



A photograph of a smiling baby with dark hair, wearing an orange shirt and denim overalls, standing in a doorway. The background shows a building with large windows and a blue wall. Overlaid on the left side of the image is the text "Secure communication solutions" in blue.

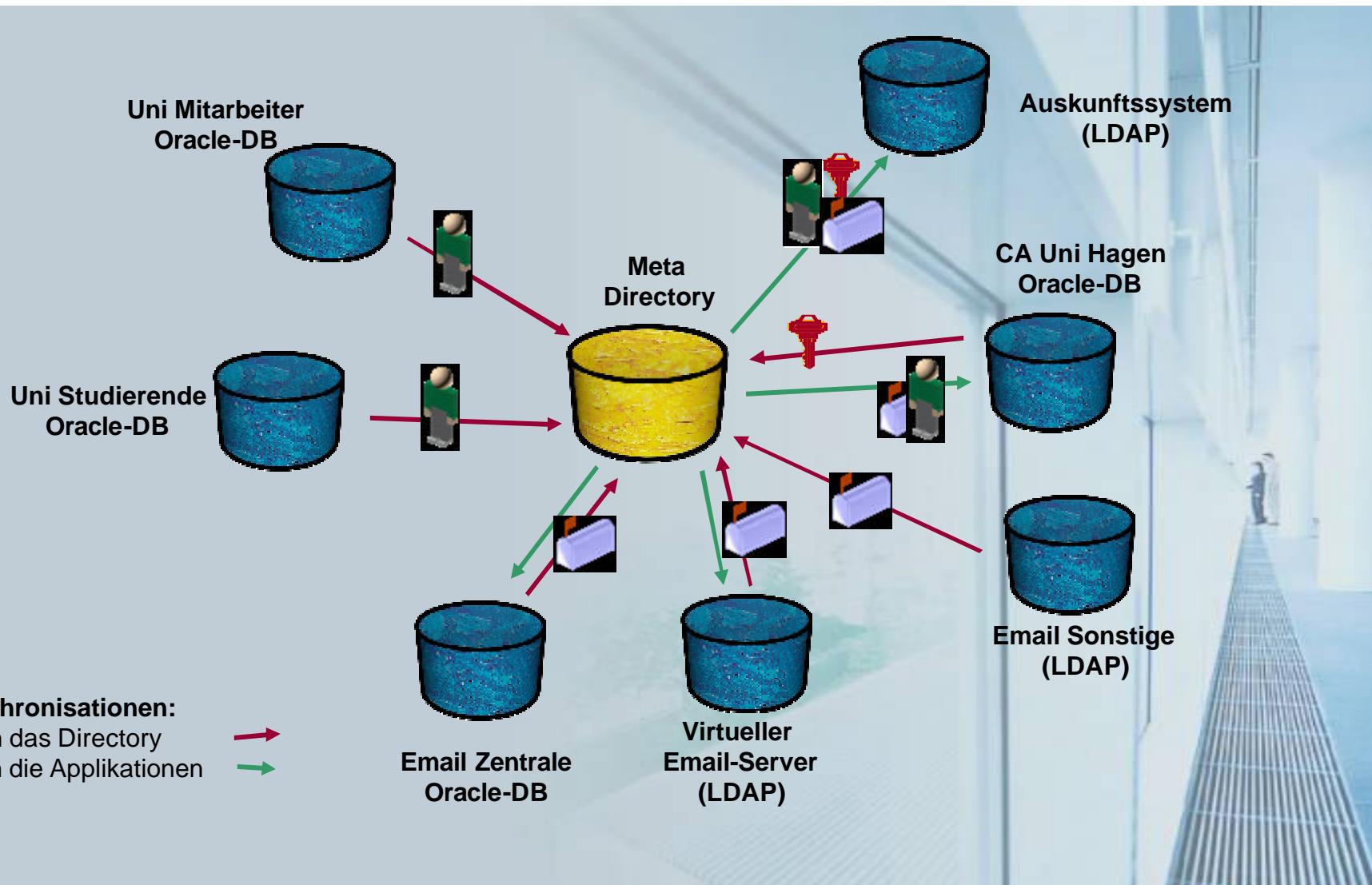
Secure
communication
solutions

Stand: 14. März 2005

Vorgehensweise, Konzept, PKI, DIT etc.

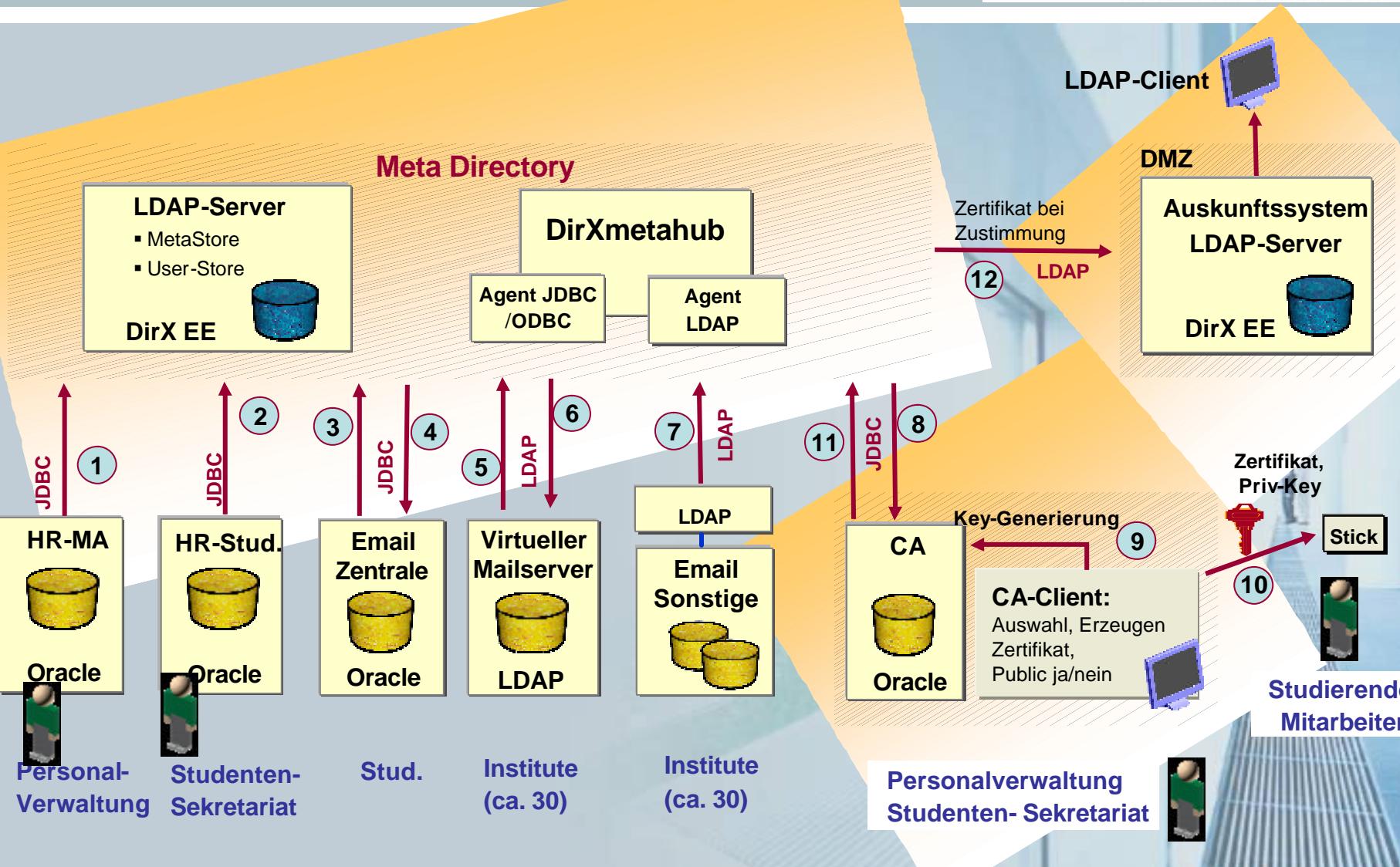
Meta Directory Uni Heidelberg

– Überblick Szenario



Meta Directory Uni Heidelberg

– Übersicht Stufe 1



Meta Directory Uni Heidelberg

– Datenflüsse (I)

1

Delta-Übernahme der Personaldaten von den Mitarbeitern bzw. Angestellten in das MetaDir, die von der Personalabteilung in der HR-Anwendung gepflegt werden; es werden keine Informationen zurückgeschrieben
Felder: Nachname, Vorname, Institut, Titel, Anrede, Anfangsdatum, Endesdatum, Geschlecht; Personalnummer

2

Übernahme der Personaldaten von den Studierenden in das MetaDir, die manuell vom Sekretariat in der HR-Anwendung gepflegt werden; es werden keine Informationen zurückgeschrieben.
Felder: Nachname, Vorname, Institut, Titel, Anrede, Anfangsdatum, Endesdatum, Geschlecht; Matrikelnummer
Besonderheit Trigger-Mechanismus: Nach Erfassung eines Datensatzes muss aus ORACLE ein Aufruf des runWorkflowTools von DirXmetahub erfolgen, damit der Einschreibende zeitnah sein Zertifikat ausgehändigt bekommt!

3

In der Regel ist das System Email Zentrale (ORACLE) das Mailsystem für Studierende (userid@ix.urz.uni-heidelberg), Matrikelnummer ist vorhanden; Mail-Adresse wird automatisch durch einen Prozess außerhalb vom MetaDir generiert und in Email Zentrale (ORACLE) abgelegt (Dieser Prozess soll erstmal bleiben). Übernahme der Mail-Adresse in das MetaDirectory über Matrikelnummer mit Systemquelle=Email-Zentrale.

Weiterhin sind auch alle MA des URZ in diesem Mailsystem, allerdings ohne Personalnummer, sondern mit einer Projektnummer (in der Regel mehrere Pro User). Für Erst-Initialisierung join evtl. über Nachname, Vorname, Institut. Personalnummer und/oder MetaID muss in ORACLE-DB übernommen werden (diese ist gleichzeitig primäre Personalnummer) -> evtl. manuelle Zuordnung bzw. Bereinigung erforderlich. Übernahme dann über diesen Identifier. Sinnvoll ist, den Status bzw. das liefernde Mailsystem zu merken.

Zuordnung von Institut zum zuständigen Mailsystem wird in einer separaten Tabelle geführt.

4

Evtl. zurückschreiben in ORACLE-DB die MetaID.

Meta Directory Uni Heidelberg

– Datenflüsse (II)

5

Auf dem virtuellen Mailserver der Zentrale sollen zukünftig möglichst viele der Instituts-Mitarbeiter verwaltet werden (heute ca. 30 von 60 Institute). Auf diesen Mailservers richten die Institute selbst ihre Mailsysteme ein und legen auch dort Benutzer und email-Adressen an, d.h. dieser Prozess soll auch erstmal bleiben (keine automatische Anlage von Mail-Accounts durch MetaDir).

Der Zugriff von MetaDir erfolgt nicht auf die einzelnen Mail-Server, sondern die Mail-Daten werden konsolidiert in einem LDAP-Server von der Uni Hd. bereitgestellt. Da die Personalnummer vorhanden ist, kann darüber die email-Adresse ins MetaDir geholt werden. Sinnvoll ist, den Status bzw. das liefernde Mailsystem zu merken.

Zuordnung von Institut zum zuständigen Mailsystem wird in einer separaten Tabelle geführt.

6

Evtl. zurückschreiben in ORACLE-DB die MetaID.

7

Alle Institute, die nicht auf dem virtuellen Mailserver der Zentrale abgedeckt sind, sondern auf einen eigenen Mailserver betreiben (ca. 30 Institute) können nur integriert werden, wenn sie ihre Daten über LDAP zur Verfügung stellen und die Email-Adresse die Personalnummer enthält (nur eine Email-Adresse!).

Zuordnung von Institut zum zuständigen Mailsystem wird in einer separaten Tabelle geführt.

Meta Directory Uni Heidelberg

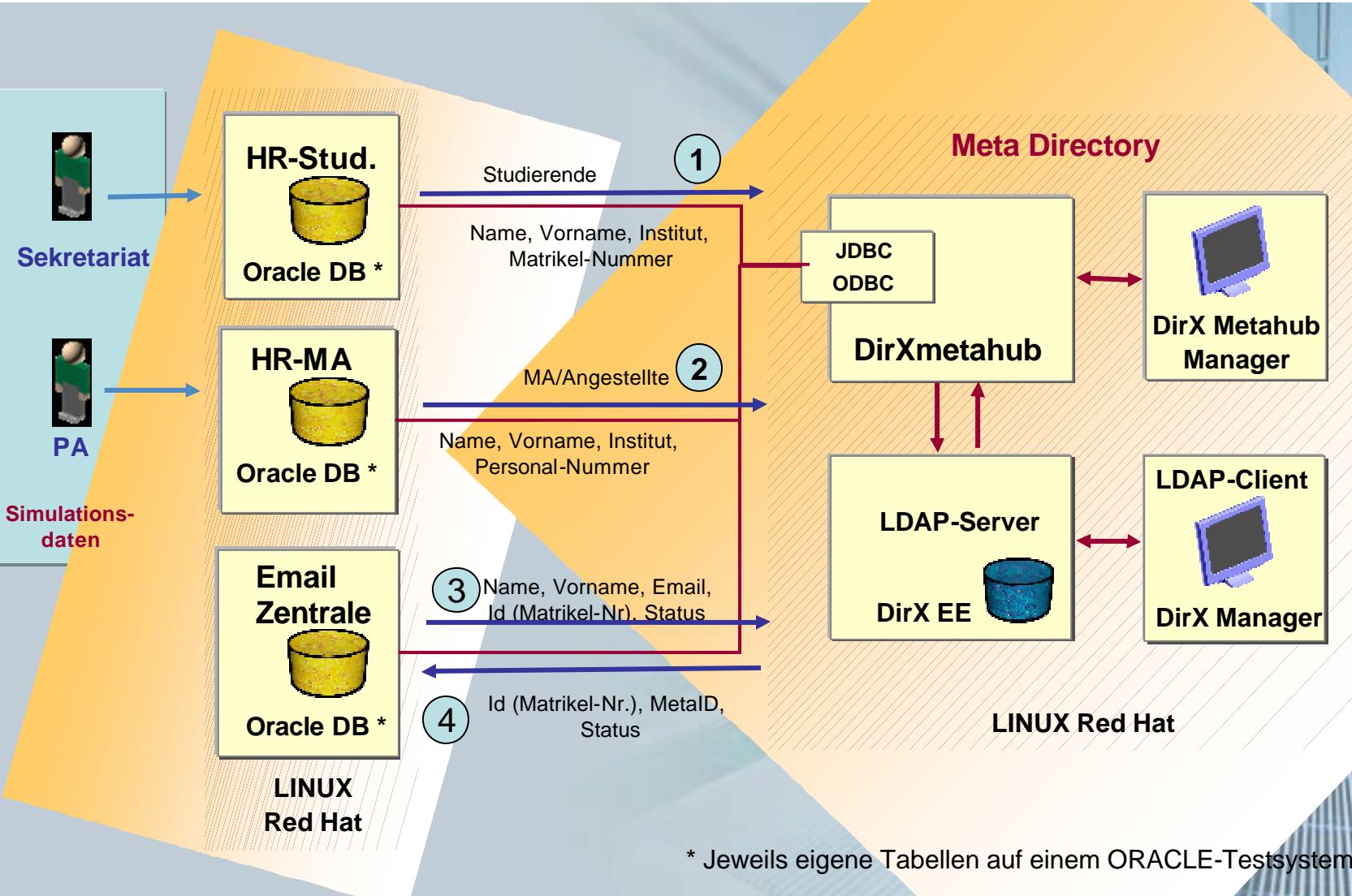
– Datenflüsse (III)

- 8 Anbindung der CA: Schreiben der Personendaten wie z.B. Nachname, Vorname, Institut, OU, uid, Typ und ID (Matrikelnummer/Personalnummer, dxmGuid) in die CA-Datenbank. Offen: MetaID oder Personal/Matrikelnummer als Identifier, oder sogar email-Adresse?
- 9 Anmelden am CA-Client mit uid/Passwort, dann Veröffentlichungsflag setzen und Freigabe; anschließend wird Zertifikat generiert und in CA-DB geschrieben
- 10 Nach Zertifikatsgenerierung schreiben des PrivatKey auf den Stick bzw. Diskette und Aushändigen an Anwender.
- 11 Anbindung der CA: Schreiben der Zertifikate inkl. Veröffentlichungsflag in das Meta Directory über die entsprechende ID. Anmelden am CA-Client mit der uid/Passwort, dann Veröffentlichungsflag setzen und Freigabe; anschließend wird Zertifikat generiert und in CA-DB geschrieben.
- 12 Synchronisation Personendaten aus Meta Directory in den Public-Certificate-Server (Auskunftssystem), für alle Personen, die das Veröffentlichungsflag auf yes gesetzt haben. Was ist mit CRL ?

Meta Directory Uni Heidelberg

– Überblick Teststellung

KARLS-UNIVERSITÄT
HEIDELBERG



* Jeweils eigene Tabellen auf einem ORACLE-Testsystem

Ziel und Definition Teststellung:

- Aufbau und Kennenlernen der Technologie auch für Uni; Erfahrungen Sammeln für das Produktionssystem
- Installation auf Universitäts-Plattform (LINUX; Red Hat); System ist vorbereitet
- Anbindung an Test-ORACLE-System mit ODBC-Agent oder JDBC-Agent für ORACLE; ORACLE-Datenbank auf separatem Testrechner
- Anbindung an Mail (ebenfalls in ORACLE)
- Testen Trigger-Mechanismus aus ORACLE (Anstoß nach Transaktion durch ORACLE, runWorkflow.bat von Metahub, techn. Voraussetzungen)
- Workflow zum Laden von Personaldaten (simulierte Testdaten), aber mit zeitlichen Anforderungen wie bei Studierenden.
- Terminabstimmung mit Hr. Lammarsch und Hr. Nippe
- Klären Remote-Zugang aus Siemens-Netz (ssh möglich von Seiten Uni)

Meta Directory Uni Heidelberg

– Funktionen Teststellung

1

Übernahme der Personaldaten von den Studierenden mit Simulationsdaten, die manuell in ORACLE eingepflegt werden. Definition der Felder durch Uni Heidelberg!

Besonderheit Trigger-Mechanismus: Nach Erfassung eines Datensatzes muss aus ORACLE ein Aufruf des runWorkflowTools von DirXmetahub erfolgen, damit der Einschreibende zeitnah sein Zertifikat ausgehändigt bekommt!

2

Übernahme der Personaldaten von den Mitarbeitern bzw. Angestellten mit Simulationsdaten, die manuell in ORACLE eingepflegt werden. Definition der Felder durch Uni Heidelberg!

3

4

Die Mail-Accounts der Zentrale werden ebenfalls in der ORACLE-Datenbank gespeichert. Bei diesem Workflow sollen die Möglichkeiten des Meta Directory getestet werden (z.B. für das Urladen ein Join versuchen über Nachname, Vorname, Institut oder falls vorhanden über Matrikelnummer; ein Zurückschreiben der Personalnummer bzw. Matrikelnummer für neue oder bisher noch nicht zugeordnete Einträge,)

DIT, DN, Zertifikatsaufbau



Directory Design

Beispiel Siemens Zertifikate

Zertifikatsangaben

Subject: dirxit=<Directory-ID>,SURNAME=Staehler,GIVENNAME=Ruediger,o=Siemens

Issuer: ...

Validity from

.....

Ablage im internen Directory

DN: CN=Staehler Ruediger,l=FFM,ou=RD,ou=Siemens,c=de
dirxit=<Directory-ID>
cn=Staehler Ruediger
commonNameNational: Stähler Rüdiger
givenName=Ruediger
givenNameNational=Rüdiger
sn=Staehler
userCertificate:

Ablage im öffentlichen Directory

DN: uid=<gehaschte Directory-ID>,ou=Siemens,o=Trustcenter
Mail: ruediger.staehler@siemens.com
uid: <Directory-ID>
userCertificate:

Directory Design

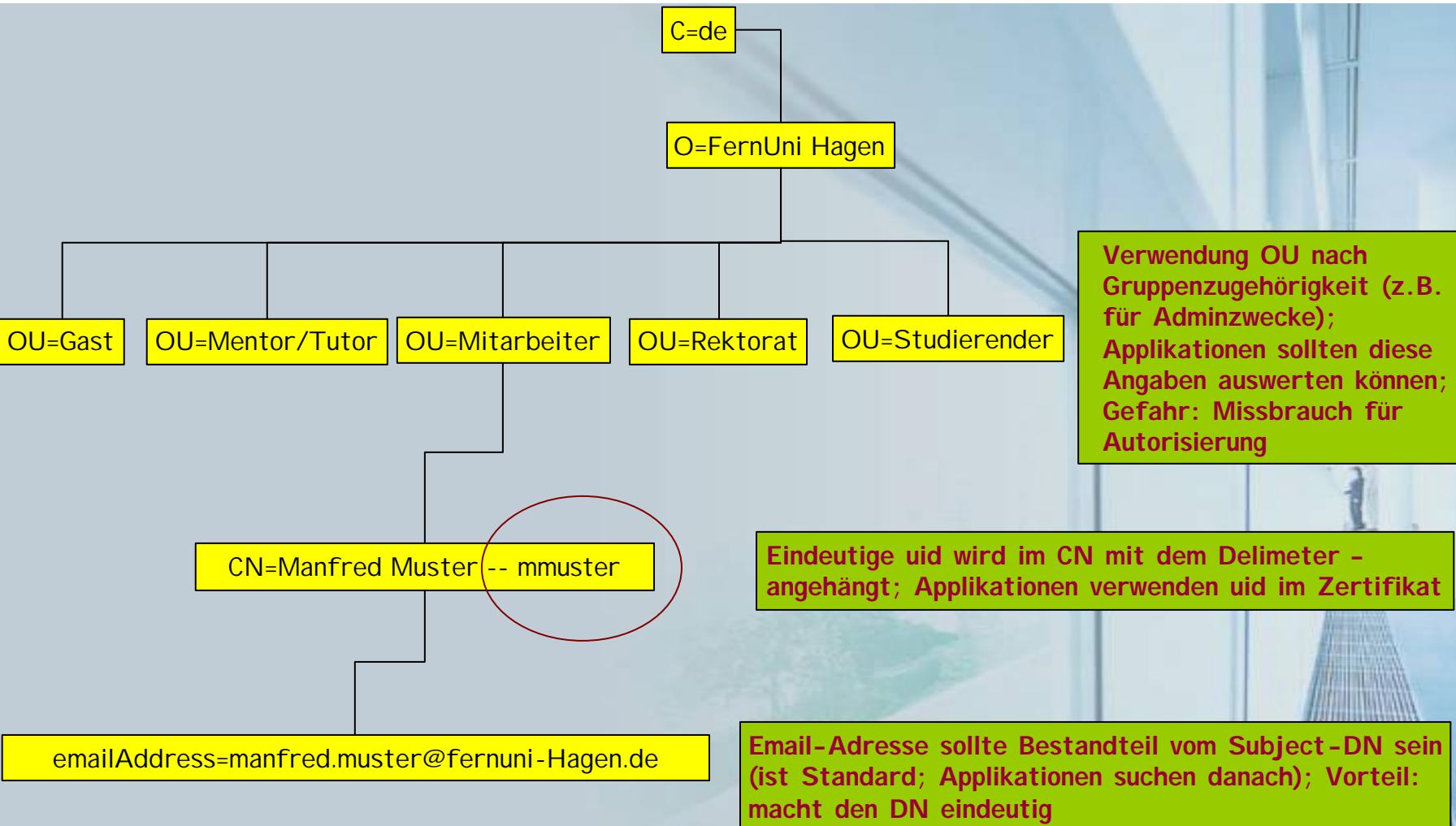
Felder in der CA-Datenbank

Name	Null?	Type
USERID	NOT NULL	VARCHAR2(15)
LASTNAME	NOT NULL	VARCHAR2(50)
FIRSTNAME		VARCHAR2(50)
EMAIL	NOT NULL	VARCHAR2(512)
PASSWORD	NOT NULL	VARCHAR2(16)
PECULIARITY	NOT NULL	CHAR(1)
ISSUETIME	NOT NULL	VARCHAR2(14)
PRINTTIME	NOT NULL	VARCHAR2(14)
PRINTSTATUS	NOT NULL	CHAR(1)
SPERRE		CHAR(1)
RES0		CHAR(1)
RES1		CHAR(1)
RES2		VARCHAR2(32)
RES3		CHAR(1)
RES4		VARCHAR2(64)

Verwendung der uid im CN ist in der Admin-Oberfläche generell einstellbar;
Applikationen greifen auf die uid direkt im Zertifikat zu; mit der uid melden sich die Anwender auch an CA an (z.B. um online Zertifikate zu beantragen)
Bei Mitarbeitern steht dort der Anmeldeaccount, bei Studierenden die Matrikelnummer

Directory Design

Subject-DN im Zertifikat Uni Hagen



Directory Design

Subject-DN im Zertifikat

Der DN in einem Zertifikat muss nicht identisch sein mit dem DIT-DN des Objektes im Directory.



Empfehlung: Keine Sonderzeichen im Subject-DN (wg. Applikationen)



C=de

O=Universitaet Heidelberg

OU=Mitarbeiter

OU=Gast

OU=Studierender

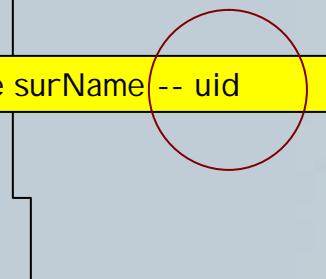
So ist der Einstieg der Root-CA der Uni Heidelberg!



Verwendung OU noch offen;



CN=givenName surName -- uid



Offen ist noch, ob eine ID als eindeutiger Identifier im CN aufgenommen werden soll: entweder MetaID, Matrikelnummer ?
Achtung: uid ist der Anmeldename für CA!!



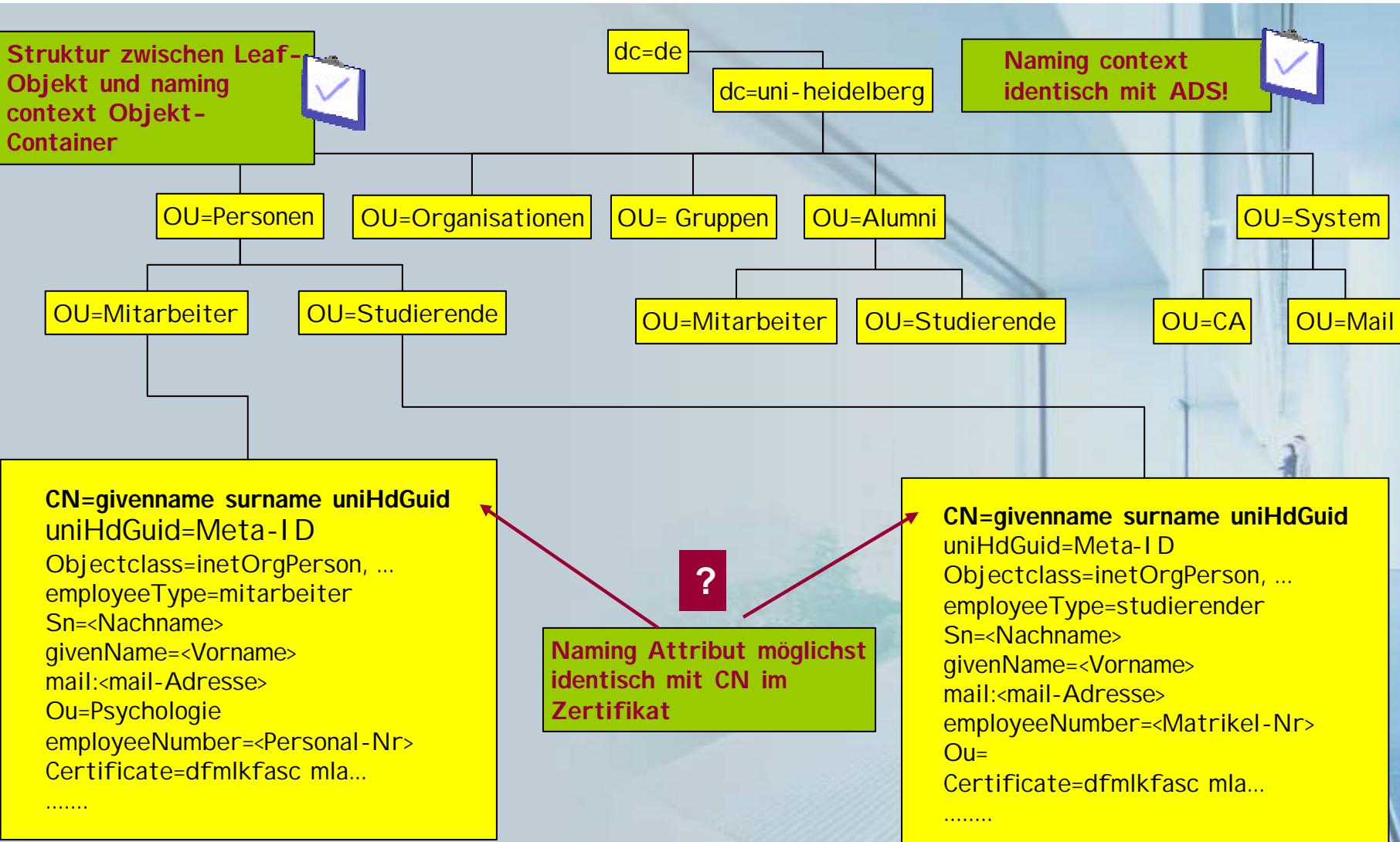
emailAddress=<mail-Adresse>

Email-Adresse sollte Bestandteil vom Subject-DN sein (ist Standard; Applikationen suchen danach)



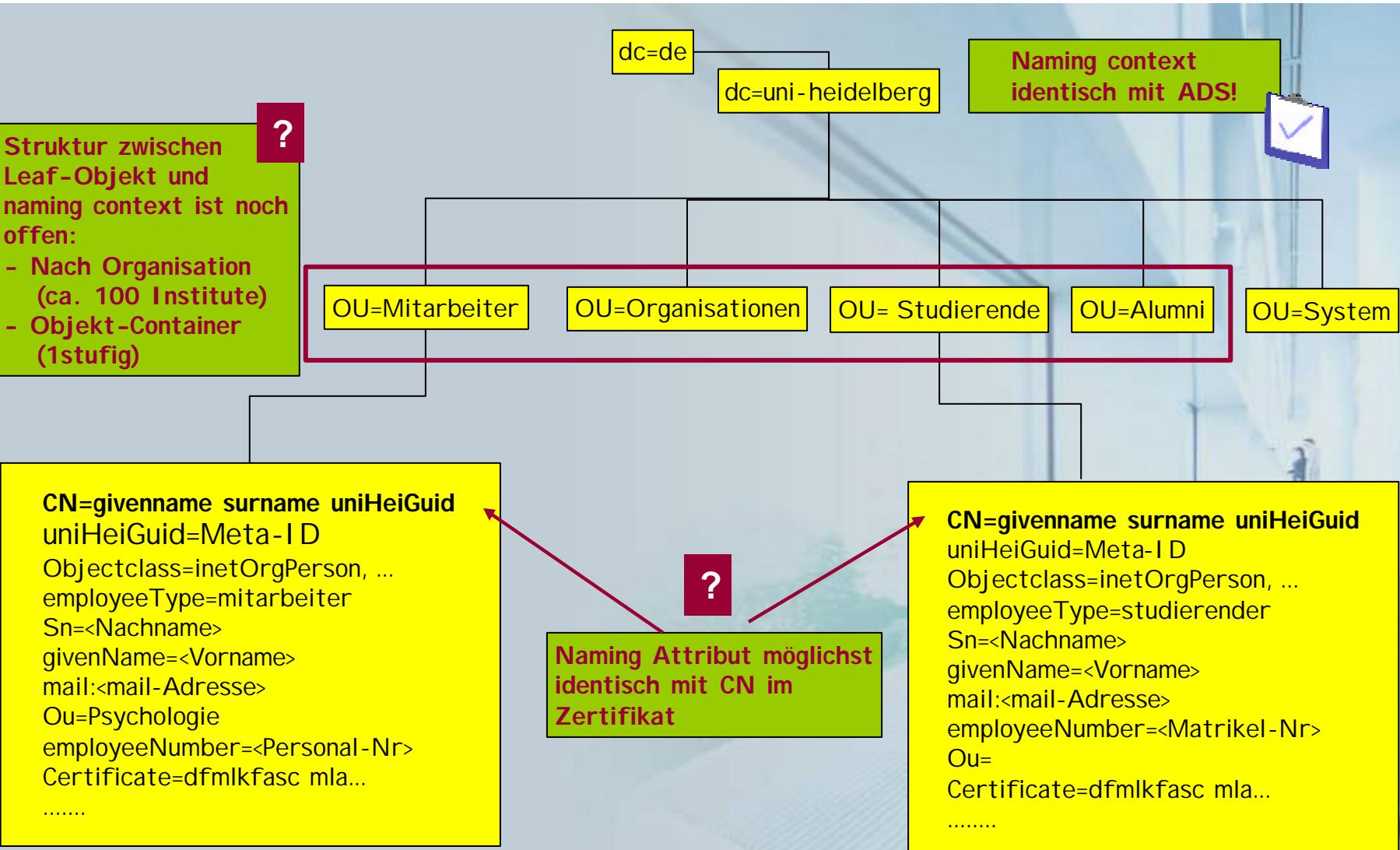
Directory Design

DIT Variante 1 (nach Objekten 2stufig)



Directory Design

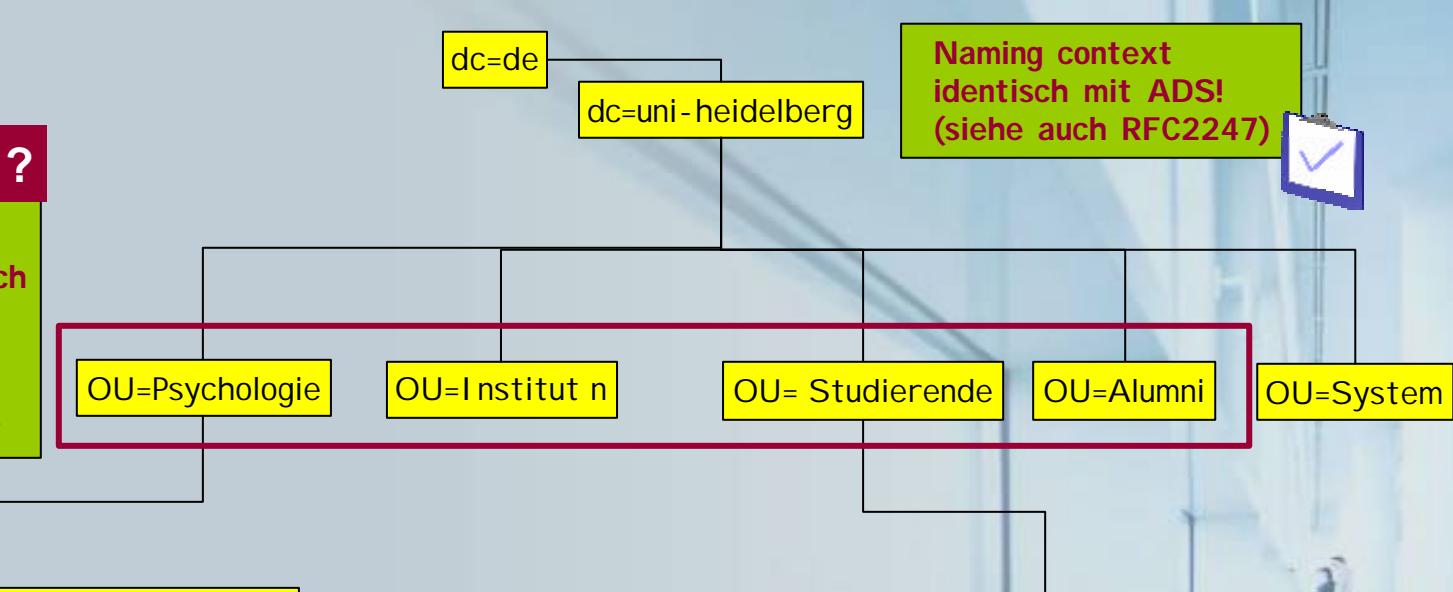
DIT Variante 2 (nach Objekten 1stufig)



Directory Design

DIT Variante 3 (nach Organisation)

Struktur zwischen Leaf-Objekt und naming context ist noch offen:
- Nach Organisation (ca. 100 Institute)
- Funktions-Container



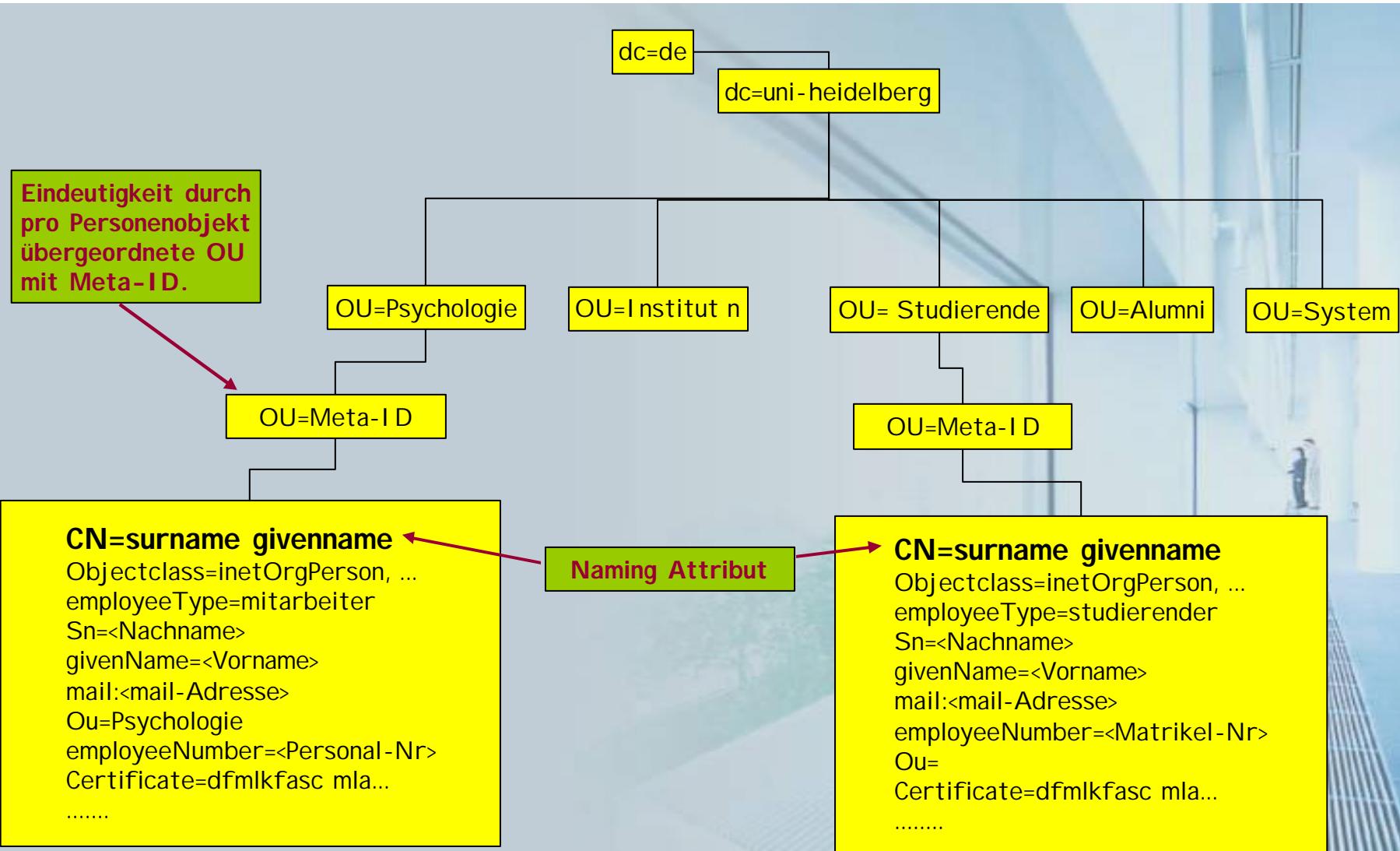
CN=givenname surname uniHeiGuid
uniHeiGuid=Meta-ID
Objectclass=inetOrgPerson, ...
employeeType=mitarbeiter
Sn=<Nachname>
givenName=<Vorname>
mail:<mail-Adresse>
Ou=Psychologie
employeeNumber=<Personal-Nr>
Certificate=dfmlkfasc mla...
.....

Naming Attribut möglichst
identisch mit CN im
Zertifikat

CN=givenname surname uniHeiGuid
uniHeiGuid=Meta-ID
Objectclass=inetOrgPerson, ...
employeeType=studierender
Sn=<Nachname>
givenName=<Vorname>
mail:<mail-Adresse>
employeeNumber=<Matrikel-Nr>
Ou=
Certificate=dfmlkfasc mla...
.....

Directory Design

DIT Variante 4 (ID als Container)



Gliederung nach Objekttypen Variante 1 oder 2:

(ou=personen ou=gruppen ou=Organisationseinheiten)

Vorteile:

- DIT ist relativ stabil, organisatorische Umstrukturierungen führen nicht zu einem Modify-DN, die in einem Directory vermieden werden sollten. Falls man im Directory Beziehungen zwischen Objekten über deren DN macht, ist ein stabiler DIT mit wenigen DN-Änderungen wichtig.
- Beim Anlegen der Objekte, die aus den HR-Systemen kommen, ist keine „Einsortierung“ in die verschiedenen Org-Einheiten (Institute) erforderlich (weniger Aufwand für die Realisierung, keine Pflege von separaten Tabellen für die Einsortierung)
- Eine Person eines bestimmten Typs (Mitarbeiter, Studierender) kann in mehreren Instituten vorkommen (Eindeutigkeit Personalnummer?)
- Zukünftige Anforderungen zur Aufnahme von weiteren Objekten (z.B. Organisationseinheiten, Accounts, Standorten) ist jederzeit flexibel und unabhängig von den Personen-Objekten möglich. Evtl. notwendige Verknüpfungen (Verlinkungen des DNs) zwischen den Objekten können über entsprechende Workflows umgesetzt werden.
- Gängige Praxis in den meisten Directory-Projekten (Unis, Industrie, ...)

Gliederung nach Objekttypen Variante 1 oder 2:

(ou=personen ou=gruppen ou=Organisationseinheiten)

Nachteile:

- Kein „schöner“ bzw. aussagekräftiger Baum -> aber: i.d.R. wird der Baum an der Oberfläche gar nicht angezeigt, sondern die Suche erfolgt über Attribute.
- eigene Berechtigungsstrukturen gemäß X.500 (ACIs) können nur pro Container festgelegt werden (eigene Autonomous Administrative Area AAA); somit könnte man keine AAA pro Institut umsetzen, um z.B. später einem Anwender zu erlauben, nur Objekte unterhalb seinem Institut zu verwalten. Die Frage ist, ob diese Berechtigungsstrukturen später wirklich benötigt werden (hängt davon ab, wie das zukünftige Identity Management – System integriert wird).
- Eine verteiltes X.500-Directory mit mehreren Rechnern ist nur auf Container-Objekte möglich; in der Praxis wird dieses verteilte X.500-Modell nicht mehr verwendet, sondern die Directories werden als Standalone-LDAP-Server aufgesetzt
- Suchanfragen an das Directory können nicht mit der Suchbasis auf Container (pro Institut) gesetzt werden; ich muss die Suchanfrage i.d.R. immer über den Naming context starten und über Attribute- oder Objektklassen-Filter die Treffermenge einschränken.

Verwendung metaID oder Personal-/Matrikelnummer als Eindeutigkeitskriterium?

Nachteile MetaID

- Mit der MetaID würde man eine zweite künstliche und technische Nummer einführen
- Höhere Anforderungen an Robustheit des Systems: ein neues Urladen der Daten erzeugt wieder neue MetaID zu einer Person!!!! Personal-/Matrikelnummer dagegen ist weiterhin in einem anderen System mit der Zuordnung zur Person vorhanden!
- Falls diese Nummer auch für die Eindeutigkeit im Zertifikat verwendet werden soll (Feld uid), dann müsste man sich als Anwender auch damit anmelden, um online Zertifikat zu beantragen

Nachteile Personal-/Matrikelnummer

- Matrikelnummer ist Teil des Passwortes bei Uni Heidelberg!
- Personal-/Matrikelnummer muss eindeutig für eine Person sein (evtl. auch mit Zusatzkennzeichen Institut)

RDN schön: cn= Nachname Vorname [ID]

Vorteile:

- Aussagekräftiger Name der Objekte im Directory -> aber: i.d.R. werden die RDNs der Objekte an der Oberfläche gar nicht angezeigt, sondern die Attribute.
- Spätere Zuordnungen zwischen Objekten (z.B. eine Person ist Mitglied in einer Gruppe über den DN) können besser und einfacher erkannt werden
- Administration auf reiner LDAP-Ebene zeigt gleich die richtigen Personennamen an (z.B. Liste mit den DNs)

Meta Directory Uni Heidelberg

– Entscheidungen für DN

	Zertifikat	Directory
Naming context	ok	ok
OU-Struktur	Empfehlung: Mitarbeiter/Studierende /Sonstige	Nach Objekttypen (DIT Variante 1)
Identifier für Eindeutigkeit	Inhalt von uid? Email-Adresse!	MetaID oder Personal-/Matrikelnummer
Naming Attribut	CN: Vorname Nachname Option: [-- uid]	CN oder ID Option: CN [ID]
Email als Teil des DN	Ja	nein

PKI-Integration mit Fernuni Hagen-CA

RUPRECHT-KARLS-UNIVERSITÄT
HEIDELBERG



Aktueller Stand FernUni Hagen

- Derzeitiges Verfahren zur Zertifikatsausgabe an Studierende ist konform zur DFN Basic Policy
- Die Beantragung und Ausgabe von Serverzertifikaten erfordert ein persönliches Erscheinen des Antragsstellers
- Derzeit wurden 500 Mitarbeiter mit Alladin eToken ausgestattet (wird von DFN-PCA neben Kobil mIdentity empfohlen)

Mögliche Ausprägungen für Uni Heidelberg

Eine Konformität zur DFN Classic Policy kann in folgender Weise erreicht werden

- 1) Identifikation des Benutzers im Studentensekretariat der Uni Heidelberg, Erzeugung und Übergabe des Schlüsselmaterials vor Ort
- 2) Identifikation des Benutzers im Studentensekretariat und persönliche Übergabe eines Pinbriefs (UserID, Passwort), Erzeugung des Schlüsselmaterials Remote auf dem Client des Antragsstellers

Anmerkung

Verfahren 1 ist vorteilhaft für die Ausgabe des Schlüsselmaterials auf Hardware Tokens (USB Token, Smartcard), Verfahren 2 ist vorteilhafter für die Ausgabe von Softtokens (näheres siehe folgende Seite)

Softtoken

Bei der Ausgabe von Softtokens ist es nicht empfehlenswert, die Zertifizierung vor Ort bei der Uni Heidelberg durchzuführen, da Zertifikate und Private Key im Browser des Clients gespeichert werden

- Rückstände im Browser müssen beseitigt werden
- Umständlicher Import/Export des Schlüsselmaterials aus dem Browser, Transport-PIN, ...
- Aufwendiger Rezertifizierungsprozess (Antragssteller muß erneut vor Ort erscheinen)

Mögliche Vorgehen falls Ausgabe von Softtokens vor Ort erfolgen soll:

- Der Antragssteller bekommt einen Pin Brief vor Ort
- Er meldet sich an einem separaten PC an der CA GUI an
- Das Zertifikat wird über die CA GUI beantragt
- Der Antragssteller exportiert das Schlüsselmaterial auf Diskette
- Der Antragssteller entfernt das Schlüsselmaterial aus dem Browser

USB Token/Smartcard

- Vor Ort Zertifizierung unkritisch, da Schlüsselmaterial die Smartcard nicht verlässt
- Aufwendiger Rezertifizierungsprozess (Antragssteller muß erneut vor Ort erscheinen)

Vor- und Nachteile der Verwendung der eMail Adresse als UserID in der CA

Für die Anmeldung an die CA (entweder durch User oder durch Sachberabeiter) ist immer eine UserID und ein Passwort erforderlich. Bei der Uni Hagen wird hierfür die Matrikelnummer für Studenten und bei Angestellten der globale Anmeldeaccount verwendet (vom Datenschutzbeauftragten abgesegnet). Weiterhin wird diese UserID auch an den CN im Zertifikats-DN angehängt.

Da die Verwendung der Matrikelnummer bei Uni Heidelberg kritisch gesehen wird, bliebe nur die MetaDirectory-ID. Die ist allerdings für den Anmeldevorgang an die CA sehr „kryptisch“. Von daher könnte auch die email-Adresse als Inhalt von UserID verwendet werden. Folge ist, dass pro User-Objekt im Directory genau eine zertifizierte email-Adresse vorhanden ist.

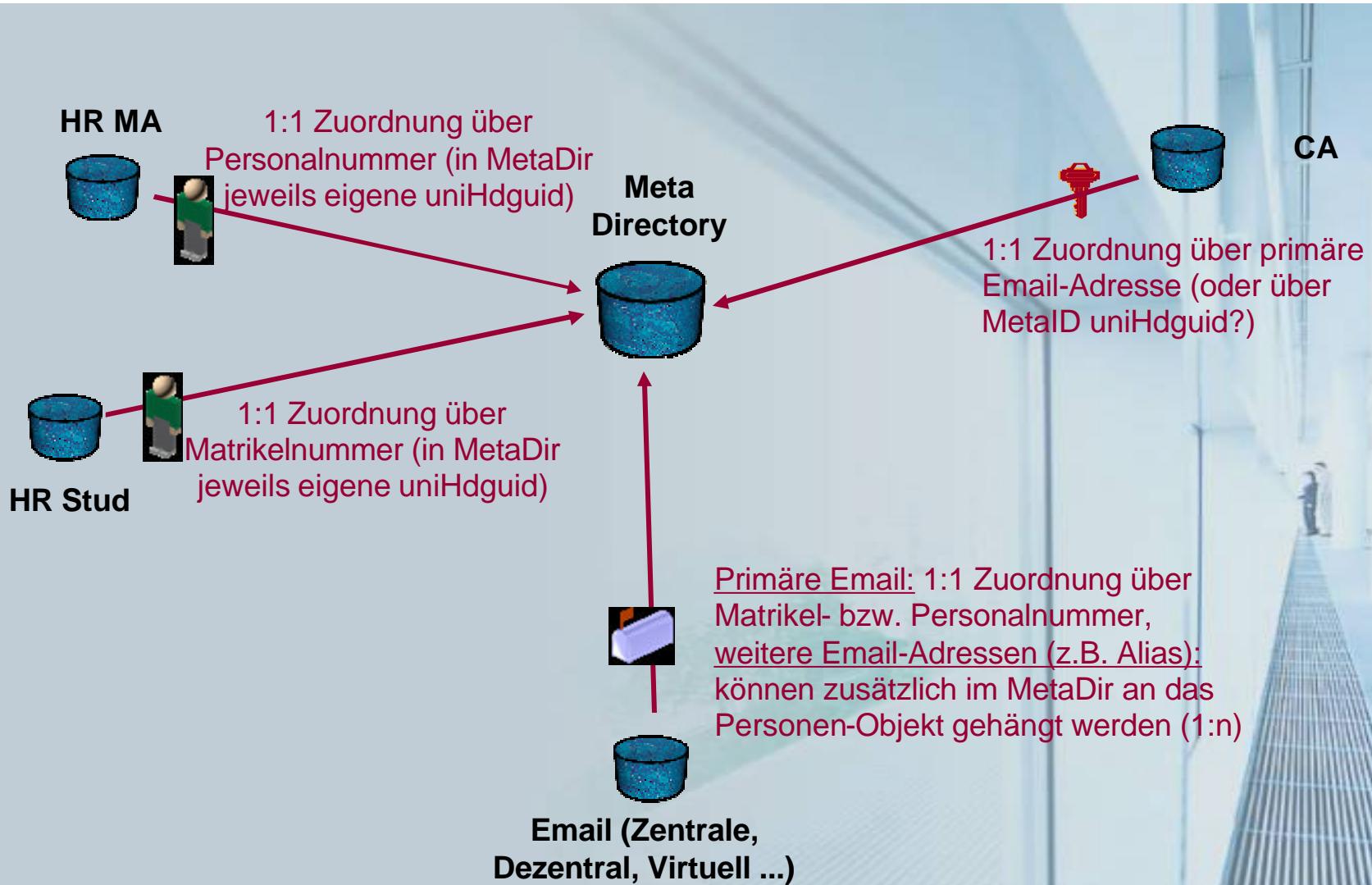
Pro:

- Email Adresse kann als Anmeldenamen für CA und andere Applikationen verwendet werden
- Email Adresse macht den Subject DN des Zertifikats ohnehin schon eindeutig
- Pro Email Adresse kann ein eigenes Zertifikat ausgestellt werden

Contra:

- userID als Bestandteil des CN im Zertifikat kann später für die Anmeldung an Applikationen nicht mehr verwendet werden (siehe Beispiel FernUni Hagen)
- Mit der MetaID im Feld UserID hätte man eine eindeutige Zuordnung zum Personen-Objekt im Directory

Zuordnungen und Beziehungen



Passwortgenerierung

Für die Initiierung der Zertifikatsgenerierung muss für den Benutzer durch das Metadirectory automatisch ein Passwort generiert und an die CA weitergegeben werden.

Pinbrief Druck

Die CA GUI muss um ein Schaltfeld für die Initiierung des Pinbriefdrucks erweitert werden. Als Trigger wird das Vorhandensein des Datensatzes und ein Flag verwendet, das anzeigt, dass der Pinbrief noch nicht erstellt wurde. Der Ausdruck muss folgende Informationen enthalten:

- Vorname, Name
- UserID = (z.B. Email Adresse)
- Passwort

Key Recovery

Ein Key Recovery wird durch die CA nicht unterstützt

Verwendung des OU-Felds im DN

Die Verwendung des OU-Felds wird empfohlen (zumindest Unterscheidung Mitarbeiter und Student)

- Erleichtert die Zuordnung von Zertifikaten
- Die CA ermöglicht die Verknüpfung von Berechtigungen an die OU-Zugehörigkeit

Zertifikatsserver - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Wechseln zu Links

Adresse: https://ca-test.fernuni-hagen.de/demo/start.php

home ca-key laden crl laden policy impressum

Zertifikatsserver

Hilfe zum Server

- Anleitung (PDF)
- Anleitung (Film)
- Supportanfrage

Zertifikat testen?

- zum Test

Password?

- zum Passwordantrag

Server-Zertifikat

- Server-Zertifikat beantragen

Server-Status

- Der Server ist betriebsbereit.



Zertifikatsserver

Der Server ist betriebsbereit.
Loggen Sie sich hier ein, wenn Sie ein Client-Zertifikat beantragen möchten.

User-ID: Password:

Anmelden

Anmeldung mit UserID und Passwort

Zertifikate suchen

Sie können hier nach Zertifikaten **anderer** Personen suchen, z.B. wenn Sie diesen Personen eine verschlüsselte E-Mail schreiben wollen.
Das Herunterladen des **eigenen** Zertifikats über diese Funktion ist nicht möglich.

Zertifikat suchen: gesuchter Name

Suchen



PKI Integration – Admin Oberfläche 1

Zertifikatsserver - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://ca-test.fernuni-hagen.de/demo-admin/config_edit.php

Firefox Help Firefox Support Plug-in FAQ

Zertifikatsserver Zertifikatsserver home logout

Zertifikatsserver

Authentisierung

- Import/Export/Löschen
- Daten bearbeiten
- Gruppen bearbeiten

Zertifikate

- Client-Zertifikate suchen
- Server-Zertifikate suchen
- Server-Zertifikat erstellen
- CRL ausstellen

Administration

- Konfiguration bearbeiten
- Datenbank-Statistik
- Webserver-Statistik

E-Mail-Adressen

Tragen Sie die E-Mail-Adressen der Server-Administratoren ein.

Alarmierung im Fehlerfall an...	webuser@kauri.fernuni-hagen.de
Absenderadresse für Alarm-E-Mails	caadmin@fernuni-hagen.de
Angefordertenungen für Serverzertifikate an...	caadmin@fernuni-hagen.de
Support-Anfragen an...	caadmin@fernuni-hagen.de

Session-Verwaltung

Definieren Sie Ihre Session-Umgebung:

Cookies erzwingen?

Ablaufzeit der Session auf Serverseite (in s): 300

Ablaufzeit der Cookies auf Clientseite (in s): 300

Updaten

Demo Package

Done ca-test.fernuni-hagen.de

PKI Integration – Admin Oberfläche 2

The screenshot shows a Mozilla Firefox browser window displaying the 'Zertifikatserver' configuration page at https://ca-test.fernuni-hagen.de/demo-admin/config_edit.php. The interface includes sections for 'Erweiterte Konfiguration' and 'Server-Design'. A blue box highlights the 'Anzeige User-ID im Zertifikat' checkbox under 'Erweiterte Konfiguration'. Another blue box highlights the 'Logo hochladen' button under 'Server-Design'. A third blue box highlights the 'Ausgangsdesign herstellen' button under 'Server-Design'. A fourth blue box highlights the 'Anpassbar auf Layout der Uni Heidelberg' text under 'Server-Design'. A fifth blue box highlights the 'Zertifikats Veröffentlichung' section.

Zertifikatserver - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://ca-test.fernuni-hagen.de/demo-admin/config_edit.php

Anzeige User-ID im Zertifikat

Erweiterte Konfiguration

Definieren Sie die Server-Umgebung:

- Anzeige der User-ID im Zertifikat
- Umlaute im Zertifikat zulassen
- Nutzer muss Veröffentlichung seines Zertifikats zustimmen
- Admin darf Passwords der Benutzer sehen

Zertifikats Veröffentlichung

Server-Design

Laden Sie Stylesheets und Logos (ausschließlich PNG-Format) hoch:

- Style-Sheet hochladen
- Logo hochladen
- Ausgangsdesign herstellen

Anpassbar auf Layout der Uni Heidelberg

Done

ca-test.fernuni-hagen.de