



IDS Niedersachsen

Klaus Scherbach

Senior Consultant

Sun Microsystems



Agenda

- Ziele des Identitäts-Managements
- Ist-Zustände im Überblick
- Soll-Konzepte
- Proof of Concept

Ziele (1)

- **Unique ID**
 - Schaffung einer elektronischen Identität
 - Identitätsaustausch innerhalb einer Universität
 - Identitätsaustausch zwischen Universitäten
- **Roaming**
 - Zugriff auf Dienste anderer als nur der "Heimat-Universität"
 - Unique ID incl. Password-Synchronisation erleichtert dies dem Nutzer („simplified Logon“)
- **SSO**
 - nur einmalige Authentifizierung in einer IT-Umgebung
 - erleichtert den gleichzeitigen Zugriff auf mehrere Services/Applikationen/ Systeme
 - denkbar auch Universitäts-übergreifend

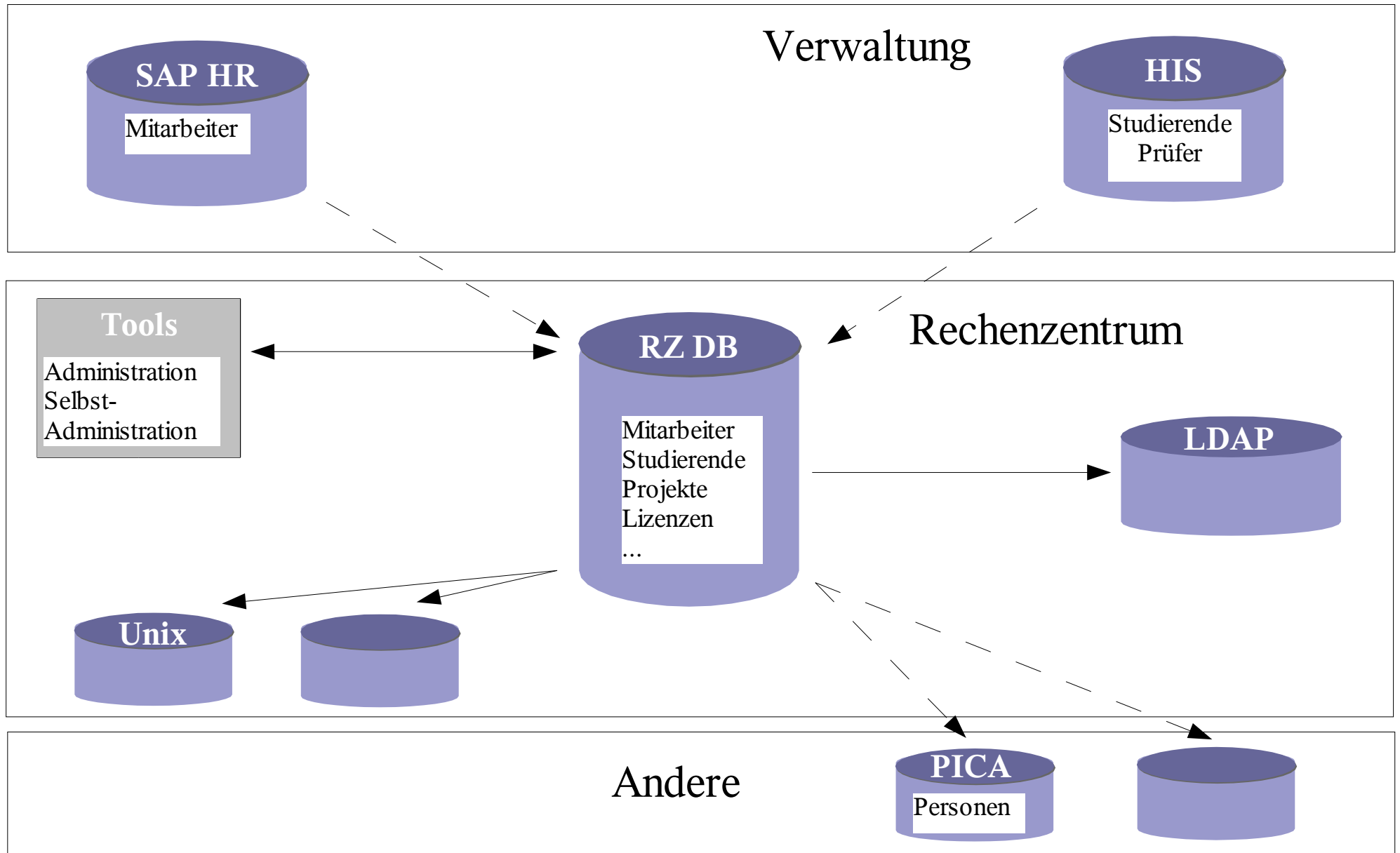
Ziele (2)

- Berechtigungen
 - Verbindung einer elektronischen Identität mit Rechten
 - Austausch von Berechtigungs-Informationen innerhalb einer Universität
 - Austausch von Berechtigungs-Informationen zwischen Universitäten

Agenda

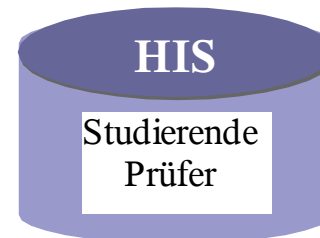
- Ziele des Identitäts-Managements
- Ist-Zustände im Überblick
- Soll-Konzepte
- Proof of Concept

Ist: ~ Hannover/ Braunschweig

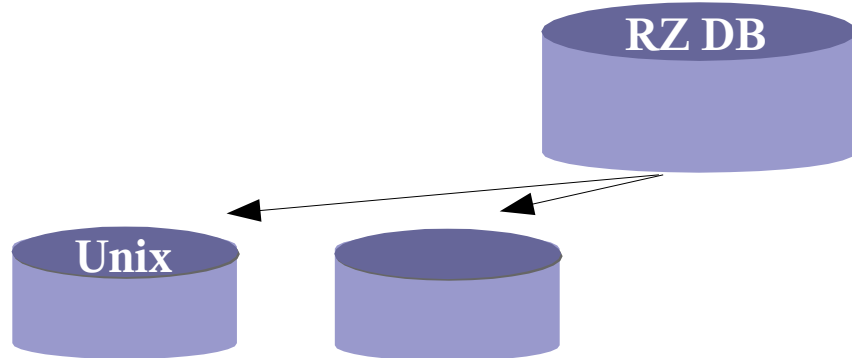


Ist: ~ Wolfenbüttel

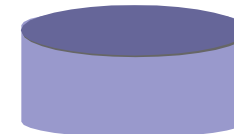
Verwaltung



Rechenzentrum



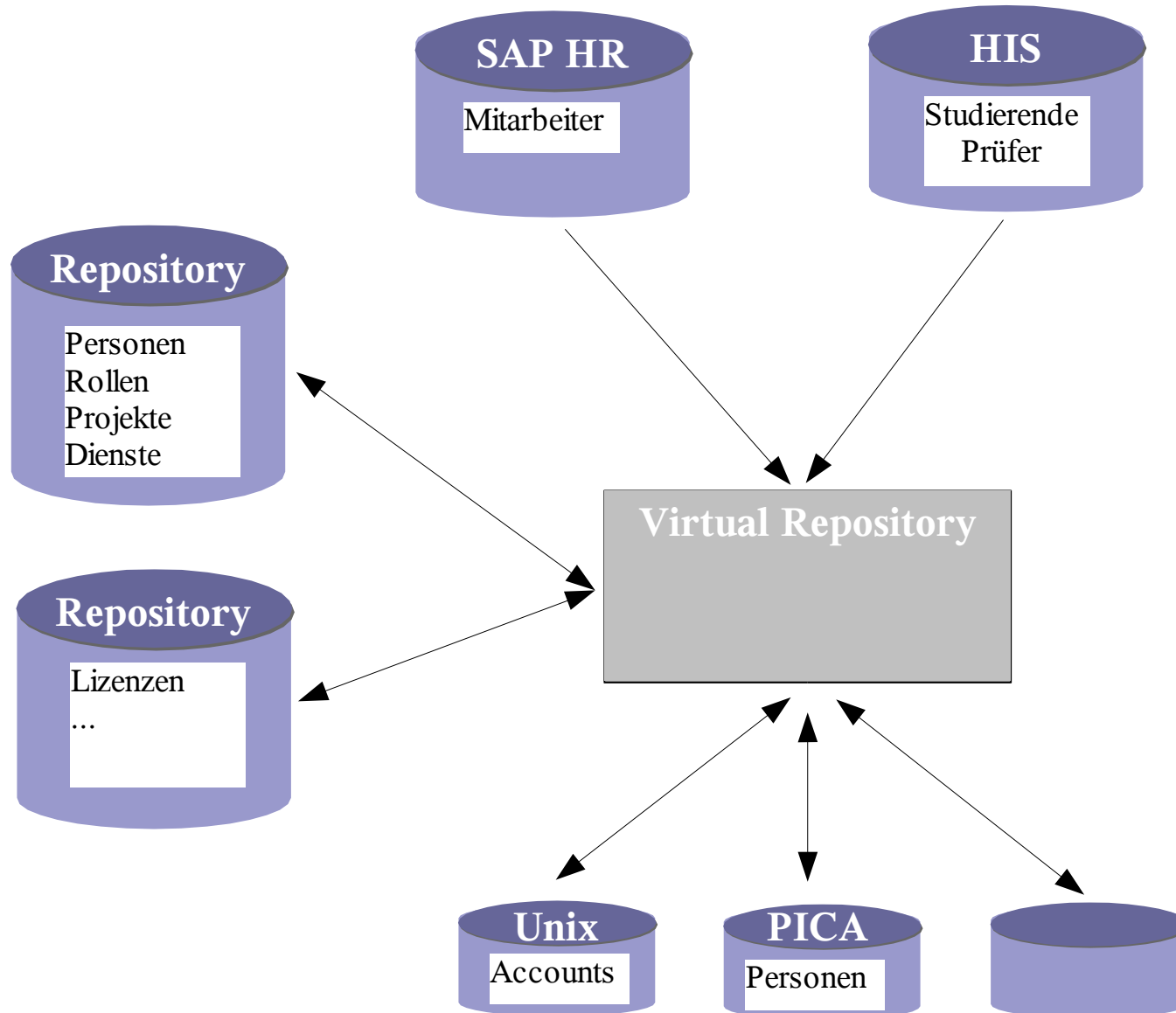
Andere



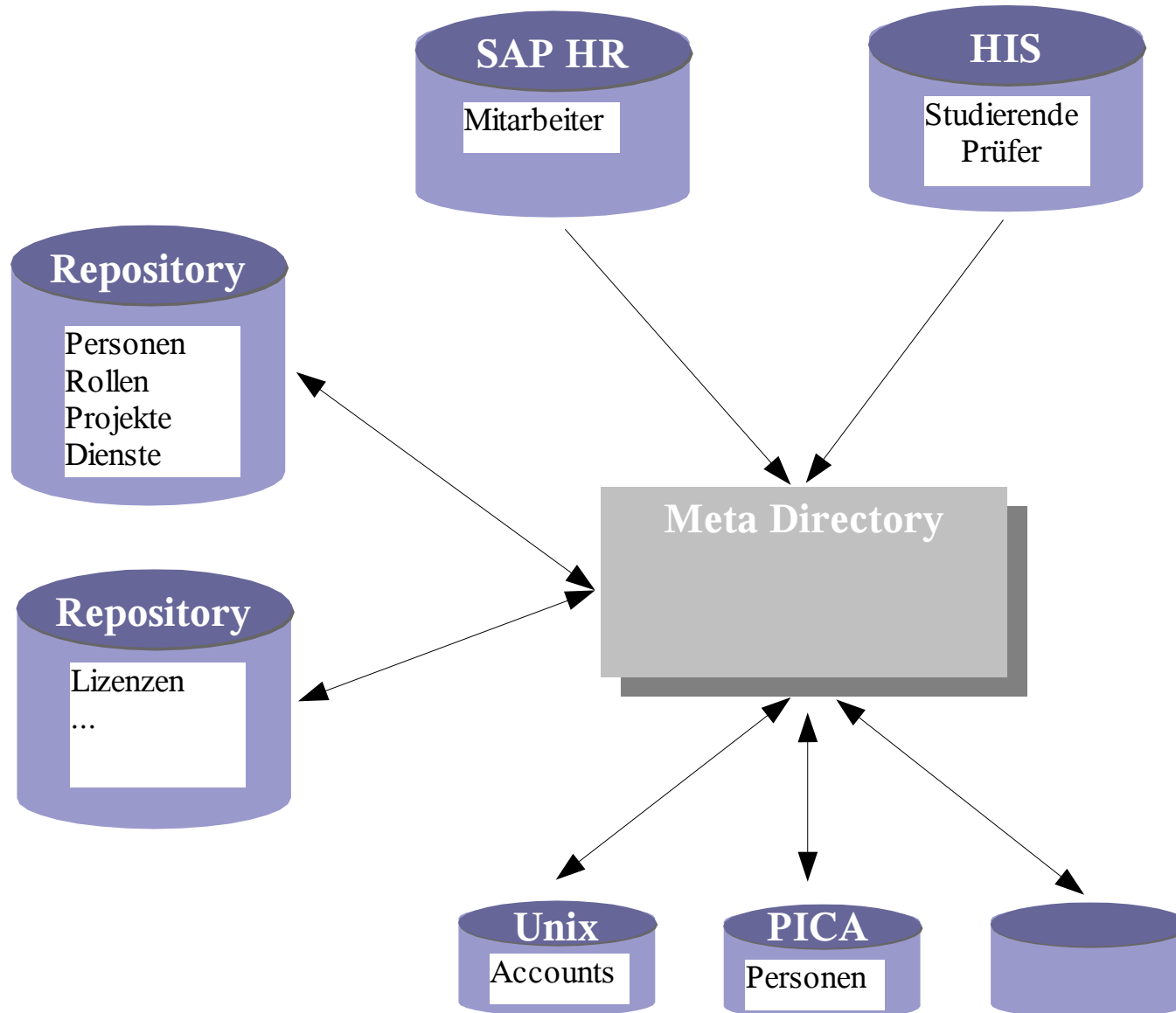
Agenda

- Ziele des Identitäts-Managements
- Ist-Zustände im Überblick
- Soll-Konzepte
- Proof of Concept

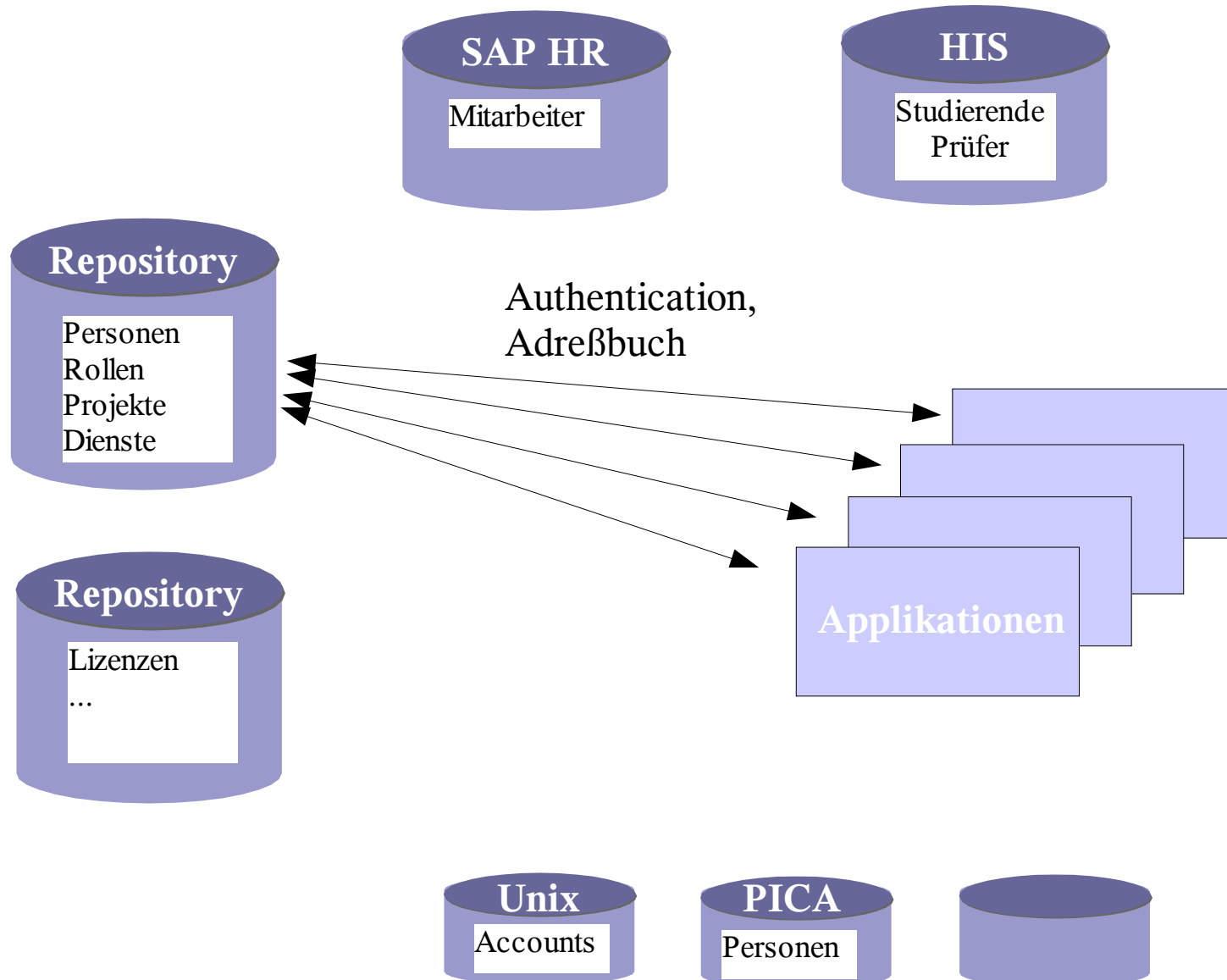
Soll: Universitäts-intern, virtuelle Sicht (1)



Soll: Universitäts-intern, Datenaustausch (2)



Soll: Universitäts-intern, Authentication (3)



Soll: Universitäts-übergreifend

Personen:

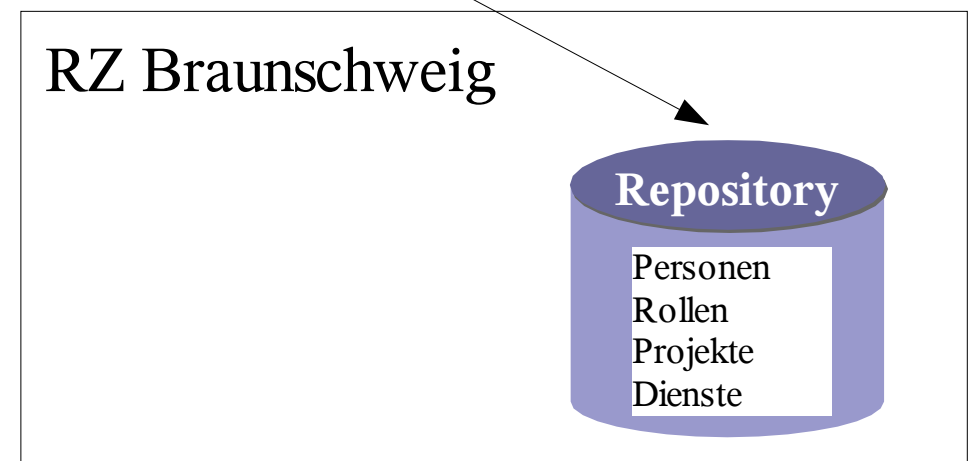
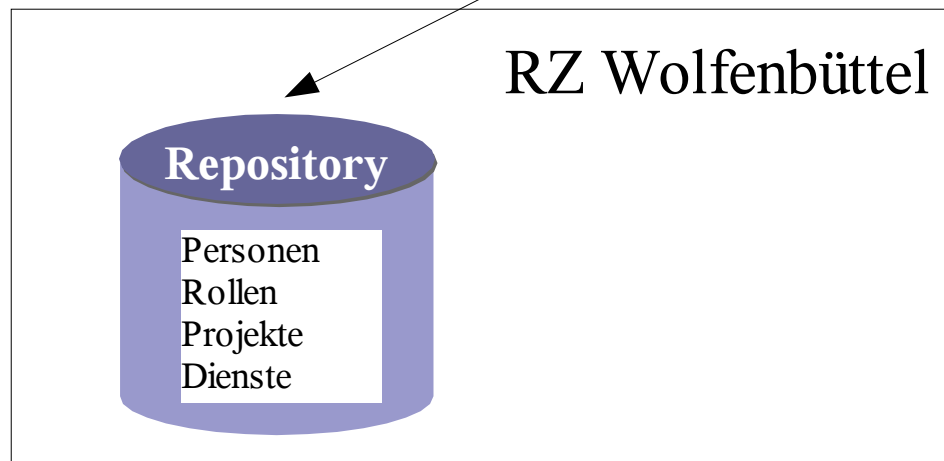
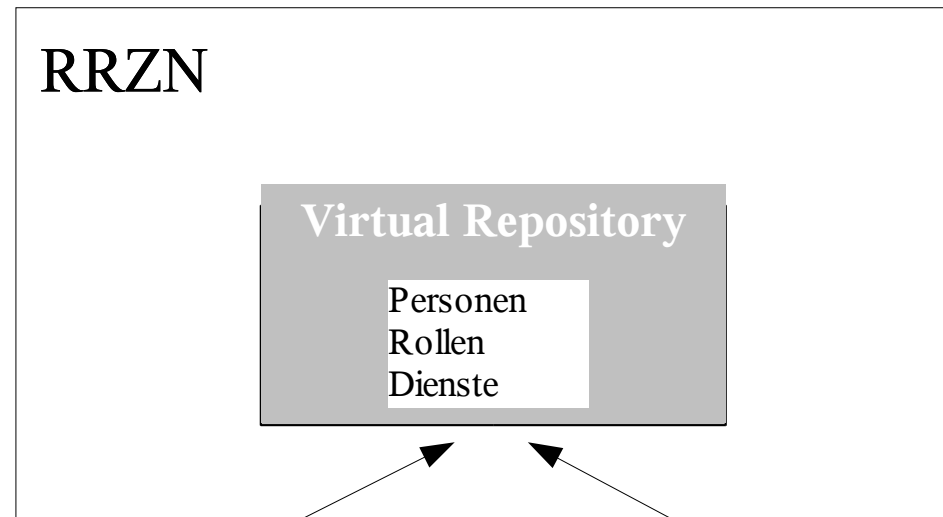
- UID
- Password (!)
- Rolle(n)
- Name
- eMail
- Adresse(n)
- Universität(en)
- ...

Dienste:

- eMail
- eLearning
- Bibliothek
- ...

Rollen:

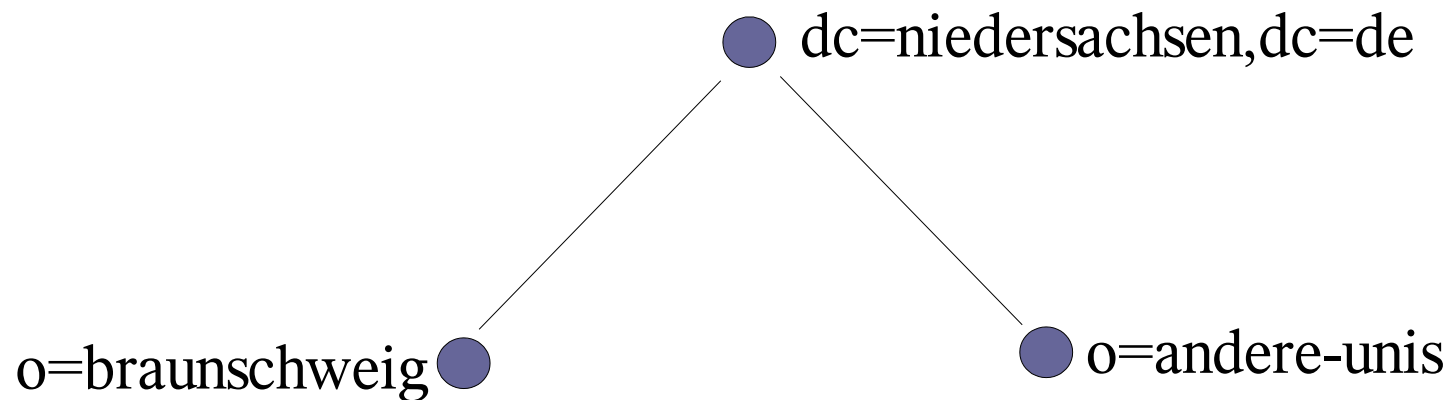
- Mitarbeiter
- Studierender
- Externer
- ...



Soll: Abgrenzung der Personengruppen

- Beispiel LDAP

- Verwendung einer separaten Organisation für Mitglieder fremder Universitäten
- Mitglieder der eigenen Universität in der Wurzel oder ebenfalls in eigener Organisation



Soll: Verarbeitungsprinzip (1)

- **Universitäts-übergreifend abgestimmte Daten**
 - Rollen/ User-Kategorien
 - gewünschte Dienste
 - Personendaten
- **Heimat-Universität legt Datensatz an**
 - auf Wunsch werden andere Universitäten mit eingetragen, deren Dienstangebot genutzt werden soll
 - es können speziell gewünschte Dienste markiert werden
 - die Person wird grob (!) kategorisiert
 - das RZ verteilt die Personendaten und weitere generierte Informationen innerhalb der Universität
 - Änderungen an den Personendaten werden dem RRZN mitgeteilt

Soll: Verarbeitungsprinzip (2)

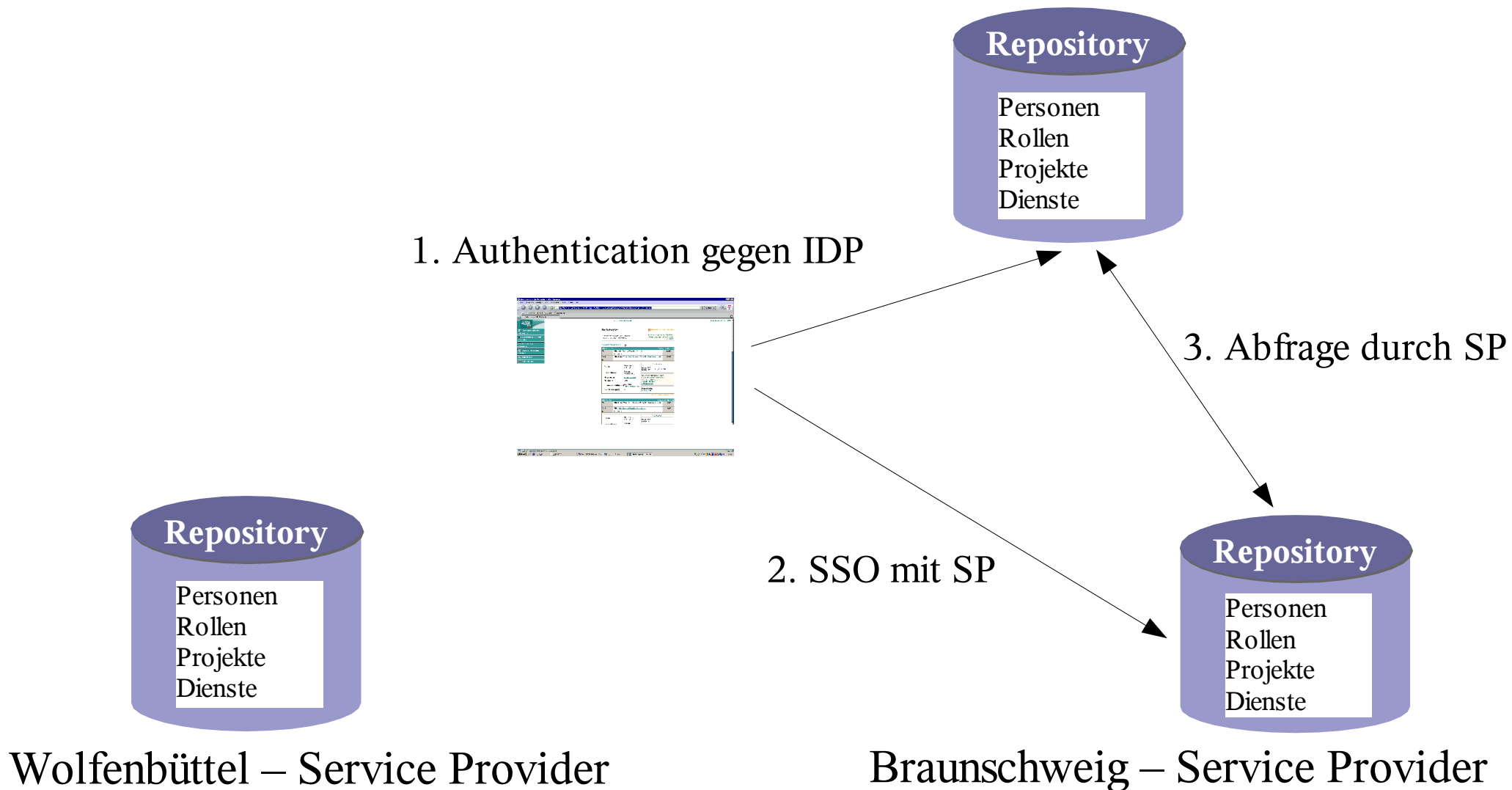
- **RRZN verteilt zwischen Universitäten**
 - das RRZN erhält die Personendaten zur Verteilung
 - die Daten werden anhand der zur Person gehörenden Liste von Universitäten verteilt
- **RZ übernimmt Personendaten**
 - optional Approval für fremde Personen
 - auf die Kerndaten der Person bestehen keine Schreibrechte
 - anhand der zur Person gehörigen Rollen und der gewünschten Dienste werden die Rechte der Person zugewiesen
 - weitere an die Person gebundene Informationen werden angelegt und innerhalb der Universität verteilt
 - Änderungen bleiben lokal innerhalb der Universität

Soll: Randbedingungen

- **RRZN verteilt auch Passwords**
 - die Verteilung verschlüsselter Passwords erfordert eine Abstimmung hinsichtlich des Verschlüsselungs-Algorithmus
 - andernfalls ist für Klartext-Passwords nur Transportsicherheit gegeben
- **Behandlung von Rechten**
 - die Einrichtung, insbesondere aber die Entfernung von Rechten durch die Heimat-Universität, z.B. auch durch die Änderung der Rolle(n), erfordert Logik auf Seite der fremden Universitäten
 - andererseits ist die Behandlung der verteilten Daten damit völlig unter Kontrolle der Universitäten

Soll: Liberty

RRZN – Identity Provider



Soll: Liberty

- Keine Unique ID erforderlich
 - IDP und SP vereinbaren bei Föderierung der Accounts implizit eine Unique ID
 - Denkbar für Universitäten, die nicht am direkten Datenaustausch teilnehmen wollen
- SSO erforderlich
 - SSO innerhalb der Universitäten muß zumindest teilweise funktionieren
 - es muß eine gewisse Universitäts-übergreifende Kooperation stattfinden (Cross Domain SSO)

Agenda

- Ziele des Identitäts-Managements
- Ist-Zustände im Überblick
- Soll-Konzepte
- Proof of Concept

Proof of Concept: Umfang (1)

- Unique ID innerhalb einer Universität
 - Schwerpunkt, Ausrichtung
 - noch kein SSO
 - Verwaltung von Berechtigungen ?
 - Repository Sun Java System Directory Server ?
 - welche Universität ?
 - Datenbestand ?
- Personen aus SAP HR und HIS
 - unidirektional, „downstream“, bis auf UID ?
 - Anlegen einer Person
 - Aktivierung einer Person ?
 - automatische Übernahme der Person

Proof of Concept: Umfang (2)

- Beziehung zur RZ-DB ?
 - Synch mit den Personen der RZ-DB oder neue Basis für Personen ?
- Accounts nach Unix, Windows und Novell
- Accounts nach PICA
- Accounts nach Hyperwave, StudIP ?
- System/ Applikation direkt auf LDAP ?

Proof of Concept: Umfang (3)

- **Selbstadministration**
 - beispielhaft, Password-, eMail- und Adress-Änderung
- **Administration, delegierte Administration**
 - beispielhaft, Gesamtsicht für RZ-Administratoren und eingeschränkte Sicht für delegierte Administratoren (Verwaltung, Institute ???)
 - beispielhaft, Ergänzung der Attribute einer initial erzeugten Person
 - beispielhaft, De/ Aktivierung einer Person ?
- **Use Case eines LDAP-basierenden Systems**
 - die bisher aufgeführten Systeme fordern eher den Ansatz eines Meta-Directories
 - wichtig wäre daher ein System, das direkt LDAP nutzt