

# **„Virtuelle“ Benutzerverwaltung mit dem Sun Java System Identity Manager**

Dr. Wilfried Stüttgen  
Marktentwicklung Forschung & Lehre  
Sun Microsystems GmbH

**ZKI-Arbeitskreistreffen,  
15.12.04**



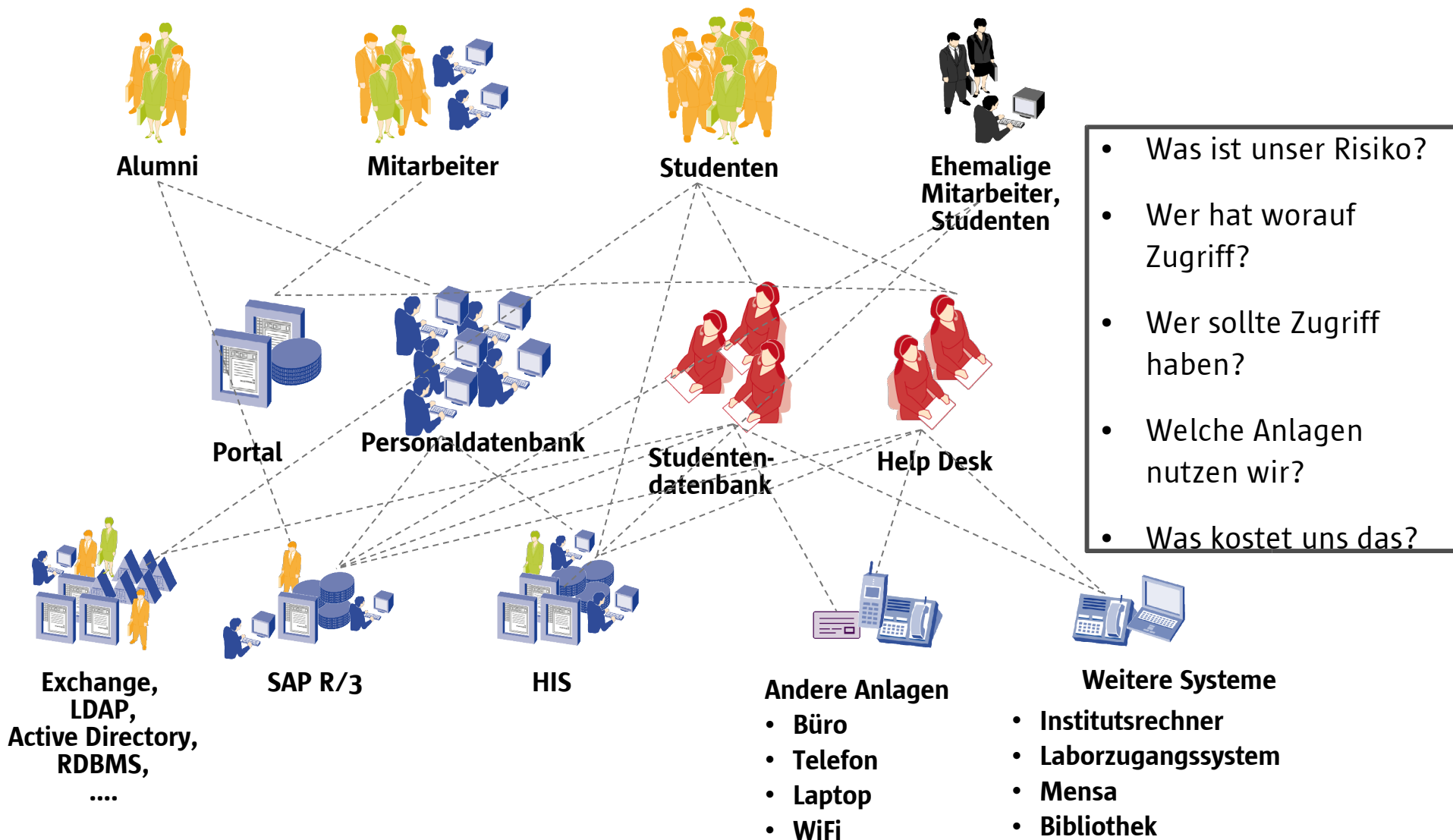


# Agenda

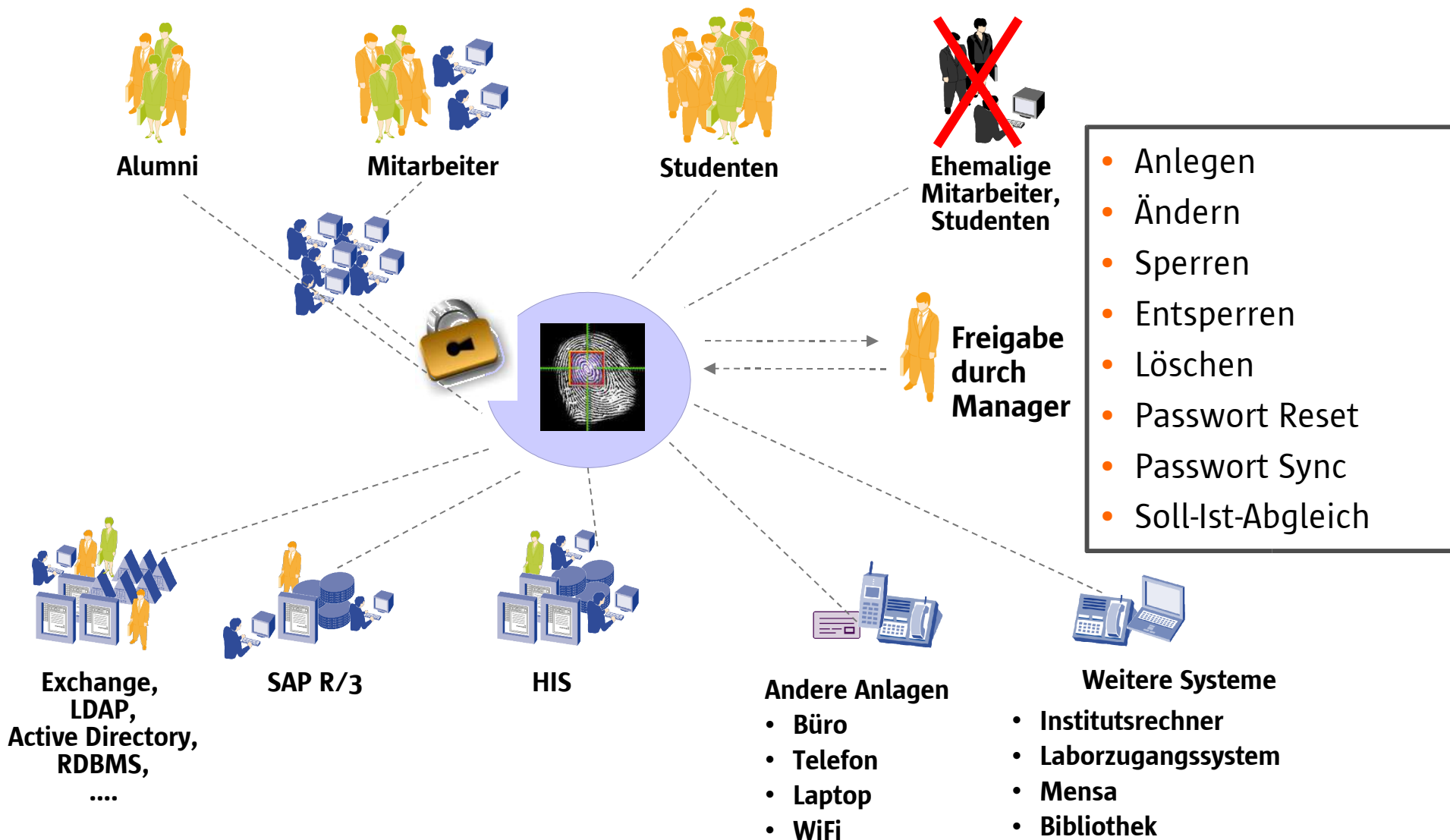
- Produktübersicht
  - Identity Manager
- Live Demonstration



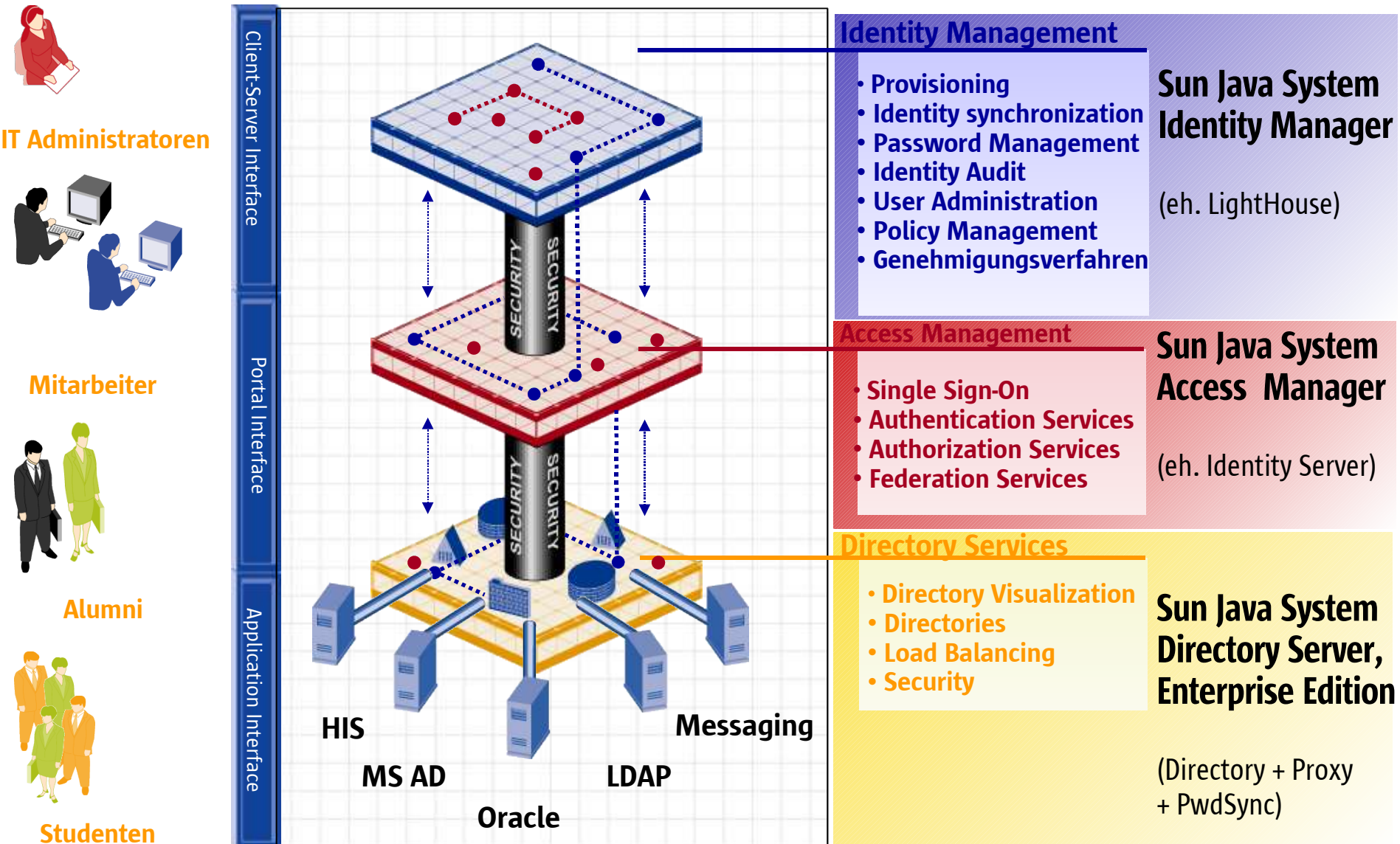
# Das Identity Chaos



## Das Ziel: Sicheres Identity Management

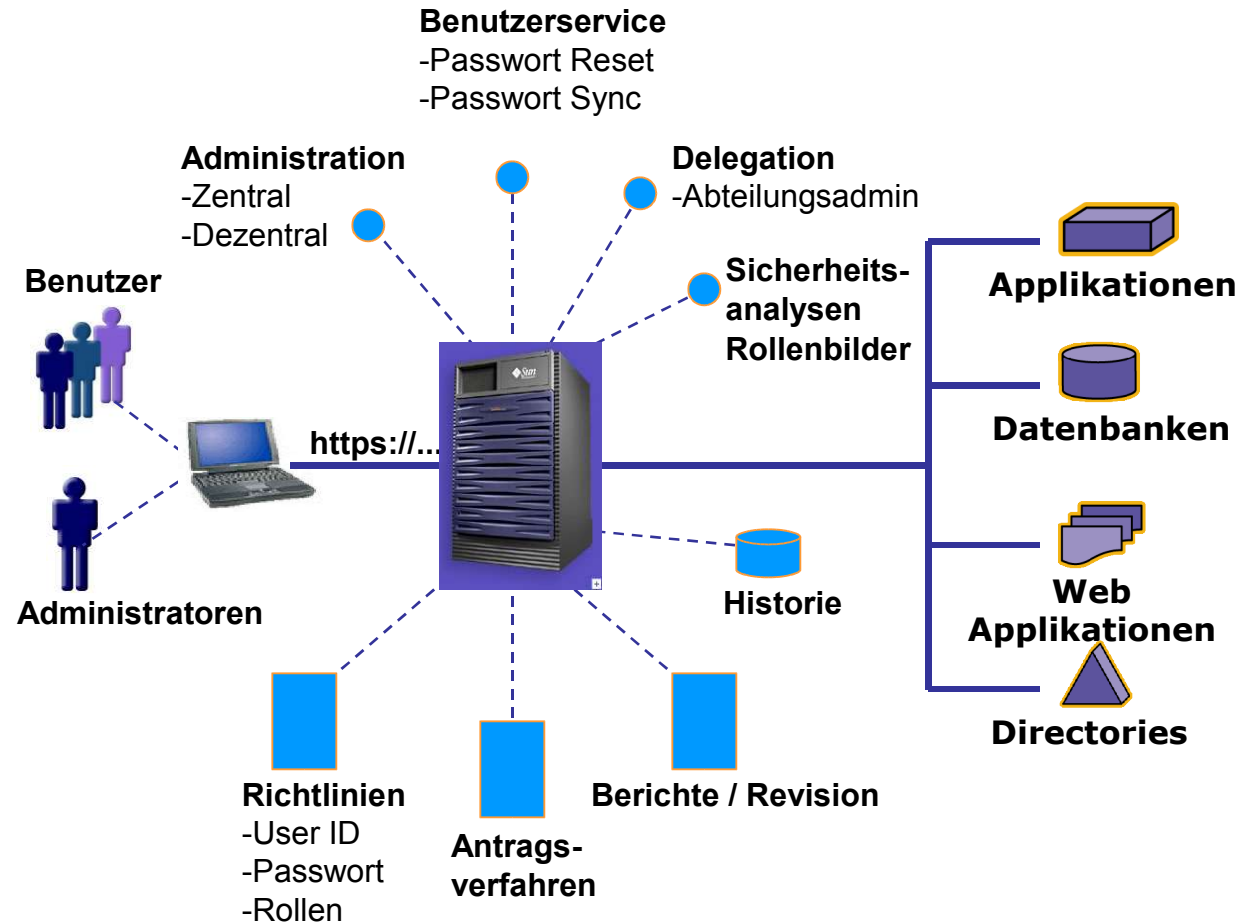


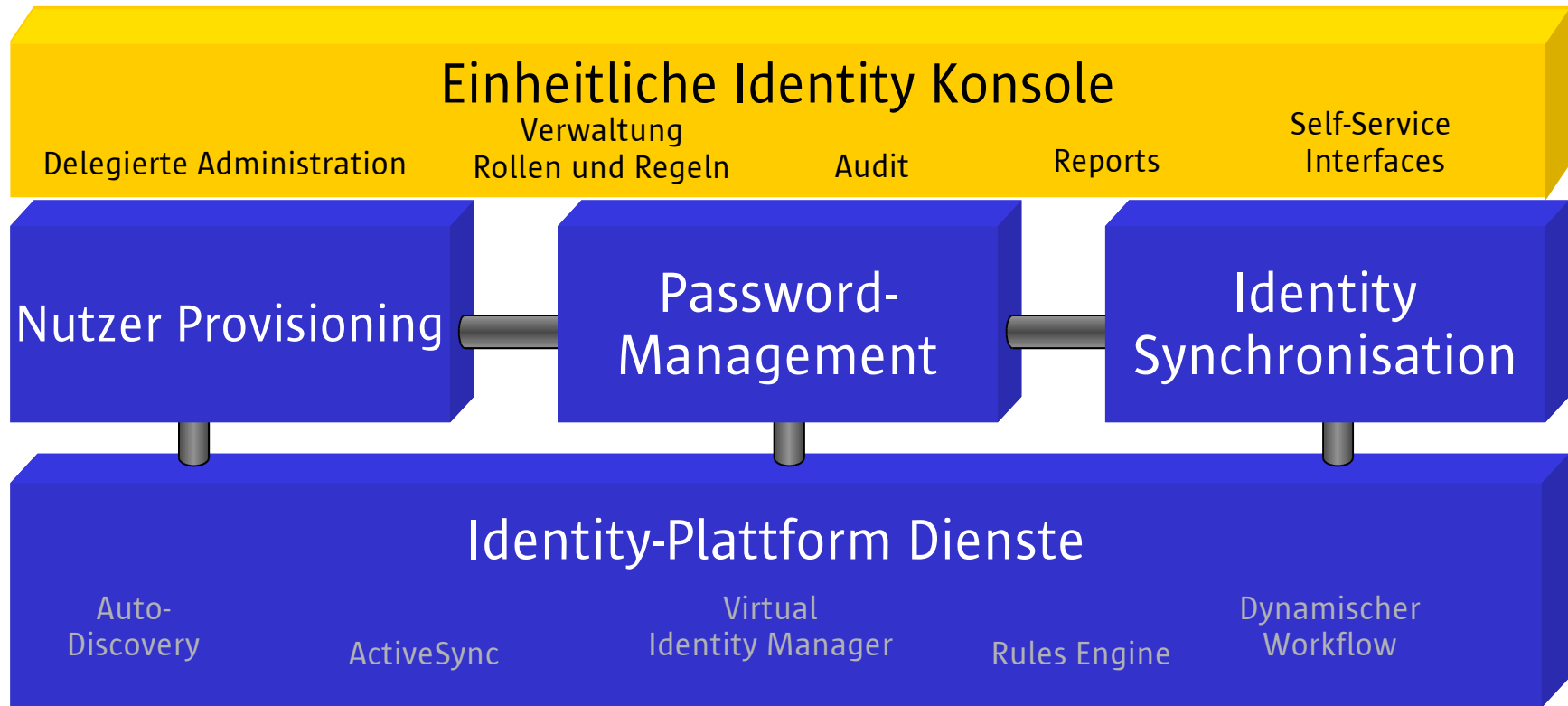
## Identity Management Suite



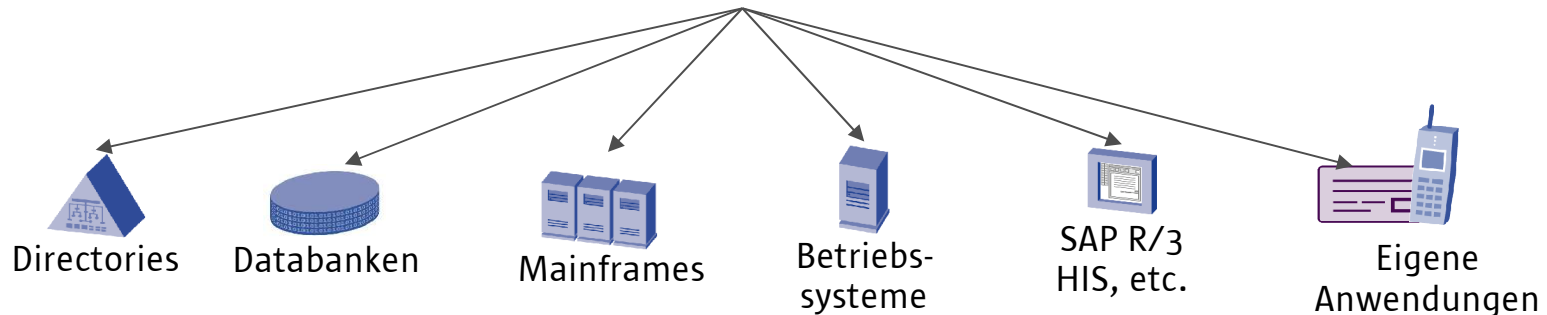


- Anlegen
- Ändern
- Sperren
- Entsperren
- Löschen
- Passwort Reset
- Passwort Sync
- Soll-Ist-Abgleich





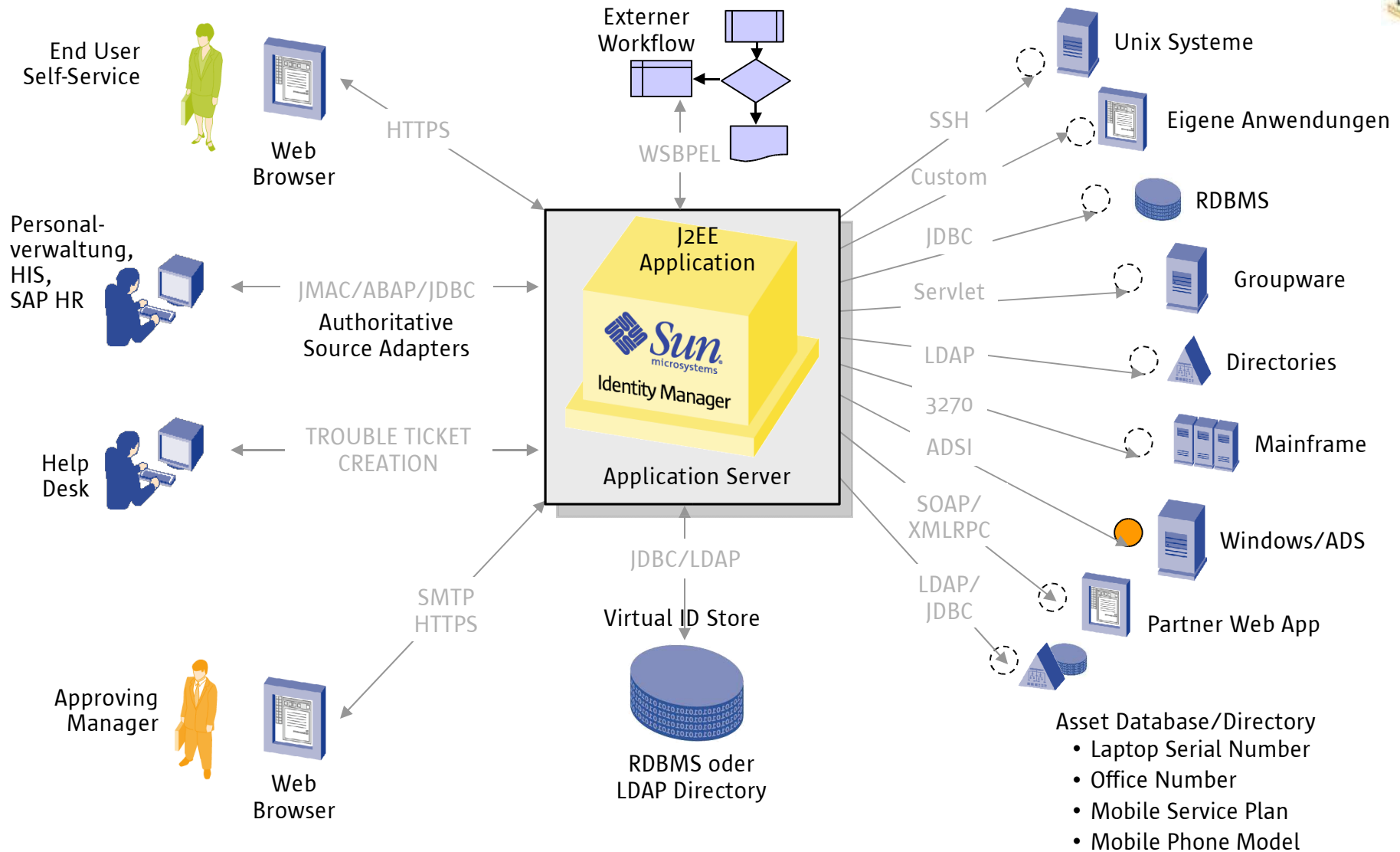
## Adapter ohne lokale Agenten



# Identity Manager Physical Architecture

○ Agent-less

● Gateway

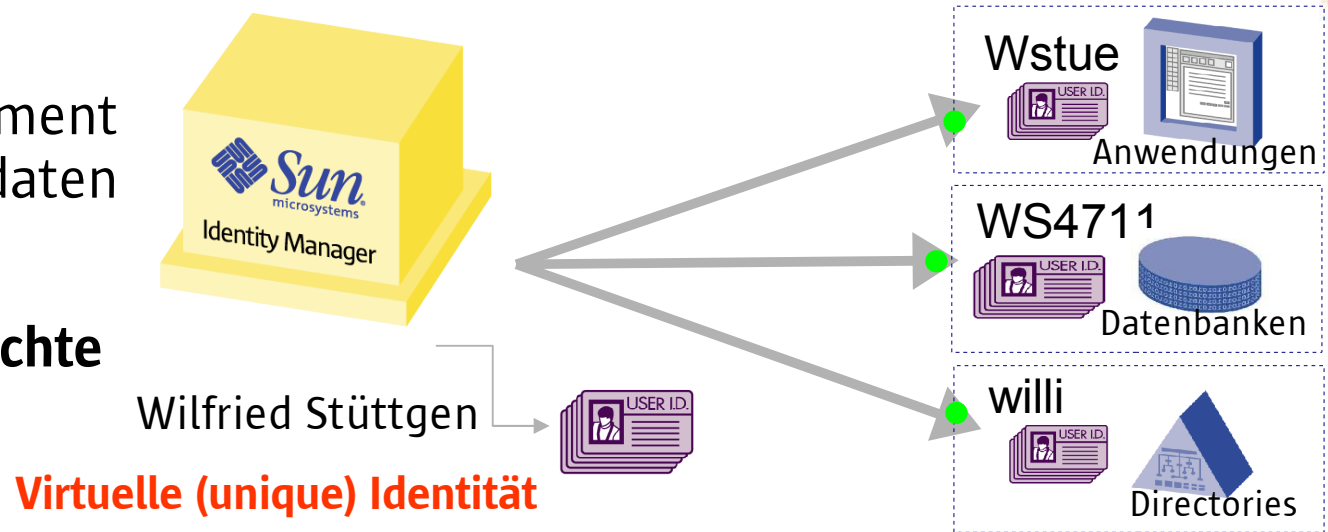




## Virtuell

Logisches Management  
verteilter Profildaten

Geringeres Risiko  
„verwaister“ Rechte



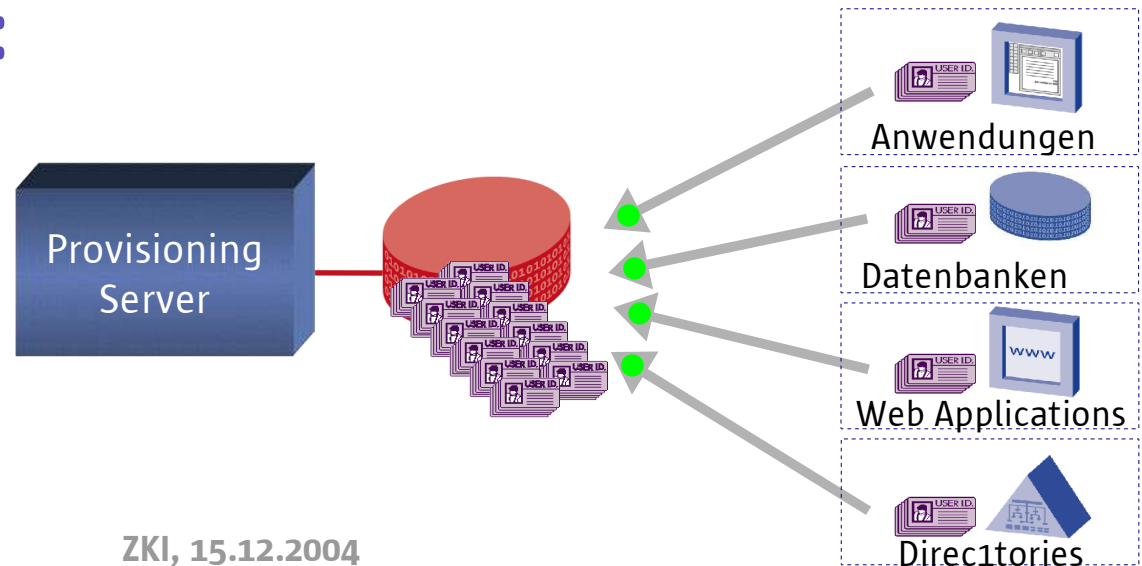
## Alternativer Ansatz: Zentrales Repository (Meta-Dir)

Schwer zu implementieren

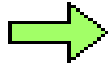
- Technisch, politisch
- MetaDirectory lastig

Schwer zu warten

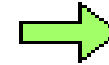
- Synchronisierung



Neuer Student,  
Mitarbeiter,  
...



Eintrag in  
HIS Modul,  
SAP,  
....  
(HIS Staging  
Tabelle)



Sun  
Identity  
Manager  
entdeckt  
neuen  
Eintrag



Identity Manager  
Authoritative  
Source Adapter



Verantwortlicher



Genehmigung



e-mail  
Benachrichtigung



Betriebssysteme



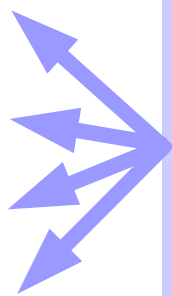
Bibliothek System



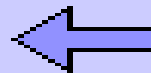
LDAP Directories



e-mail



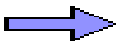
Anlegen  
des neuen  
Benutzers



Automatischer  
Start des  
Genehmigungs  
verfahren



Identity  
Manager  
wendet  
Regeln, Rollen  
und Policies  
auf den neuen  
Eintrag an.



Überwachung von Änderungen und  
Reporting





- Directory Servers
  - Sun JS Dir.Server, LDAP V3, MS AD, Novell eDir, Novell NDS, Oracle Internet-Dir.
- Database Servers
  - IBM DB2, Informix, MS SQL, MySQL, Oracle 8i / 9i, Sybase
- Applications
  - HIS, Oracle 11 eBusiness Suite, Peoplesoft, SAP R/3 Enterprise, SAP HR, Siebel CRM
- Helpdesk
  - Peregrine Service Center, Remedy Helpdesk
- Message Plattformen
  - Lotus Notes, MS Exchange, Novell Groupwise
- Operating Systems
  - Red Hat, Solaris, HP-UX, HP OpenVMS
  - IBM OS/400, IBM AIX, W2k / 2003, NT4
- Security Managers
  - CA ACF2, CA TopSecret, nTrust
  - RACF, RSA SecureID
- Web-Access Control-Plattformen
  - Sun JS Identity-Server, nTrust GetAccess, Tivoli Access Manager
  - Netegrity Siteminder, Oblix NetPoint, Open Network Directory Smart, RSA Cleartrust

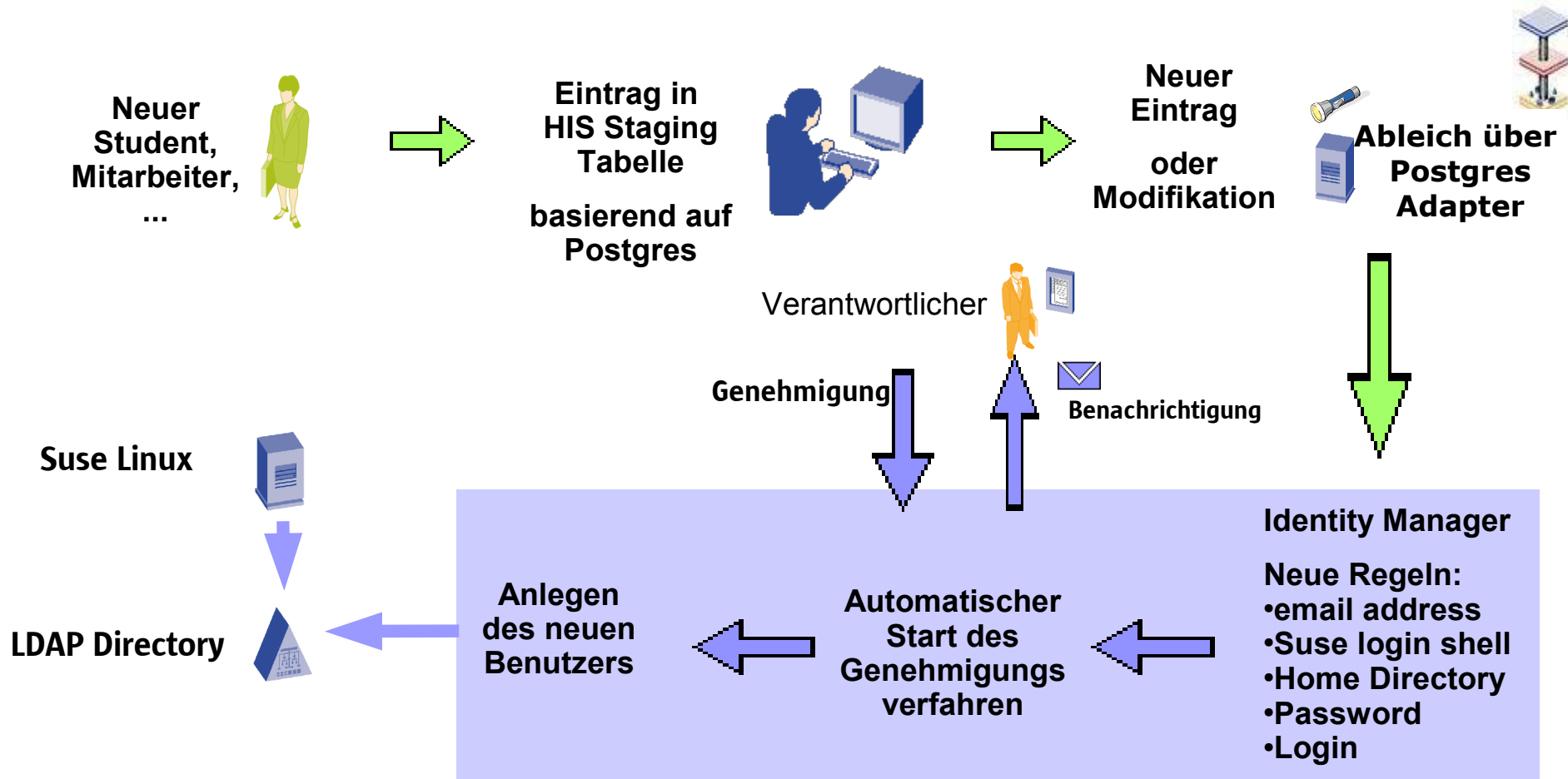


- alle Module / Forms etc. in Repository
- alles in XML / Java
- eigene Sprache: XPress
- integrierter Debugger
- intensives Logging (in Repository)
- eigene Resource-Adapter “leicht” in Java zu erstellen



# Alleinstellung

- Adapter ohne lokale Agenten
  - Kein Eingriff ins Quell-/Zielsystem
  - Geringer Wartungsaufwand
- Virtual Identity Manager
  - Daten bleiben bei den 'Besitzern'
  - Datenschutz eher unkritisch
- Basis Java und XML
  - Verwendung ausschliesslich von Standards



## Anpassungen:

- Konfiguration Postgres und LDAP Adaptor
- Konfiguration der Regeln
- Konfiguration der UserForm
- Konfiguration HIS\_role
- LDAP Attribute Studentnumber

**Aufwand inkl. Installation, Anpassungen, Tests – ca. 1.5 Tage**



**Haben Sie Fragen?**

[wilfried.stuettgen@sun.com](mailto:wilfried.stuettgen@sun.com)

