordering
- Extensible (selbstdefiniert)

LDAP Strukturen / Informationsmodell: Objektklassen

Objektklassen:

Eine Objektklasse wird durch folgende Komponenten definiert

- Name
- Object Identifier (OID)
- Vererbung
- Typ
- Liste möglicher und / oder notwendiger Attributtypen

LDAP Strukturen / Informationsmodell: Objektklassen

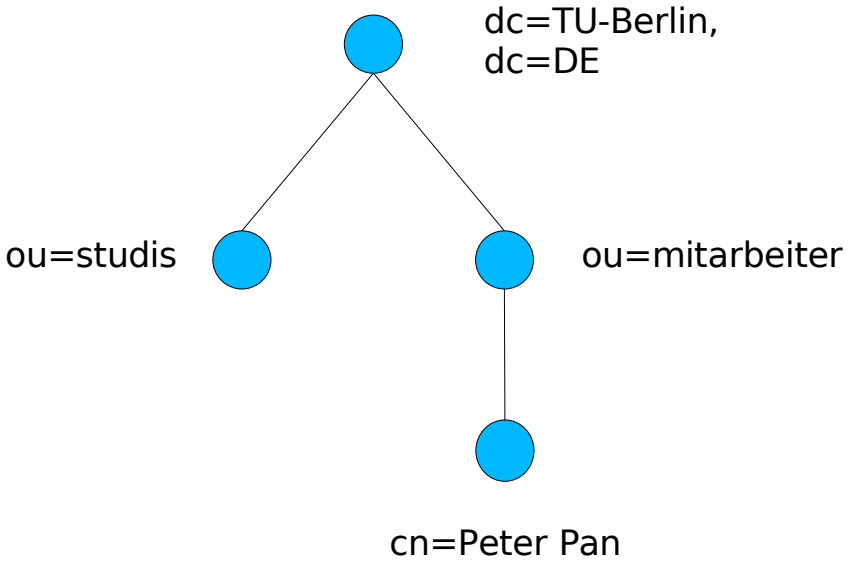
```
# Diese Datei enthält die Definitionen der Objektklasse tubAccount und ihrer Attributtypen.
#
# tubAccountOwner
# DN eines Personeneintrags unter ou=people.
attributetype ( 1.3.6.1.4.1.10238.400.1.1.61
        NAME 'tubAccountOwner'
        DESC 'DN des Besitzers des Accounts'
        EQUALITY distinguishedNameMatch
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.12' SINGLE-VALUE )
...
...
...

# tubAccountStatus
# String mit den Werten "aktiv", "deaktiviert" und "gesperrt".
attributetype ( 1.3.6.1.4.1.10238.400.1.1.64
        NAME 'tubAccountStatus'
        DESC 'Status eines Accounts'
        EQUALITY caseIgnoreMatch
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

# tubAccount
# In diese Objektklasse gehören TU Accounts
objectclass ( 1.3.6.1.4.1.10238.400.1.1.60
        NAME 'tubAccount'
        AUXILIARY
        MUST (tubAccountOwner $ tubAccountStatus)
        MAY (tubAccountExpirationDate $ tubAccountService
            )
        )
```

LDAP Namensraum / DIT

Einträge werden als Knoten in einem Baum gespeichert

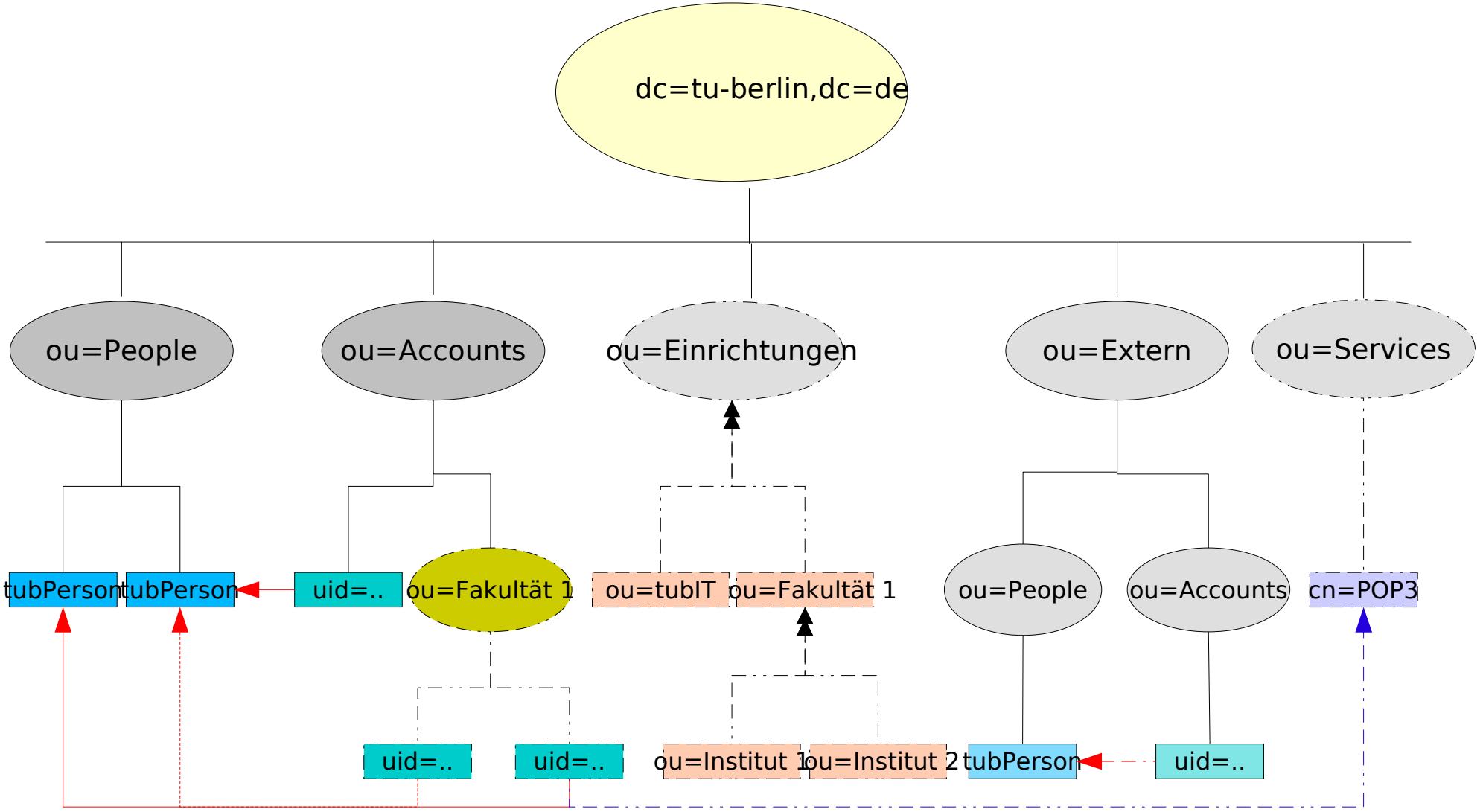
- Jeder Koten hat beliebig viele Nachfolgeknoten.
- Jeder Knoten, mit Ausnahme der Wurzel, hat genau einen Vorgängerknoten.
- Einträge einer Ebene werden durch einen eindeutigen Bezeichner, den ***Relative Distinguished Name (RDN)*** referenziert. Der RDN muss aus einem oder mehreren Attributen des Eintrags gebildet werden.
- Die eindeutige Position eines Knotens im Baum wird durch den *Distinguished Name (DN)* beschrieben, der durch rekursives Aneinanderfügen der RDNs entsteht:

LDAP Namensraum / DIT



In obigem Beispiel hat der unterste Knoten den
RDN: *cn=Peter Pan*, der komplette DN ergibt sich zu
DN: *cn=Peter Pan, ou=mitarbeiter, dc=TU-Berlin, dc=DE*.
Die RDNs und DNs der Knoten der mittleren Ebene lauten:
RDN: *ou=studis*
ou=mitarbeiter
DN: *ou=studis, dc=TU-Berlin, dc=DE*
ou=mitarbeiter, dc=TU-Berlin, dc=DE

LDAP Namensraum / DIT



LDAP Operationen

- Authentifizierungsoperationen
  - bind
  - unbind
  - abandon
- Abfrageoperationen
  - search (searchlevels: base, one ,sub)
  - compare
- Änderungsoperationen
  - add
  - delete
  - modify
  - modifyDN

Alle Operationen sind DN orientiert.

LDAP Anwendungen

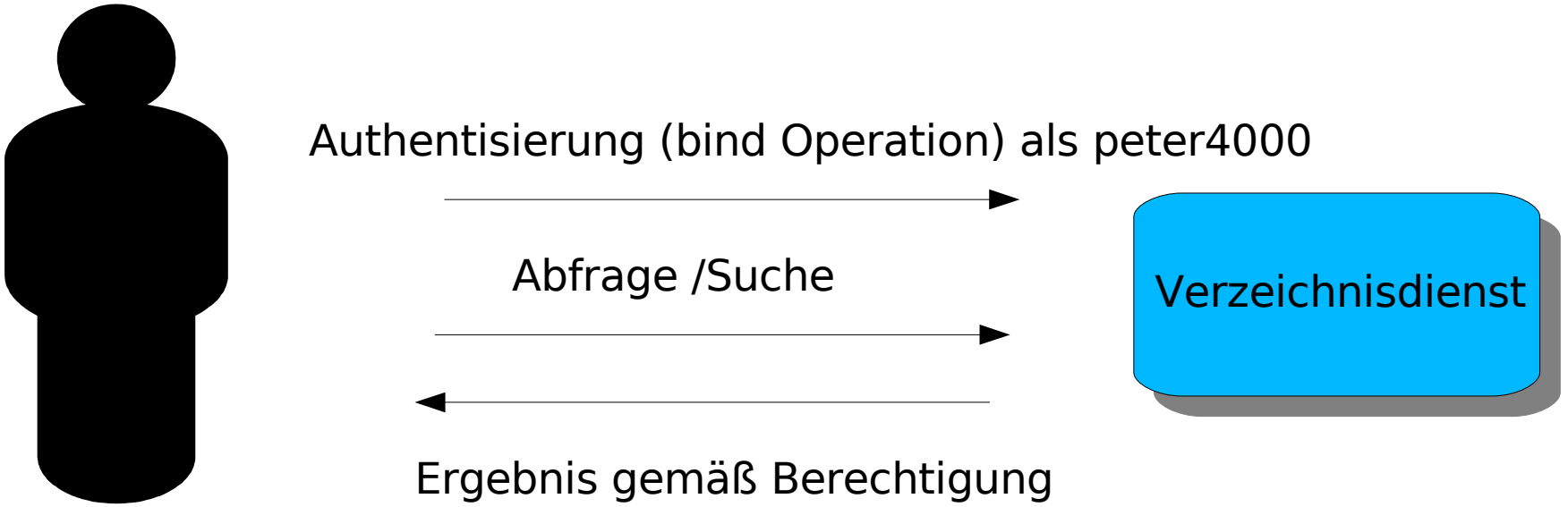
LDAP ist geeignet für Anwendungen, die

- Daten erheblich häufiger lesen als schreiben.
- triviale Abfragen stellen:
  - Existenzanfrage
  - Attributanfrage (DN, Attribute) -> (Werte)
  - Objektauslese (DN) -> (Attribute, Werte)

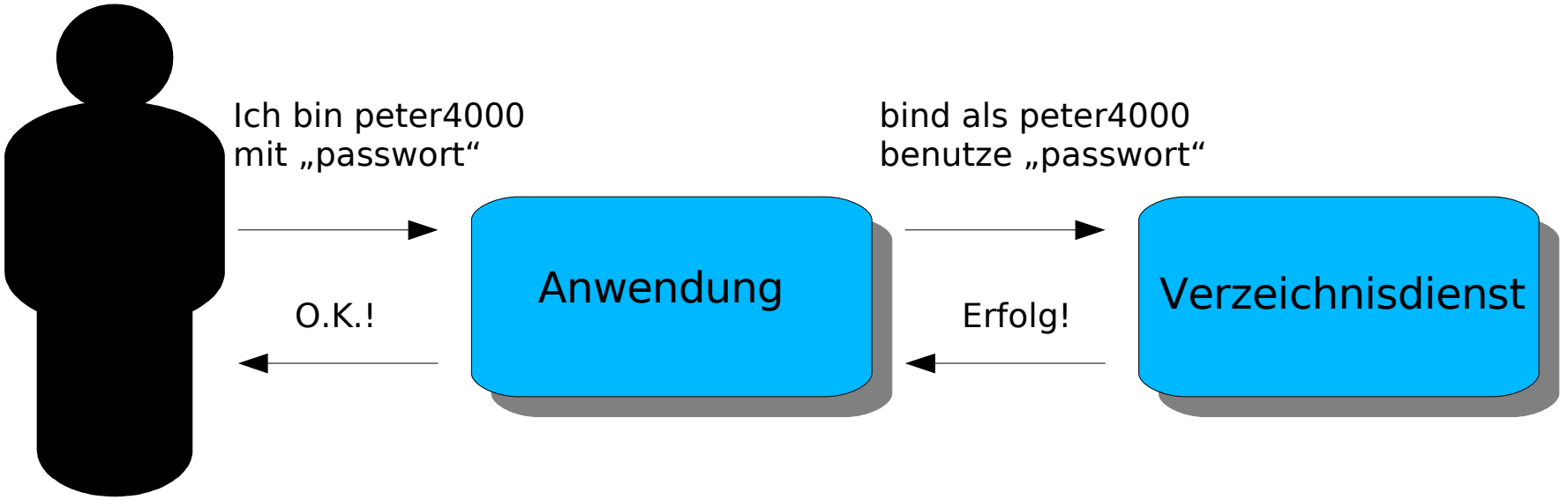
LDAP ist nicht geeignet für:

- Daten die Transktionssicherheit und referentielle Integrität erfordern.
- Zusammenfügen von Datensätzen.

Authentisierung als LDAP Nutzer



LDAP als Authentisierungsdienst



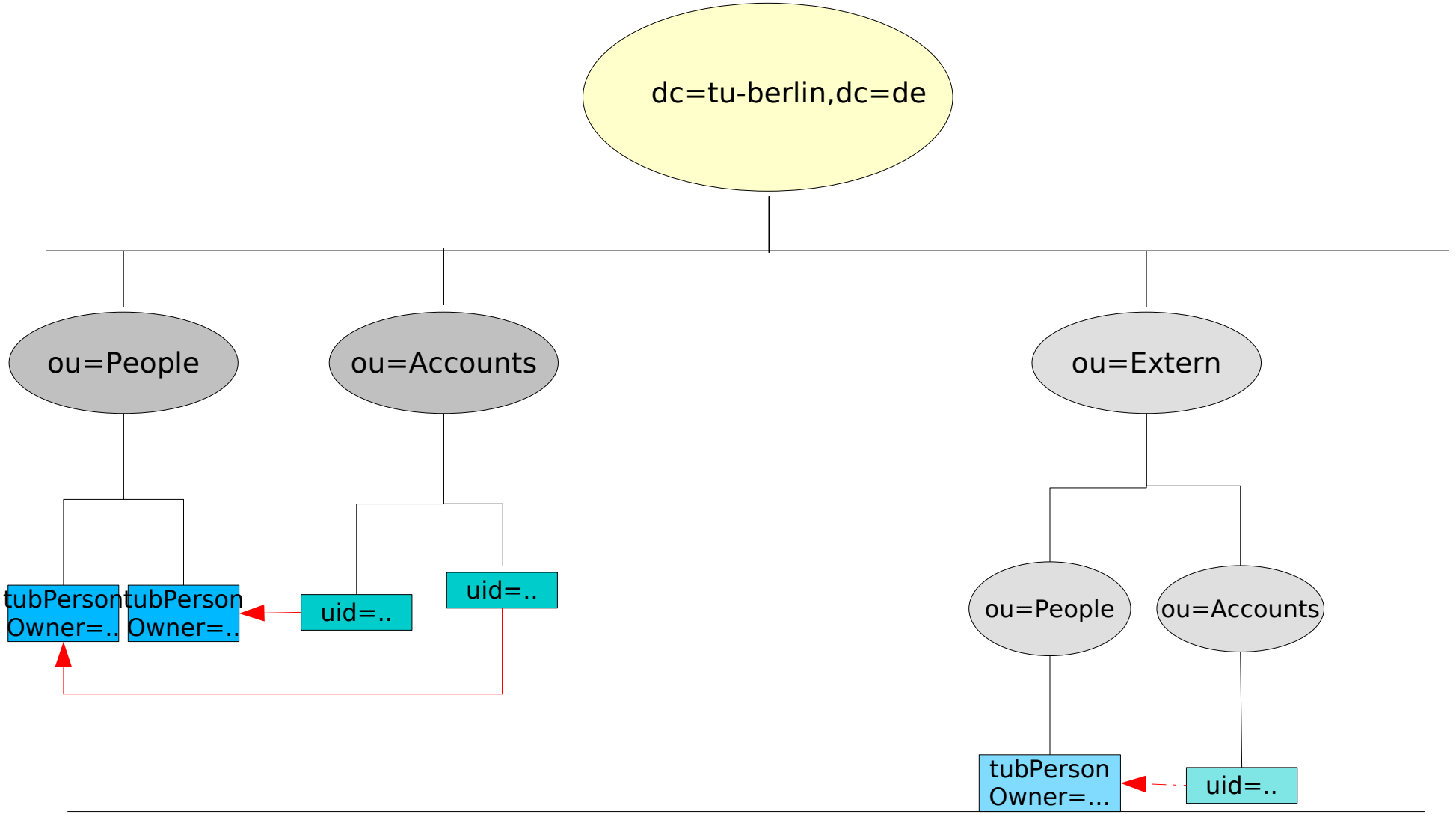
Authentisierungsmethoden:

- Simple Bind
  Authentisierung über einen Eintrag mittels DN und Passwort. Passwort geht ungeschützt über das Netz!

- Simple Bind mit TLS
  Vor dem Bind wird die gesamte Session verschlüsselt.

- Authentisierung über SASL
  SASL = Simple Authentication And Security Layer

tubIT LDAP


dc=tu-berlin,dc=de
ou=People
ou=Accounts
ou=Extern
tubPerson Owner=..
tubPerson Owner=..
uid=..
uid=..
ou=People
ou=Accounts
tubPerson Owner=...
uid=..

Accounteintrag:

```
dn: uid=peter4000,ou=Accounts,dc=tu-berlin,dc=de
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: tubAccount
uid: peter4000
uidNumber: 530
gidNumber: 100
cn: Peter Pan
homeDirectory: /home/users/p/peter4000
tubAccountOwner: tubPersonOM=16908001087,ou=People,dc=tu-berlin,dc=de
tubAccountStatus: aktiv
gecos: Peter Pan,E-N 50,24383
loginShell: /bin/sh
userPassword:: e2NyeXB0fW10dmlTeUhKdE9OLWs=
```

Personeneintrag:

```
dn: tubPersonOM=16908001087,ou=People,dc=tu-berlin,dc=de
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: eduPerson
objectClass: tubPerson
tubPersonOM: 16908001080
sn: Pan
cn: Peter Pan
eduPersonPrimaryAffiliation: 4000
eduPersonAffiliation: Mitarbeiter
givenName: Peter
tubPersonGender: m
```

Anschluß an den tubIT Verzeichnisdienst

- alle Besitzer eines tubIT Accounts können über den tubIT Verzeichnisdienst authentifiziert werden.
- Server: ldap.tu-berlin.de
- privilegierte Nutzer können Gast Accounts einrichten
  - Account berechtigt zur Nutzung von WLAN und WWW.
  - 21 Tage gültig, erlischt automatisch.

Fragen?

Ansprechpartner:

- Gerd Schering, schering@tubit.tu-berlin.de
  Tel.: 24383, Raum: E-N 007
  LDAP-Struktur und Konzeption

- Klaus Lemkau, Klaus.Lemkau@TU-Berlin.DE
  Tel.: 24229, Raum E-N K 044
  LDAP Betrieb

- Stefan Schnieber, Stefan.Schnieber@TU-Berlin.DE
  Tel.: 24383, Raum: E-N 007
  Kerberos