



Agenda



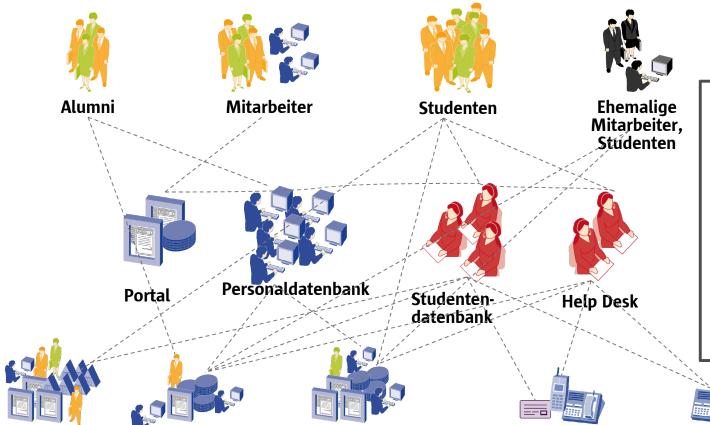
- Produktübersicht
 - Identity Manager
- Live Demonstration

Unvollständig, manuell, unsicher



Das Identity Chaos





- Was ist unser Risiko?
- Wer hat worauf Zugriff?
- Wer sollte Zugriff haben?
- Welche Anlagen nutzen wir?
- Was kostet uns das?

Exchange, LDAP. **Active Directory,** RDBMS.

SAP R/3

HIS

Andere Anlagen

- Büro
- Telefon
- Laptop
- WiFi

ZKI, 15.12.2004

Institutsrechner

Laborzugangssystem

Weitere Systeme

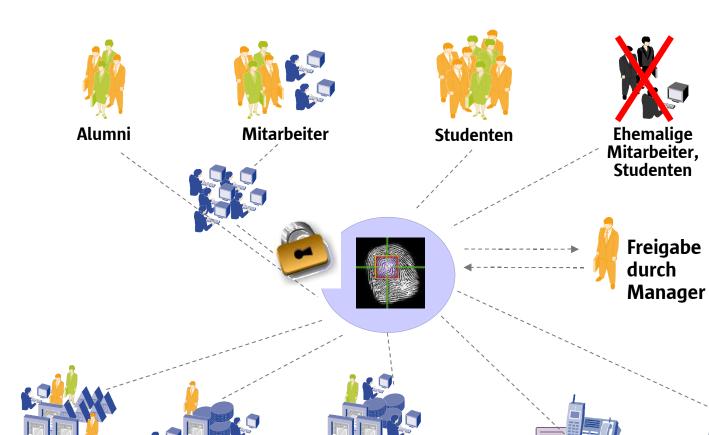
- Mensa
- Bibliothek

Einheitlich, automatisiert und sicher



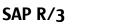
Das Ziel: Sicheres Identity Management





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

Exchange, LDAP. **Active Directory,** RDBMS.



HIS

Andere Anlagen

- Büro
- Telefon
- Laptop
- WiFi

Weitere Systeme

- Institutsrechner
- Laborzugangssystem
- Mensa
- Bibliothek

ZKI, 15.12.2004

Komplexität in mehreren Dimensionen



Identity Management Suite





IT Administratoren



Mitarbeiter

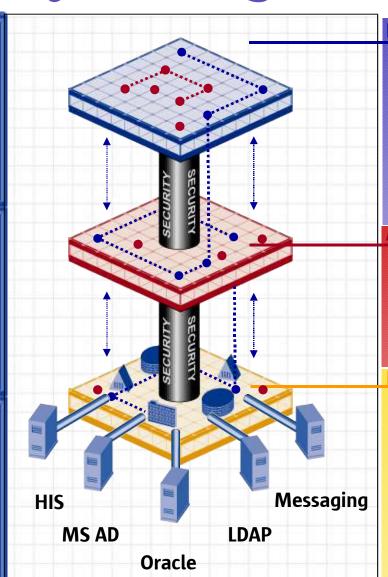


Alumni



Application Interface

Studenten



Identity Management

- **Provisioning**
- **Identity synchronization**
- **Password Management**
- **Identity Audit**
- **User Administration**
- **Policy Management**
- Genehmigungsverfahren

Sun Java System **Identity Manager**

(eh. LightHouse)

ccess Management

- Single Sign-On
- **Authentication Services**
- **Authorization Services**
- **Federation Services**

Sun Java System **Access Manager**

(eh. Identity Server)

irectory Services

- Directory Visualization
- Directories
- Load Balancing
- Security

Sun Java System **Directory Server, Enterprise Edition**

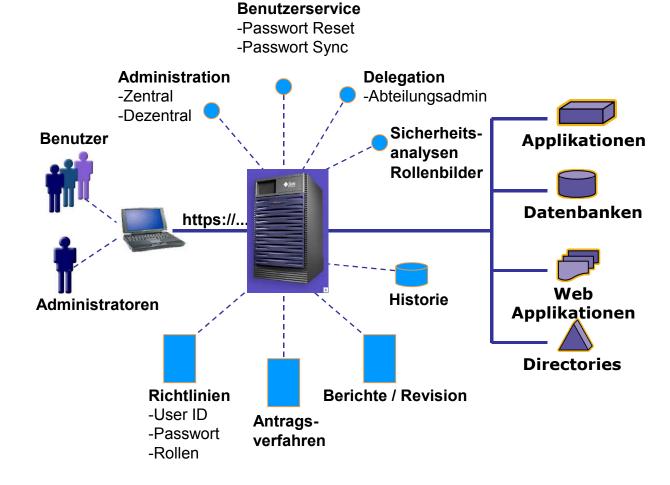
(Directory + Proxy + PwdSync)

Identity Life Cycle Management





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



Sun Java System Identity Manager





Einheitliche Identity Konsole

Delegierte Administration

Verwaltung Rollen und Regeln

Audit

Reports

Self-Service Interfaces

Nutzer Provisioning

Password-Management Identity Synchronisation

Identity-Plattform Dienste

Auto-Discovery

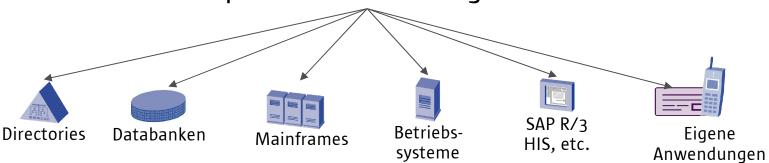
ActiveSync

Virtual Identity Manager

Rules Engine

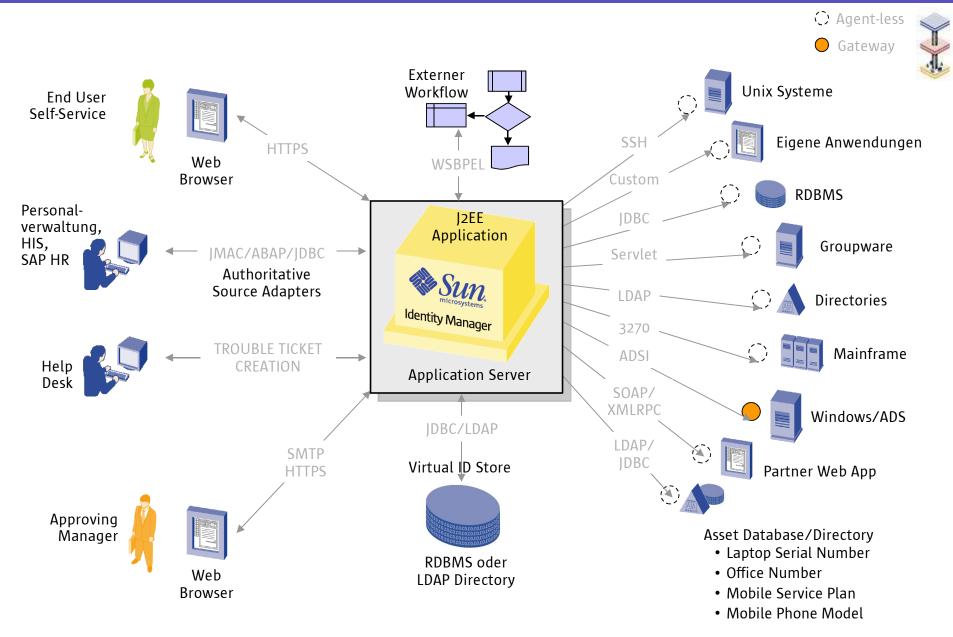
Dynamischer Workflow

Adapter ohne lokale Agenten



Identity Manager Physical Architecture





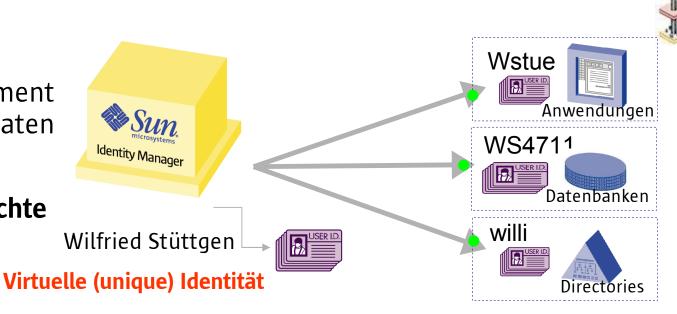
Virtuell versus Zentrales Verzeichnis



Virtuell

Logisches Management verteilter Profildaten

Geringeres Risiko "verwaister" Rechte



Alternativer Ansatz:

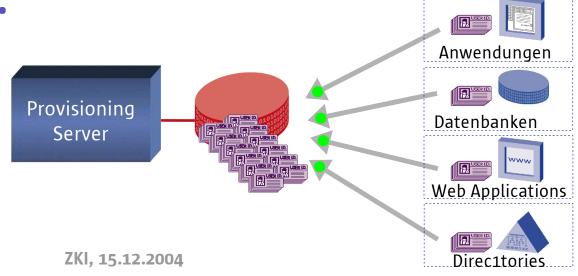
Zentrales Repository (Meta-Dir)

Schwer zu implementieren

- Technisch, politisch
- MetaDirectory lastig

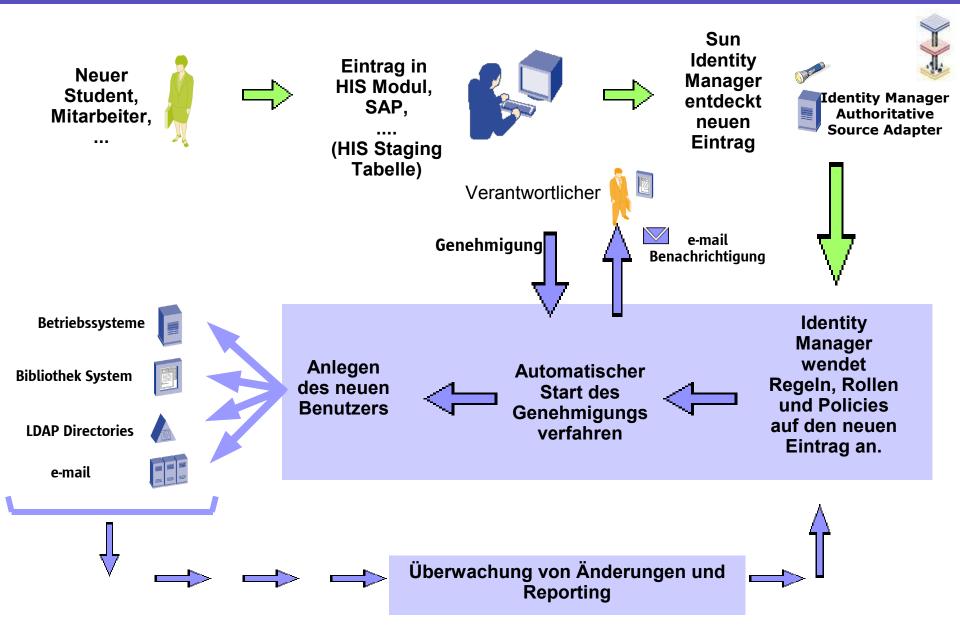
Schwer zu warten

Synchronisierung



Automatische Provisionierung





Resources Adapter





- 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 Plattforms
 - 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-Platforms
 - 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



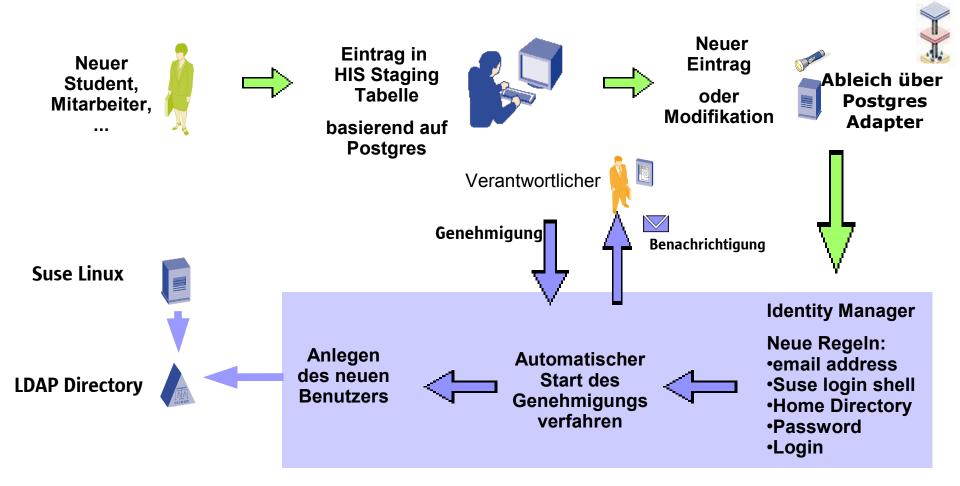
Alleinstellung



- 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

Demo Szenario





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

