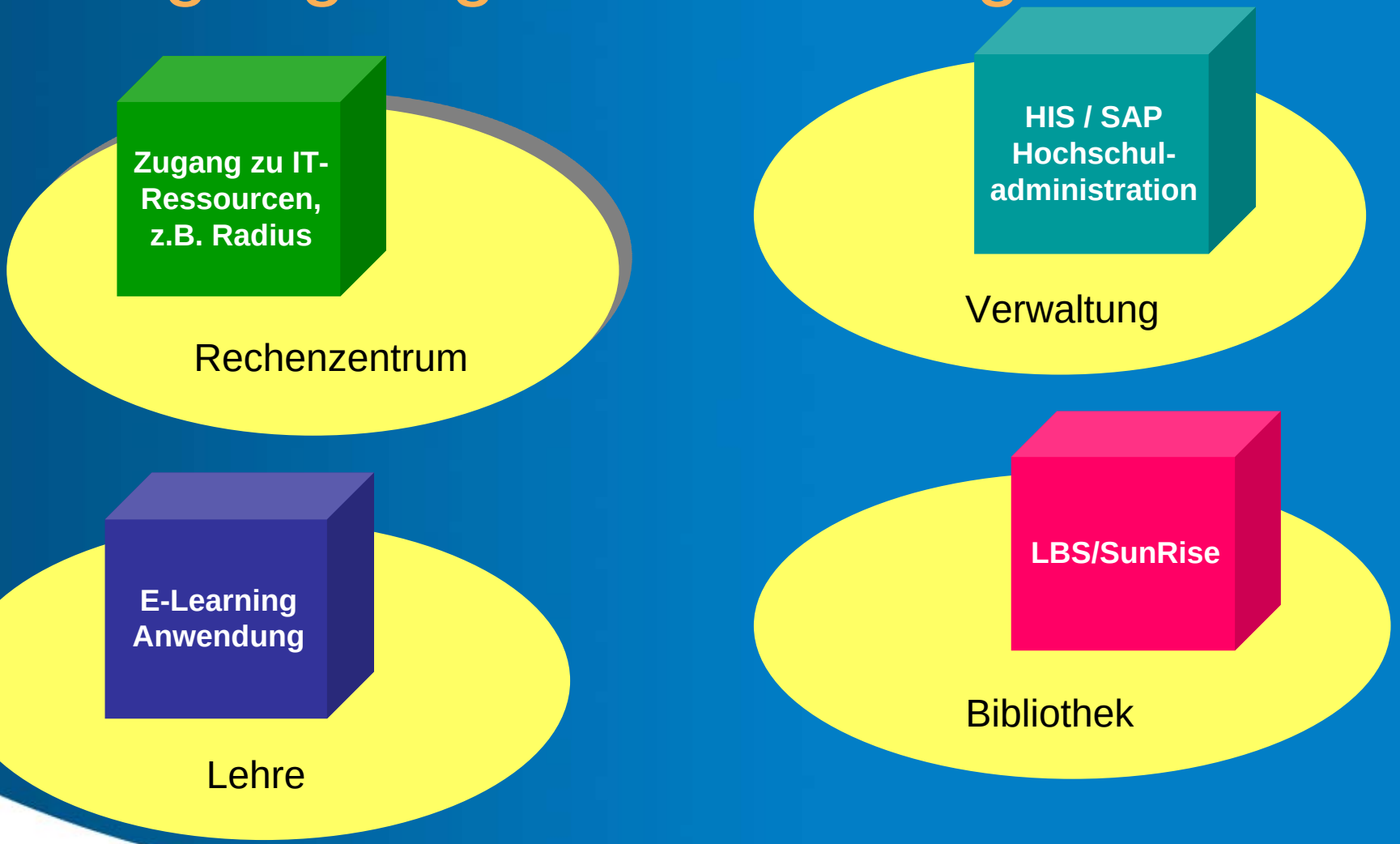
Anwendungsintegration an Hochschulen am Beispiel Identity Management

Münster, 7. Sept. 2006

OCLC PICA

At the heart of your information

Ausgangslage: Anwendungsinseln



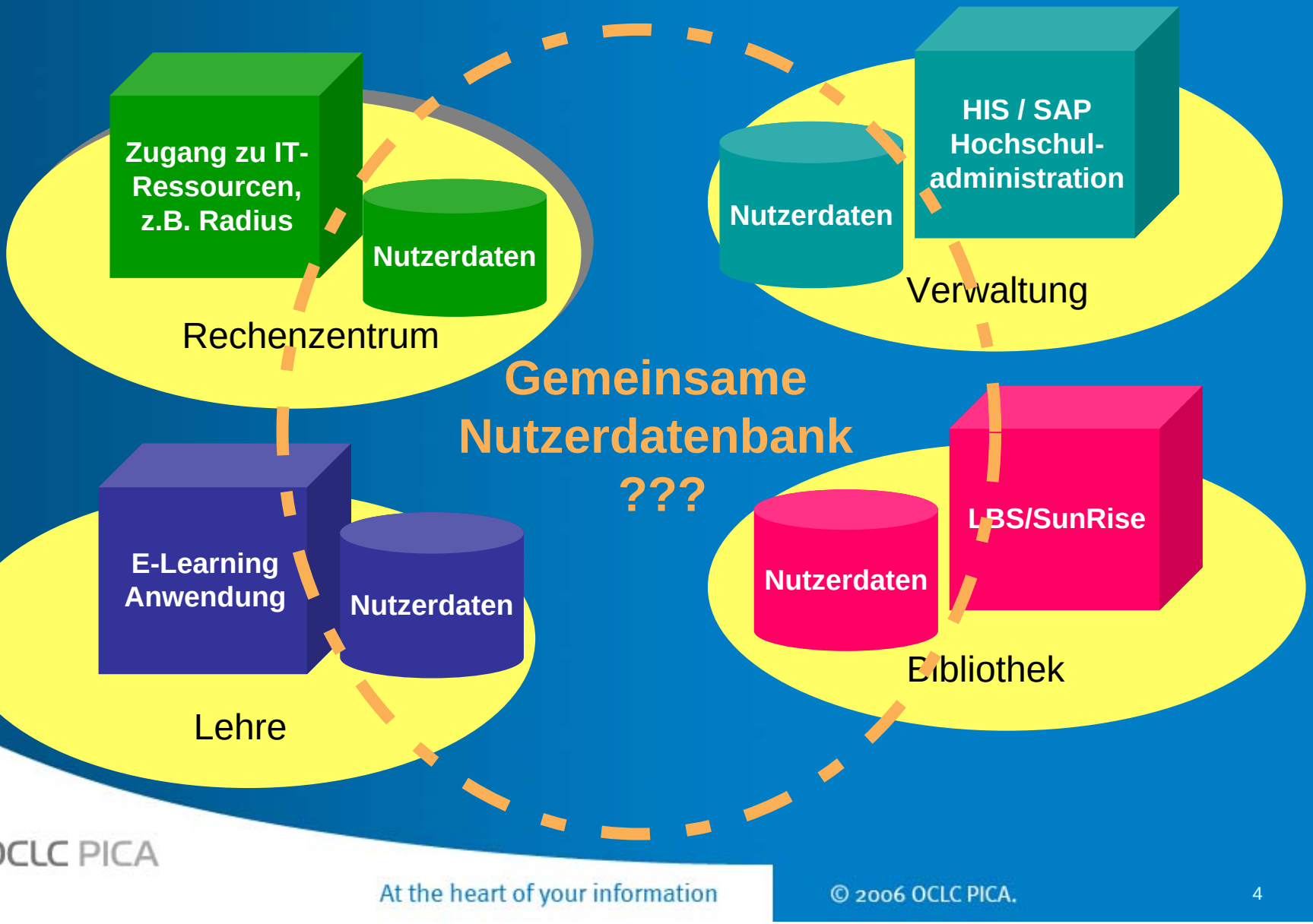
Ziele einer Integration

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

Erster Schritt

Eine gemeinsame Nutzerdaten-basis für alle Anwendungen

Gemeinsame Nutzerdatenbasis



Warum nicht?

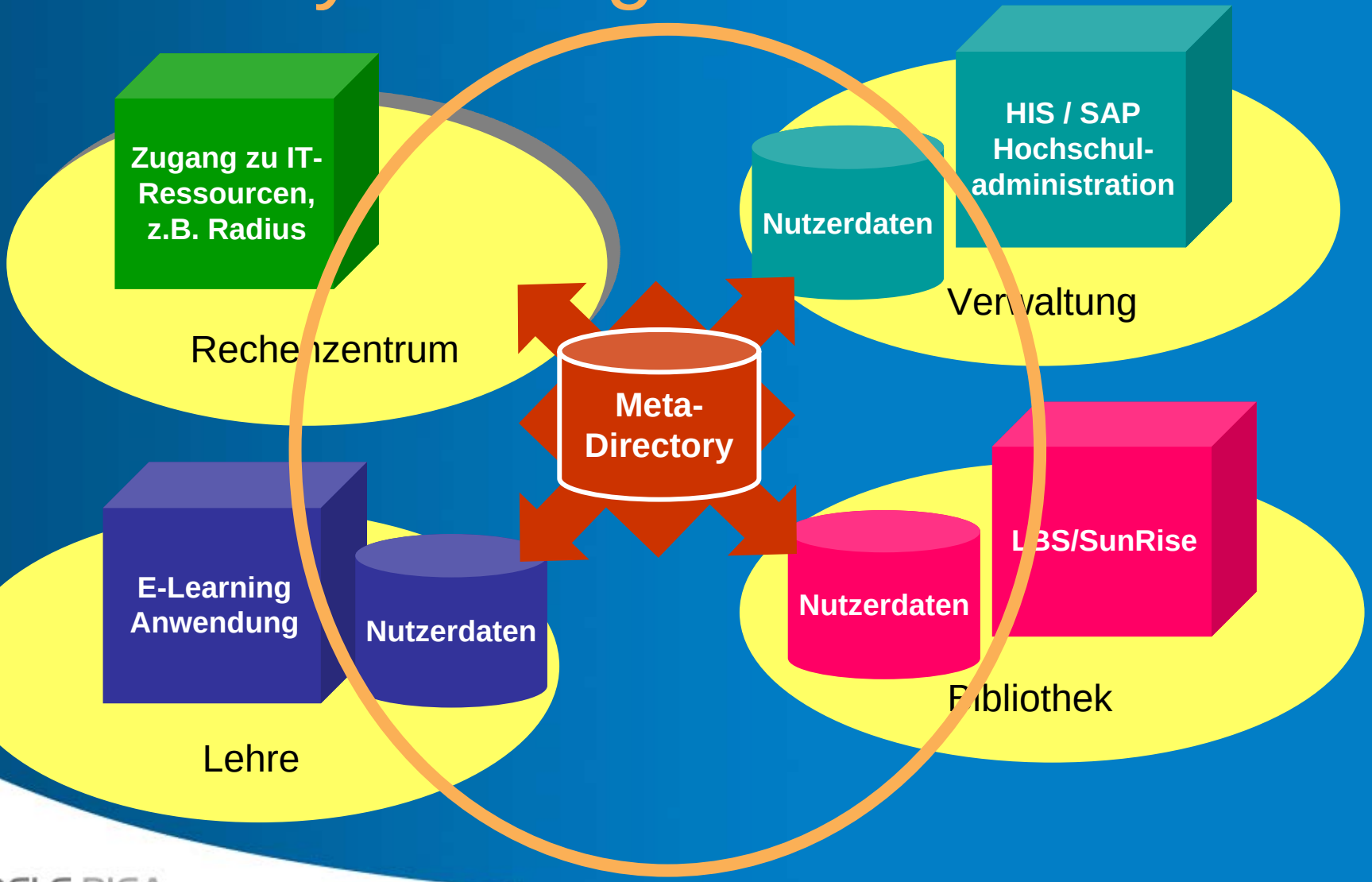
- Unterschiedlicher Funktions- und Datenumfang der Applikationen
- Unterschiedliche Workflows für die Nutzerdatenverwaltung in den Anwendungen
- Schnittstellenfrage

→ “Auslagerung” der Nutzerverwaltung nicht für alle Systeme möglich

Lösung: Identity Management

- Zentrale Verwaltung von Nutzerdaten
- Nutzerdatenabgleich der Subsysteme mit dem zentralen System
- Rückfluss von Informationen von den Subsystemen an das zentrale System
- Aktuelle Daten
- Keine Doppelerfassung
- Spezifika der Subsysteme bleiben erhalten

Indentity Management



Identity Mangement System

- ermöglicht Zugriff auf / Austausch von Nutzerdaten (uni- / bidirektional)
- legt Datenstruktur und Regeln fest
- Rechte- und Rollenverwaltung
- Schnittstellen zur Versorgung der angeschlossenen Subsystemen
- Einheitliche Authentifizierung des Nutzers unabhängig von der jeweiligen Anwendung -> Single-Sign-on

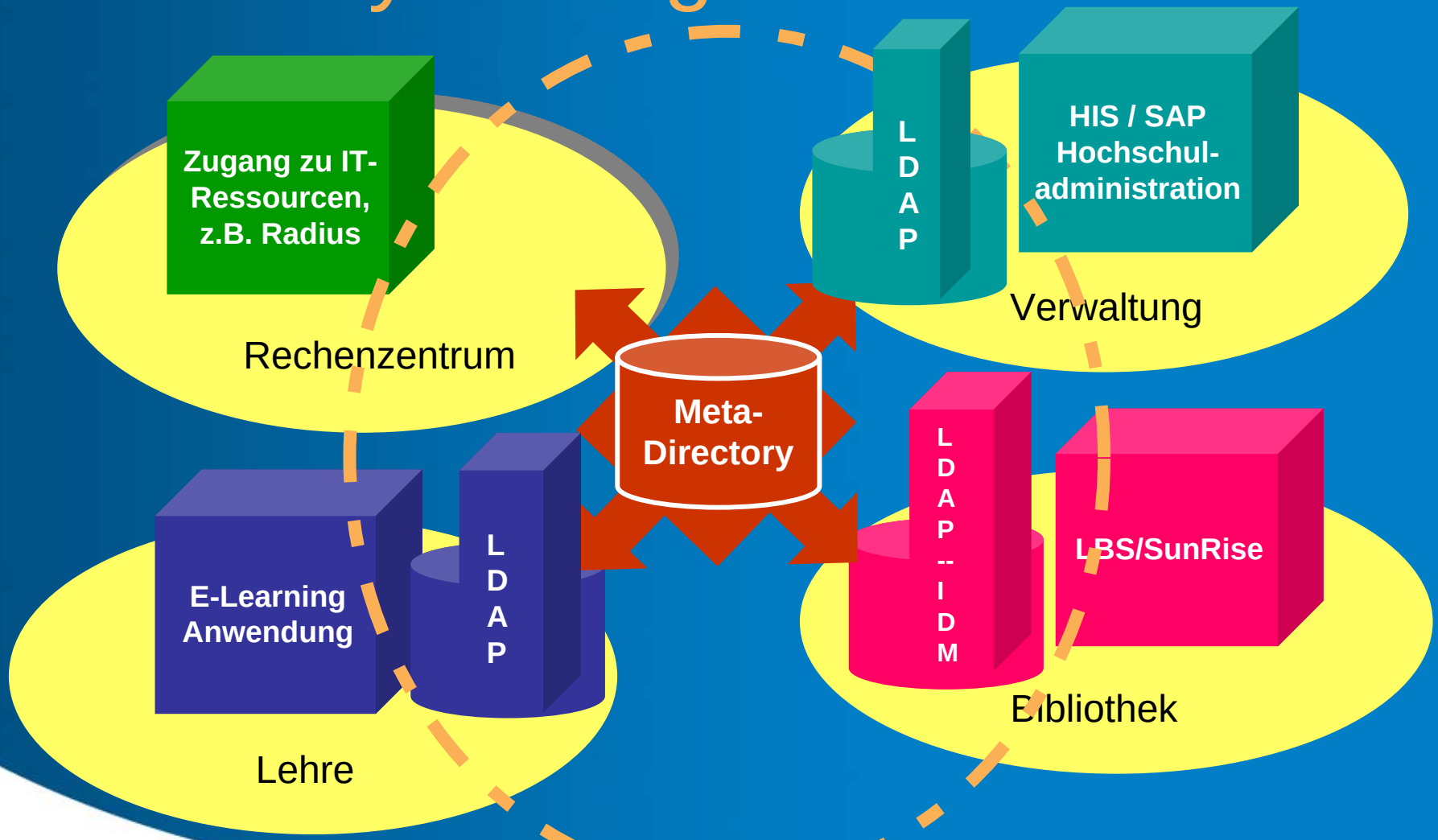
IDM-Systeme am Markt

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

Protokoll für IDM : LDAP

- Etabliertes 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

Indentity Management



Aufgaben für das BMS

- Bibliotheksmanagementsystem tauscht Nutzerdaten mit dem IDM-System aus
- Aktive und passive Rolle
- Online-Verarbeitung der Änderungen
- Authentifizierung gegen ein LDAP-Directory auch für nicht im LBMS erfasste Nutzer
- Öffnung aller Anwendungen für die Integration in eine SSO-Umgebung

IDM-Connector

für LBS / SISIS-SunRise

OCLC PICA

At the heart of your information

IDM-Connector

- 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

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

Status

- Kopplung mit SISIS-SunRise ab Version V3.5
- Kopplung mit LBS ab Version V4 2.6
- Pilotierung läuft seit Juli/August 2006 mit verschiedenen IDM-Systemen
- Freigabe September 2006

Ausblick

- Erweiterung des Identity Servers
  - Unterstützung weiterer Protokolle
    - Shibboleth
    - a-select, …
- Referenzimplementierungen mit möglichst vielen unterschiedlichen IDM-Systemen
- Generell: Entwicklung aller Bibliotheks-anwendungen in Richtung einer SOA

Vielen Dank
für Ihre Aufmerksamkeit !

OCLC PICA

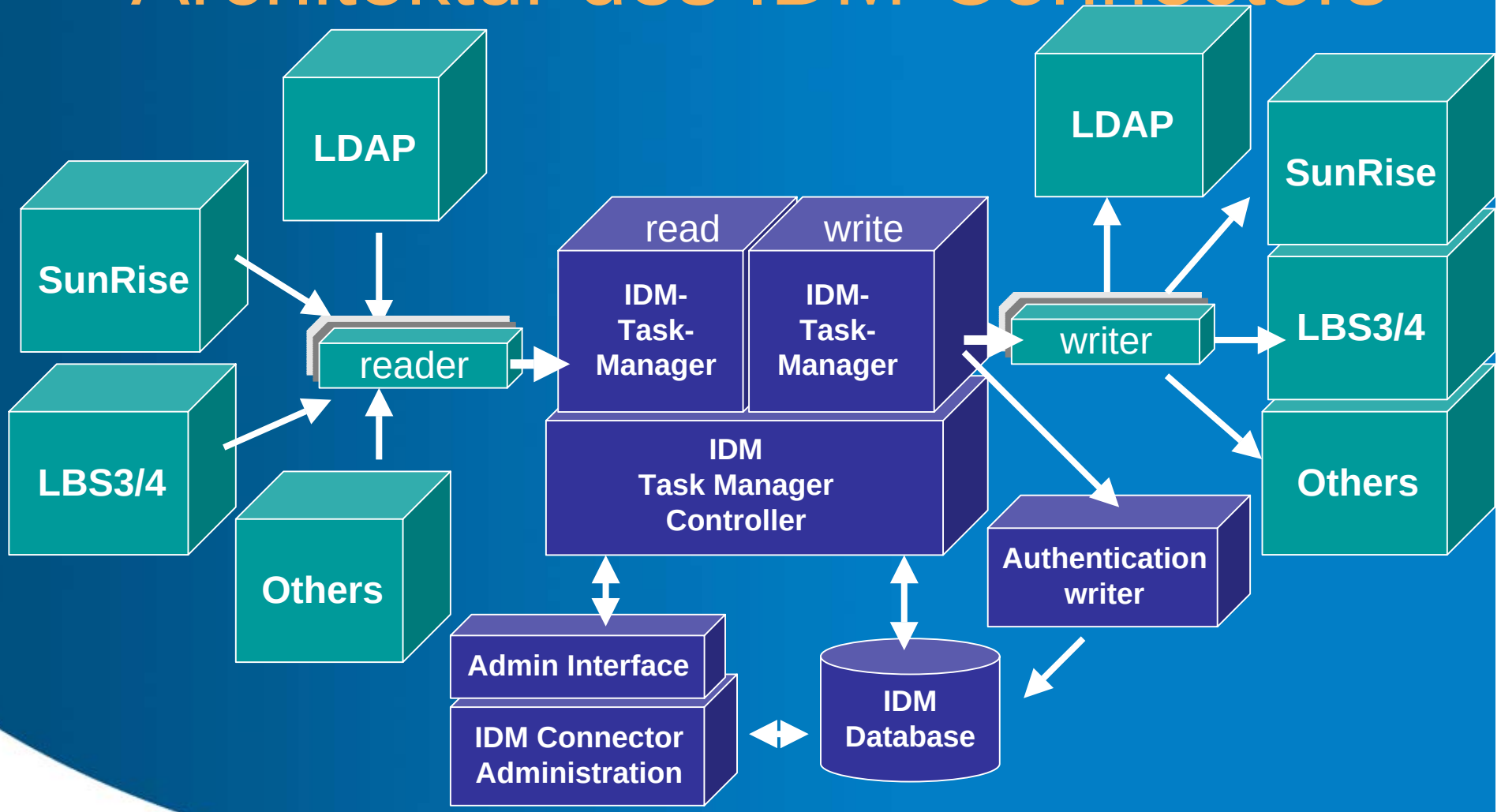
At the heart of your information

Anhang

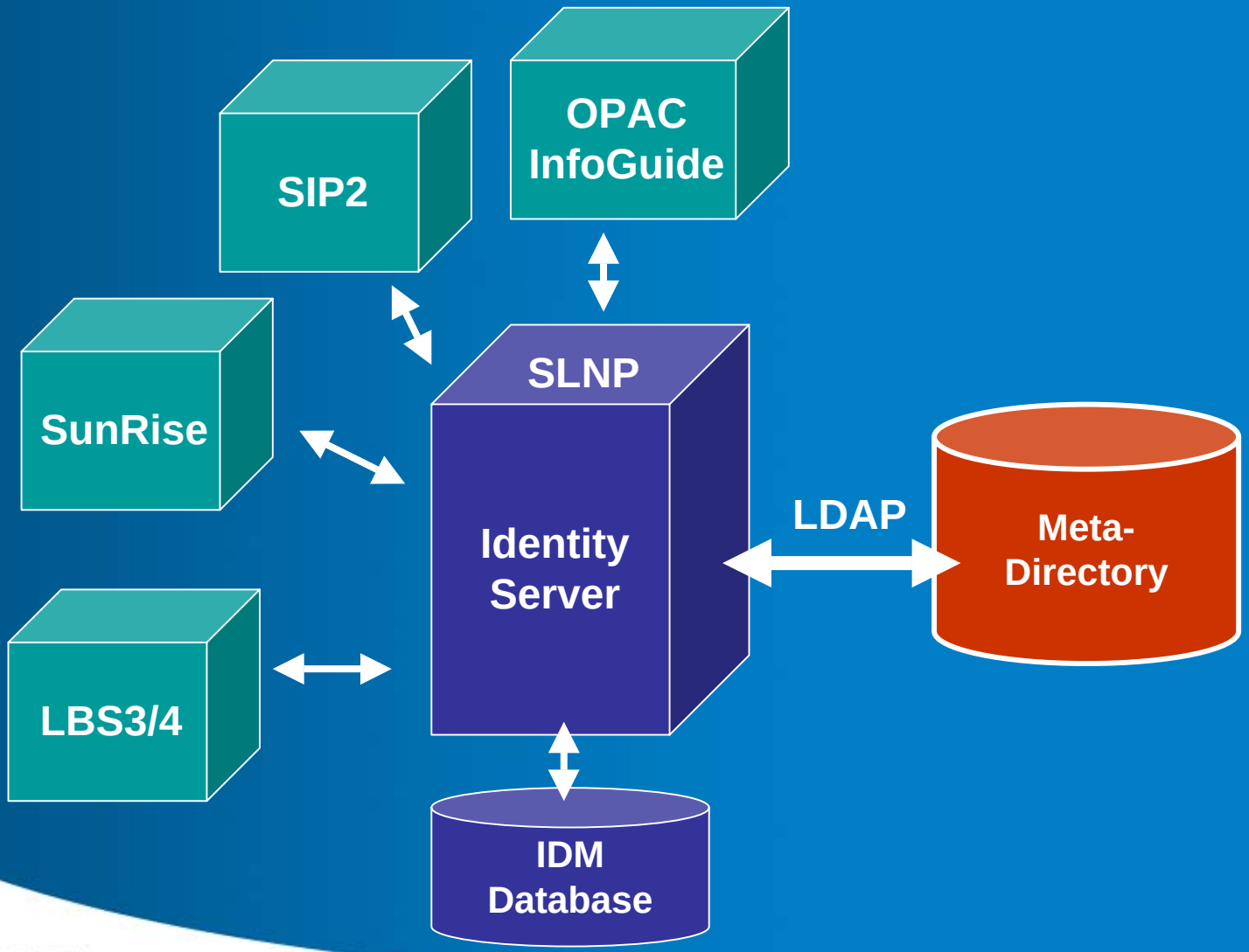
OCLC PICA

At the heart of your information

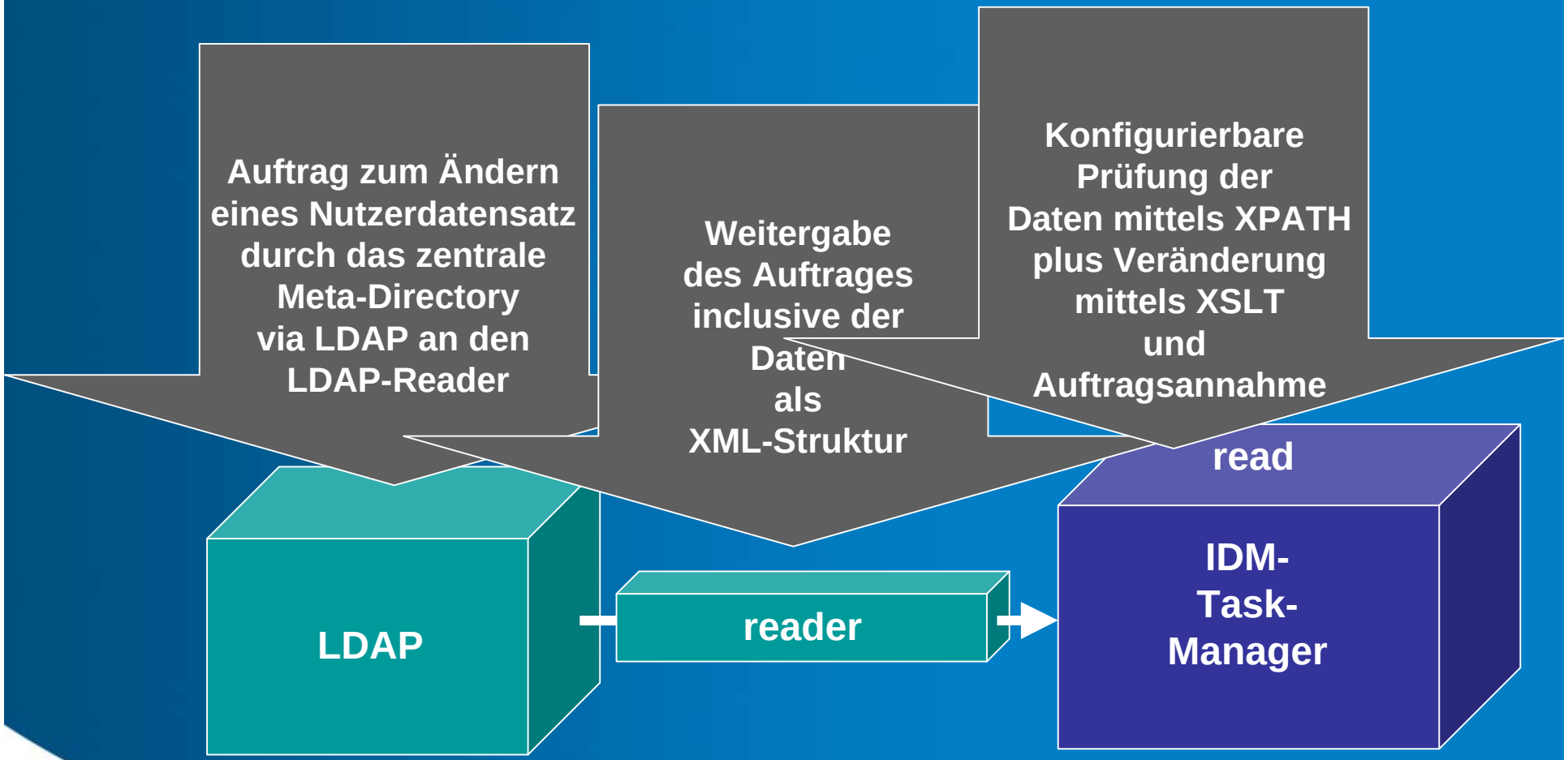
Architektur des IDM-Connectors



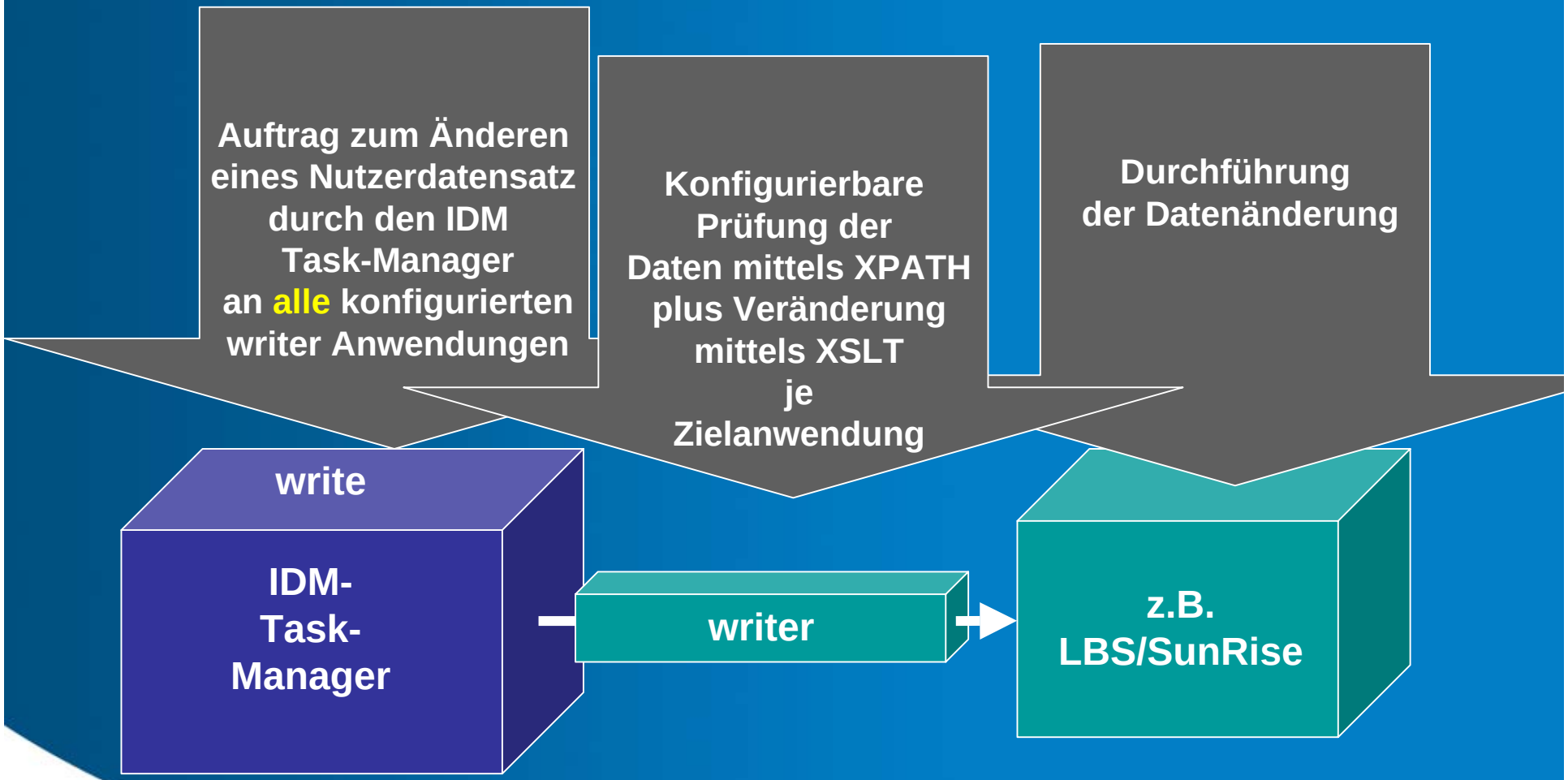
Architektur des Identity Servers



Arbeitsweise des IDM-Connectors I



Arbeitsweise des IDM-Connectors II



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