Integrierte IT-Service-Management-Lösungen anhand von Fallstudien

Identity Management

Dr. Kirsten Bönisch et al.,
Prof. Dr. Heinz-Gerd Hegering

Institut für Informatik
Ludwig-Maximilians-Universität München

Sommersemester 2008

Identity Management.
Agenda.

- Scope
  Was ist Identity Management?
- Anforderungen
  Wofür brauchen Unternehmen Identity Management?
- Theorie
  Grundprinzipien des Identity Managements.
- Herausforderungen
  Was macht Identity Management so komplex?

Identity Management.
Agenda.

- Scope
  Was ist Identity Management?
- Anforderungen
  Wofür brauchen Unternehmen Identity Management?
- Theorie
  Grundprinzipien des Identity Managements.
- Herausforderungen
  Was macht Identity Management so komplex?

Identity Management - Scope.
Was ist Identity Management?

- Identität
  - juristische oder natürliche **Person**
  - technisches **Objekt/System**
  - besteht aus einer (Mindest-)Anzahl von Attributen
    - Stammdaten: Name, Abteilung, Standort, …
- Management von Identitäten (in der IT)
  - Identität
    - ist **identifiziert** und **authentisiert**
    - hat **Zugriff** auf alle erforderlichen IT-Ressourcen (aber nicht auf mehr)
  - Zugriffsrechte und deren Erteilung sind „**revisionssicher**“
- Provisionierung
  - Vorgang der **Eintragung** der gewünschten Rechte in die angeschlossenen Systeme („**IT-Ressourcen**“)

Identity Management - Scope.
Ausgangsfrage.

Wie kann man
den richtigen Identitäten
zum richtigen Zeitpunkt
effizient und nachvollziehbar
Zugang zu den richtigen IT-Ressourcen
verschaffen?

- Die Antwort beinhaltet
  - **Regeln**, wie Endbenutzer an Berechtigungen kommen
  - **Workflows**, um die Berechtigungen zu beantragen
  - **Technik**, mit der die Berechtigungen in die Systeme und Applikationen geschrieben („provisioniert“) werden
  - Abläufe und Technik zur **Kontrolle** und **Auditierung** dieser Vorgänge
  - … und natürlich **Entwurf, Umsetzung und Weiterentwicklung** dieser Prozesse und Systeme

Identity Management.
Agenda.

- Scope
  Was ist Identity Management?
- Anforderungen
  Wofür brauchen Unternehmen Identity Management?
- Theorie
  Grundprinzipien des Identity Managements.
- Herausforderungen
  Was macht Identity Management so komplex?

Identity Management - Anforderungen.
Ausgangslage I.

- Fehlender Komfort für den Endbenutzer
  - **Rechtebeantragung** und -erteilung dauert **lange** und ist **aufwändig**
  - Häufig „**klappt der Zugriff nicht**“
  - Wenig Möglichkeiten, Rechte z.B. vom Vorgänger zu übernehmen („**ich will die gleichen Rechte wie der Kollege**“)

- Hohe Kosten in der IT
  - **Mehrfache** Benutzer-Verwaltung in Einzelapplikationen **aufwändig** und **teuer**
  - **Mehrfacher** Aufbau und Betrieb von Benutzer-Management-Lösungen ist teuer
  - **Kontrollen** müssen **manuell** durchgeführt werden

Identity Management - Anforderungen.
Ausgangslage II.

- Unzureichende Sicherheit
  - Differenzierte Rechteverwaltung aufwändig; daher oft pauschale **Einrichtung** von „**Superusern**“
    - „**Ich gebe Dir gleich alle Rechte, dann musst du nicht noch mal fragen**“
  - Rechte werden nicht gelöscht, wenn sie nicht mehr benötigt werden
    - „**Vielleicht brauche ich das noch mal**“
- Fehlende Nachvollziehbarkeit
  - Keine Möglichkeit zur Feststellung, wer zu welcher Zeit auf was Zugriff hatte
  - **Unerwünschte Rechtekombinationen** technisch nicht zuverlässig zu verhindern
  - **Erfüllung gesetzlicher Anforderungen** aufwändig oder unmöglich („Compliance“)

Identity Management - Anforderungen.

Anforderungen aus Endbenutzersicht.

- Komfortabel
  - Nutzer bekommen mit **wenig Aufwand alle Rechte**, die für Aufgabe erforderlich sind
    - Beantragung einfach und schnell
    - Rechte sinnvoll gruppiert
    - Kein IT-Know-How erforderlich
  - Vision: **zu jeder Aufgabe/Rolle im Unternehmen automatische Erteilung der erforderlichen Rechte**
- Standardisiert
  - Einheitlicher **Einstiegspunkt**
  - Einheitliche **Logik** zur Beantragung
  - Möglichst **wenig Passwörter**, Token, Anmeldenamen, …
  - (Single Sign On und Passwortsynchronisation, wo möglich)

Identity Management - Anforderungen.

Anforderungen aus Unternehmenssicht.

- Standardisiert
  - Einheitliche **Genehmigungs-Workflows**
  - Einheitliche **Authentisierungsverfahren**
  - Zentrale **IdM-Datenbasis**
- Kostengünstig
  - Automatische Rechteerteilung, wo möglich
  - **User Self Service**, wo möglich
  - Flächendeckende Nutzung des IdM-Systems
- Sicher
  - Rechteerteilung **nur über das IdM-System**
  - Rechteerteilung **nur nach Genehmigung**
  - **Rechteentzug**, wenn Genehmigungsgrund entfällt
- Auditierbar
  - Alle Administrationsschritte nachvollziehbar

Identity Management - Anforderungen.
Identitätstypen und Mengengerüst.

- Mitarbeiter (100T)
- Externe Dienstleister und deren Mitarbeiter (100T)

- Applikations- und Gruppenaccounts (10T)

- PCs und Server (100T)
- Telefone, Mobile Devices (100T)
- Weitere IT-Hardware (Drucker, Switches) (100T)

- Kunden (1Mio/Jahr)

- Fahrzeuge (1Mio/Jahr), Steuergeräte (100/Auto)

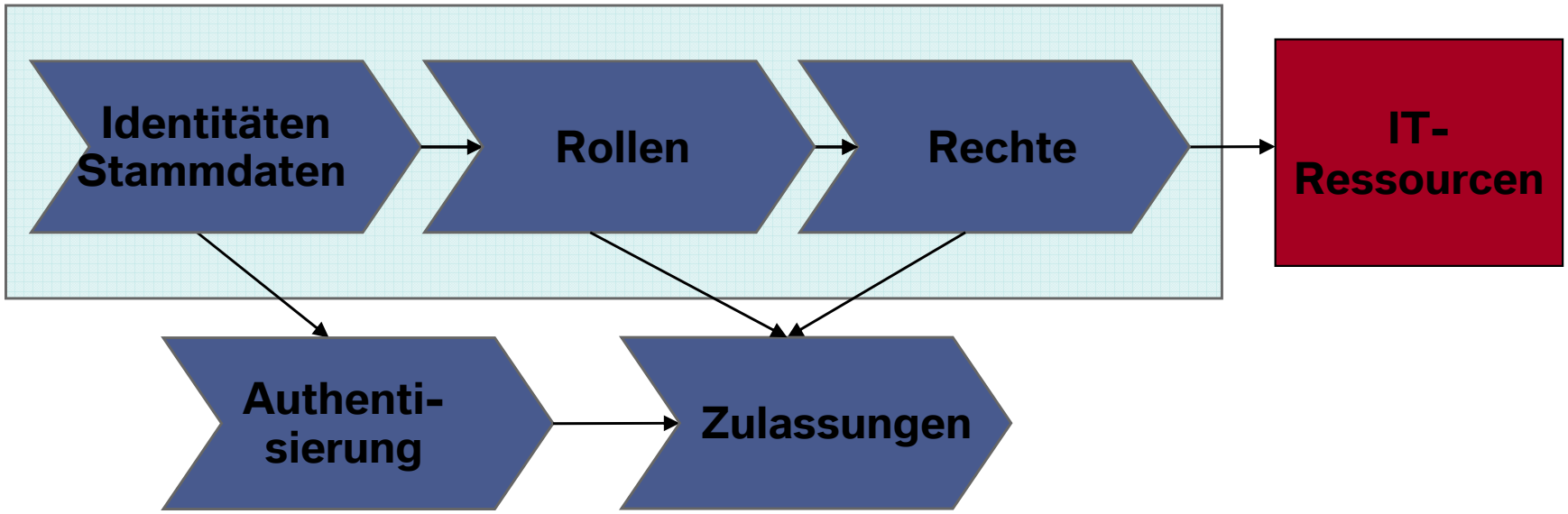
- TV-Receiver, Schließanlagen, ...

Identity Management.
Agenda.

- Scope
  Was ist Identity Management?
- Anforderungen
  Wofür brauchen Unternehmen Identity Management?
- Theorie
  Grundprinzipien des Identity Managements.
- Herausforderungen
  Was macht Identity Management so komplex?

Identity Management - Theorie.

Abläufe - Überblick.



Identity Management - Theorie.
Stammdaten. Authentisierungsinformationen.

- Stammdaten
  - Eindeutige **Beschreibung einer Identität**
    - Erforderlicher Umfang abhängig vom Identitätstyp
  - Hohe Datenqualität Voraussetzung für ein erfolgreiches Identity Management

- Authentisierungsinformationen
  - Verwaltung aller **für eine Authentisierung erforderlichen Informationen**
    - Anmeldenamen
    - Passwörter, Zertifikate, TANs, Token, …
  - **Prozesse** zur Verteilung, Freischaltung, Sperrung, …
  - Müssen bei der Accountanlage u.U. mit übertragen werden
    - Erfordert eine intelligente Lösung, um Sicherheitslücken durch Passwortspeicherung zu vermeiden

Identity Management - Theorie.
Zulassungen. Rechte.

- Zulassung (= Account)
  - **Voraussetzung zur Nutzung** einer IT-Ressource.
  - „Zulassung erteilt“ heißt
    - IT-Ressource **kennt** Nutzer
    - IT-Ressource kann Nutzer **authentisieren**
  - Zulassung beinhaltet **keine Berechtigungen**.

- Recht
  - (Einzel-)Berechtigung innerhalb einer IT-Ressource
  - **Erfordert Zulassung** auf die Ressource
    („das System muss den Benutzer kennen“)

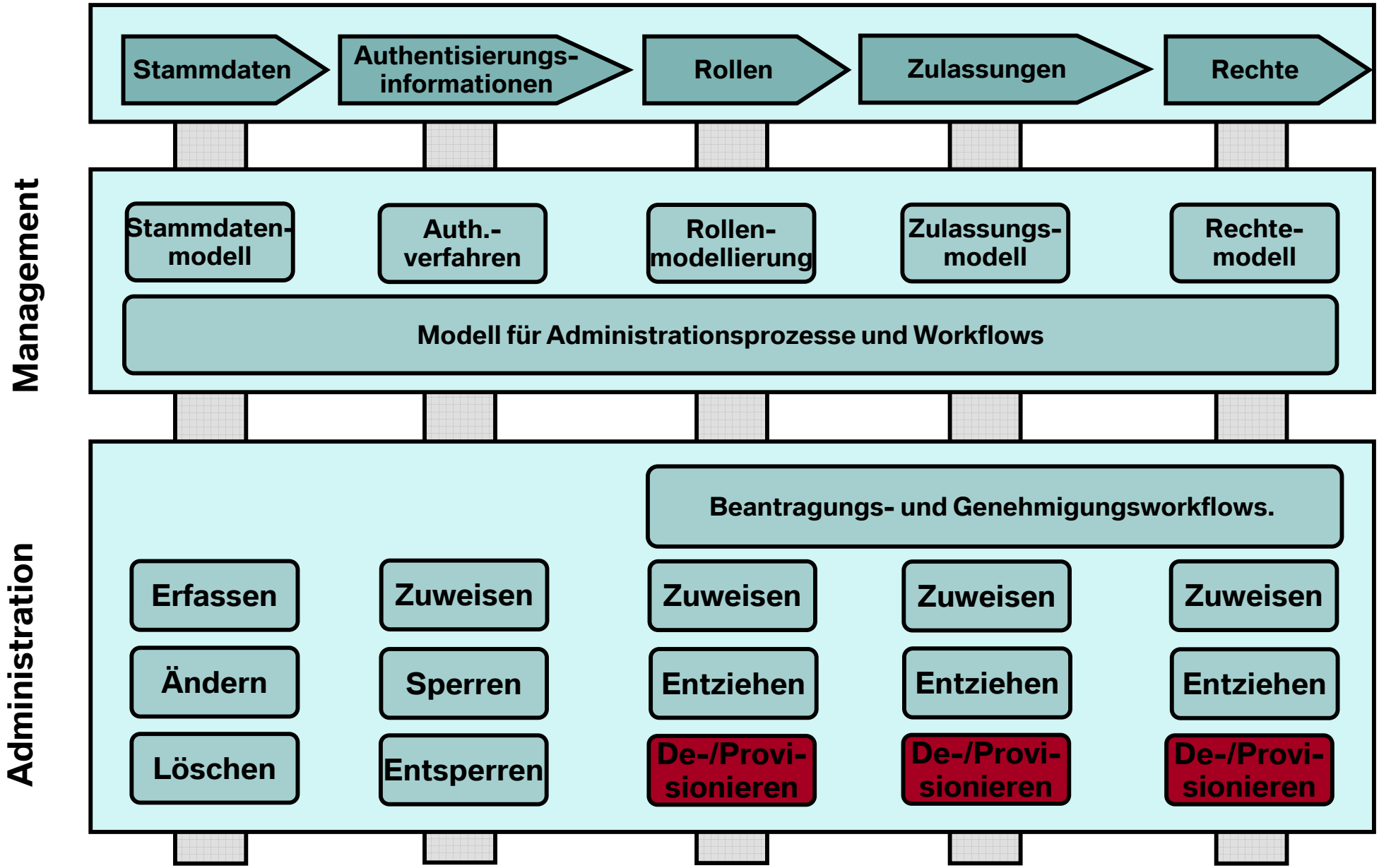
- Zentrale Verwaltung aller Zulassungen sinnvoll

- Zentrale Verwaltung von Rechten, wenn erforderlich

Identity Management - Theorie.
Rollen.

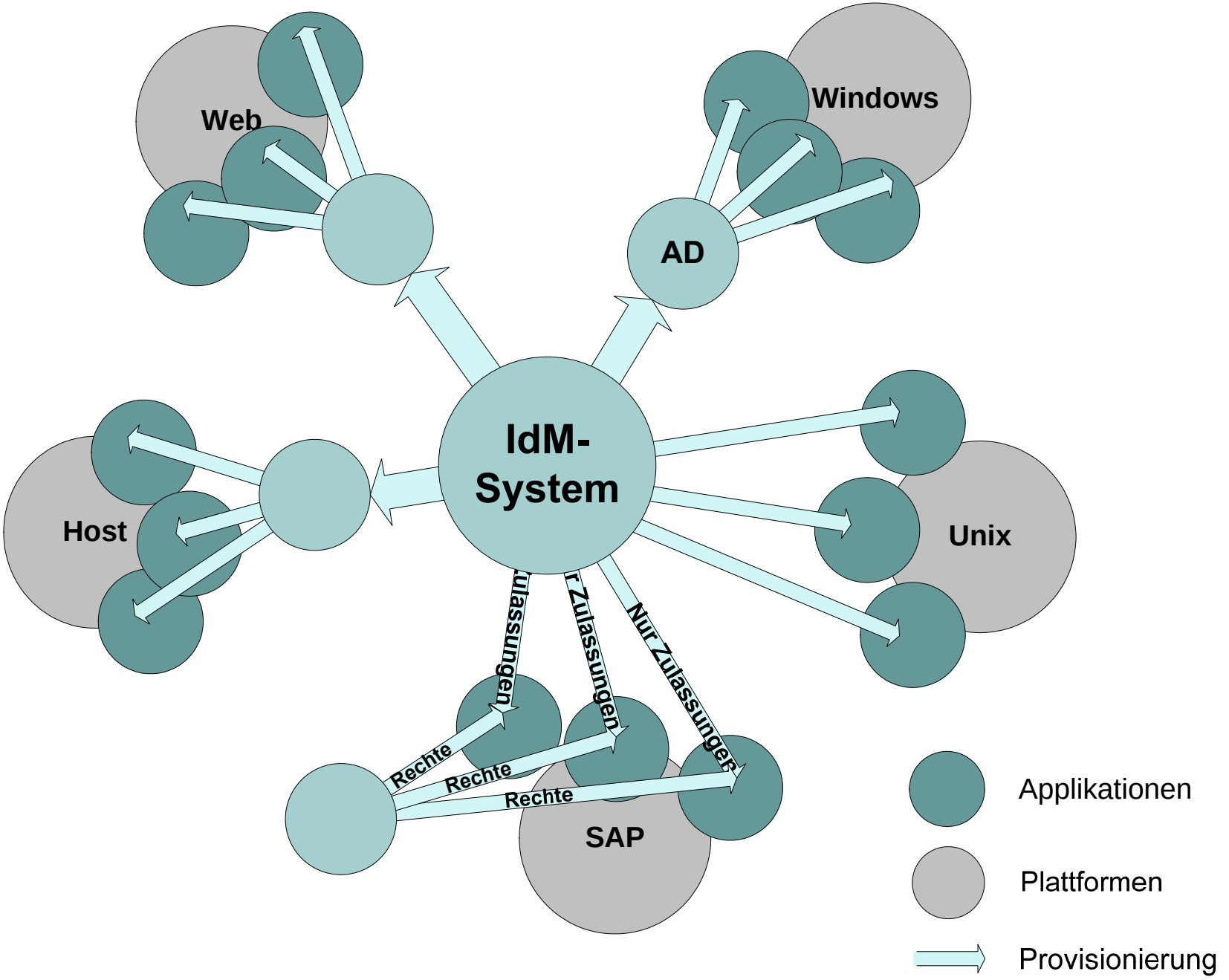
- Aus IT-Sicht: Rolle gruppiert Rechte
  - Rolle „Mitarbeiter“: Windows-Account, E-Mail-Postfach, Zugang zum Internet, Zugriff auf die Personalanwendung, Telefon, Firmenausweis
- Aus Fachbereichs-Sicht: Rolle fasst typische IT-Berechtigungen einer Aufgabe zusammen
  - „Controller“= „Mitarbeiter“+Zul. Finanzanwendungen
  - „Controller Werk 1“ = „Controller“+Rechte Daten Werk 1
  - Spezialfall Parametrisierte Rolle: „Controller (Werk X)“ = „Controller“ + Recht (Werk X)
- Nur der Fachbereich kann den Inhalt einer Rolle definieren („Rollenmodell“)
  - Effizienz der Rollen abhängig von Wiederverwendbarkeit
  - Rechtezuteilung auch ohne Rolle möglich

Identity Management - Theorie.
Notwendige Prozesse.



Identity Management - Theorie.

Beispiel für ein IdM-System.

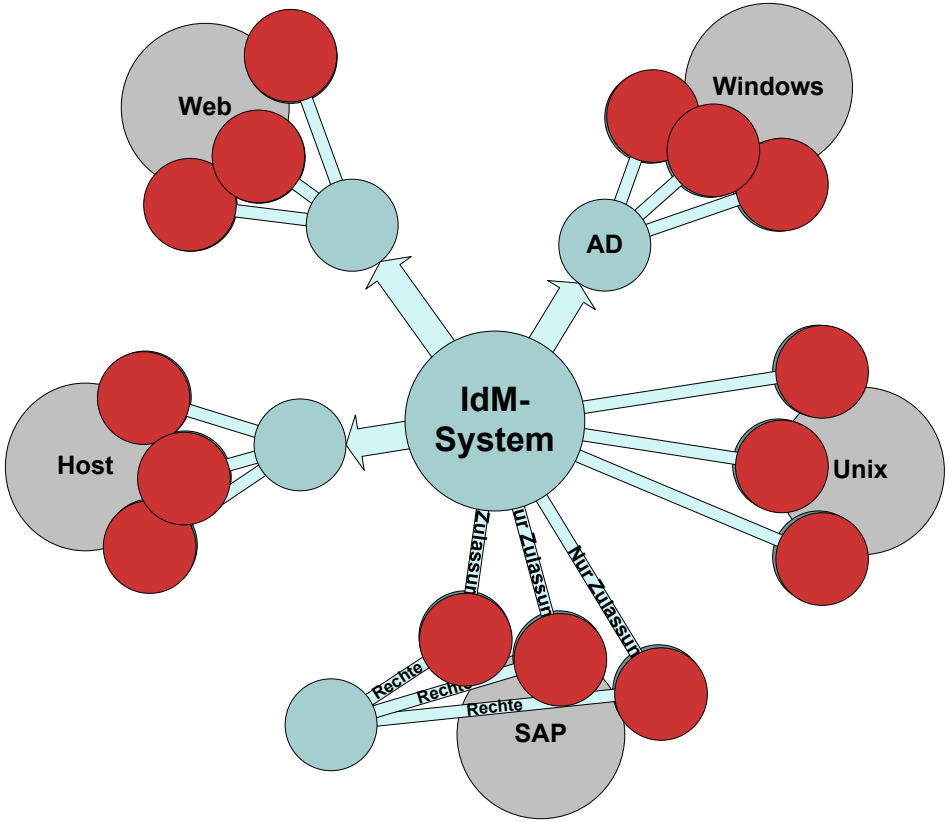


Identity Management.
Agenda.

- Scope
  Was ist Identity Management?
- Anforderungen
  Wofür brauchen Unternehmen Identity Management?
- Theorie
  Grundprinzipien des Identity Managements.
- Herausforderungen
  Was macht Identity Management so komplex?

Identity Management - Herausforderungen.

Was macht Identity Management so komplex?



- Reichweite von Prozess und System sehr groß
  - ALLE Applikationen sind betroffen
  - ALLE Endbenutzer sind betroffen
  - Anforderungen sind komplex und inhomogen
  - Vorhandene Rechteverwaltungen müssen migriert werden

Identity Management - Herausforderungen.
Zu beachtende Aspekte.

- Anforderungsmanagement
  - **Große Zahl** von Anforderern (alle Applikationen, alle Benutzer)
  - Anforderungen, die sich u.U. widersprechen
- Erforderliche **Flexibilität** der Technik
  - Zukunftsfähiges Zentralsystem, daher hohe Komplexität
  - Trotzdem „**einfach**“ in der Handhabung
- **Beherrschbarkeit** von Systems und Prozess
  - „5000 Berechtigungen als Drop-Down-Liste nicht akzeptabel“
- Finanzierung in Unternehmen schwierig
  - Hohe Anfangsinvestitionen, Sicherheits- und Komfortgewinn erst mittelfristig
  - **Quick Wins** suchen!

Identity Management - Herausforderungen.
Umsetzung.

- Kein „Big Bang“
  - Nicht alle vorhandeneren Berechtigungen zu einem Zeitpunkt auf ein zentrales IdM-System umstellen.
    - Endbenutzer-Interface
    - Modelle für alle Berechtigungen
    - Technische Anbindung aller Systeme („Provisionierung“)
    - Modellierung von Rollen und Rechten
- Migrationsaufwand
  - Schaffung von Identitäten (Matching von Accounts)
  - Endbenutzerkommunikation
  - Rückwärtskompatibilität der Datenstrukturen
- Migration dauert Jahre!

Identity Management.
Agenda.

- Scope
  Was ist Identity Management?
- Anforderungen
  Wofür brauchen Unternehmen Identity Management?
- Theorie
  Grundprinzipien des Identity Managements.
- Herausforderungen
  Was macht Identity Management so komplex?

Identity Management.
Die 10 Top-Trends 2008.

1. OpenID, Infocards – Identity 2.0
2. Governance, Risk Management, Compliance
3. Modularität und Offenheit statt monolithischer Suiten
4. SOA und IAM
5. Authentifizierung und Autorisierung im Kontext
6. Privacy und Datenschutz
7. Mehr Anbieter – nicht weniger …
8. Endlich sicheres Online-Banking
9. Enterprise Information Management
10. Federation reift – wenn auch nur langsam

Quelle: Kuppinger Cole + Partner

Das wärs für heute...

Vielen Dank für Ihre Aufmerksamkeit.

- Fragen / Diskussion
- Verbesserungsvorschläge
- Die Folien sind bereits auf die Web-Seite der Vorlesung:
  http://www.nm.ifi.lmu.de
- Sie haben das Semester überstanden!
- In diesem Sinne:
  Einen schönen Abend ...
  ... und weiterhin viel Erfolg!!!