



# Identity Management - mit Sicherheit Kosten senken

## Identity Management Day

15. Februar 2005

Jürgen Bachinger

Hewlett-Packard GmbH

Antje Hüllinghorst

Triaton GmbH ein  
Unternehmen von HP

© 2004 Hewlett-Packard Development Company, L.P.  
The information contained herein is subject to change without notice



# Identity Management – mit Sicherheit Kosten senken



- Teil 1: Einführung und Grundlagen
  - Komponenten und Lösungsbausteine
  - Business Case
- Teil 2: Fallstudie ThyssenKrupp
  - Ausgangssituation
  - Architektur und Vorgehensmodell
  - Herausforderungen bei der Implementierung

# Adaptive Enterprise – die Herausforderung



Das Business verändert sich ständig!

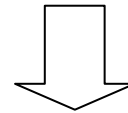


Und die IT muss folgen ...

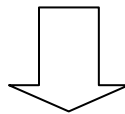
# IdM – das Grundproblem

## Viele getrennte Systeme

- Getrennte Benutzer- / Rechteverwaltung
- Systemübergreifende Transaktionen

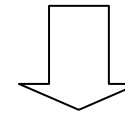


## Hohe Komplexität



## Sicherheitsprobleme

- Aufschreiben von Passwörtern
- Zu hohe, inkonsistente oder veraltete Berechtigungen



## Aufwendige Administration

- Redundanzen und Änderungsanomalien
- Hoher Support (Passwortreset)

# Komponenten des Identity Managements



## Management Komponenten

User Mgmt

Access  
Control Mgmt

Privacy  
Mgmt

Federation  
Mgmt

Consumable Value

Single Sign-On

Personalization

Self Service

Life Cycle

Provisioning

Longevity

Security

Authentication

Authorization

Auditing

Data Repository

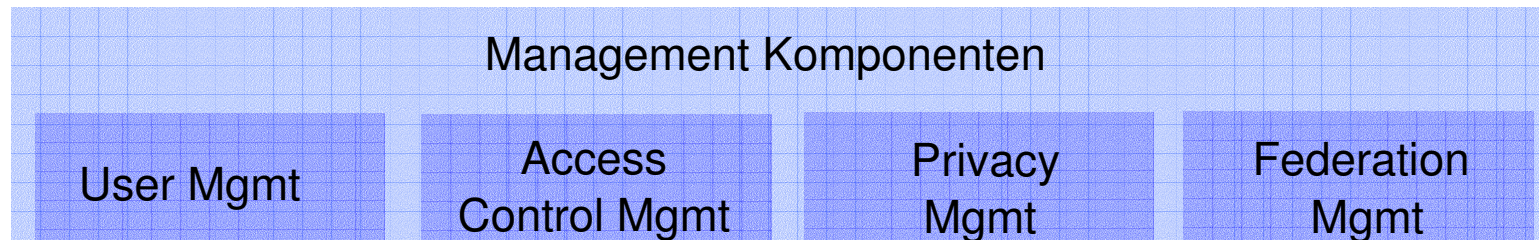
Directories

Meta-Directories

Virtual Directories

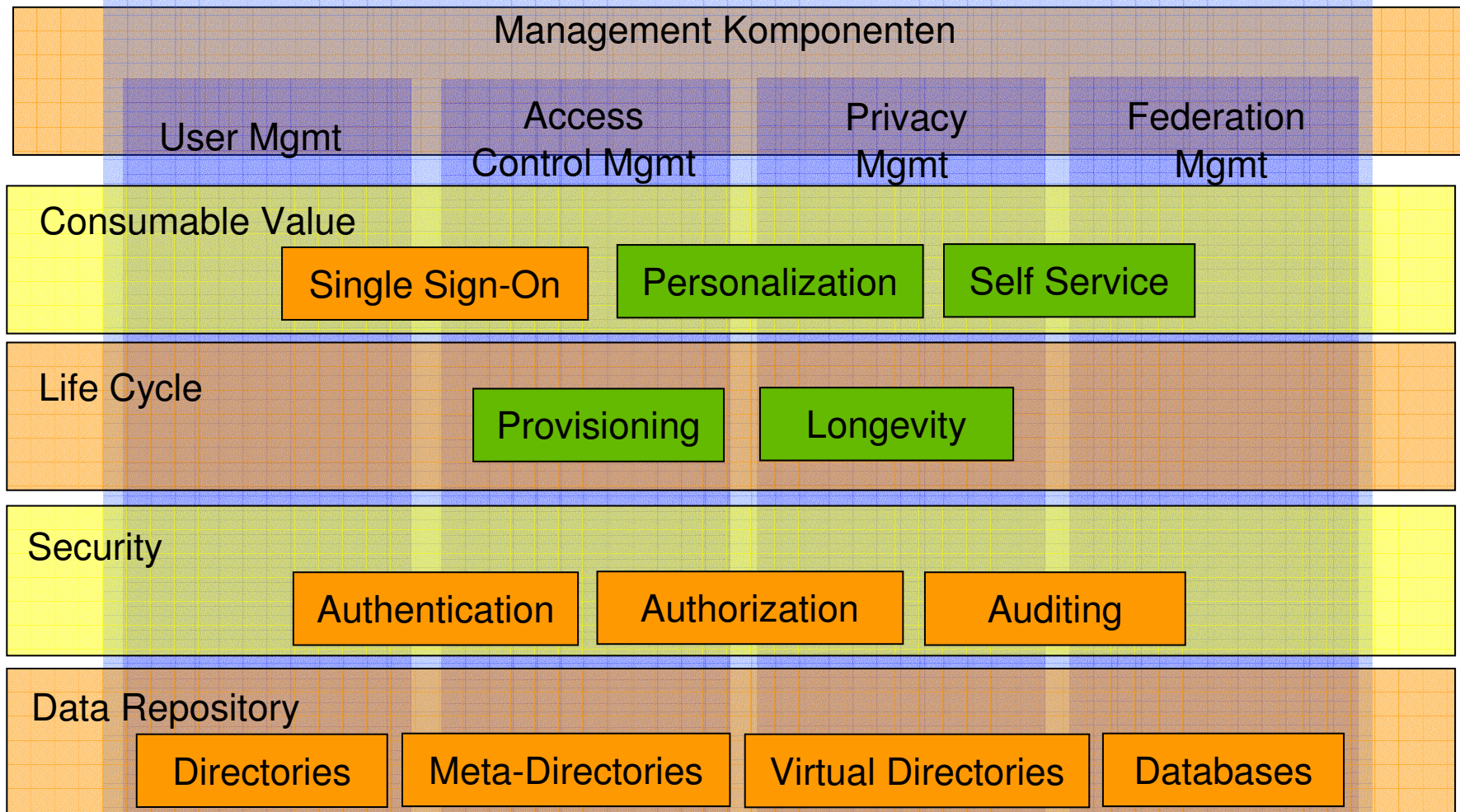
Databases

# Lösungsbausteine – Directory Integration



- Enterprise Directory
  - Zentraler Datenpool
  - Beispiel: Microsoft ADS
  - Problem: Schemadefinition, Zugriff
- Meta Directory
  - Directory Synchronisation (HP Tool: LDSU)
  - LDAP / RDBMS
- Virtual Directory
  - Einheitliche Schnittstelle
  - Dynamischer Zugriff

# Lösungsbausteine – Identity Provisioning



HP Open View Select Identity

# Lösungsbausteine – Access Management

- Zugang zu Anwendungen
  - Single Sign On
  - Passwort-Synchronisation
  - Passwort-Management
- Berechtigungen
  - LDAP basierende Anwendungen
  - Web-Services
    - SAML
    - Liberty ID-WSF

# Business Case

- Reduzierung von Risiken
  - Keine trivialen oder aufgeschriebenen Passwörter
  - Aktuelle, konsistente und angemessene Berechtigungen
- Einhaltung von Gesetzen und Regelungen
  - Kontrollierte und nachvollziehbare Zugriffe
- Flexibilität und Effizienz
  - Administrativer Aufwand wird reduziert
  - Prozesse werden beschleunigt

# Business Case – Enterprise Directory

- Vorteile eines Enterprise Directory
  - Geschäftsprozesse werden beschleunigt
  - Verwaltungsaufwand wird minimiert
  - Einfachere Entwicklung neuer Anwendungen
- **Beispiel** (Quelle: Gartner Group)
  - Unternehmen mit 25.000 Mitarbeiter
  - 15 verschiedene Directories
  - Umstellung auf ein einheitliches Directory
  - Einsparung von \$24/User => Gesamteinsparung \$600.000

# Business Case – User Self Service

- Große Anzahl von potentiellen Anwendern
  - Nur bei Bedarf: hoher Aufwand im User Management
  - Freigabe für alle: ineffizienter Einsatz von Ressourcen
- Lösung: User Self Service
  - Workflow für Freigabe
  - Anstoß durch Anwender
  - Freigabe (halb-) automatisch
- Beispiel (Quelle: RSA Security)
  - Regierungsbehörde in USA – Studentenkredite
  - Vorher: Kontoabfrage, Überweisungen, etc. per 0800-Nummer
  - Neu: User Self Service => Einsparung: 50% im Call Center

# Business Case – Password Reset

- Ausgangssituation
  - Viele Passworte
  - Unterschiedliche Passwort-Regeln
- Auswirkungen
  - Hohe Belastung im Support
  - Ausfallzeiten bei Anwendern
- Lösungen
  - Passwortmanagement / -Synchronisation
  - Single Sign On



## Teil 2: Case Study ThyssenKrupp AG

- Vorstellung Kunde
- Vorgeschichte
- Ziele, Auslöser und Anforderungen
- Projektrahmenbedingungen
- Lösung
- Stand und Ausblick
- Zusammenfassung
- Lessons learned



# Der Kunde

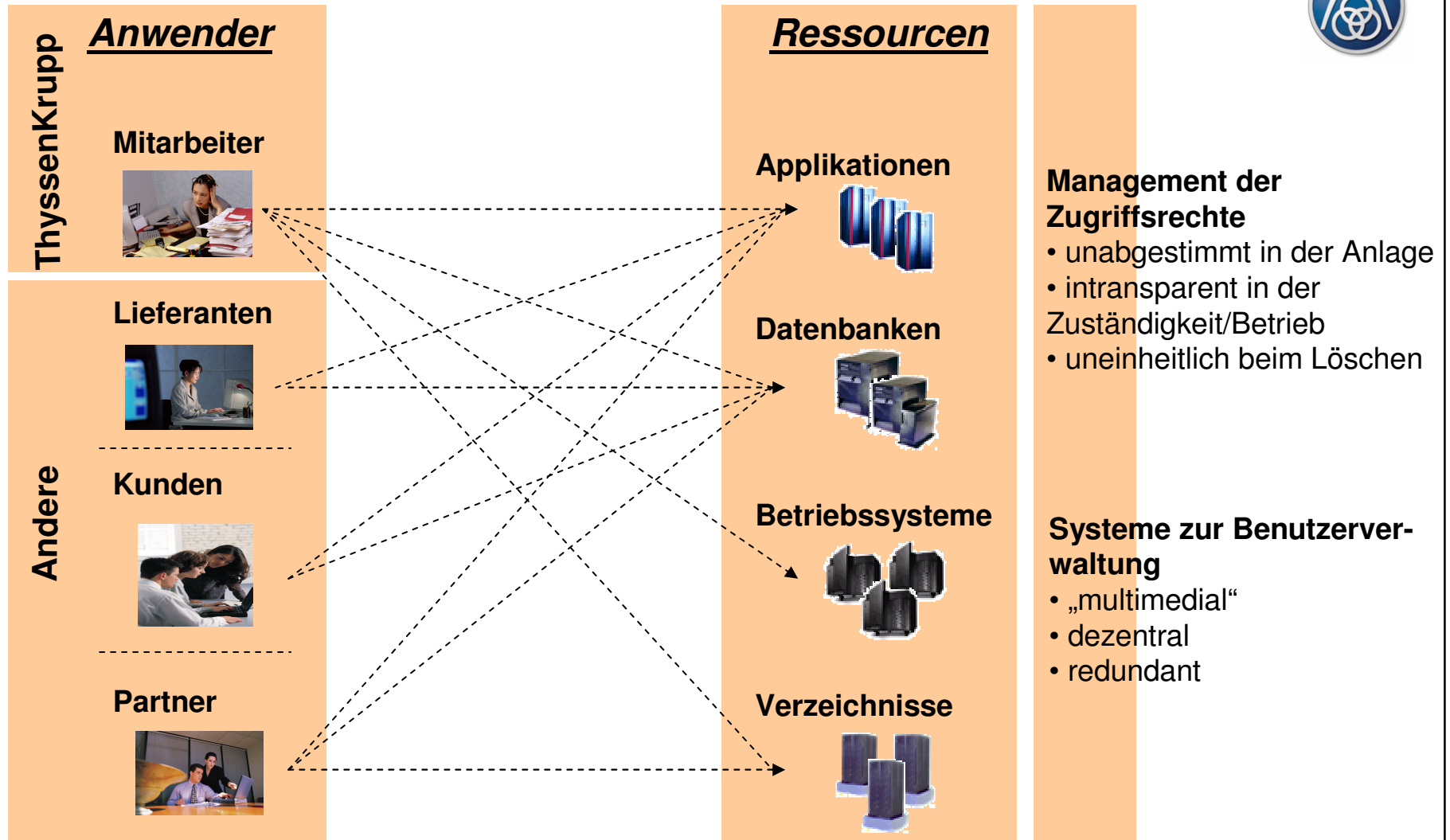
- ThyssenKrupp ist einer der größten Technologiekonzerne weltweit. Mehr als 184.000 Mitarbeiter arbeiten rund um den Globus für die Schwerpunktbereiche Stahl, Industriegüter und Dienstleistungen. Sie erwirtschafteten im Geschäftsjahr 2003/2004 einen Umsatz von mehr als 39 Milliarden Euro
- Es gibt ca. 700 einzelne Konzernunternehmen (KUs), aufgeteilt auf fünf Segmente
- Die ThyssenKrupp AG ist die Holding des Konzerns
- Die einzelnen KUs sind dezentral organisiert und eigenständig



# Die Vorgeschichte

- 2001/2002: Die TKAG bietet den einzelnen KUs, Kunden und Lieferanten immer mehr Online-Services
- Fragestellung: Woher kommen die Benutzerdaten für das Access Management?
- Anfang 2003: Workshop zur Festlegung der weiteren Vorgehensweise
- Fazit: Identity Management bedeutet mehr und ist wichtiger als Access Management und Provisioning
- Idee: Aufbau eines Meta-Directories
- Aber: Anforderungen des Konzerns zu komplex, kein „einfaches“ Design möglich
- Focus auf Identity Management
- Entscheidung: Identity Management Produkt wird gekauft

# Ausgangssituation





# Die Ziele der TKAG mit IDM

- Eindeutige Identifikationsnummer für jeden Konzernmitarbeiter, um z.B. Rentenansprüche über ein ganzes „Konzernleben“ verfolgen zu können
- Aufbau eines Systems zur Vorhaltung von Mitarbeiterdaten aller Konzernmitarbeiter (ca. 184.000). Darüber hinaus Kunden, Lieferanten, TK Rentner, etc. (ca. 300.000)
- Kostensenkung für Zugriffs- und Benutzermanagement
- Einsparungen, z.B. durch einheitlichen Passwortreset, Programmierrichtlinien, einheitliche Architektur etc.
- Erhöhung der Datensicherheit



# Der Auslöser des Projekts

- 2003: Der ThyssenKrupp Konzern plant die Ausgabe von Belegschaftsaktien (BA)
- Das BA-System wird von Triaton programmiert
- Aktuelle Daten aller Konzernangehörigen werden benötigt
- IDM wird der AG angeboten, BA als der erste Anwendungsfall ausgewählt
- ROI wird über die Funktion „Passwortreset“ gerechnet
- Der Vertrag über IDM wird unterschrieben



# Die konkreten Projektanforderungen

- System muss mandantenfähig sein
- Alle KUs müssen ihre Daten selber pflegen können, da die KUs Eigner der Personaldaten sind
- Die Pflege darf nicht zu komplex sein
- Die Struktur muss sowohl Konzernmitarbeiter als auch Partner, Kunden etc. beinhalten
- EVA-Prozesse müssen abbildbar sein
- Die Verfolgung einer Person über ihr „Konzern-Leben“ muss gewährleistet sein
- Der Datenbestand muss möglichst aktuell sein



# Die Projektrahmenbedingungen

- Projektaufwand: ca. 1.800 PT
- Projektteam:
  - Kern: vier Leute aus den beteiligten Bereichen
  - Erweitert: ca. 20
  - Wichtig: Beteiligung von Konzernbetriebsrat, Konzerndatenschützern, HR-Mitarbeitern
- Zusagen: Verfügbarkeit des Systems von 99,5%
  - 24x7, 365 Tage im Jahr



# Die Lösung

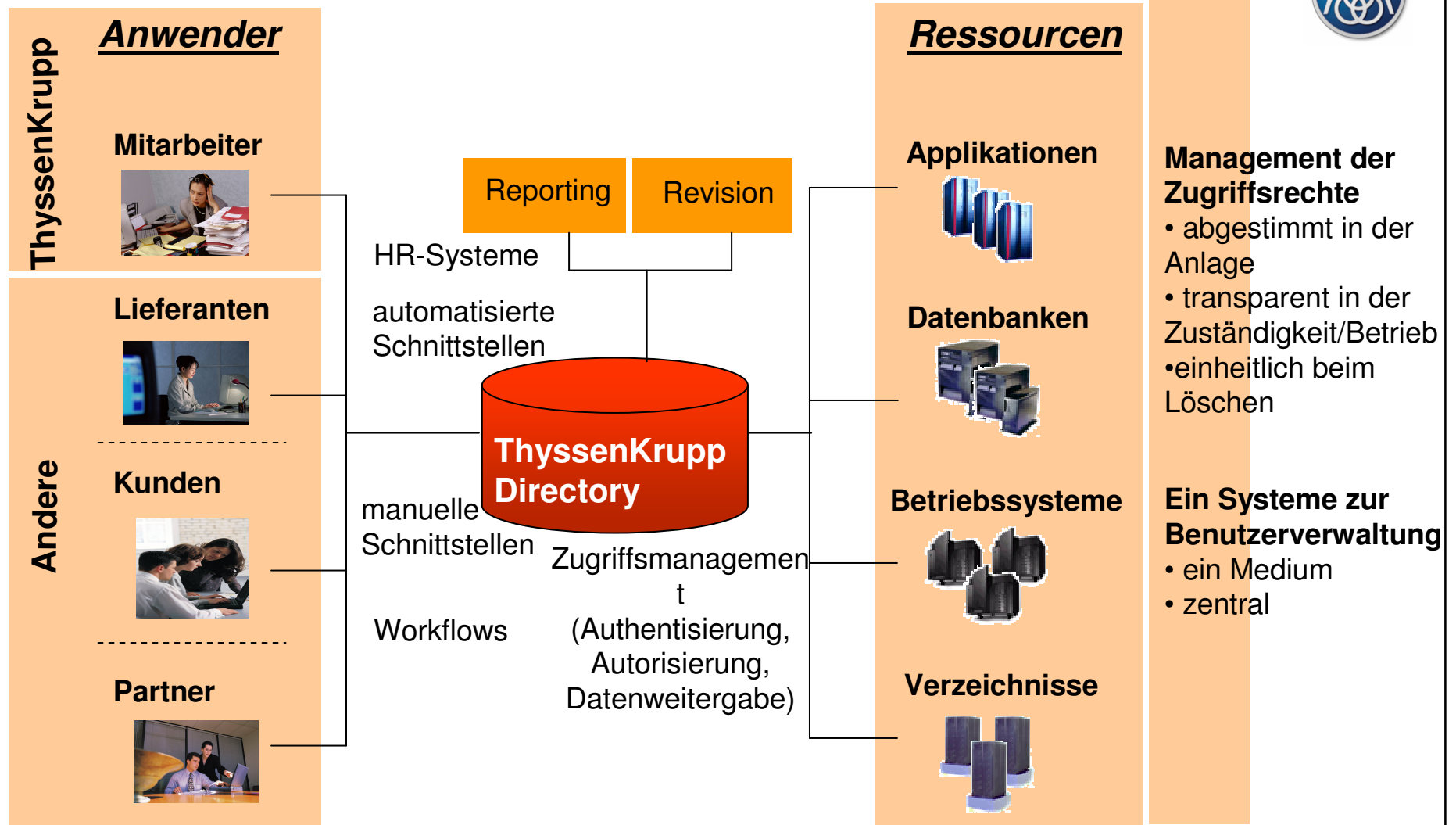
- Design einer flachen Verzeichnis-Hierarchie
- Jeder TK Mitarbeiter bekommt eine eindeutige, achtstellige Nummer (TK Id) zugewiesen
- Klasse „TK Person“ mit TK spezifischen Attributen wird eingerichtet
- Strukturen für Partner und Kunden werden angelegt
- Steuerung von Pflegerechten an Mitarbeiterdaten über Firmenzugehörigkeit (FKZ)
- Aufteilung nach Segmenten
- Initialbefüllung des IDM mit 110.000 Personen



# Aktueller Stand

- Aktueller Datenbestand befindet sich im IDM
- Kopplung von IDM an ein Access Management System ist erfolgt
- Zentrales Directory für den gesamten Konzern zur Authentisierung und Autorisierung an WEB-Anwendungen wurde aufgebaut
- Weitere Projekte im IDM-Umfeld:
  - Definition und Implementierung HR-Schnittstelle
  - PIN-Rollout
  - Anbindung TKnet
  - Anbindung Adressmanager für Konzernmailadressen
  - Anbindung Exchange

# Zielzustand





# Lessons learned

- **Der Kunde muss von Anfang an aktiv mitarbeiten!**
- Die Anforderungen müssen klar definiert sein
- Die Implementierung von Tools ist nur ein kleiner Teil des Gesamtprojekts
- Die Definition von Prozessen ist extrem wichtig
- Einbeziehung von Betriebsrat, Datenschützern, HR etc.
- HP und Triaton erbringen alle Dienstleistungen rund um das Thema „Identity Mangement“:
  - Beratung
  - Implementierung und
  - Betrieb!

# Vielen Dank für Ihr Interesse



February 5, 2005

# Zusammenfassung

- Identity Management ist ein komplexes Thema
- Keine schlüsselfertigen Lösungen
- Integration unterschiedlicher Bausteine notwendig
- Hohes Potential zur ...
  - Erhöhung der Sicherheit
  - Effizienzsteigerung
  - Reduktion der Kosten
- Identity Management lohnt sich!



i n v e n t