

---

**Prof. Dr. Matthias H. Hartmann**

**Identity Management**

**Bochum, 20. Oktober 2005**

## Agenda

### **n Identity Management bei Aristoteles**

*Aristoteles formulierte vor über 2000 Jahren den Satz der Identität, der bis in die Neuzeit das philosophische Denken beherrschte.*

### **n Metasystem für Identity Management**

*Identity Management bedarf eines vereinheitlichenden Identitäts-Metasytems, um digitale Identitäten koppeln zu können.*

### **n Identity Management in der Unternehmens-Architektur**

*Die Einführung eines Identity Management erfordert eine Prüfung der Unternehmens-Architektur auf Systemkonsequenzen anhand von sieben Gesetzen*

# **Identity Management bei Aristoteles**

## Aristoteles formulierte vor über 2000 Jahren den Satz der Identität.

### Aristoteles: Satz der Identität

- n Aristoteles (384-322 v. Chr.)  
Logik der Schlussfolgerung: Syllogistik als Teilgebiet der Logik  
= Verfahren zur Trennung von wahren von falschen Aussagen
- n Formulierung von drei logischen Gesetze:
  - Satz der Identität ( $a=a$ )
  - Widerspruchsfreiheit des Denkens  
(keine Aussage ist zugleich wahr und falsch)
  - Gesetz des ausgeschlossenen Dritten  
(eine Aussage ist entweder wahr oder falsch, ein Drittes gibt es nicht)
- n mit Prinzip der notwendigen Unterordnung des Besonderen unter das Allgemeine gilt:
  - Alle Menschen sind sterblich (Prämisse/Obersatz)
  - Sokrates ist ein Mensch (Prämisse/Untersatz)
  - Sokrates ist sterblich (Conclusio/Schlusssatz)

# Die Unterscheidung zwischen wahr und falsch ist in der modernen Erkenntnistheorie eine Arbeit mit Hypothesen.

**Karl Raimund Popper: Objektive Erkenntnis**

Kübeltheorie	Scheinwerfertheorie
<ul style="list-style-type: none"><li>n Problem vorhanden</li></ul>	<ul style="list-style-type: none"><li>n Problem vorhanden</li></ul>
<ul style="list-style-type: none"><li>n Mensch sucht nach Informationen zum Problem</li></ul>	<ul style="list-style-type: none"><li>n Mensch bildet eine Hypothese zur Lösung</li></ul>
Konsequenz:	<ul style="list-style-type: none"><li>n Mensch sucht nach Informationen zur Verifikation oder Falsifikation der Hypothese</li></ul>
<ul style="list-style-type: none"><li>n Keine Lösung, aber eine Vielzahl von Informationen</li></ul>	Konsequenz:
<ul style="list-style-type: none"><li>n Gefühl der Enttäuschung, da viel gearbeitet wurde, jedoch kein Ergebnis vorliegt</li></ul>	<ul style="list-style-type: none"><li>n Beweis oder Widerlegung der Hypothese</li></ul>
	<ul style="list-style-type: none"><li>n Erkenntnis gesteigert („dazugelernt“)</li></ul>
	<ul style="list-style-type: none"><li>n Hohe Motivation</li></ul>

# Die Systemtheorie unterstützt bei der Ordnung von Wissen bzw. Elementen in einen Gesamtzusammenhang.

## Systeme als Modelle der Wirklichkeit

- n System: das Zusammengeordnete (griech.);  
gedanklich: geordnete Wissensgesamtheit oder  
gegenständlich: Gebilde von Elementen in Beziehungen
- n Begriffe: Funktion, Struktur, Prozess, Lenkung,  
funktional-abstrakt versus phänomenologisch-deskriptiv; funktionale Äquivalenz
- n Der Präsident General Motors Europe Louis R. Hughes wurde 1993 zitiert mit den Worten:  
*„Einige Japaner hätten ihm bei Werksbesichtigungen anvertraut, dass es eigentlich ohne Belang sei, was man ihm zeige, er werde es ohnehin weder verstehen noch durchsetzen können. (...) Es habe intensiver Analysen bei Gemeinschaftsunternehmen in Kalifornien mit Toyota bedurft, berichtete Hughes, bis die GM-Manager nach fünfjähriger Erfahrung endlich gemerkt hätten, dass ein ganzes System dahinter stehe. Es sei nicht das Durchsetzen einzelner Strategien, das von Material, Personal, Systemen und technischen Anlagen abhinge. Man müsse es wirklich als ganzheitliches System sehen.“*  
Quelle: Spira, J.-Ch.: Bei Lean Production ändert sich im Werk auch der „Lebensstil“, in: BddW v. 14.7.1993, S. 8.

# **Metasystem für Identity Management**

## **Digitale Identitäten sind Datensätze (Kennung und Attribute), die Objekte in IT-Netzen möglichst eindeutig repräsentieren.**

### **Begriff der Identität**

- n** lat. identitas, aus lat. Idem, **derselbe/dasselbe**
  - Zwei Autos derselben Automarke sind zwei gleiche Autos; aber:
  - Dasselbe Auto habe ich heute schon zwei Mal gesehen.
  - Dinge sind identisch, wenn alles, was vom einen ausgesagt wird, auch vom anderen ausgesagt werden sollte.
  
- n** **Digitale Identitäten** sind Datensätze (Kennung und Attribute), die Objekte in IT-Netzen möglichst eindeutig repräsentieren. Als Objekte können beteiligt sein:
  - Natürliche oder juristische Personen
  - Systemkomponenten (Geräte, HW-Module)
  - Anwendungen
  - Services

# Identity Management ist der kontrollierte Einsatz von digitalen Identitäten und Berechtigungen.

## Identity Management

- n Identity Management ist der kontrollierte **Einsatz von digitalen Identitäten** und Berechtigungen sowie deren Erzeugung, Pflege, Nutzung und ggf. Löschung mit dem Ziel, **vertrauenswürdige Prozesse plattformübergreifend** und standardisiert nutzbar zu machen.
- n Identity Management ermöglicht **Unternehmen, Institutionen und Personen**, diese global zu verwenden und den gesamten **Lebenszyklus** und die damit verbundenen Berechtigungen dieser Identitäten zu **steuern**.
- n Wesentliche Begrifflichkeiten in diesem Zusammenhang sind:
  - **Access Management** ist die anwendungsspezifische Verwendung von Berechtigungen
  - **Provisioning** umfasst das Anlegen, Ändern und Löschen von Benutzerkonten auf unterschiedlichen Systemressourcen
  - **Zertifikats-Management** stellt eine Public Key Infrastruktur (PKI) zur Verfügung, die als Basistechnologie innerhalb Identity Management eingesetzt werden kann

## **Identity Management bedarf eines vereinheitlichenden Identitäts-Metasytems, um digitale Identitäten koppeln zu können.**

### **Identität-Metasytem**

- n Die unterschiedlichen Bedürfnisse der Beteiligten verlangen nach einer Integration der vielfältigen beitragenden Systeme und Kommunikationstechniken, sowie der Art und Weise, wie Systeme Accounts verwalten.
- n Für die IT-Welt gibt es historische Beispiele:
  - abstrakte Display Services, die durch Geräte Treiber möglich wurden
  - Sockets und TCP/IP versus Unified Ethernet, Token Ring, Frame Relay, X.25
- n Notwendigkeit eines “vereinheitlichenden Identitäts-Metasytem”,
  - um eine einheitliche Sprachlogik in der Systemlandschaft zu gewährleisten
  - das es ermöglicht, digitale Identitäten „lose“ zu koppeln.
- n Eine Festlegung auf dominante Technologien ist zu vermeiden – **sie werden sich iterativen Erkenntnisfortschritt entwickeln.**

# **Identity Management in der Unternehmens-Architektur**

# Integrierte Geschäftsprozesse erfordern ein ganzheitliches Identity Management.

## Gründe für ein Identity Management (I)

- n **Unternehmensübergreifende automatisierten Zusammenarbeit** lässt sich nicht mit unternehmensweiten technischen Lösungen unterstützen.
- n Denken in **kompletten Geschäftsprozessen** verlangt eine einheitliche Infrastruktur.
- n **Reduktion der Fertigungstiefe** einzelner Unternehmen zugunsten eines Netzwerkes von Lieferanten und Abnehmern.
  - Der logischen Vernetzung folgt die elektronische Vernetzung.
  - Externe Partner werden an bisher interne Geschäftsprozesse angeschlossen.
- n **Föderale Systemstrukturen** erfordern eine Integration von Benutzeridentitäten und Zugriffsrechte
- n **Ressourcenvirtualisierungen** (Grid-Computing, Web-Services)
  - erfordern eindeutige digitale Identitäten
  - automatisierte Rechteprüfungen

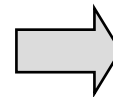
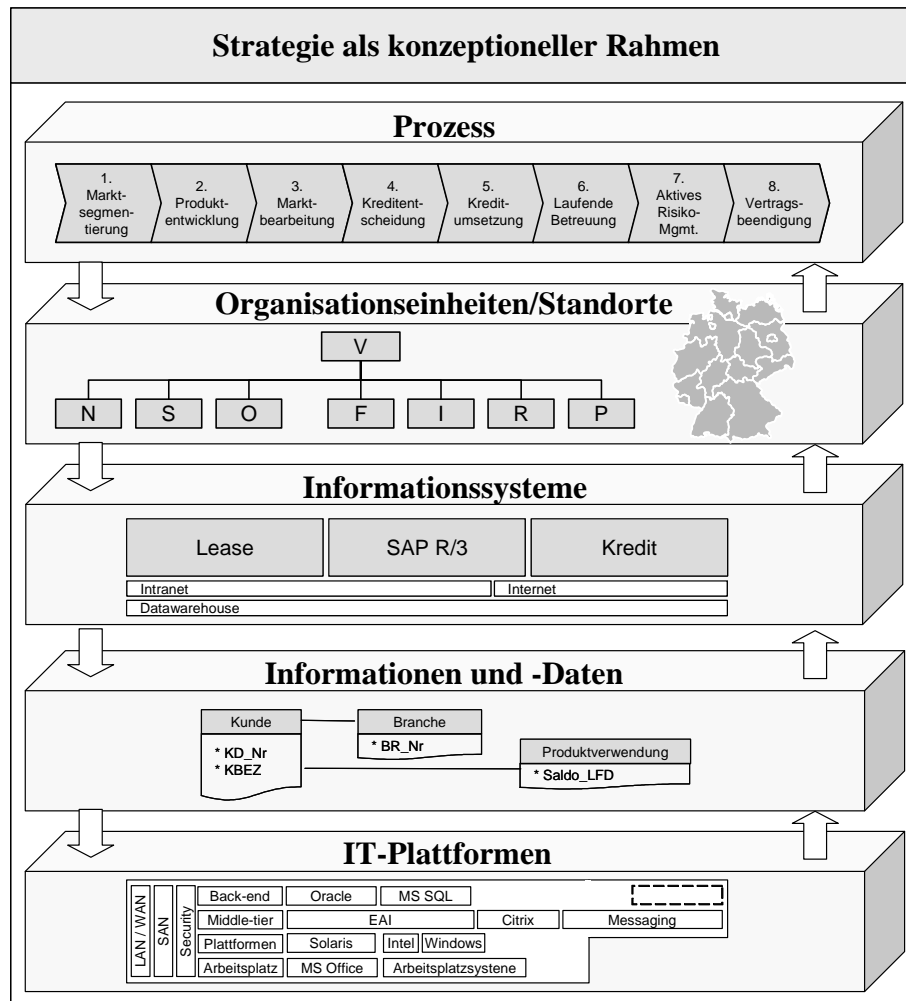
# Die Dynamik der Wandels ist ein Argument für die Implementierung von Identity Management.

## Gründe für ein Identity Management (II)

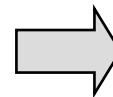
- n **Steigende Dynamik** im Wirtschaftsleben: Das einzig Beständige ist der Wandel:
  - Mitarbeiter bleiben für kürzere Zeit mit einer Geschäftsrolle verknüpft, wechseln Abteilungen, arbeiten in Projekten, gehen für einige Wochen zu einer Niederlassung
  - Zeitweise externe Kräfte benötigen interne Ressourcen
  
- n **Höheres Sicherheitsbewusstsein**: Erfahrungen mit den Gefahren des Internet
  - Die hohe IT-Abhängigkeit
  - "Leih' mir 'mal Dein Passwort!"
  
- n **Externe Auflagen**:
  - Behördliche Regelungen definieren entsprechende Anforderungen (BaFin, ...)
  - Basel II definiert den Rahmen für operative Risiken
  - Nur nachgewiesene Risikoreduktion senkt die Kosten

# Die Implementierung eines Identity Management erfordert eine Prüfung der Unternehmensarchitektur – nicht nur der Systeme.

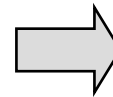
## Identity Management in einer Unternehmens-Architektur



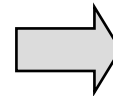
**Auswirkungen auf die Prozesse ?**



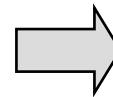
**Auswirkungen auf die Organisation ?**



**Auswirkungen auf die Systeme ?**



**Auswirkungen auf die Informationen ?**



**Auswirkungen auf die Plattformen ?**

# **Kim Cameron hat sieben Gesetze des Identity Management formuliert, die bei einer Implementierung nützlich sein können.**

## **7 Gesetze des Identity Management**

1. Die Systeme, die die Digitale ID bearbeiten, dürfen Benutzer identifizierende Informationen nur mit der Zustimmung des Benutzers offen legen.
2. Die Lösung, die die geringst mögliche identifizierende Information bekannt gibt und die Verwendung am besten begrenzt, wird die stabilste Langfristlösung sein.
3. Digitale Identitäts-Systeme dürfen identifizierende Informationen nur an Parteien herausgeben, die einen notwendigen und berechtigten Platz in der Identitätsbeziehung haben.
4. Ein vereinheitlichendes Identitäts-Metasytem muss sowohl „*omnidirektionale*“ IDs für öffentliche Objekte wie auch „*unidirektionale*“ Identifikatoren für private Objekte (Personen) unterstützen.
5. Ein vereinheitlichendes Identitäts-Metasytem muss die Zusammenarbeit von vielfältigen Identitätstechniken unterschiedlicher Identitätsherausgeber kanalisieren und ermöglichen.
6. Ein vereinheitlichendes Identitäts-Metasytem muss den menschlichen Nutzer als durch eine geschützte und über alle Fragen erhabene Mensch-Maschine-Kommunikation integriert definieren.
7. Ein vereinheitlichendes Identitäts-Metasytem muss eine einfache und widerspruchsfreie Erfahrung bieten, während sie gleichzeitig die Trennung der Umgebungen über vielfältige Betreiber und Technologien ermöglicht.

Quelle: <http://www.identityblog.com>, Kim Cameron, Architect of Identity and Access Microsoft Corporation

# Identity Management etabliert sich zur Zeit im Bewußtsein des Managements.

## Ausblick

- n Unternehmen implementieren automatisierte und **unternehmensübergreifende Geschäftsprozesse** mit dem Internet als Trägermedium.
- n Dualistische Einteilung der Netzwelt nicht mehr aktuell (**internes Intranet** und **externes Internet**). **Spezielle Extranets** als Behelfskonstrukt.
- n Implementierung eines ganzheitlichen Identity Managements für eine **sichere** und **feingranulare Zugriffssteuerung** erforderlich
- n Aktuelle Bestrebungen zur Ressourcenvirtualisierung wie **Web-Services** oder **Grid-Computing** erhöhen den Handlungsdruck weiter.
- n Gleichzeitig haben viele Marktangebote eine für einen unternehmensweiten Einsatz **hinreichende Reife** erlangt.
- n Eine **Amortisationsdauer**n von unter zwei Jahren lassen Investitionen in bestimmte Systeme auch in wirtschaftlich schwierigen Zeit als sinnvoll erscheinen.
- n Es ist ratsam die Implementierung einzelner Lösungen in eine Gesamtarchitektur einzubetten.

# Prof. Hartmann lehrt und forscht an der FHTW Berlin und verfügt über 14 Jahre internationale Projekterfahrung in der Beratung.

**Prof. Dr. Matthias H. Hartmann**

## Universität / Hochschule

- n **Professur** an der Fachhochschule für Technik und Wirtschaft, Berlin
- n **Lehre:** Consulting, Informationsmanagement, Produktion und Logistik
- n **Forschung:** Strategie, Prozesse, Controlling, Informations- und Technologiemanagement

## Top-Management-Beratung

- n 14 Jahre internationale Projekterfahrung in der Unternehmensberatung, u.a. bei A.T. Kearney
- n Strategie, Prozesse, IT, Programm- u. Projektmanagement, Outsourcing, Due Diligence, ...
- n Industrie, Finanzdienstleister, Telekom, Medien, Energie, Medizin, Öffentliche Betriebe, ...



## Prof. Dr. Matthias H. Hartmann

D-12207 Berlin, Marienstraße 25

Tel: +49 (0) 30 34703780

Fax: +49 (0) 30 34703781

Mobil: +49 (0) 172 8134771

e-mail: [matthias.hartmann@berlin.de](mailto:matthias.hartmann@berlin.de)