Einsatz von Verzeichnisdiensten in Großorganisationen

Ergebnisse einer
Voruntersuchung

April 1999

Dr. Horst Walther
SiG Software Integration GmbH

Inhaltsfolie

- Der Verzeichnisdienst - ein neues Element der Infrastruktur
- Was ist ein Verzeichnisdienst ?
- X.500 und LDAP - Wie kam es dazu?
- X.500 - Die Standard-Serie
- Nutzen - Was bringen Verzeichnisdienste?
- Einsatz - Wie lassen sich Verzeichnisse nutzen?
- Wie lassen sich Verzeichnisse integrieren?
- Wie wirken Meta-Verzeichnisdienste?
- Das Integrationswerkzeug Metaverzeichnisdienst
- Wohin geht der Markt?
- Markt - Wie ist das Angebot positioniert?
- Wo liegt der Bedarf?
  - E-Mail-Adressen
  - Berechtigungen
  - Zertifikate
- Projektaktivitäten

Verzeichnisdienst - ein neues Element der Infrastruktur

- Ein Verzeichnisdienst ist eine wichtige Infrastrukturkomponente für viele betriebliche Anwendungen ...

Er ...

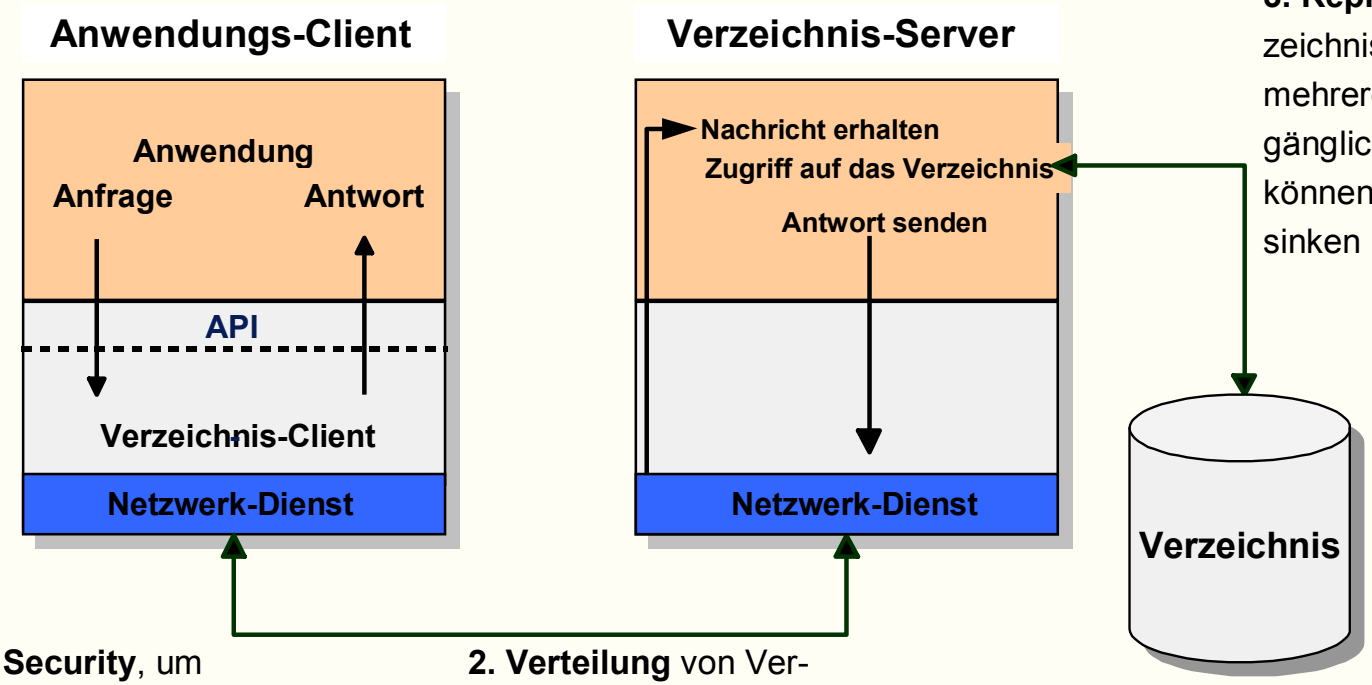
- **wird von jeder Anwendung genutzt.**
- **ermöglicht die Pflege von Informationen an einer einzigen Stelle.**
- **bietet eine universelle, einfach zu bedienende Oberfläche für den Zugriff.**
- **ist im Intranet unverzichtbar.**

Fast jede Anwendung und jedes System verwalten heute noch ein eigenes Verzeichnis. Z.B.:

- **SAP:** Personalwesen, Benutzerverwaltung, Kreditoren, Debitoren, etc.
- **RACF:** Verwaltung der Zugriffsrechte von Personen und Rollen auf geschäftliche und technische Objekte
- **Windows NT:** Active Directory auch für **MS Exchange**
- **Lotus Notes:** Notes Namens- und Adressbuch, Zugriffs-kontrollisten der Datenbanken, etc.

Was ist ein Verzeichnisdienst ?

- Ein Verzeichnisdienst stellt der „Anwendungsumwelt“ ein Verzeichnis bereit.
- Dazu übernimmt er vier Aufgaben ...



3. Replikation von Verzeichnissen, damit sie mehreren Benutzern zugänglich gemacht werden können und die Fehlerraten sinken

1. Security, um Informationen vor Eindringlingen zu bewahren

2. Verteilung von Verzeichnissen über entfernte Computer in einem Netzwerk

4. Partitionierung von Verzeichnissen zur Verteilung auf verschiedene Speicher bei einer großen Anzahl an Objekten

X.500 und LDAP - Wie kam es dazu?

Mit X.500 wurde 1993 der erste Standard publiziert.

X.500 ...

- ist ein ISO- (International Standards Organisation) und ITU- (International Telecommunications Union) Standard.
- beschreibt, wie globale Verzeichnisse strukturiert werden sollten.
- sieht eine hierarchische Organisation mit Levels für jede Informationskategorie (z.B. Land, Stadt, Organisation, ...) vor.
- unterstützt X.400 Systeme.
- ist das Ergebnis von Gremien-Arbeit der Telekommunikationsgesellschaften. (Top-Down-Prinzip)

Der umfassende Standard

LDAP ist der pragmatische Zugang der Internet-Gemeinde zu X.500.

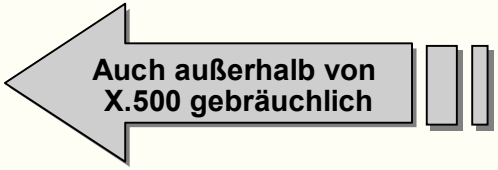
LDAP ...

- steht für Lightweight Directory Access Protocol und soll X.500/DAP ersetzen.
- entstand aus dem Bedarf, „schlanken“ Clients Zugriff auf X.500 zu ermöglichen.
- nutzt nicht das X.500 zugrundeliegende (mächtige) OSI-Protokoll, sondern das weit verbreitete TCP/IP.
- wird betreut durch die Internet Engineering Task Force (IETF). Interessierte können ihre Lösungen zur Standardisierung einreichen. (Bottom-Up-Ansatz)

Der leichte Zugang zu X.500

X.500 - Die Standard-Serie

- X.500 11/93 Überblick über Konzepte, Modelle und Dienste
- X.501 11/93 Modelle
- X.509 11/93 Authentisierungs-Framework
- X.511 11/93 Abstrakte Dienste Definition
- X.518 11/93 Verfahren für verteilte Verarbeitung
- X.519 11/93 Protokoll Spezifikationen
- X.520 11/93 Ausgewählte Attribut Typen
- X.521 11/93 Ausgewählte Objekt Klassen
- X.525 11/93 Replizierung
- X.581 11/95 Verzeichnis-Zugriffs Protokoll
- X.582 11/95 Verzeichnis-System Protokoll



Quelle: http://www.itu.ch/itudoc/itu-t/rec/x/x500up.html

Nutzen - Was bringen Verzeichnisdienste?

- Die Information im Verzeichnis kann verwendet werden, um ...
  - Anwender so zu **authentisieren**, daß sie sich mit einem Namen und Password bei verschiedenen Systemen anmelden können
  - Web-Seiten zu **personalisieren**
  - ein Network **Quality of Service** (QoS), z.B. Netzwerkbandbreite gemäß dem Status des Anwenders, aufzubauen
  - **Gruppenzugehörigkeiten** von sich anmeldenden Anwendern zu erkennen
  - Konfigurationsinformation netzwerkweit für den Travelling User bereit zu stellen
  - **Ereignisse** auszulösen. Ereignisse können z.B. das Ausscheiden eines Mitarbeiters, oder eine Beförderung sein

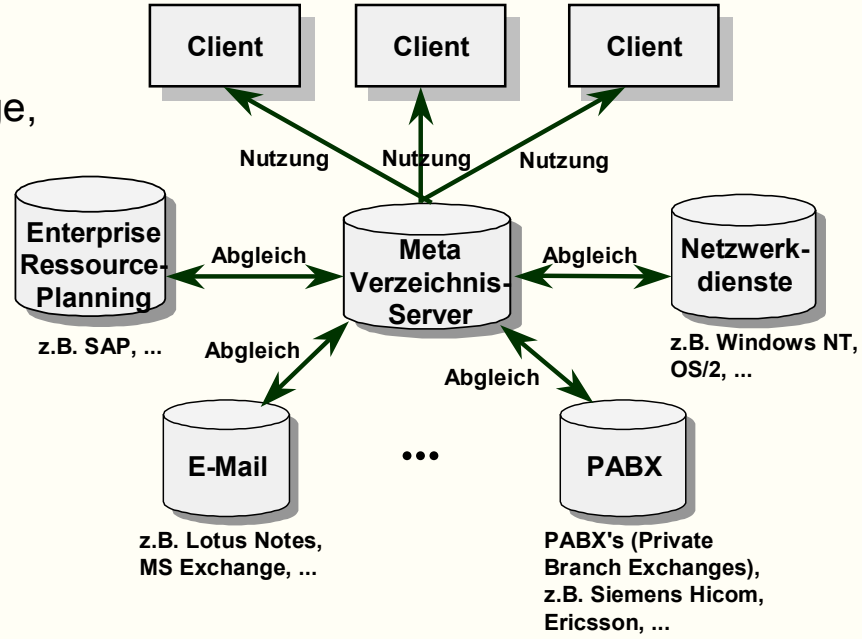
Einsatz - Wie lassen sich Verzeichnisse nutzen?

- Einige Standard-Produkte werden mit einem eigenen Verzeichnisdienst geliefert ...
  - **Microsoft** - Active Directory Service mit Windows 2000
  - **Lotus** - Domino Directory Service mit Lotus Domino 5.0
- **Vorhandene** - nicht genormte - Verzeichnisdienste werden weiter bestehen bleiben
- Das universelle Einheitsverzeichnis wird es nicht geben
  - Gruppenweit für eingeschränkte Informationssätze (E-Mail, Zertifikate, ...)
  - In eingeschränkten Bereichen (institutsweit) vollständige Informationssätze
- Wie lassen sich diese verschiedenen Verzeichnisdienste sinnvoll integrieren?

Wie lassen sich Verzeichnisse integrieren?

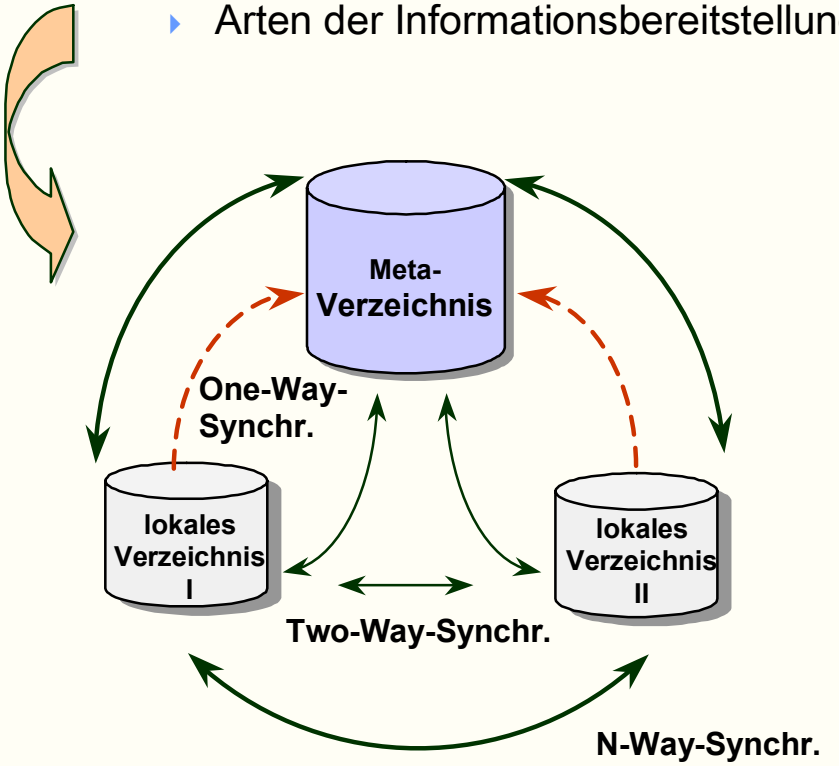
- Ein Metaverzeichnis kann Anwendungen mit konsistenten Informationen aus vielfältigen Datenquellen versorgen.

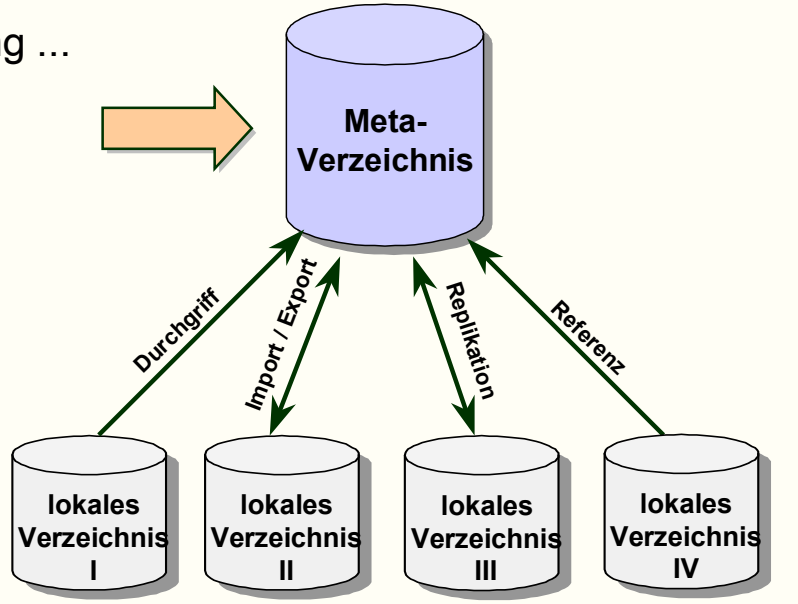
- Metaverzeichnisdienste ...
  - verfügen über Integrationswerkzeuge, die Aufgaben der Datenextraktion, -modifikation und -umformatierung übernehmen,
  - bestehen aus einem Verzeichnis-dienst und Werkzeugen für die Befüllung und Synchronisation,
  - erlauben die flexible Integration von Altanwendungen und Verzeichnisdienst.



Wie wirken Meta-Verzeichnisdienste?

- Metaverzeichnisse lassen sich klassifizieren nach ...
  - Wegen des Informationsflusses ...
  - Arten der Informationsbereitstellung ...

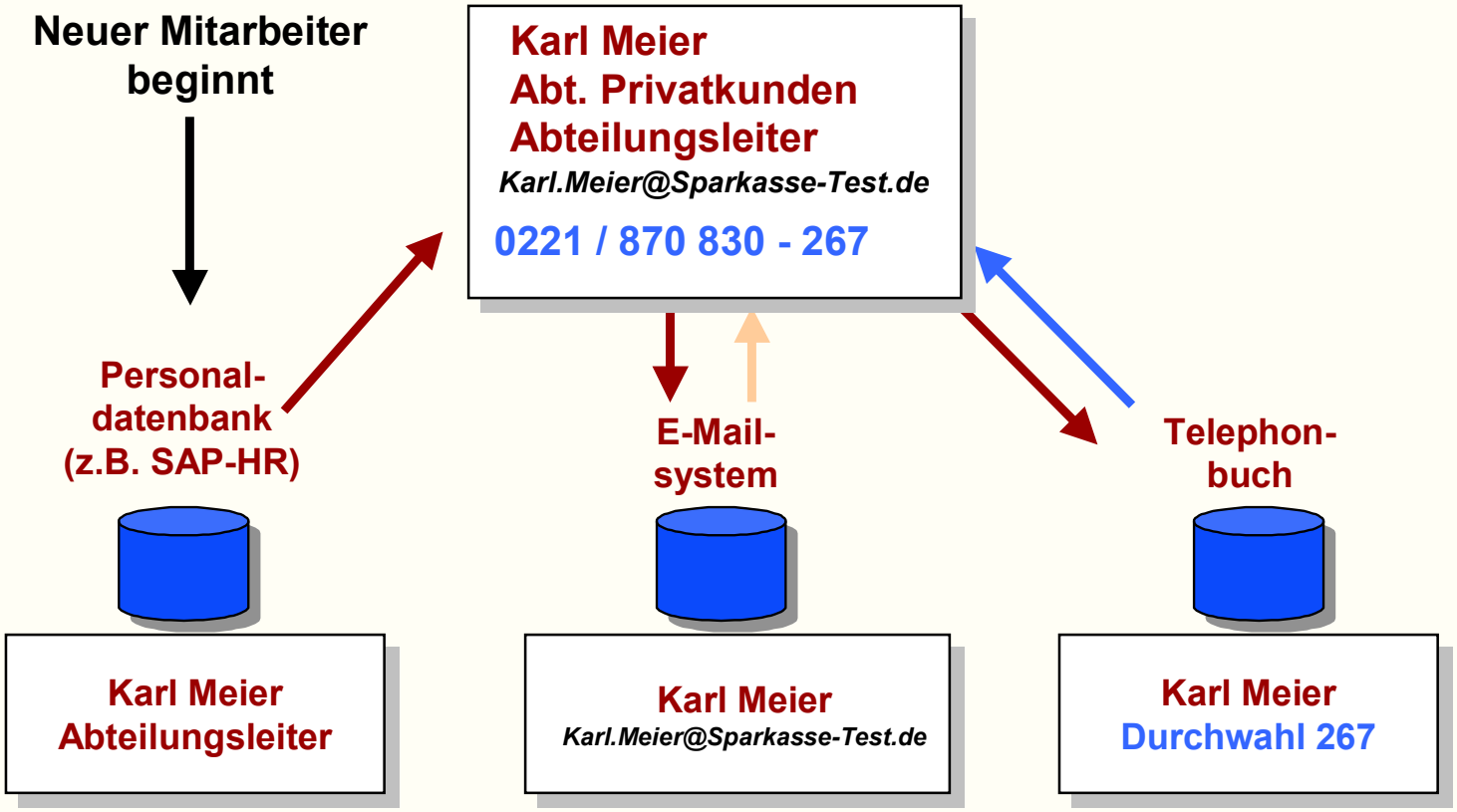




= Informationsfluss

Das Integrationswerkzeug Metaverzeichnisdienst

- Verzeichnisgestützte Abbildung von Abläufen



Wohin geht der Markt?

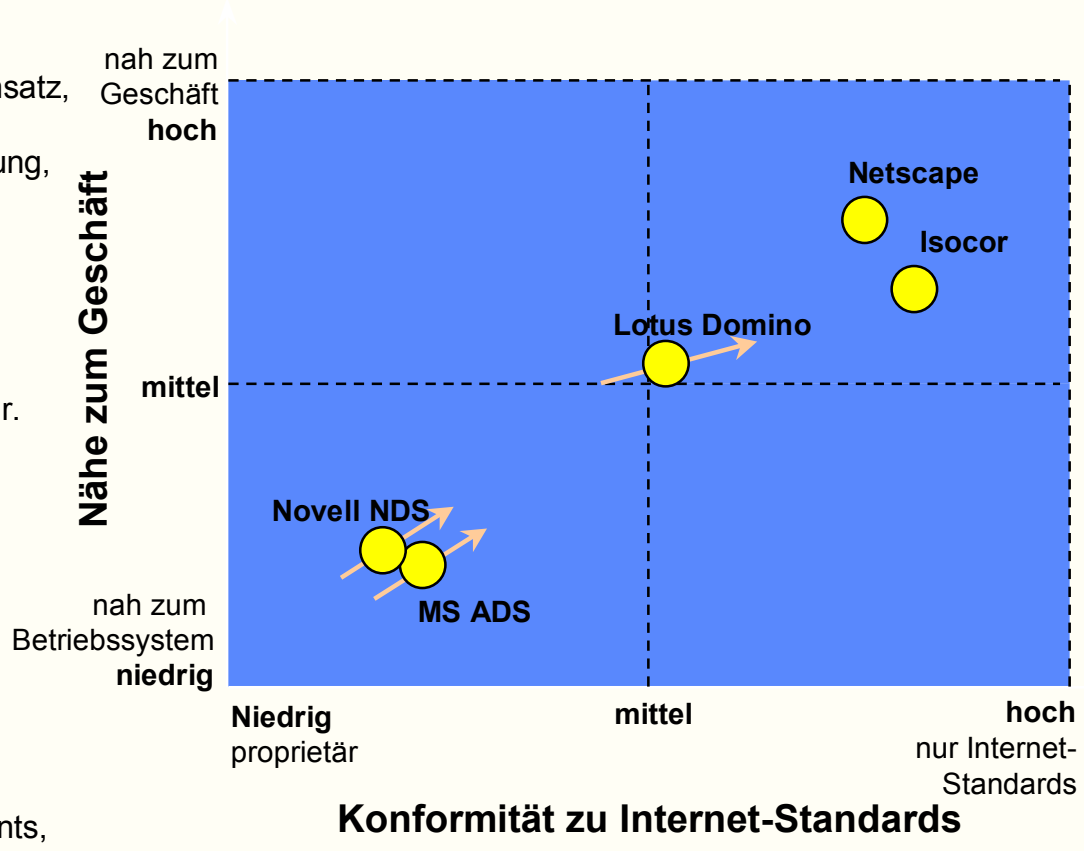
- Alle großen Hersteller haben die absolute Notwendigkeit der Unterstützung von Verzeichnisdiensten erkannt:
  - **Microsoft** verspricht mit der Integration von Active Directory Service (ADS) in Windows 2000 den „großen Wurf“.
  - **Novell** hat ihn mit der erstaunlichen Kombination Netware Directory Service (NDS) und dem Netzmanagement-Tool Z.E.N.works offenbar im Netware-Umfeld bereits gelandet.
  - **Netscape** hat ein sehr leistungsfähiges reines LDAP-Verzeichnis entwickelt und das eigene Geschäft darauf aufgebaut. Netscape propagiert Metaverzeichnisse.
  - **IBM** wird allmählich all seine Verzeichnisdienste und die darauf zugreifenden Anwendungen LDAP-fähig machen
  - Daneben ist mit dem Domain Name System (**DNS**) des Internet ein sehr leistungsfähiges Verzeichnis seit Jahren im harten Praxisbetrieb erprobt.

Verzeichnisdienste entwickeln sich zu einer notwendigen und selbstverständlichen Infrastrukturkomponente.

Markt - Wie ist das Angebot positioniert?

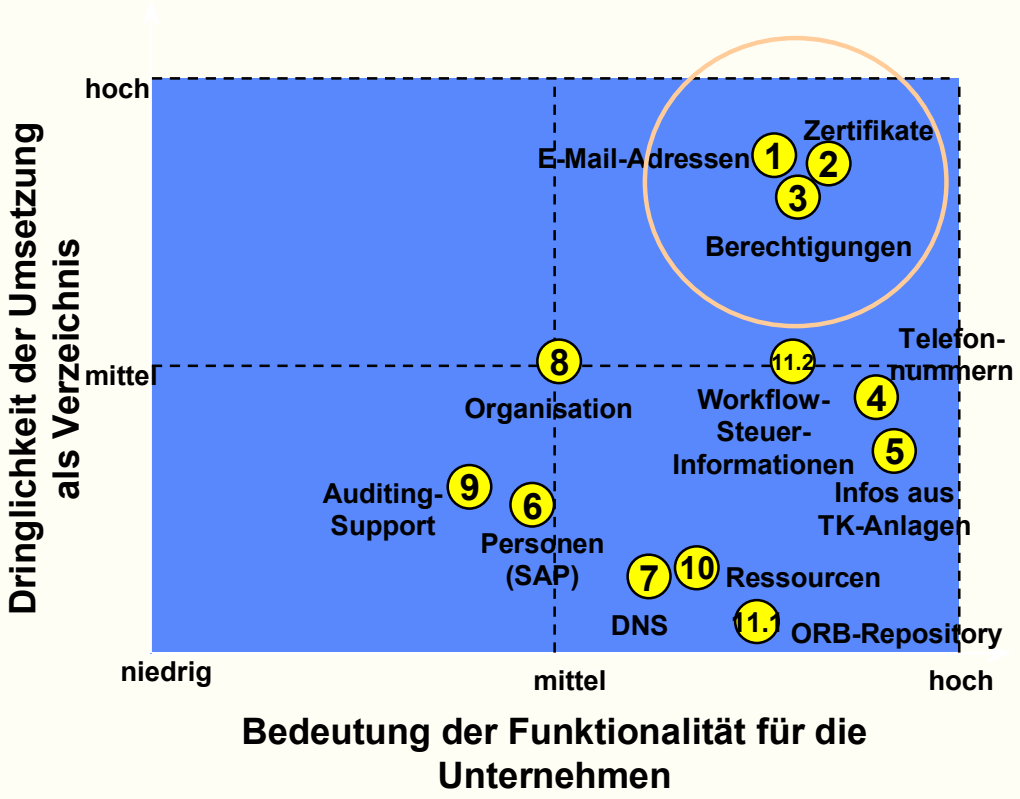
- Wie positionieren sich die Anbieter mit ihren Produkten?

  - **Netscape**
    Ausgeprägter Metadir.-Ansatz, Fokus auf eCommerce, Betonung der Außenwirkung, reiner Internet-Ansatz
  - **Lotus**
    Portabel und skalierbar, Bekenntnis zu Internet-Standards, auf dem Weg zum Metadir.
  - **Novell**
    Systemnah konzipiert. Stärken im Ressourcen-management durch Z.E.N.Works, Metadirectory als Ziel
  - **Microsoft**
    Teil von Windows2000, Inter-Verzeichnis-Kommunikation über Agents, Metadirectory als Ziel



Wo liegt der Bedarf?

Wir haben den Bedarf analysiert, potentielle Wirkungsfelder diskutiert und je nach **Bedeutung** und **Dringlichkeit** priorisiert ...



E-Mail-Adressen

- Durch die Zunahme der Bedeutung von E-Mails ist eine zentrale Verwaltung von E-Mail-Adressen erforderlich geworden:
  - zunehmend werden E-Mails innerhalb der Gruppe **systemübergreifend** versandt (Lotus Notes / MS Exchange)
  - auch der E-Mail-Verkehr mit **externen Partnern** und Kunden ist angestiegen
  - die E-Mail-Adresse eines Empfängers aus einer anderen Region ist beim Absender oft **nicht zugreifbar** und die Art der E-Mail-Adresse ist ihm meist **nicht bekannt** (Lotus Notes, X.400, SMTP)

Ein bundesweiter Verzeichnisdienst für E-Mail-Adressen erleichtert die Suche und automatische Übernahme der Empfängeradressen in E-Mails oder E-Mail-Verteilerlisten.

Berechtigungen

- Die zentrale Verwaltung von Berechtigungsprofilen (Rollen, Rechte, ...) enthält Informationen für Authentisierung, Autorisierung und Accounting
  - Das **Single-Sign-On** wird damit unterstützt
  - Von **Workflow**-Systemen werden diese Berechtigungsprofile benötigt

Notwendiger Bestandteil von plattformübergreifender logisch-zentraler Administration und logisch-zentralem **Auditing**

Zertifikate

- Das Deutsche Signaturgesetz schreibt ein öffentlich zugängliches Zertifikatsverzeichnis vor ...
  - Hohe Anforderungen an die Performance des Verzeichnisses (ca. 30 Millionen Einträge) und die Verfügbarkeit,
  - Zugriff auf das Verzeichnis über plattformunabhängige Clients: Browser, die über LDAP zugreifen,
  - Zugriff auf öffentliche Schlüssel (public key) sowohl von Personen, als auch von Software und Systemen (=Instanzen)

Dieser Verzeichnisdienst ist damit Teil einer umfassenden kryptographischen Infrastruktur (Public Key Infrastruktur, PKI)

Projektaktivitäten

- **Vorphase**
  - Vorgehen Entwurf
  - Vorgehen abgestimmt
  - Fragebögen, Termine
- **Hersteller-Workshops**
  - Netscape
  - Microsoft
  - Novell
  - Lotus
  - ISOCOR
  - (IBM)
- **Planung und Empfehlung**
  - Bewertung der WS
  - Empfehlung
  - Planung
  - Abstimmung
  - Präsentation