



# Anwendungsintegration an Hochschulen am Beispiel von Identity Management

Norbert Weinberger - Sun Summit Bonn 26.4.2006

# Ausgangslage: Anwendungsinselfn

Zugang zu IT-  
Ressourcen,  
z.B. Radius

Rechenzentrum

HIS / SAP  
Hochschul-  
administration

Verwaltung

E-Learning  
Anwendung

Lehre

LBS/SunRise

Bibliothek

# Ziele einer Integration

- **Geschäftsprozessoptimierung /  
Verbesserung des Workflows zwischen den  
Bereichen**
- **Realisierung neuer Anwendungen –  
z.B. Hochschulportal**
- **Verknüpfung von Diensten  
z.B. e-Learning und elektronische Quellen der  
Bibliothek**

**Erster Schritt**

**Eine gemeinsame Nutzerdaten-  
basis für alle Anwendungen**

Zugang zu IT-  
Ressourcen,  
z.B. Radius

Nutzerdaten

Rechenzentrum

Nutzerdaten

HIS / SAP  
Hochschul-  
administration

Verwaltung

Gemeinsame Nutzerdatenbank ?

E-Learning  
Anwendung

Nutzerdaten

Lehre

Nutzerdaten

LBS/SunRise

Bibliothek

# Warum nicht einfach eine gemeinsame Nutzerdatenbank ?

- Alle beteiligten Systeme müssten in der Lage sein, mit einer “ausgelagerten” Nutzerverwaltung zu arbeiten
- Aufgrund des unterschiedlichen Funktions- und Datenumfangs der Applikationen ist dies jedoch nicht bei allen Systemen gegeben
- Ausserdem gibt es häufig definierte Workflows für die Nutzerdatenverwaltung in den Anwendungen
- Schnittstellenfrage

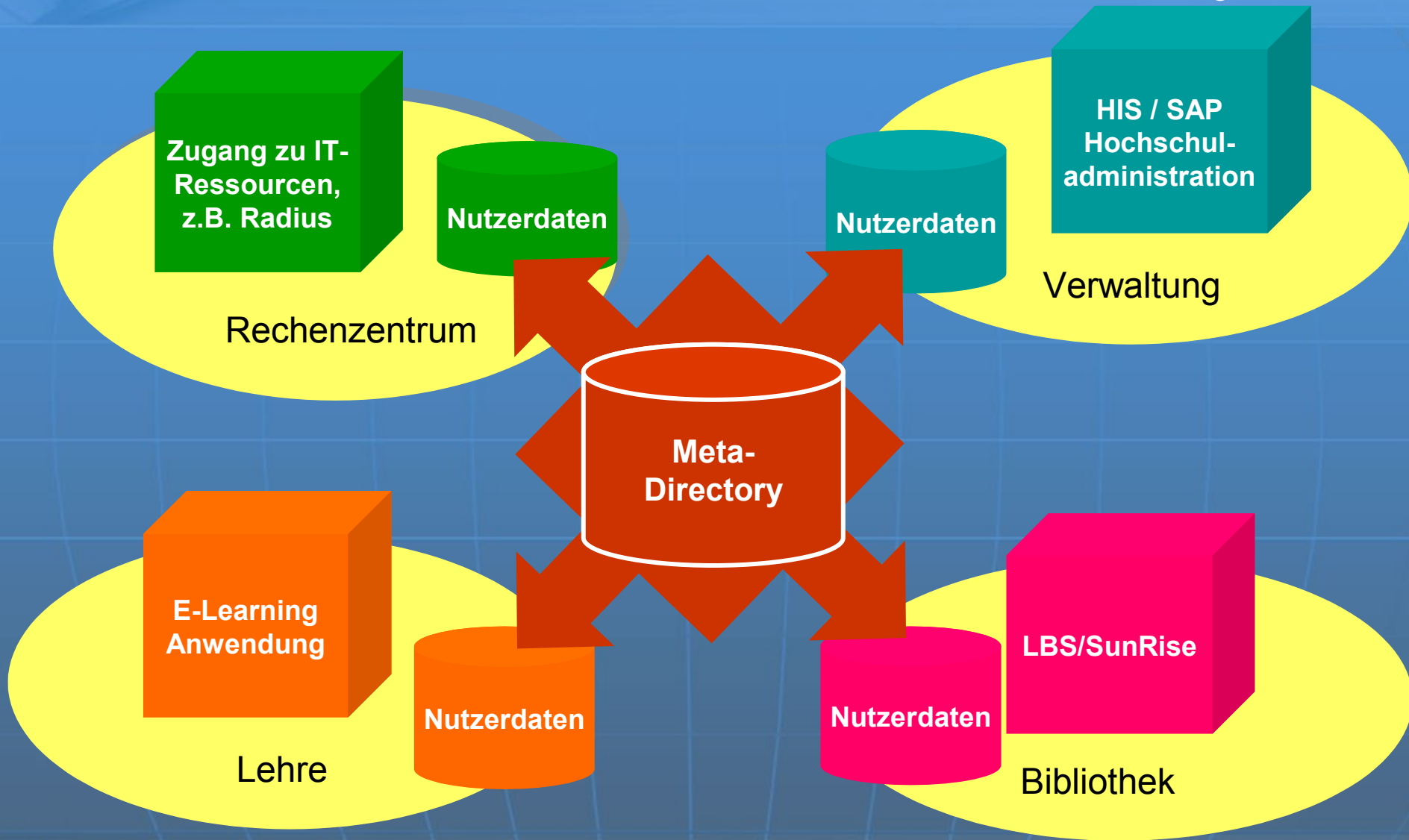
# Lösungsansatz: Identity Management

- **Zentrale Anwendung für die Verwaltung von Nutzerdaten**
  - die Festlegung des Workflows, der Datenstruktur, der Rechte und Rollen sowie der Regeln für den Austausch/Zugriff von/auf Nutzerdaten zwischen den Anwendungen
  - Bereitstellung von Schnittstellen zur Versorgung der angeschlossenen Subsystemen
  - Einheitliche Authentifizierung des Nutzers unabhängig von der jeweiligen Anwendung -> Single-Sign-on

# Identity Management Lösungen

- Sun Java Directory
- Siemens Dir.X
- IBM Tivoli Directory Server
- Novell eDirectory
- Microsoft Active Directory Service
- ..... und weitere .....

# Variante zentrales Meta-Directory

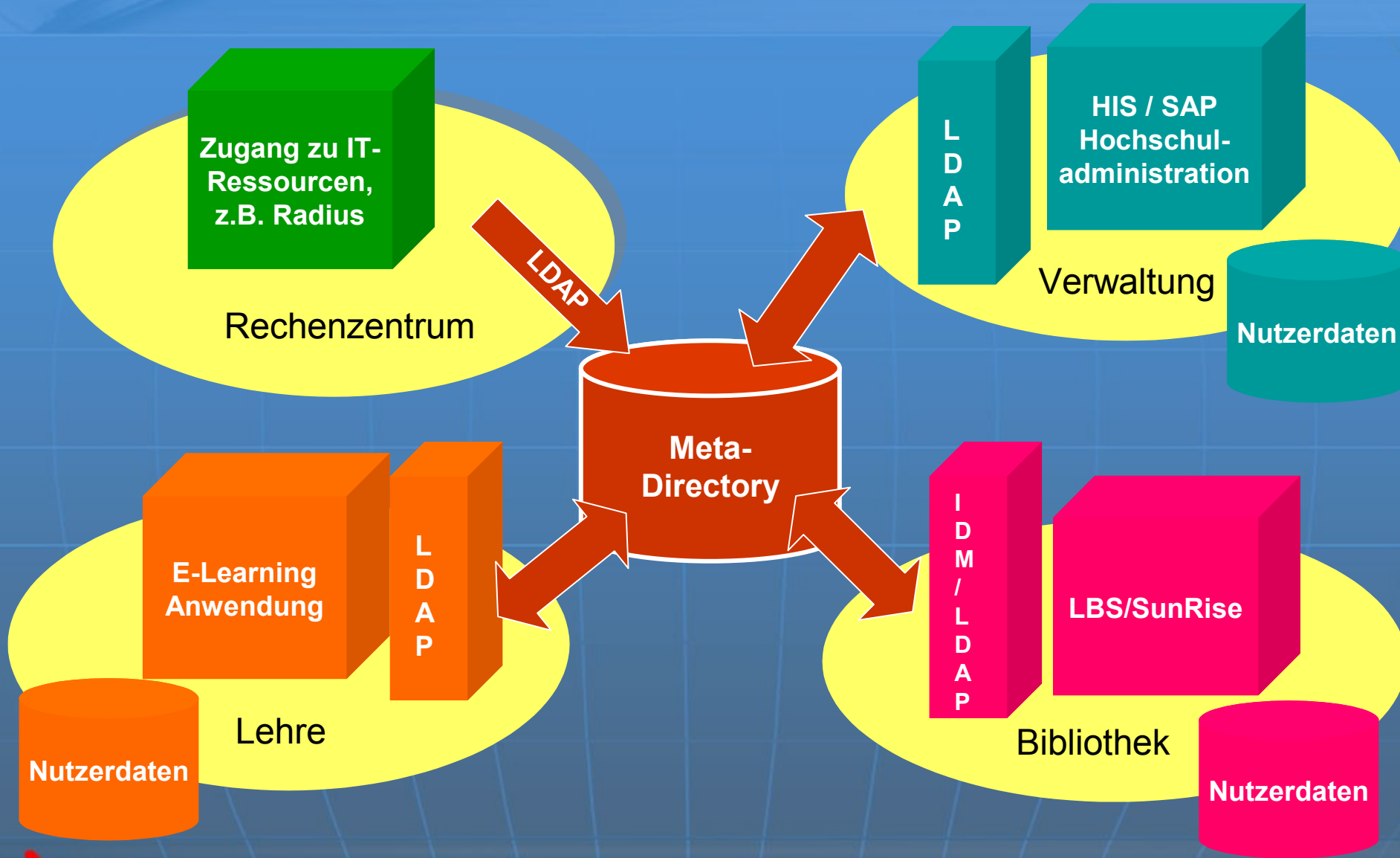




# LDAP als Protokoll für IDM

- Etabliertes und offenes Protokoll für den Datenaustausch zwischen Verzeichnisdiensten
- Verschlüsselung des Datentransfers sichergestellt – z.B. über SSL
- Access Control Lists regeln den Zugriff auf die verschiedenen Datenelemente des Verzeichnisses
- Zusätzliche Funktionen in LDAP V3 erlauben eine bessere Automatisierung von Abläufen

# Authentifizierung / Provisionierung von Nutzerdaten



# Aufgaben für die Bibliotheksanwendung

- Aktive und passive Rolle bei dem Austausch von Nutzerdaten mit dem IDM System
- Online Verarbeitung der Nutzerdatenänderungen
- Authentifizierung gegen ein LDAP Directory /  
Öffnung der Anwendungen für die Integration in eine SSO Umgebung

# IDM-Lösung für LBS/SunRise

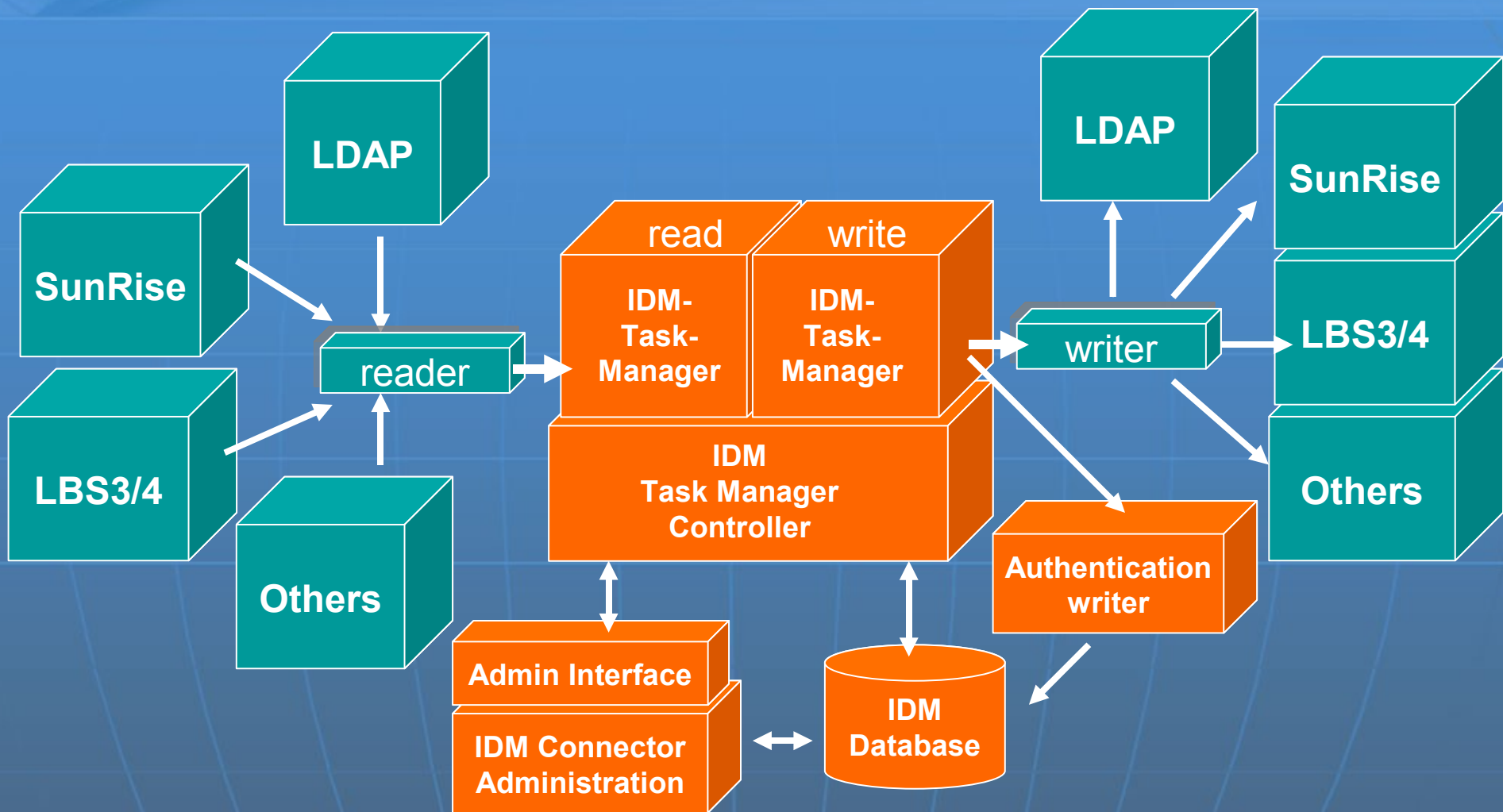
## → IDM-Connector

- Online Synchronisation von Nutzerdaten in LBS/SunRise mit beliebigen Anwendungen
- Festlegung von Regeln für den Austausch und das Mapping der Daten pro Anwendung
- Ausführliche Protokollierung von Datenupdates sowie Benachrichtigung bei Problemfällen

## → Identity-Server

- Unterstützung von LDAP für die Authentifizierung im WebOPAC/InfoGuide sowie für SB-Anwendungen

# Architektur des IDM-Connectors

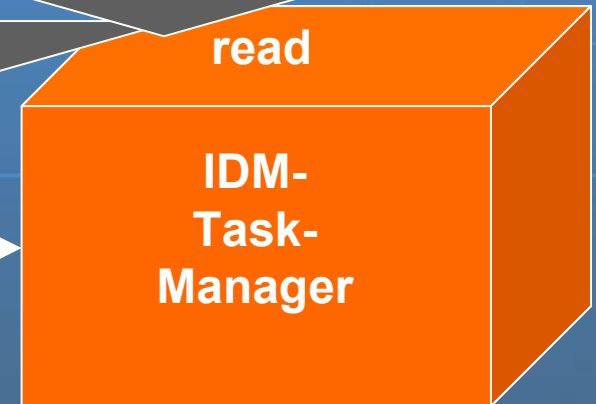
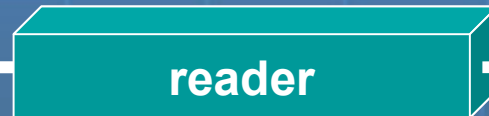


# Arbeitsweise des IDM-Connectors I

Auftrag zum Ändern eines Nutzerdatensatz durch das zentrale Meta-Directory via LDAP an den LDAP-Reader

Weitergabe des Auftrages inclusive der Daten als XML-Struktur

Konfigurierbare Prüfung der Daten mittels XPATH plus Veränderung mittels XSLT und Auftragsannahme



# Arbeitsweise des IDM-Connectors II

Auftrag zum Ändern eines Nutzerdatensatz durch den IDM Task-Manager an **alle** konfigurierten writer Anwendungen

Konfigurierbare Prüfung der Daten mittels XPATH plus Veränderung mittels XSLT je Zielanwendung

Durchführung der Datenänderung

write

IDM-  
Task-  
Manager

writer

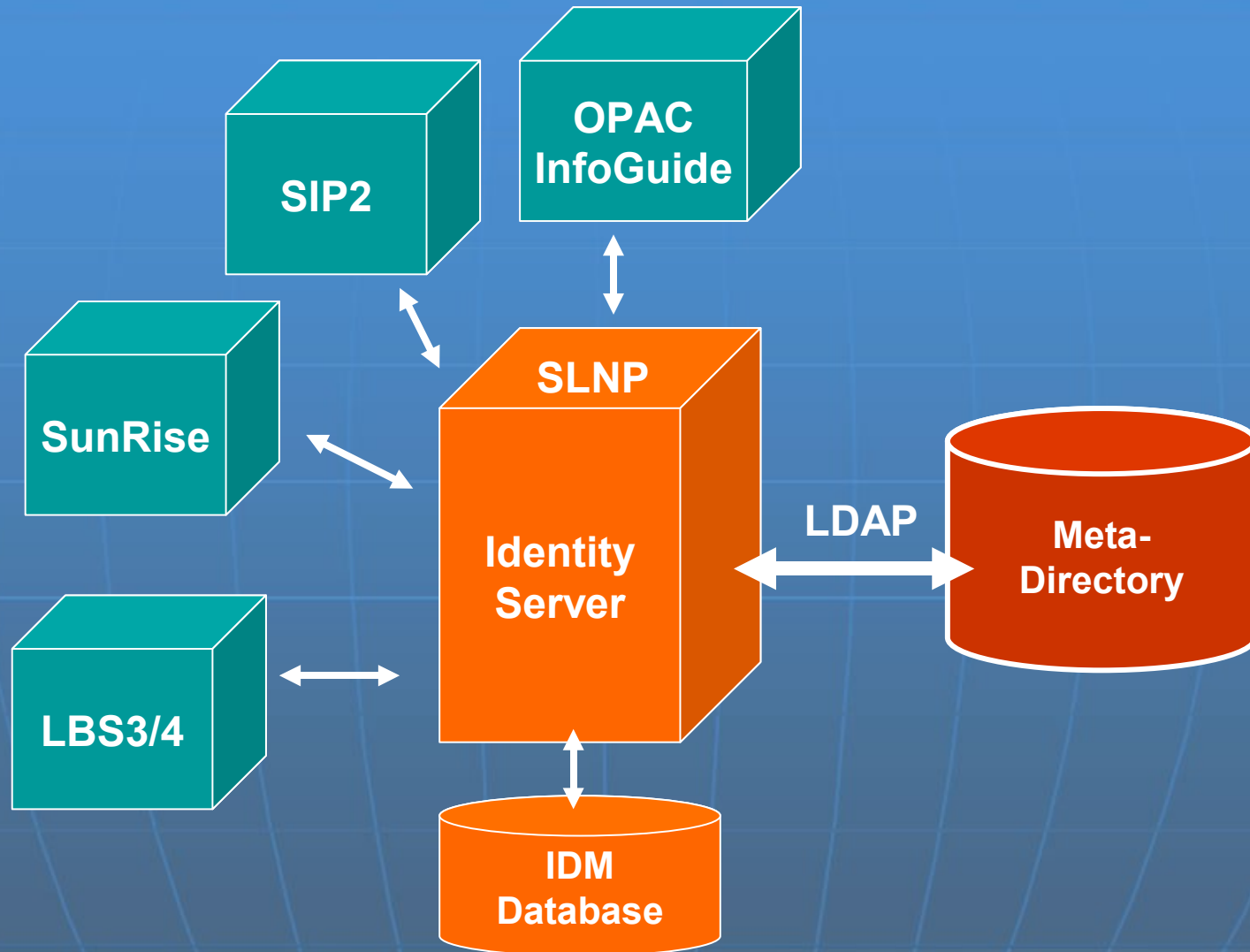
z.B.  
LBS/SunRise

# Der Identity Server

- Erlaubt den Komponenten des Bibliothekssystems die Authentifizierung eines Nutzers mit seiner globalen oder lokalen ID
- Dazu verwendet er parametrisierbar seine eigene IDM Datenbank oder den LDAP Dienst des zentralen Meta-Directories
- Die Kommunikation mit den lokalen Komponenten erfolgt über SLNP und wird mittels Zertifikaten verschlüsselt



# Architektur des Identity Servers



# Technisches Umfeld

- Implementierung in Java
- Connectoren zu den Lokalsystemen via SLNP / Corba
- Anwendungsseitige “Trigger” für die Provisionierung durch das Lokalsystem
- Eigenständige Admin als Plug-in in die SunRise Administration

# Administrationsfunktionen

## → Konfiguration

- IDM Connector
- reader und writer targets
- XSLT

## → Verwaltung

- Generelle Informationen des IDM Connectors
- Status der reader und writer
- start/stop der reader und writer

## → Statistiken

- Informationen zu den Tasks und targets
- Suchinterface für Statistikanfragen

## SISIS-SunRise Administration

## IDM

## Konfiguration

[Allgemeine Parameter](#)[XSLT Konfiguration](#)[XPath Konfiguration](#)[Targetkonfiguration](#)[Readerkonfiguration](#)[Writerkonfiguration](#)

## Verwaltung

[Allgemeine Informationen](#)[Reader - Administration](#)[Writer - Administration](#)[Task - Administration](#)

## Statistiken

[Recherche](#)

## Targetkonfiguration

[Hilfe](#)

Targetname	Target1
<input type="button" value="Bearbeiten"/> <input type="button" value="Neu"/> <input type="button" value="Löschen"/>	

## Target Target1 bearbeiten

<input type="button" value="Speichern"/>
------------------------------------------

Target ID	
Targetname	<input type="text"/>

## Readerkonfiguration

Reader	<input type="checkbox"/>
Art	fremdes Target
Klassenname	<input type="text"/>
Stylesheet	STYLE1
Taskzuweisungen	<input type="checkbox"/> Insert <input type="checkbox"/> Update <input type="checkbox"/> Löschen <input type="checkbox"/> Blocken <input type="checkbox"/> Freischalten

## Writerkonfiguration

Writer	<input type="checkbox"/>
Art	fremdes Target
Klassenname	<input type="text"/>
Stylesheet	STYLE1
Writer Threads	<input type="text"/>

# Status

- Kopplungsmöglichkeit mit SunRise ab Version V3.5 und LBS4 2.6
- Erste Pilotierung ab Juli/August 2006 mit verschiedenen IDM Systemen
- Freigabe August/September 2006

# Ausblick

- Erweiterung des Identity Servers
  - Unterstützung weiterer Protokolle
    - Shibboleth
    - a-select, ...
- Möglichst viele Referenzimplementierungen mit unterschiedlichen IDM Systemen
- Generell: Entwicklung aller Bibliotheksanwendungen in Richtung einer SOA

**Vielen Dank  
für Ihre Aufmerksamkeit !**