



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **(Enterprise) Identity and Access Management**

Prof. Dr. (TU NN)

**Norbert Pohlmann**

Institut für Internet-Sicherheit – if(is)  
Westfälische Hochschule, Gelsenkirchen  
<http://www.internet-sicherheit.de>

**if(is)**  
internet-sicherheit.

# Identity and Access Management

## → Ziele der Vorlesung

- Gutes Verständnis für die verschiedenen Ebenen (Module) eines „Enterprise Identity and Access Management System“
- Erlangen der Kenntnisse über die Aufgaben, Prinzipien und Mechanismen eines „Identity and Access Management System“
- Nachvollziehbarkeit von „Identity and Access Management“ Prozessen und Workflows anhand von praxisnahen Beispielen erlernen

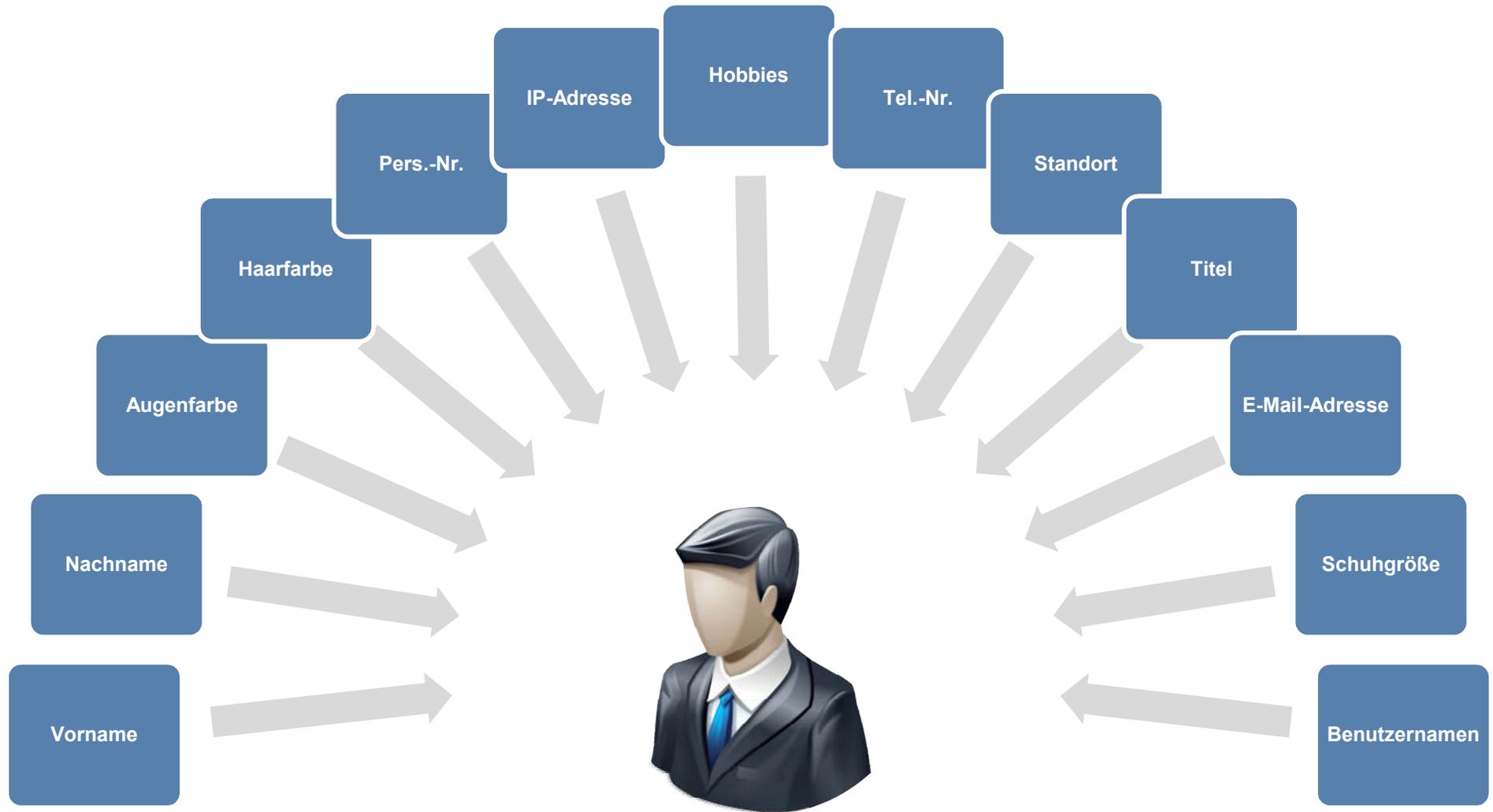
- **Definitionen**
- **Notwendigkeit**
- **Key Concepts**
- **IdMS-Lebenszyklus**
- **Single Sign-On**
- **Circle of Trust**
- **Zusammenfassung**

## ■ Definitionen

- Notwendigkeit
- Key Concepts
- IdMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- Zusammenfassung

# Definitionen

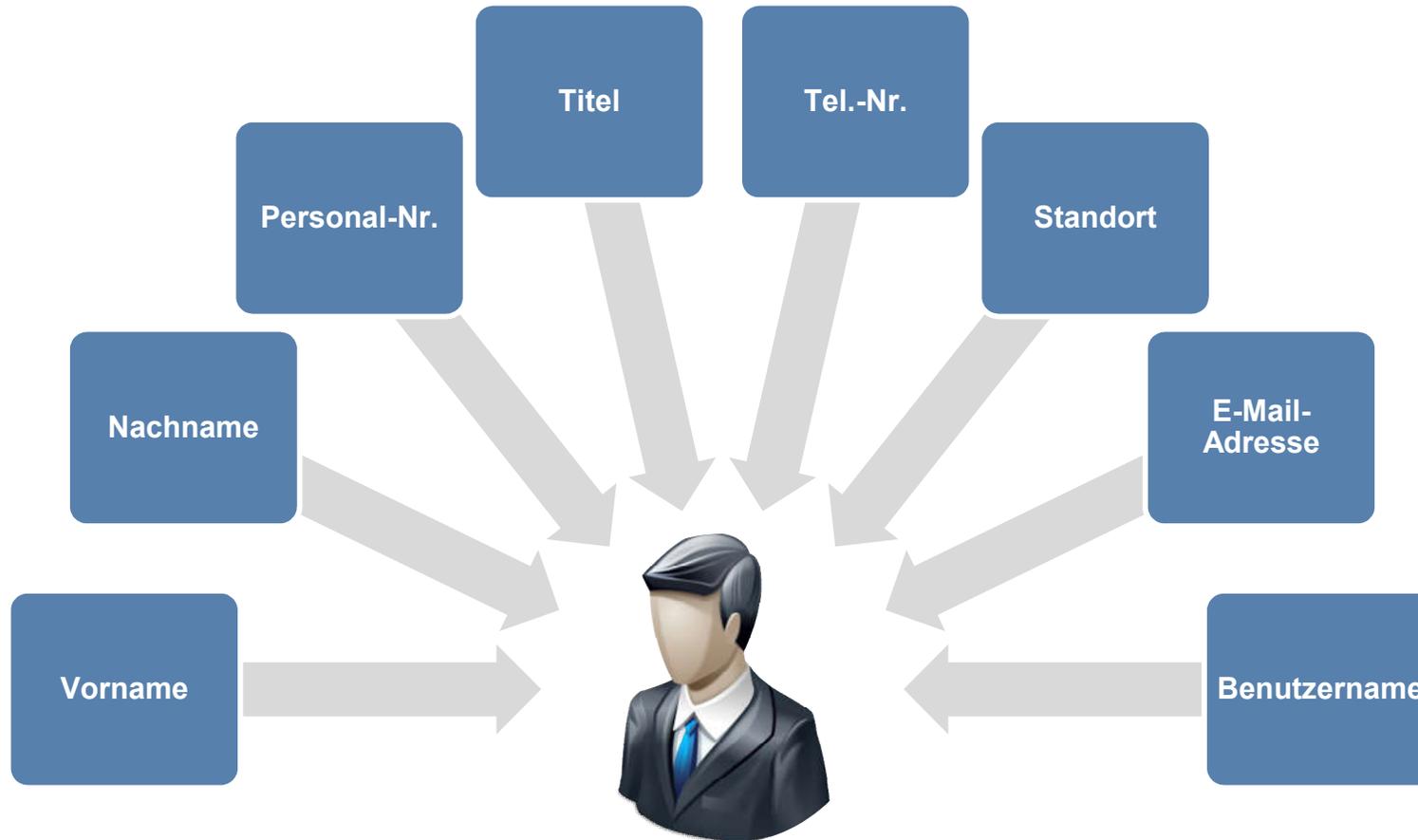
## → Entität



- Eine **Entität** (Person, Rechner, etc.) setzt sich zusammen aus der sie **beschreibenden Attribute**.

# Definitionen

## → Digitale Identität



- Eine **digitale Identität** ist die **Teilmenge der Attribute einer Entität**, welche diese Identität in einem bestimmten Kontext im Unterschied zu anderen Entitäten **eindeutig bestimmbar** machen.

# Definitionen

## → Identity and Access Management

### Enterprise Identity and Access Management

- In der Fachwelt hat sich bisher keine einheitliche Auffassung, was exakt unter Identity and Access Management zu verstehen ist, durchgesetzt.
- In der Mehrheit der Definitionen bezieht sich der Begriff **Enterprise Identity and Access Management (IAM)** im Kern auf
  - die Kombination von Verfahren der **Organisationsführung** einerseits
  - und **Technologie** andererseits,welche es Organisationen durch eine breite Palette von Prozessen und Funktionalitäten erlauben
  - die **Einhaltung gesetzlicher Vorschriften**
  - sowie die **Integrität, Vertrauenswürdigkeit und Verfügbarkeit von Informationen**gewährleisten zu können.

# Definitionen

## → Identity and Access Management

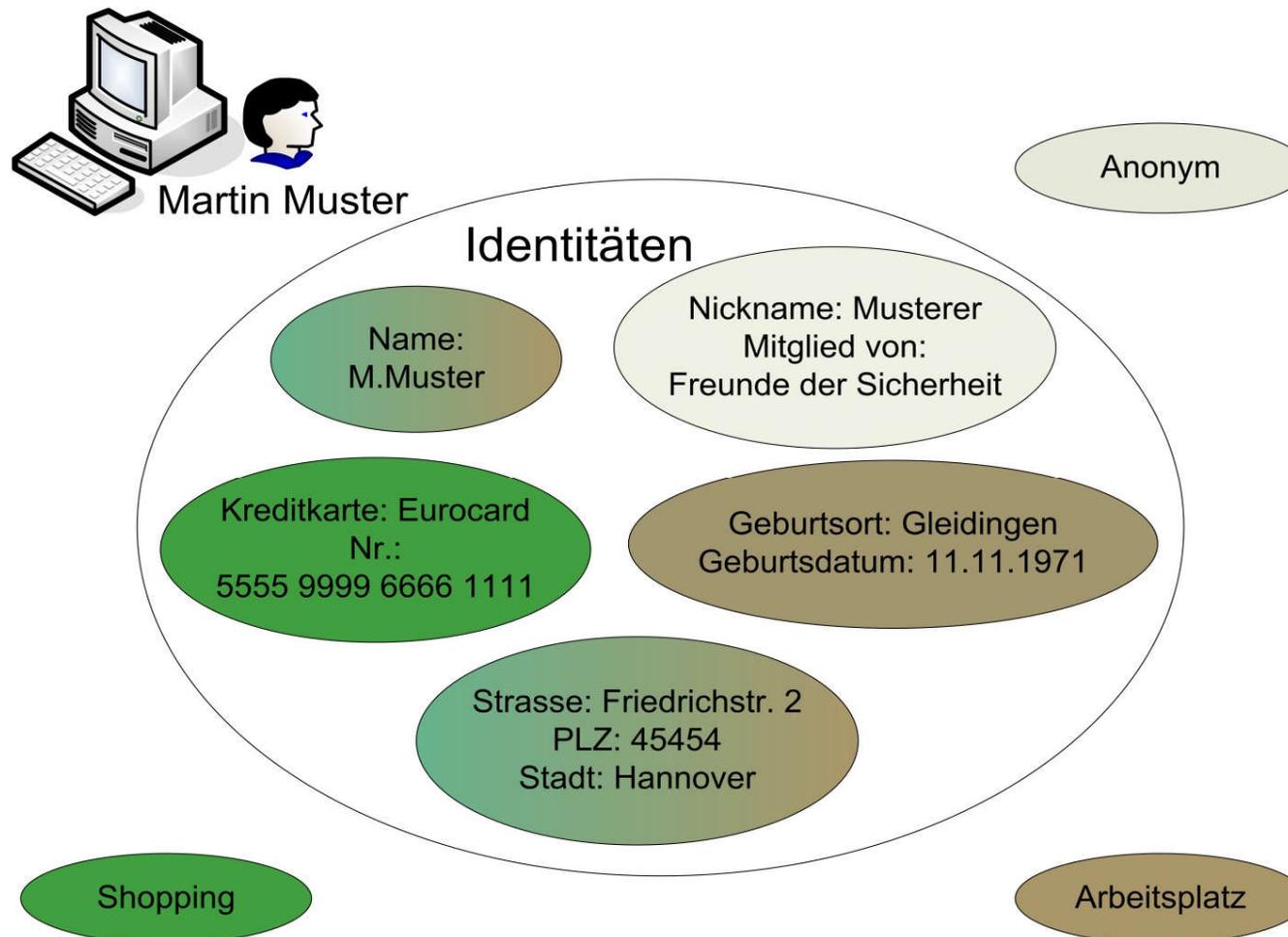
### Definition des Institut für Internet-Sicherheit – if(is):

- Der Begriff (Enterprise) **Identity and Access Management (IAM)** beschreibt jeglichen Einsatz von digitalen Identitäten, deren Attributen, sowie deren Berechtigungen und schließt die Erzeugung, Nutzung, Pflege und Löschung dieser digitalen Identitäten mit ein.
- Das **Ziel** ist es,
  - **vertrauenswürdige,**
  - **Identitätsbezogene und**
  - **regelkonforme Prozesse**durchzusetzen, die **unabhängig von Organisationen und Plattformen** standardisiert nutzbar sind.

- Definitionen
- **Notwendigkeit**
- Key Concepts
- IdMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- Zusammenfassung

# Notwendigkeit (1/4)

- Einfaches Szenario, warum Identity Management Systeme benötigt werden



# Notwendigkeit (2/4)

- Unüberschaubare Mengen an
  - Benutzerkonten
  - Zugriffsrechten
- Passwörter & Accounts werden vergessen
- Einfache & immer gleiche Passwörter
  - Identitätskollaps



**Mitgliedsname**

Haben Sie Ihren Mitgliedsnamen [vergessen?](#)

**Passwort**

Haben Sie Ihr [Passwort vergessen?](#)

▶ Ihre Angaben zum Einloggen sind ungültig. Bitte versuchen Sie es erneut.

# Notwendigkeit (3/4)

## Folgen:

- Erhöhte Kosten
- Komfortverlust
- Steigender Administrationsaufwand
- Fehlende Kontrolle
- Informations- bzw. Datenverlust
- Unüberschaubare Sicherheitsrisiken
- Sicheres organisationsübergreifendes Arbeiten unmöglich

# Notwendigkeit (4/4)

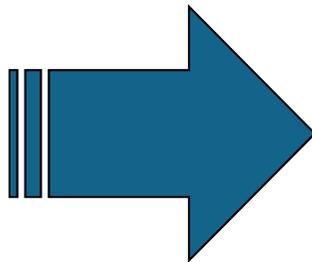
- Organisationen sind auf Zusammenarbeit mit Partnern angewiesen, dies verlangt nach
  - Sicherem Austausch von identitätsbezogenen Daten
  - Vertrauensverhältnissen
  - Verwendung einheitlicher Standards
  - Koppelung von Geschäftsprozessen
  - Need-to-Share Prinzip
  - Sicheres Einbinden externer Personen in interne IT-Systeme
  
- Cloud Computing benötigt technische Aspekte zur
  - Weitergabe von Identitäten
  - Authentifizierung und Autorisierung

# Notwendigkeit

## → Einführung durchgängiges Beispiel

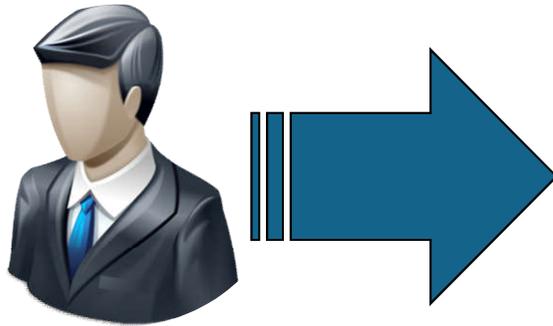
### Beispiel für Enterprise Identity and Access Management

- Am Beispiel des Lebenszyklus der digitalen Identität eines Mitarbeiters, soll gezeigt werden
  - warum Enterprise Identity and Access Management Systeme benötigt werden
  - und wie sie funktionieren
- Das Beispiel zieht sich durch die gesamte Beschreibung des Identity and Access Management Modells (siehe **Key Concepts**)

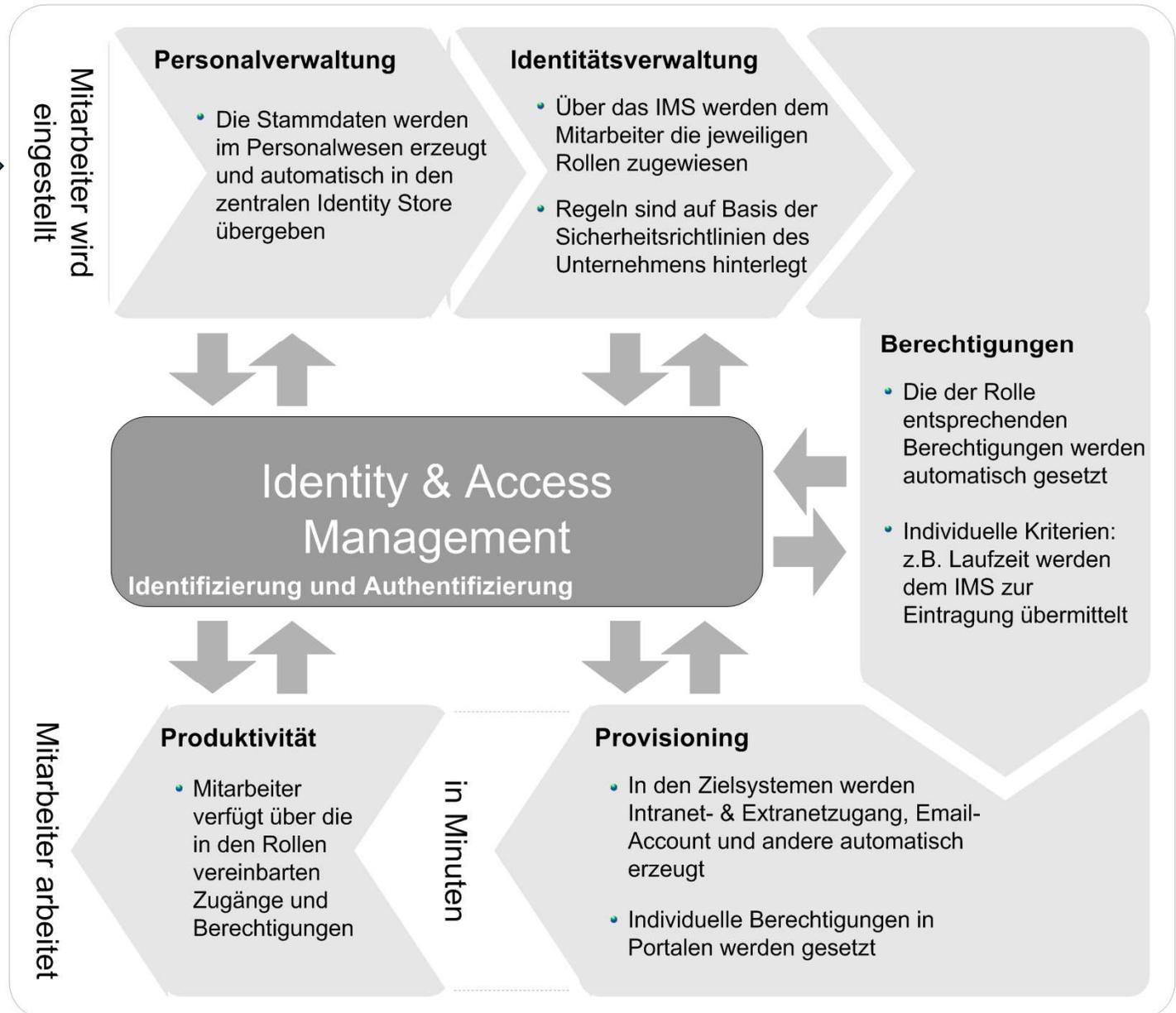


# Notwendigkeit

## → Einführung durchgängiges Beispiel



- Typisches Identity Management **Szenario** innerhalb eines Unternehmens
- Der **Zeitraumen** von der Einstellung bis zur vollständigen Integration des Mitarbeiters



- Definitionen
- Notwendigkeit
- **Key Concepts**
- IdMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- Zusammenfassung

# Key Concepts

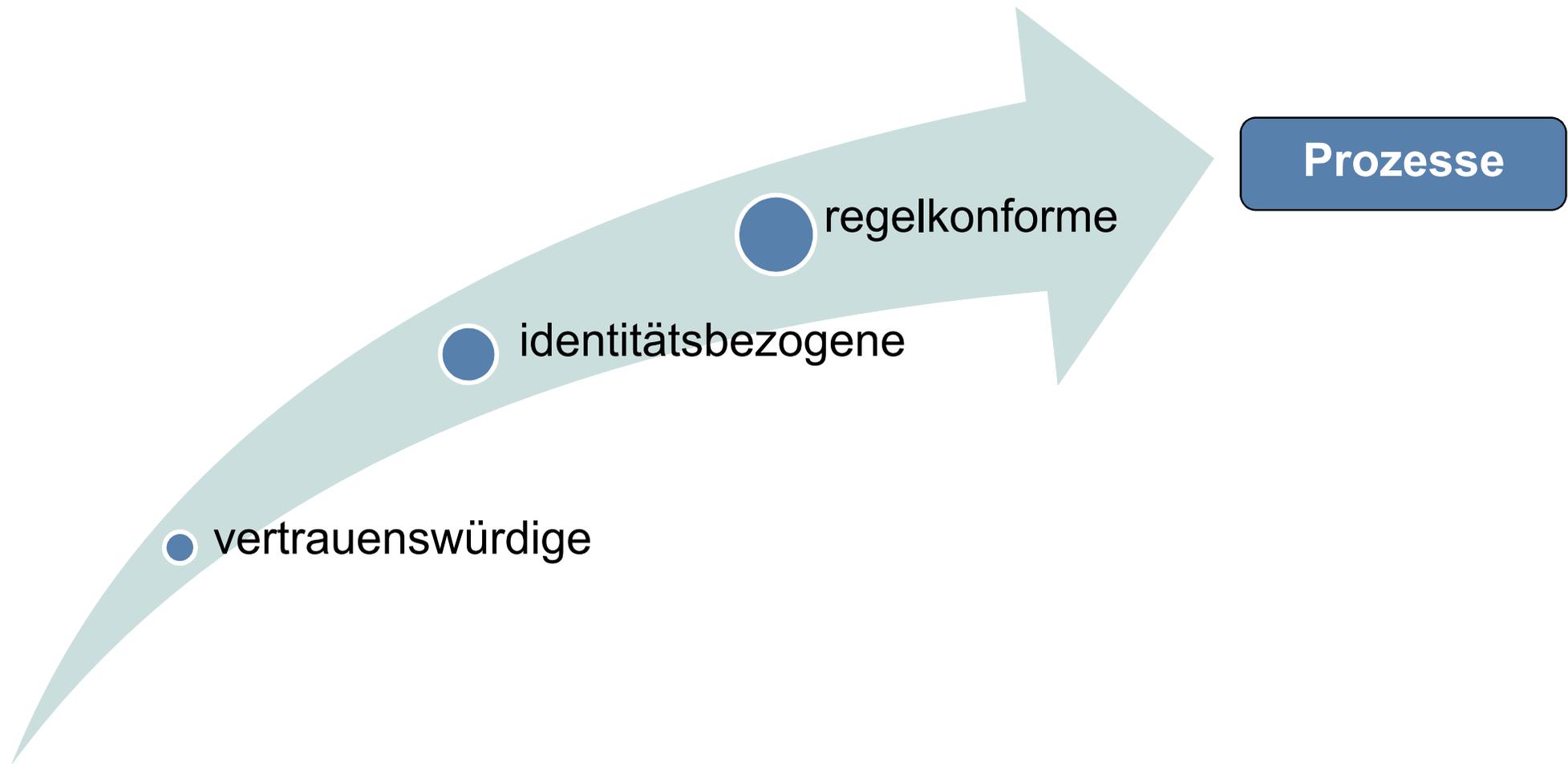
## → Anforderungen

- Sichere und komfortable **Authentifizierung**
- Strukturierte **Identitäts-Datenspeicherung und -verwaltung**
- **Zusammenführung** von Identitätsdaten
- Identitäten über ihren **gesamten Lebenszyklus** begleiten
- Vermeidung von **Überberechtigungen**
- **Schutz von Informationen** und Zugriffen
- **Organisationsübergreifende** Nutzung von Identitäten
- **Vertrauen** zwischen Diensteanbietern herstellen

# Key Concepts

## → Anforderungen

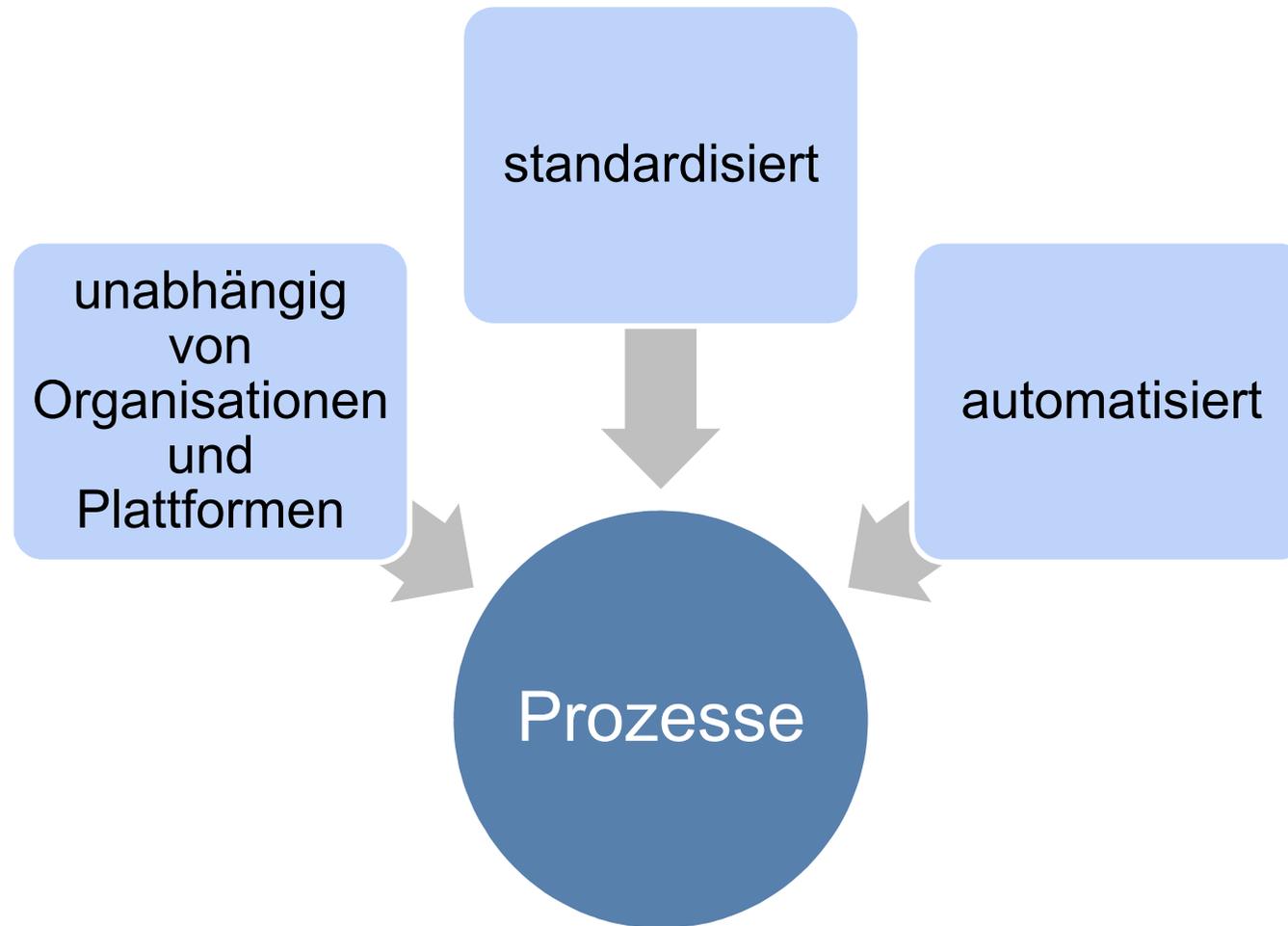
- Identity and Access Management soll ermöglichen:



# Key Concepts

## → Anforderungen

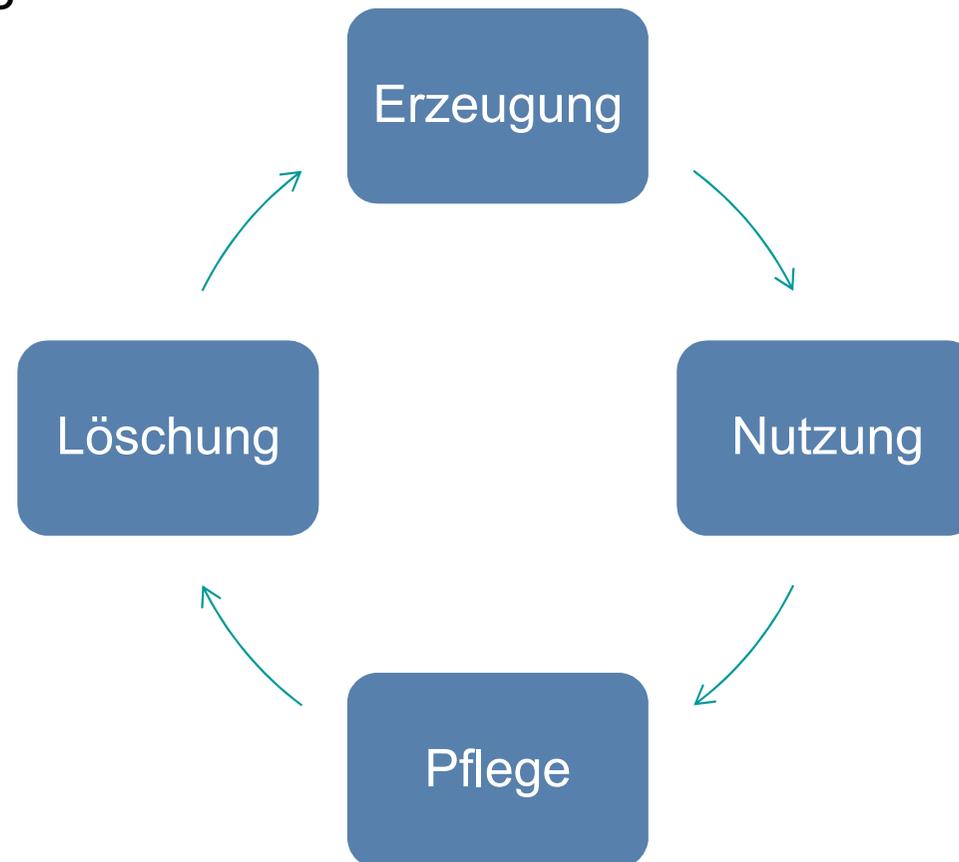
- Prozesse müssen sein:



# Key Concepts

## → Anforderungen

- Enterprise Identity and Access Management soll:
  - digitale Identitäten und ihren gesamten **Lebenszyklus** verwalten
  - insbesondere, deren **vertrauenswürdige Attribute** sowie Berechtigungen



# Key Concepts

## → Aufbau eines Enterprise IAM

### Strukturierung eines IAM-Modells in sieben Module:

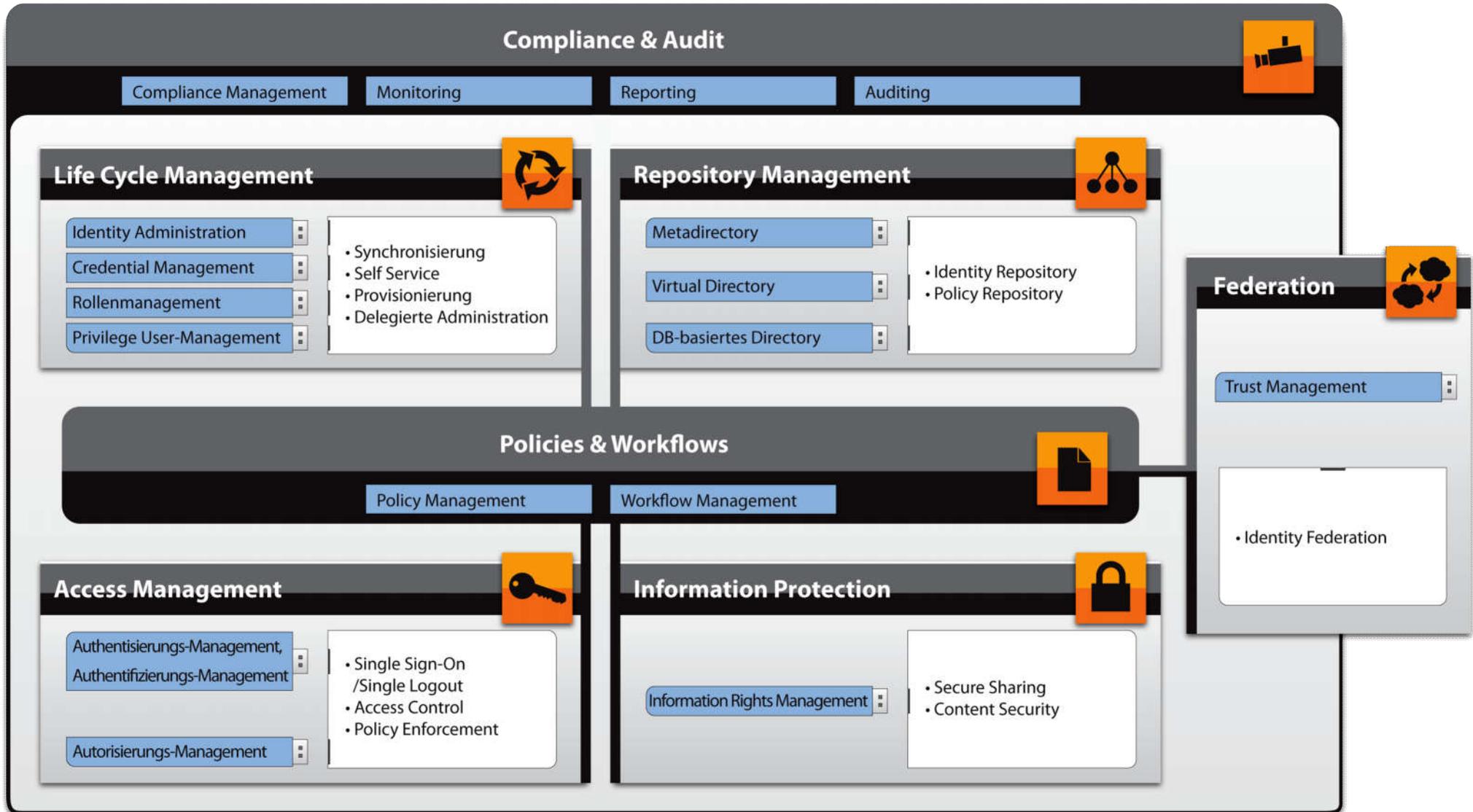
- Policies & Workflows
- Repository Management
- Life Cycle Management
- Access Management
- Information Protection
- Federation
- Compliance & Audit

Typische Struktur für  
die Anwendung in  
Unternehmensnetzwerken

- Diese **Module** bestehen aus **Komponenten** und diese enthalten wiederum (technische) **Funktionen**

# Key Concepts

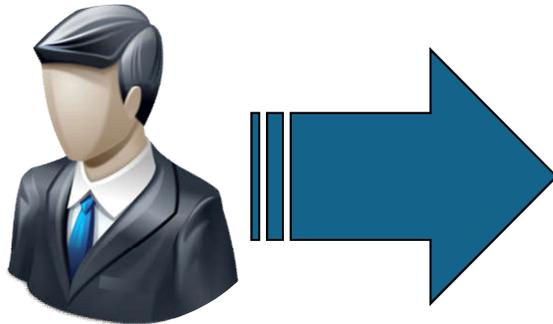
## → Ein Enterprise-IAM-Modell



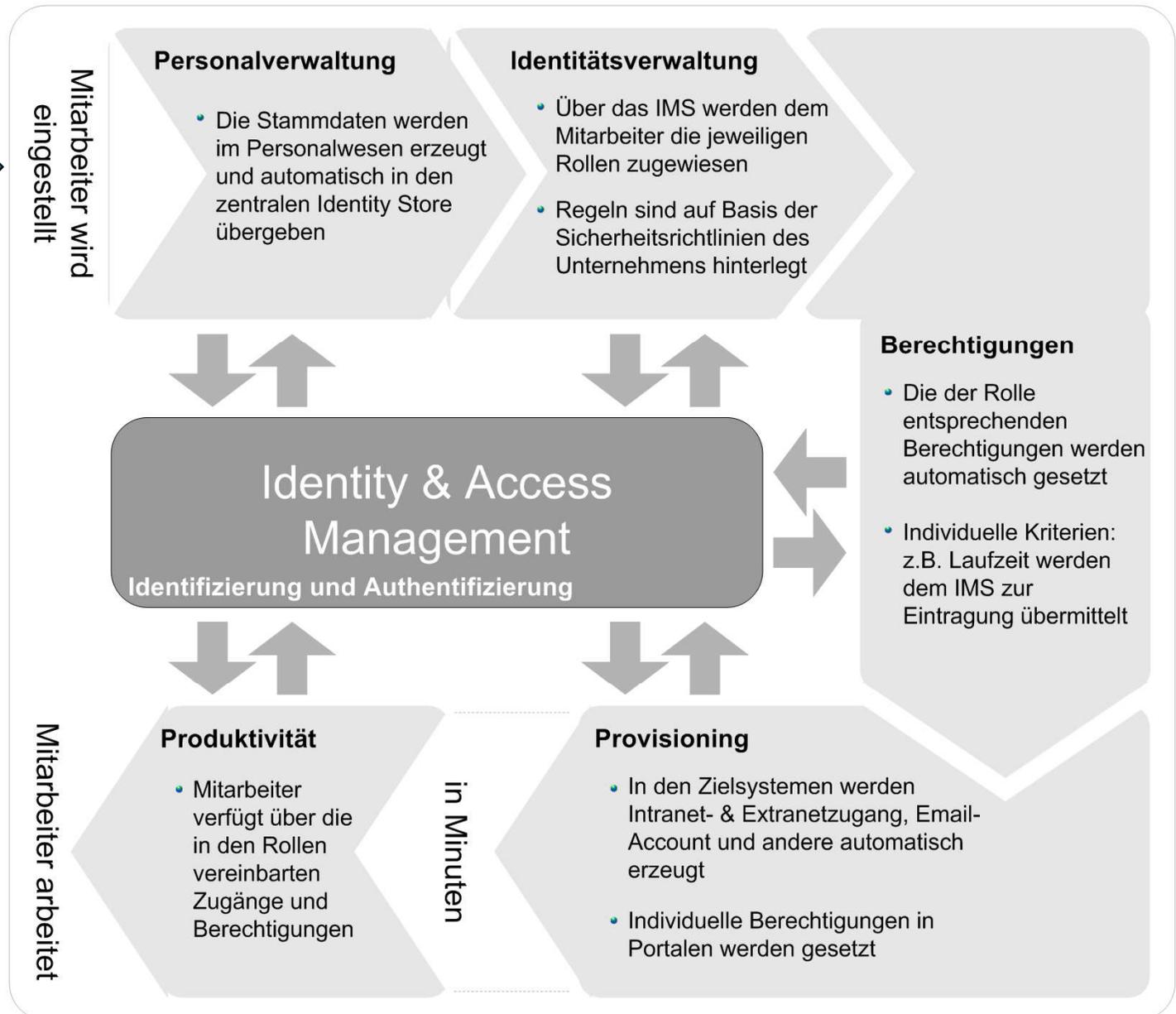
**Module** (grau/schwarz) → **Komponenten** (blau) → **Funktionen**

# Key Concepts

## → Beispiel



- Typisches Identity Management **Szenario** innerhalb eines Unternehmens
- Der **Zeitraumen** von der Einstellung bis zur vollständigen Integration des Mitarbeiters



# Key Concepts

## → Modul: Policies & Workflows

### Basis des Identity Managements:

- Die Verwaltung von Richtlinien und automatisierten oder organisatorischen Arbeitsabläufen ist zentral für den Erfolg von IdM

### Policies (Richtlinien):

- Definieren die zu erreichenden Ziele in den anderen Modulen

### Workflow (Arbeitsablauf):

- Definiert die notwendigen Ablaufstrukturen in den anderen Modulen
- Automatisierte Teilprozesse



# Key Concepts

## → Modul: Policies & Workflows

### Beispiel für Policies & Workflows:

- Ein Mitarbeiter (def. als Entität) kommt neu in ein Unternehmen
- Eine **Richtlinie** für die Personalverwaltung regelt, welche Stammdaten zur Erzeugung einer neuen digitalen Identität benötigt werden und wie diese jeweils geprüft werden müssen
- Ein **Workflow** gibt vor, wie diese Daten in das System der Personalverwaltung eingepflegt werden müssen
- Eine weitere **Richtlinie** regelt in welchen Abständen die Daten in ein Directory übernommen werden müssen
- Zuletzt beschreibt ein **Workflow** wie die Daten in das zuständige Directory hinzugefügt/kopiert werden



# Key Concepts

## → Modul: Repository Management

### Basis:

- Eine **übersichtliche Verzeichnisstruktur**, bzw. ein exakt geordneter Verzeichnisdienst sind die Basis eines funktionierenden Identity Management Systems
- Grundlage für Life Cycle Management

### Bedeutet:

- Identity Import aus maßgeblichen Instanzen (z.B. Personalverwaltungssysteme, etc.)
- Bereinigung, Vereinheitlichung und Zusammenführung der importierten Identitäten zu einer eindeutigen digitalen Identität pro Entität

### Mehrwert:

- Erreichen einer **einzigen digitalen Identität** pro Benutzer/Entität



# Key Concepts

## → Modul: Repository Management

### Beispiel für Repository Management:

- Die digitale Identitäten eines Mitarbeiters, genauer deren Attribute, werden beim Zugriff auf Applikationen im Rahmen seiner Tätigkeit im Unternehmen benötigt
- Die strukturierte **Identitäts-Datenspeicherung und –verwaltung** in einem Metadirectory erlaubt eine Authentifizierung anhand der jeweils aktuellen Attributwerte; von überall im Unternehmen
- Ebenso wird die **Richtlinie** zur Bestimmung der korrekten Stärke einer Authentifizierung aus einem zentralen Repository abgerufen



# Key Concepts

## → Modul: Life Cycle Management

### Basis:

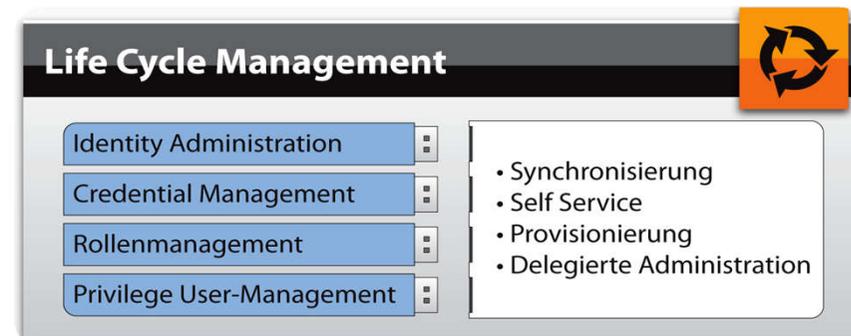
- Integration und Verwaltung von Identitäten
- Synchronisierung
- Grundlage für das Access Management

### Bedeutet:

- Das Identity Management behandelt den kompletten Lebenszyklus von digitalen Identitäten und den mit ihnen verknüpften Prozessen

### Mehrwert:

- Automatisierung der Vorgänge

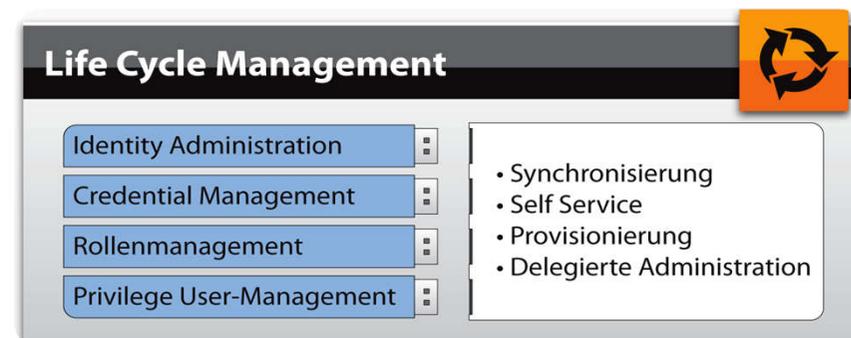


# Key Concepts

## → Modul: Life Cycle Management

### Beispiel für Life Cycle Management:

- Der Mitarbeiter benötigt durch die Zuordnung (siehe Workflow) zu einem neuen Projekt Rechte zum Zugriff auf Applikationen (siehe Access Management) auf die er zuvor nicht zugreifen konnte (bspw. über eine neue Rolle)
- Er beantragt diese Rechte in einem Webfrontend (Self Service)
- Der Projektleiter hat sein Recht zur Genehmigung dieser Rechte an einen Vertreter delegiert
- Dieser genehmigt dem neuen Projektmitarbeiter diese Rechte nach Prüfung in seinem Webfrontend
- Das System provisioniert diese Rechte anschließend in die Applikationen



# Key Concepts

## → Komponente: Identity Administration

### Basis:

- Überprüfung von Identitäten
- Angebot von Authentifizierungsdiensten

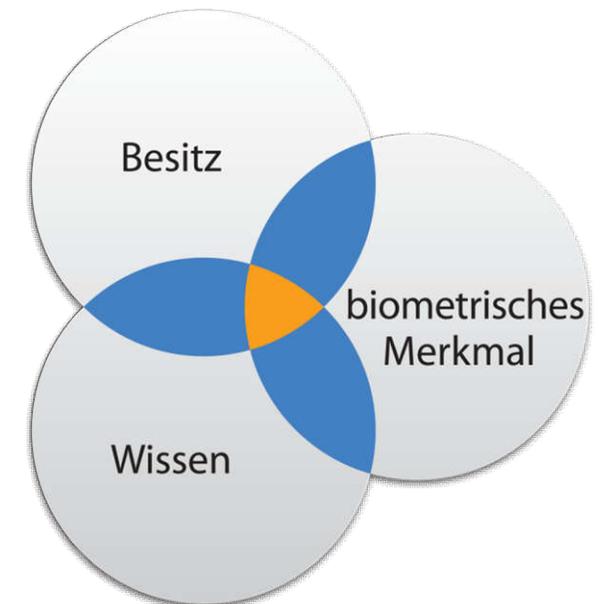
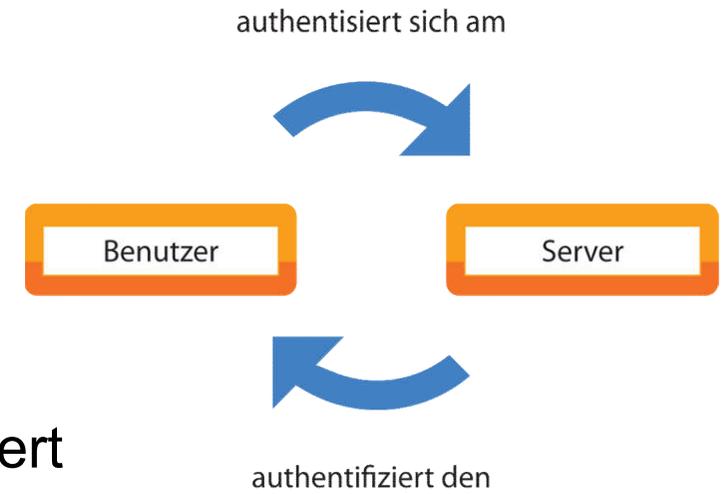
### Bedeutet:

- Das Identity and Access Management ist gefordert Authentifizierungsdienste anzubieten, die den entsprechenden Sicherheitslevel vorgeben, der vorher mit den angeforderten Services abgeglichen wird

### Mehrwert:

- Automatisierung
- Erreichen hoher Sicherheitslevel
- Konzeptionell bedingte höhere Sicherheit

→ **Siehe Vorlesung "Authentikationsverfahren"**



# Key Concepts

## → Funktion: Provisioning

### Basis:

- Das **übergreifende Anlegen, Ändern und Löschen** von Benutzerdaten und Berechtigungen auf unterschiedlichen System-Ressourcen

### Bedeutet:

- Ressourcenübergreifende Bereitstellung von Passwörtern, E-Mail-Adressen, Accounts und Berechtigungen

### Mehrwert:

- Bereitstellungszeit einer kompletten Identität wesentlich verkürzt
- Abstimmung der Vorgänge
- Automatisierung
- Vermeidung von Sicherheitslöchern durch fehlerhaftes Löschen von Identitäten
- Deutlich verminderter Arbeitsaufwand für Administratoren

# Key Concepts

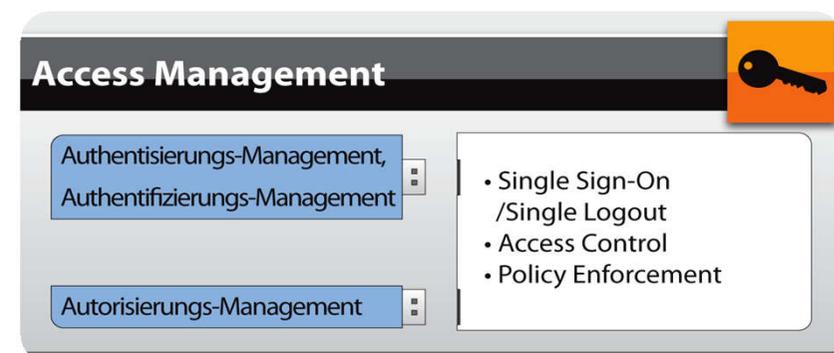
## → Modul: Access Management

### Basis:

- Entscheidung über **Zugriffsberechtigungen** auf der Basis von Benutzeridentitäten/-rollen, Attributen und Richtlinien (Policy Decision)
- Durchsetzen der Zugriffsentscheidungen (Policy Enforcement)
- Beinhaltet die notwendigen technischen Mechanismen für
  - den Zugriff auf ein IAMS sowie
  - die Kontrolle (Access Control) und
  - das Durchsetzen (Enforcement) des Zugriffs

### Mehrwert:

- Automatisierung der Vorgänge
- Vermeidung von Überberechtigung

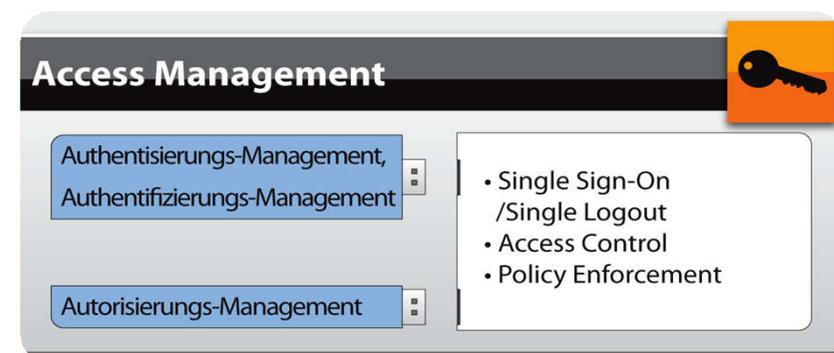


# Key Concepts

## → Modul: Access Management

### Beispiel für Access Management:

- Der Mitarbeiter benötigt Zugriff auf viele unterschiedliche Applikationen
- Er bekommt eine SmartCard mit einem **Personenzertifikat** der unternehmenseigenen PKI
- Hiermit meldet er sich Morgens an der Domäne an und dadurch gleichzeitig an einem **Single Sign-On** System an
- Dieses sorgt dafür, dass er beim Zugriff auf eine Applikation automatisch authentifiziert wird, ohne sich erneut anmelden zu müssen
- Am Ende seines Arbeitstages meldet er sich von der Domäne ab, wodurch ein **Single Logout** Mechanismus ihn an allen Applikationen abmeldet



# Key Concepts

## → Komponente: Autorisierungs-Management

### Basis:

- Anwendungsübergreifende **Berechtigungs- und Richtlinienverwaltung**

### Bedeutet:

- Berechtigungen: **Attribute, Rollen, Gruppenzugehörigkeiten**
- **Automatische Zuordnung** der Berechtigungen, regel- und richtlinienbasiert

### Mehrwert:

- **Automatisierung** der Vorgänge
- Vermeidung von **Überberechtigung**

# Key Concepts

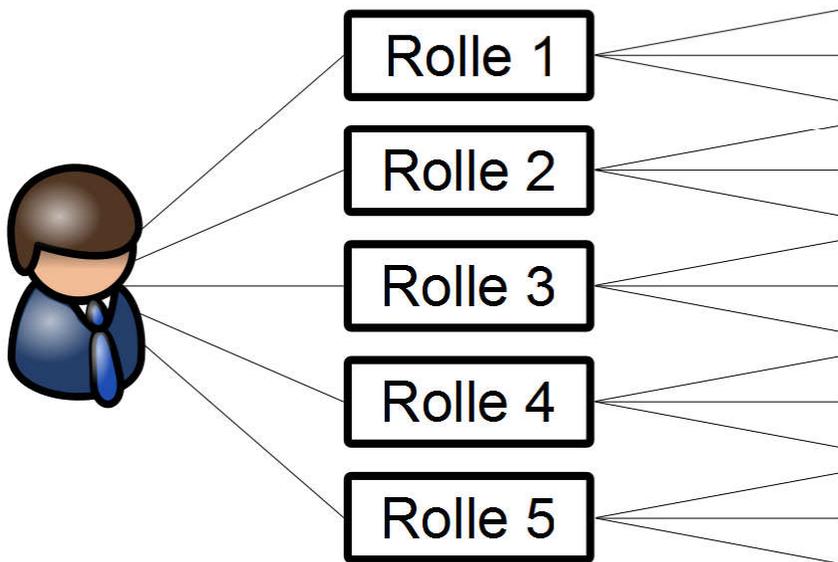
## → Funktion: Access Control

### Authentifikations-Basierte Access Control (NBAC) Modelle:

- Grob- und feingranulare Policy Decision und Enforcement

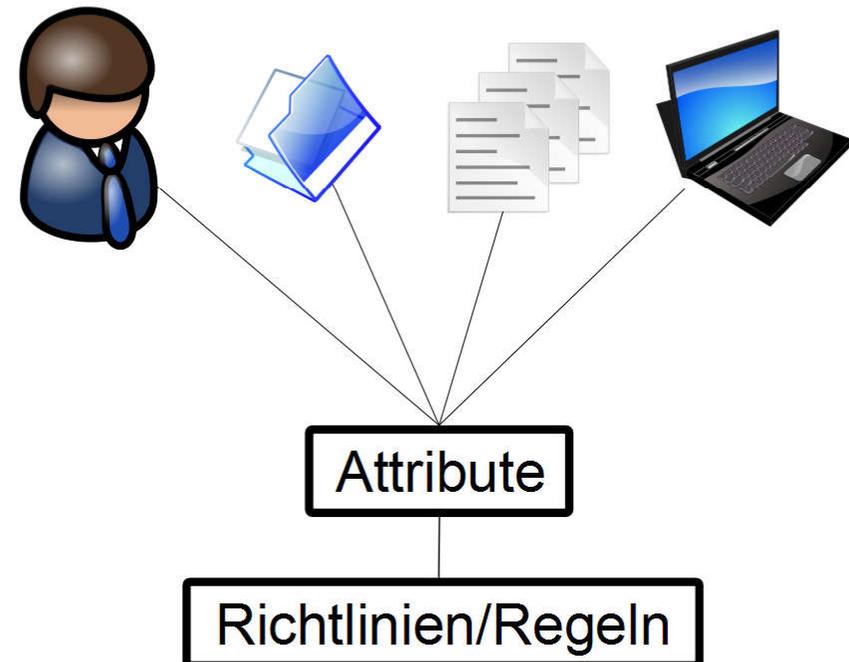
#### Role-Based Access Control

Nutzer -> Rollen -> Berechtigungen



#### Attribute-Based Access Control

Subjekt + Aktion + Resource + Umgebung



# Key Concepts

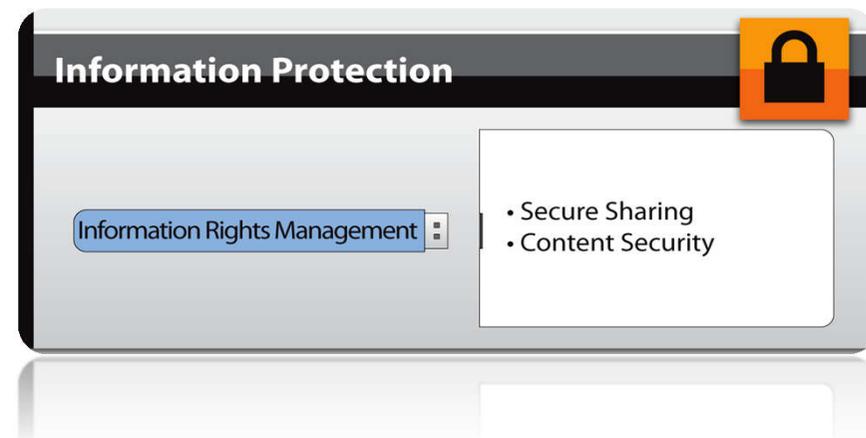
## → Modul: Information Protection

### Basis:

- Über **Policies** werden Informationen nur Personen mit entsprechenden Berechtigungen zugänglich gemacht
- Eine **Information Rights Management (IRM) Infrastruktur** sorgt für Verschlüsselung der Daten und regelt den Zugriff
- **Nachverfolgbarkeit** wird über spezielle Dienste gewährleistet

### Mehrwert:

- Durchgängig angemessenes Schutzlevel
- Schutz von Informationen, auch über Organisationsgrenzen hinweg

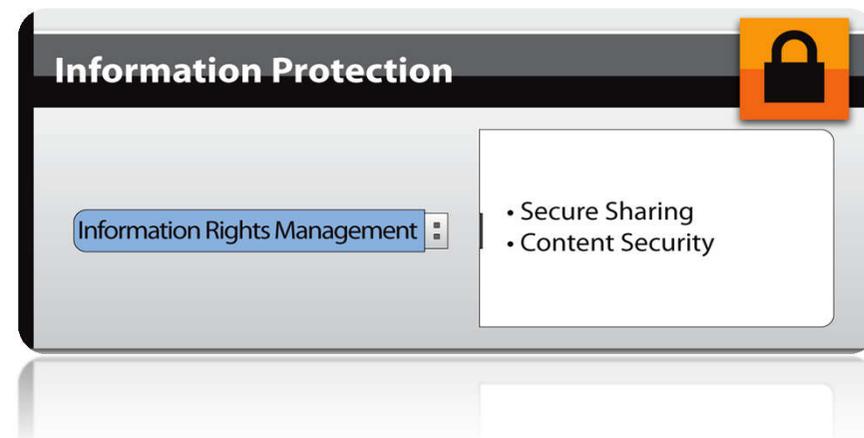


# Key Concepts

## → Modul: Information Protection

### Beispiel für Information Protection:

- Ein Mitarbeiter generiert im Rahmen seiner Tätigkeit **unternehmenskritische Informationen**
- Er muss diese Mitarbeitern und externen Partner zugänglich machen, jedoch sicherstellen, dass **keine unbefugten Personen** Zugriff erhalten
- In seiner Office-Applikation wählt er bei Abspeicherung des Dokumentes die Personen aus, die dieses später lesen können sollen
- Er kann sicher sein, dass das Dokument nun in verschlüsselter Form vorliegt und nur mit Hilfe einer **IRM-Infrastruktur** geöffnet werden kann



# Key Concepts

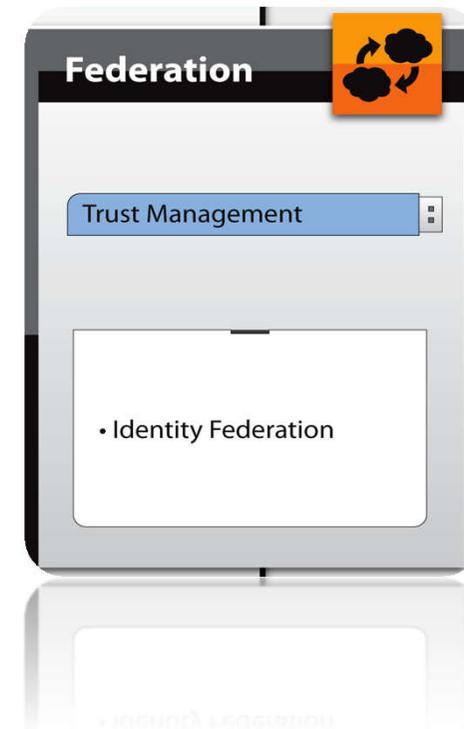
## → Modul: Federation

### Basis:

- **Austausch** von Identitäts- und Authentifizierungsinformationen zwischen unterschiedlichen Organisationen
- **Aufbau von Vertrauensverhältnissen** auf partnerschaftlicher Basis
- Föderierte Autorisierung von Identitäten

### Mehrwert:

- Gemeinsames, sicheres und vertrauenswürdiges Arbeiten auch über Organisationsgrenzen hinweg

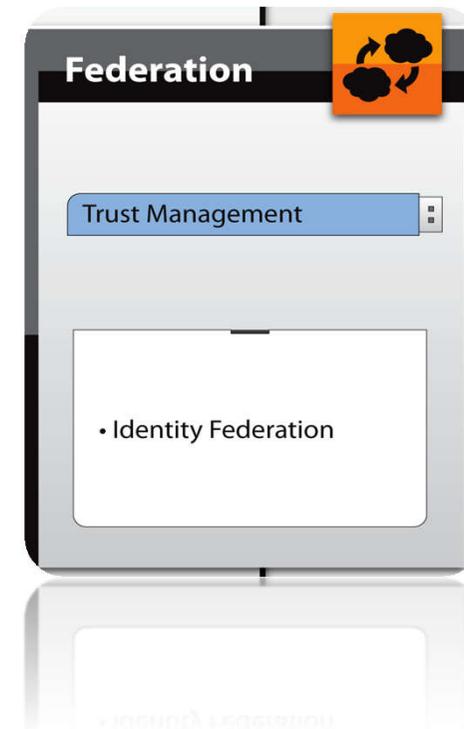


# Key Concepts

## → Modul: Federation

### Beispiel für Federation:

- Der Mitarbeiter muss für einige Zeit mit Applikationen eines Projektpartners arbeiten
- Bei dem Zugriff auf die Applikationen muss er sich wie gewohnt mit seiner SmartCard authentifizieren
- Anschließend kann er wie gewohnt auf die fremde Applikation zugreifen



# Key Concepts

## → Modul: Compliance & Audit

### Compliance & Audit

Compliance Management

Monitoring

Reporting

Auditing



### Basis:

- Dienste und Prozesse zur **Überwachung und Überprüfung aller Vorgänge** im Identity and Access Management System

### Mehrwert:

- Einhaltung von **Vorschriften**
- Erkennung und **Bewertung von Risiken**
- Vergleich eines **Soll-Ist-Zustandes**
- Einhaltung der **Rechtskonformität**

# Key Concepts

## → Modul: Compliance & Audit

### Compliance & Audit

Compliance Management

Monitoring

Reporting

Auditing

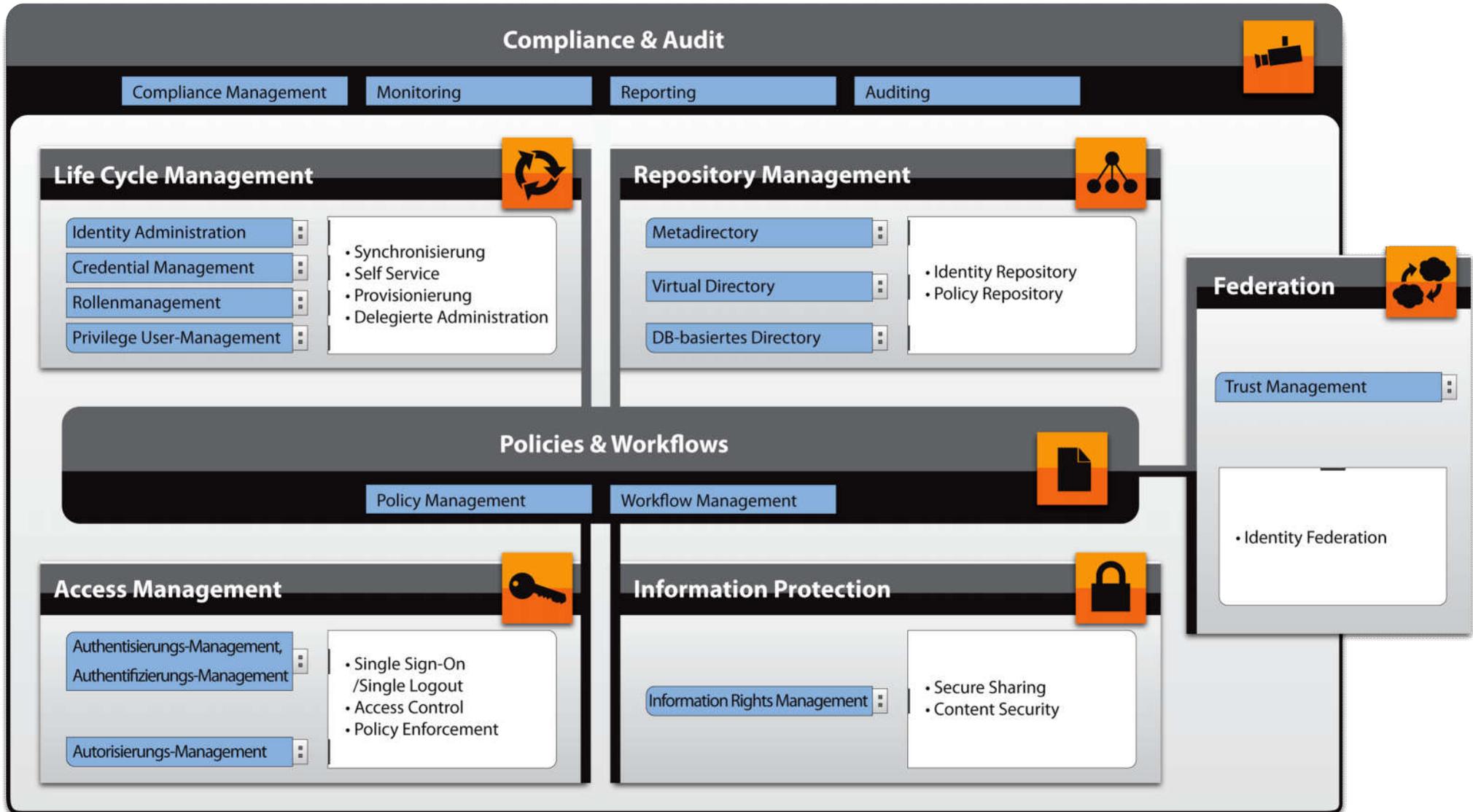


### Beispiel für Compliance & Audit:

- Der Mitarbeiter hat während seiner Tätigkeit weisungsgemäß zwei Transaktionen durchgeführt die eine Verletzung einer Richtlinie bedeuten
- Seinem Vorgesetzten fallen diese Vorgänge auf und er möchte den Gründe hierfür erfahren
- Anhand einen hierfür vorgesehenen Dienst gesendeten Logdateien der Applikation, mit deren Hilfe die Transaktionen ausgeführt wurden, lässt sich die Situation nachvollziehen und der Vorgang durchgängig verifizieren

# Key Concepts

## → Ein IdM-Modell

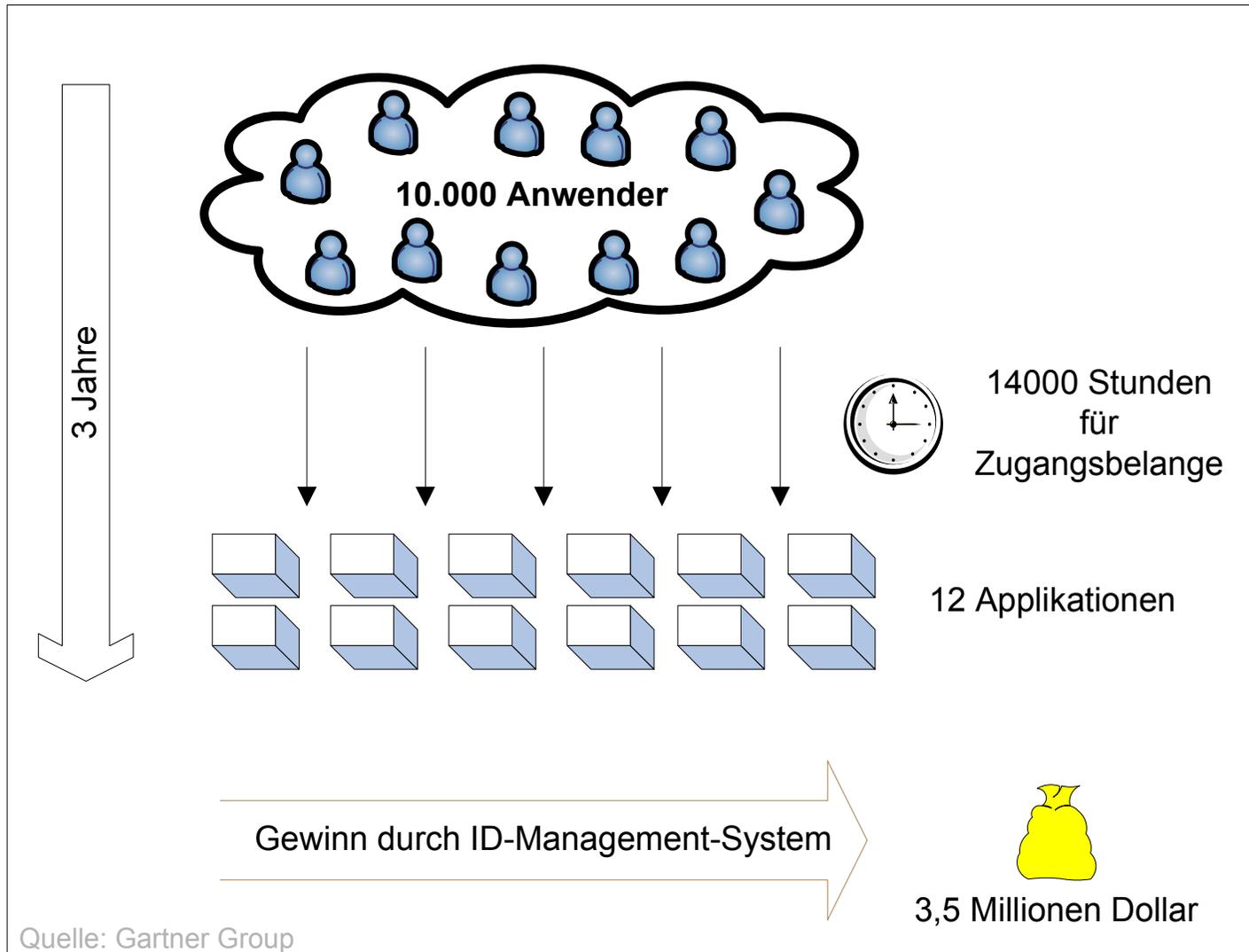


Ganzheitliche Betrachtung

# Key Concepts

## → Kostenszenario

- Kostenersparnis durch Identity Management Systeme



Quelle: Gartner Group

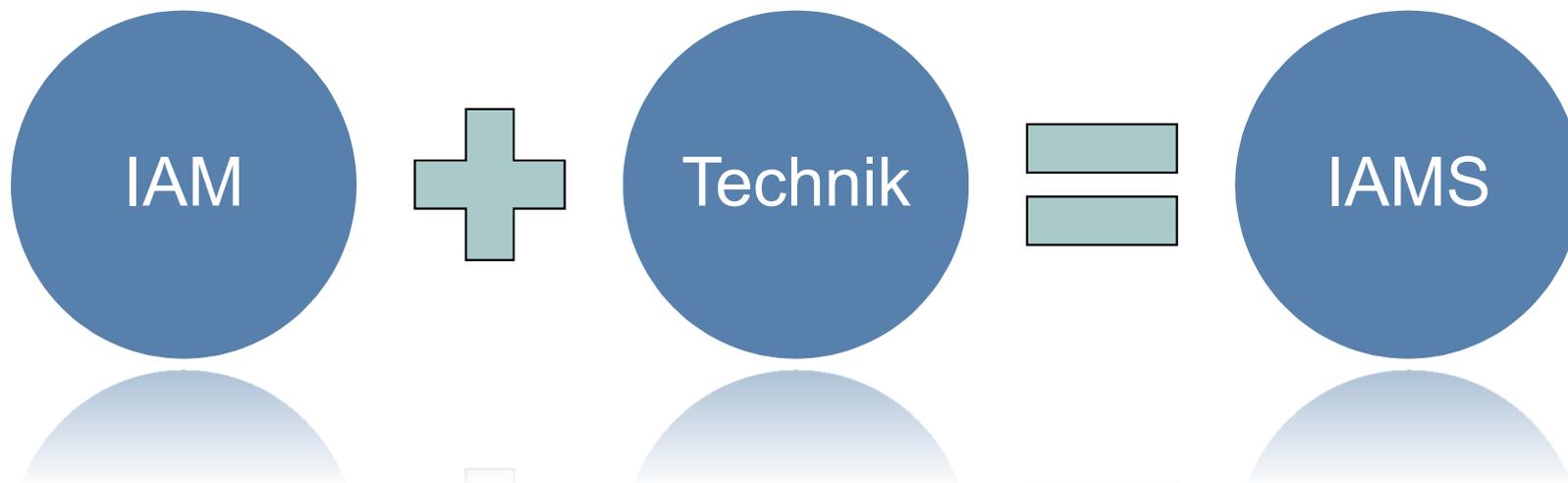
# Key Concepts

## → Technologie

### ■ Technologien eines Identity and Access Management System (IAMS)

- Verzeichnisdienste
- Single Sign-On / -Logout
- Circle of Trust
- Föderation oder zentrale Datenhaltung
- Einbindung von Webservices

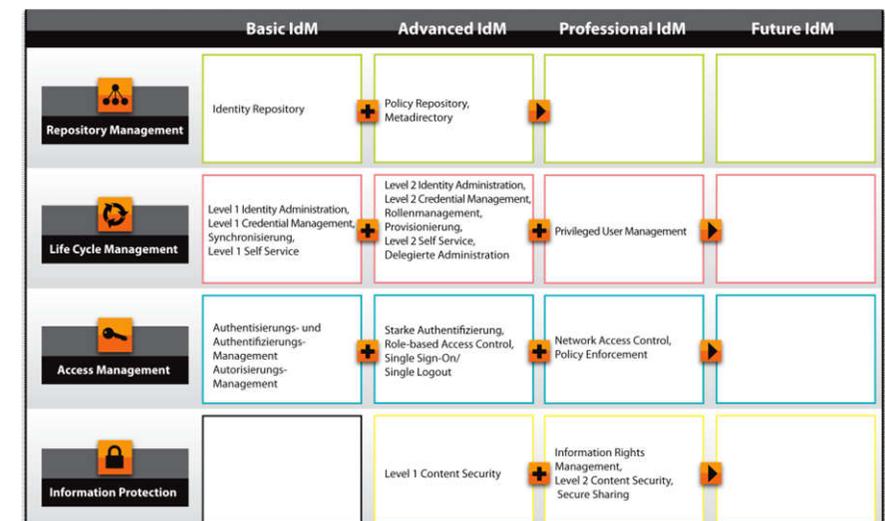
Typische Struktur für  
die Anwendung in  
Firmennetzwerken



- Definitionen
- Notwendigkeit
- Key Concepts
- **IdMS-Lebenszyklus**
- Single Sign-On
- Circle of Trust
- Zusammenfassung

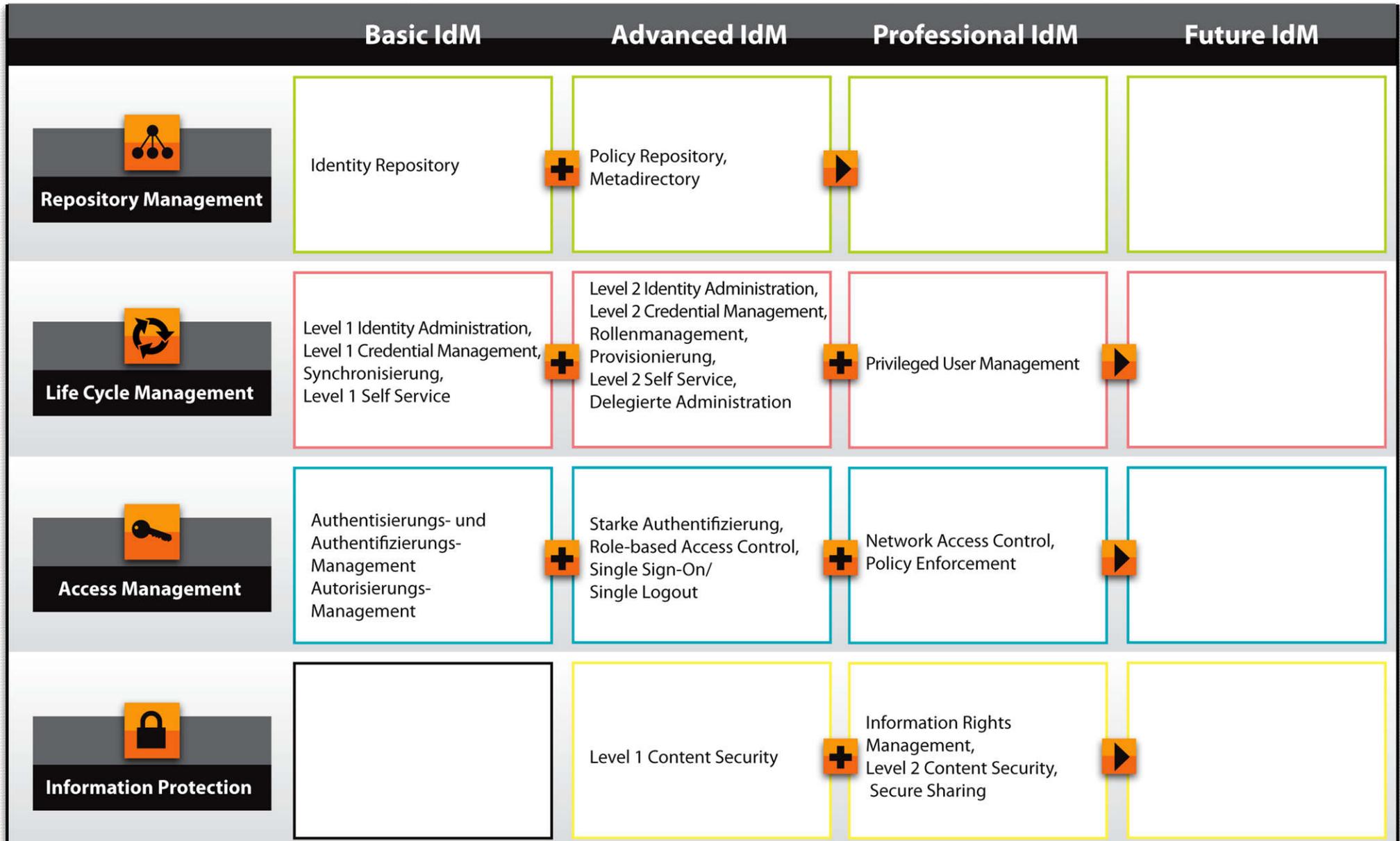
# IAMS-Lebenszyklus

- **Umsetzung** eines IAMS, gleichzeitig **Langzeit-Roadmap** für ein umfassendes IAMS
- **Schrittweises Vorgehen** anhand von **Reifegraden**, eingeteilt in **vier Abstufungen**
- Komponenten und Funktionen werden mit unterschiedlichen Reifegraden, sog. **Leveln**, dargestellt
  - Bestimmte Komponenten und Funktionen **nur schrittweise** eingeführt werden können oder sollten
  - Vorgeschlagene **Umsetzung ist in keinem Fall abschließend**
- IAM := konstanter, nie endender **Prozess**  
→ alle **Module durchlaufen** immer wieder den **Prozess der Überprüfung, Anpassung und Erneuerung**



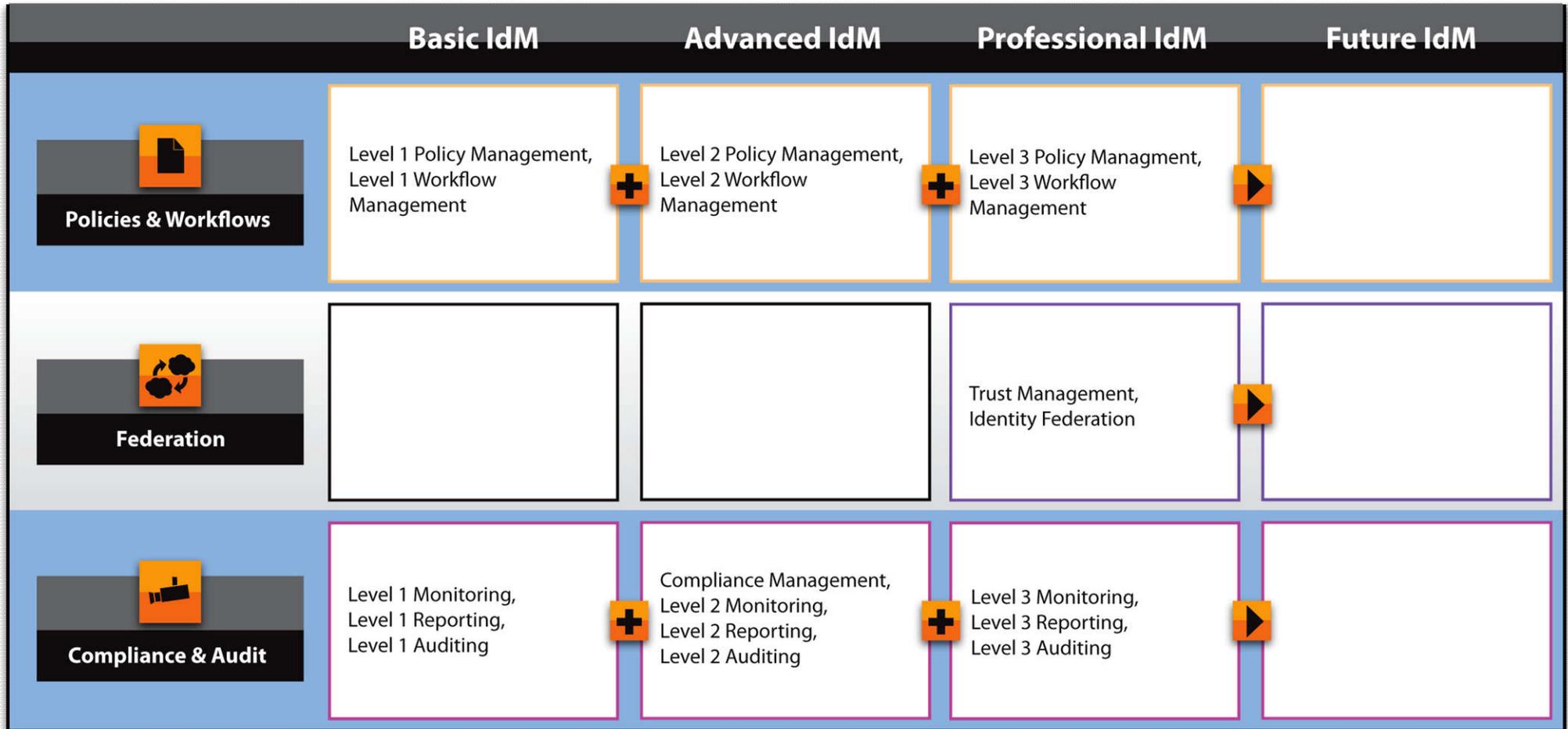
# IAMS-Lebenszyklus

## → Reifegradbetrachtung Teil 1



# IAMS-Lebenszyklus

## → Reifegradbetrachtung Teil 2



### Zyklische Reifegradbetrachtung

Ebenso wie IdM / IAM ein dynamischer Prozess ist, so ist auch das technische System einer ständigen Erneuerung unterworfen

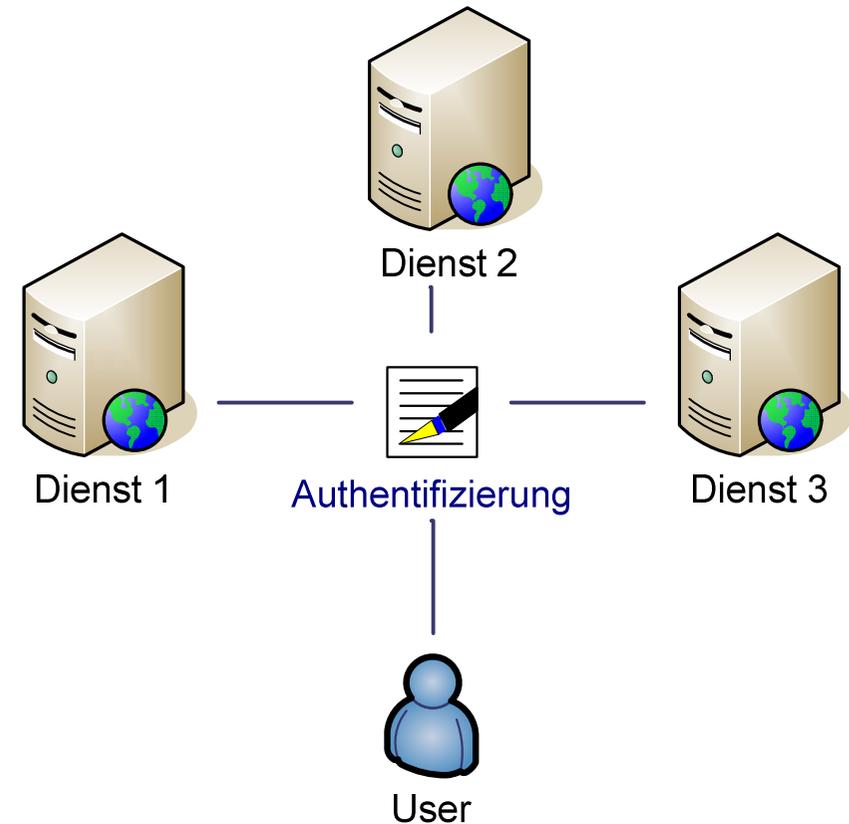
- Definitionen
- Notwendigkeit
- Key Concepts
- IdMS-Lebenszyklus
- **Single Sign-On**
- Circle of Trust
- Zusammenfassung

- Einmalige Authentifizierung → Nutzung weiterer Dienste ohne erneute Authentifizierung
- Sicherheitsgewinn, da nur noch ein Passwort genutzt werden muss, dass komplexer gewählt werden kann
- Komfortgewinn für den Nutzer
- Unterschiedliche Interpretationen:
  - **Portallösung**
    - Nutzung mehrerer Dienste innerhalb eines Portals
    - Nutzung von Cookies
    - Verbreitung besonders in Intranet Systemen
  - **Ticketingsystem**
    - Nutzer erhält Daten (Ticket) welche bei den angeschlossenen Servern bekannt sind
  - **Lokale Lösung**
    - Siehe "Unechtes SSO"

# Single Sign-On

## → Echtes SSO

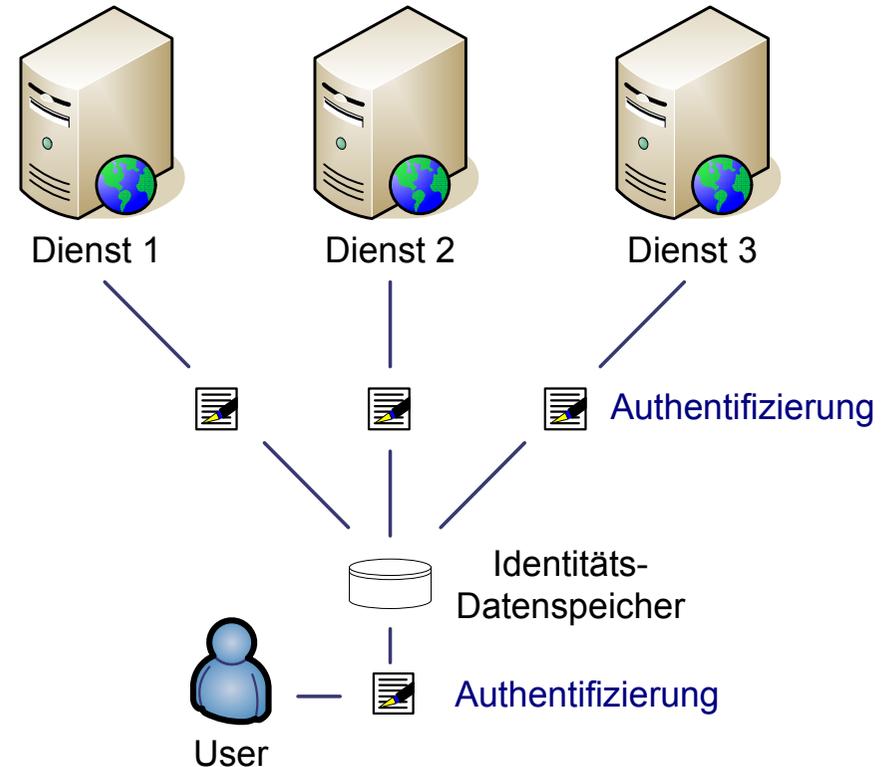
- Serverseitig implementiert
- Kommunikation der Server untereinander → **Identity Federation**
- Vorausgehende vertragliche Vereinbarung zw. den Anbietern → **Trust Management**
- Vorteile:
  - Hoher Komfort
  - Hohe Sicherheit
  - Volle Mobilität
- Nachteile:
  - Aufwendige, komplexe Implementierung



# Single Sign-On

## → Unechtes SSO

- Identitätsdaten-Eingabe-Automatismus
- Einmalige Authentifizierung an einem Identitätsdatenspeicher (Software, USB-Stick)
- Clientseitig implementiert
- Anbieterunabhängig
- **Vorteile:**
  - Sofort einsetzbar
  - Technischer Aufwand gering
- **Nachteile:**
  - Plattform- & betriebssystemabhängig
  - Eingeschränkt mobil



### *Web Single Sign-On*

- URL-“Besitz“ bestimmt Identität
- Dezentraler Mechanismus
- Identitätsverwalter frei wählbar, z.B.:  
<https://openid.internet-sicherheit.de/NorbertPohlmann>

### *Art der Authentisierung*

- Im Standard nicht spezifiziert
- Liegt beim Identitätsverwalter
- Benutzername/Passwort, nPA, ...

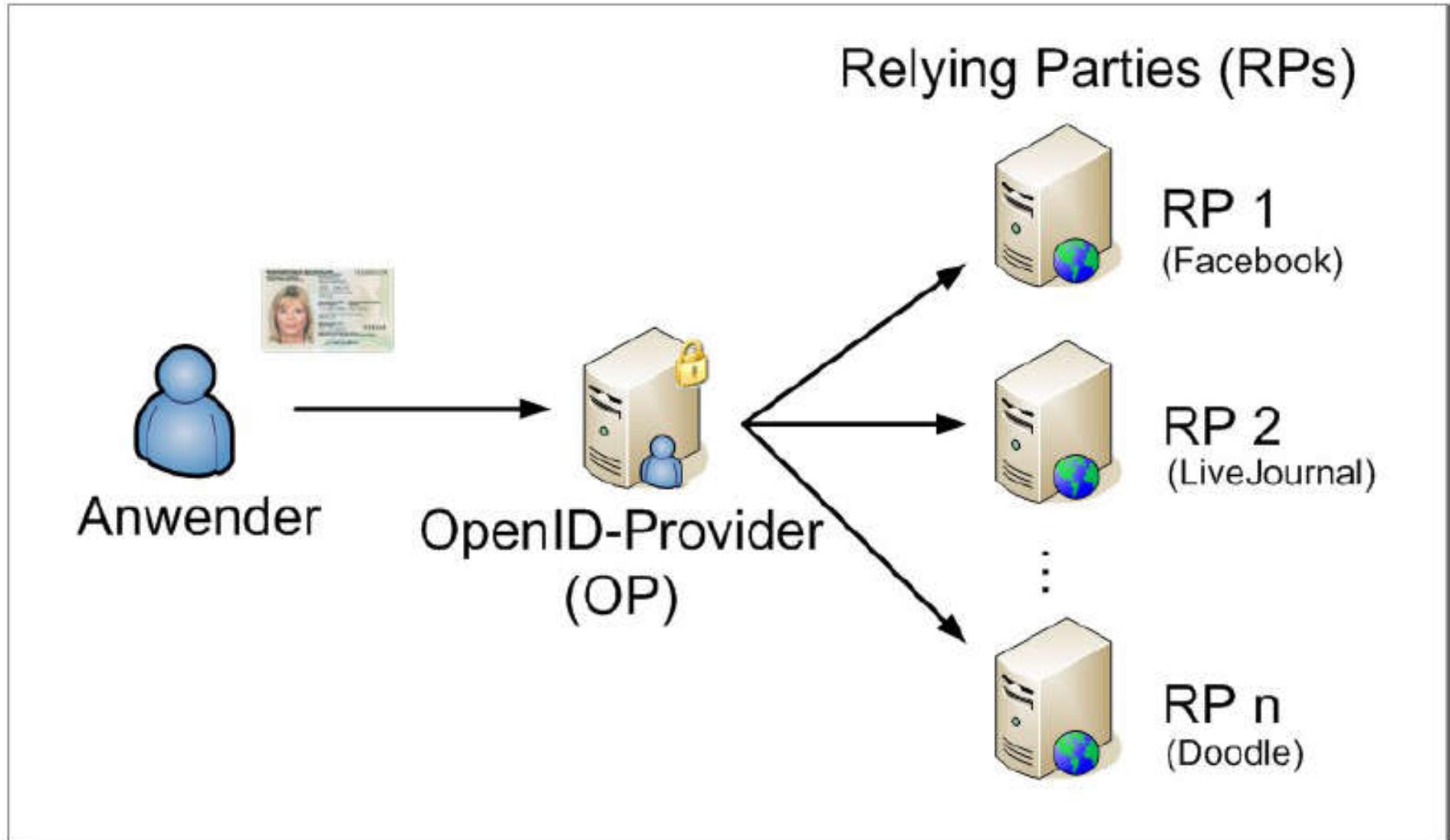


### *Nutzen*

- Einmaliger Login mit OpenID
- Anschließende Nutzung aller Dienste mit OpenID-Unterstützung

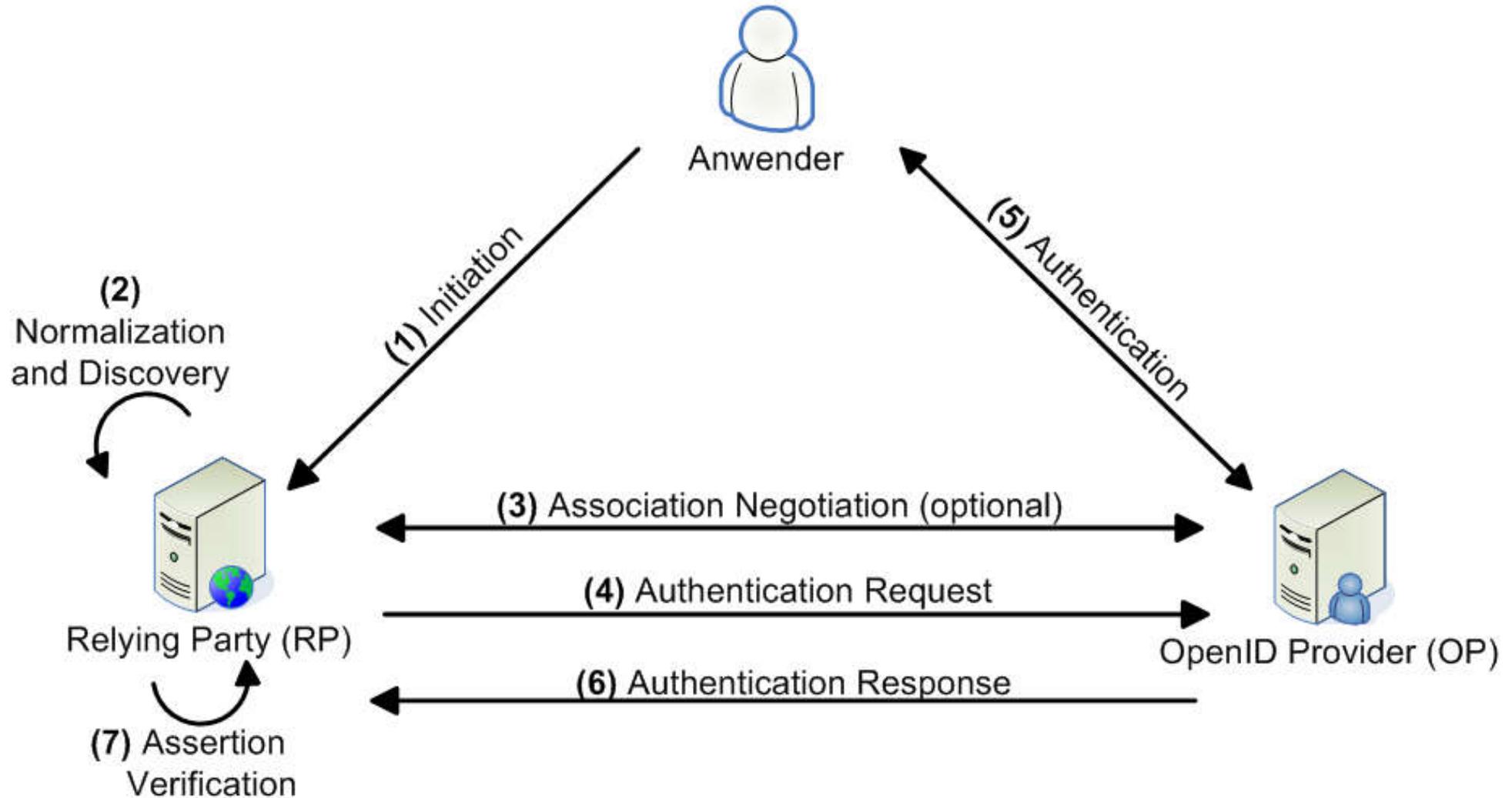
# OpenID

## → Gesamtbild



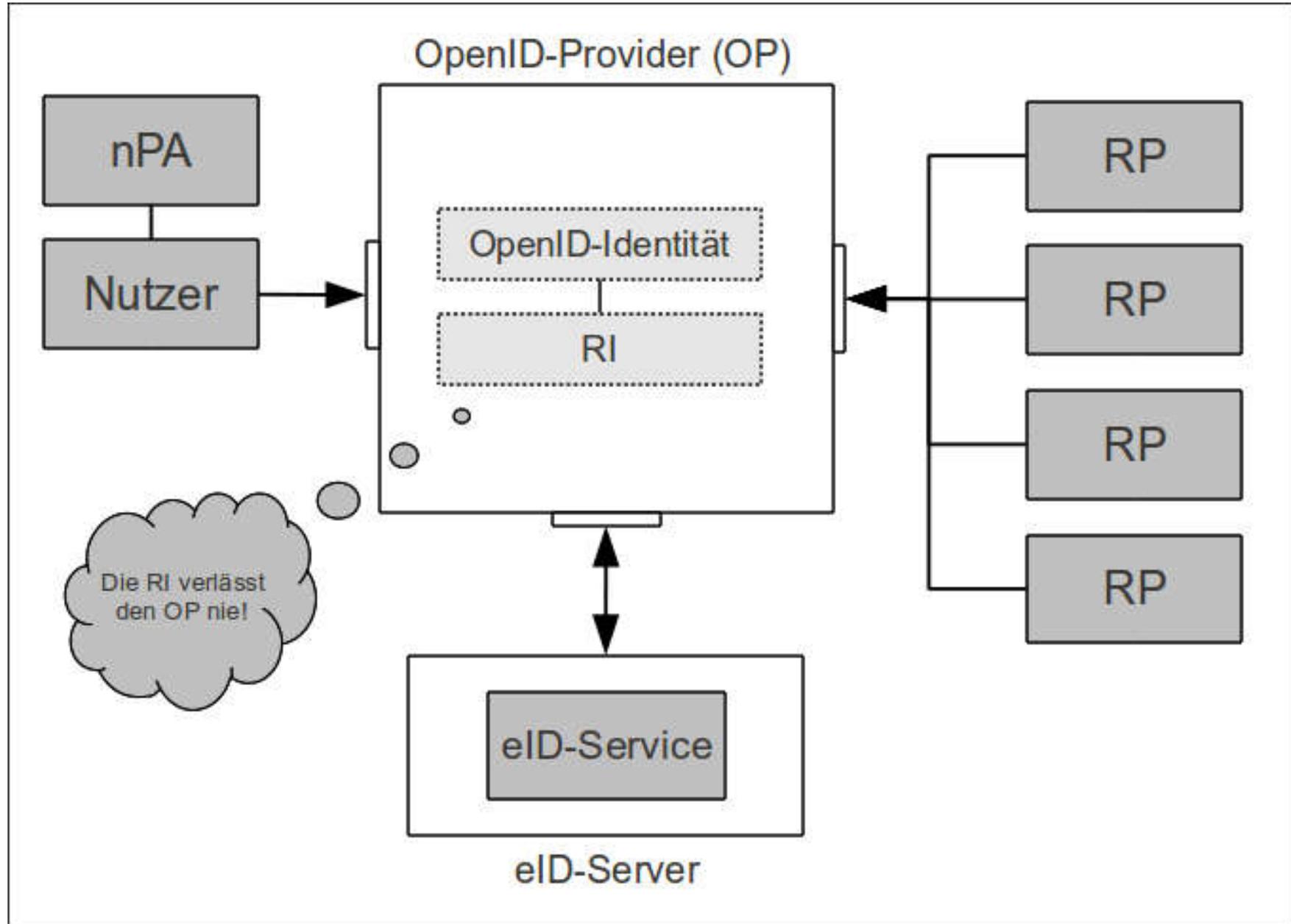
# OpenID

## → Protokollablauf



# OP mit nPA-Unterstützung

## → Konzept und Schnittstellen



- Definitionen
- Notwendigkeit
- Key Concepts
- IdMS-Lebenszyklus
- Single Sign-On
- **Circle of Trust**
- Zusammenfassung

# Circle of Trust (CoT)

## → Konzept

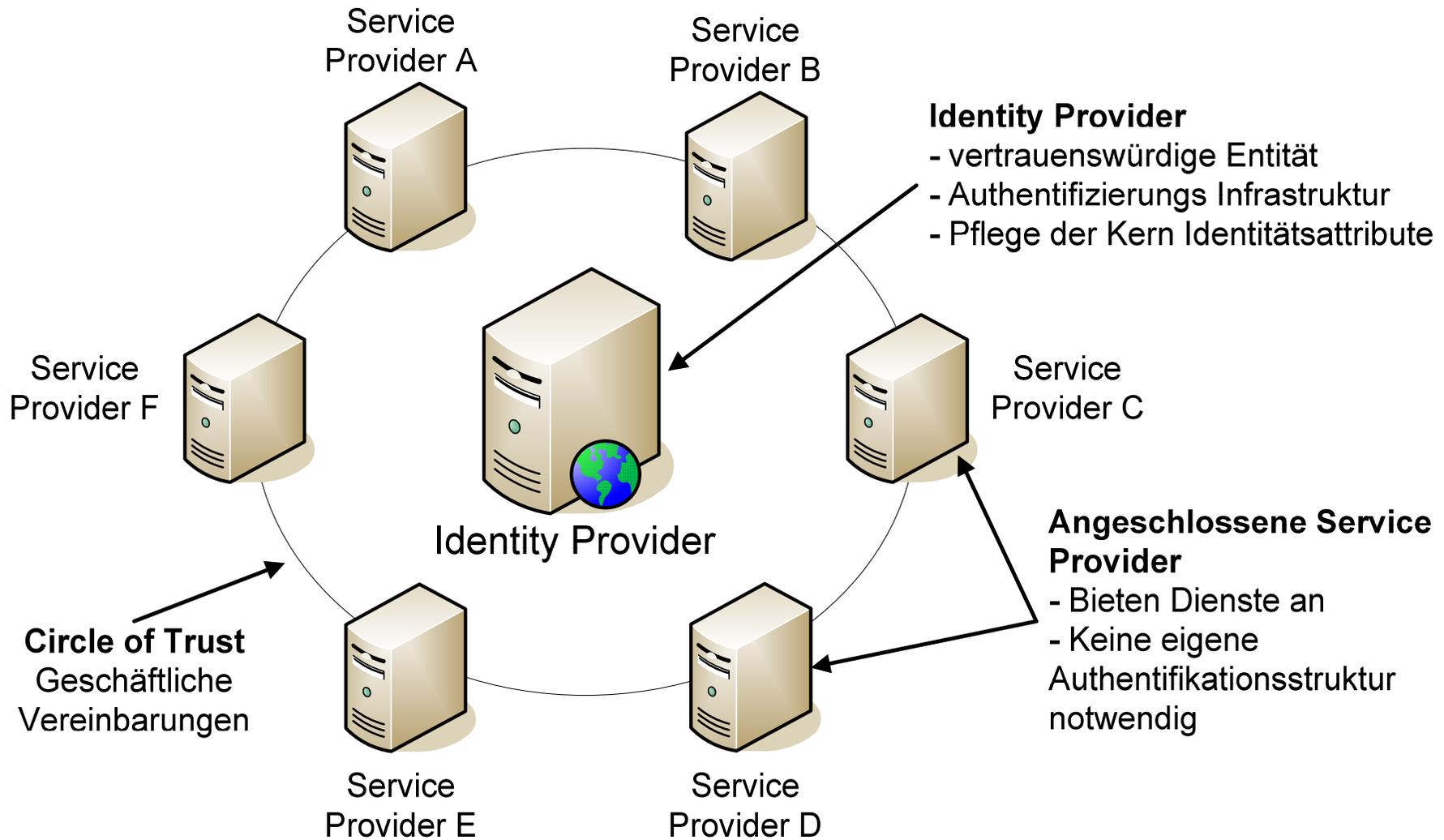
- Konzept, um echtes **Single Sign-On** und weitere vernetzte Dienste anzubieten
- Basierend auf geschäftlichen Vereinbarungen zwischen Diensteanbietern (Einigung auf Technologie notwendig)

Bestehend aus:

- **Identity Providern**
  - Stellt Authentifizierungsinfrastruktur
  - Vertrauenswürdigste Instanz innerhalb des Circle of Trust (CoT) für den Nutzer, da vom Nutzer gewählt
  - Kennt alle angeschlossenen Service Provider
  - Verwaltet die Identitätsinformationen des Nutzers
- **Service Providern**
  - Diensteanbieter
  - Authentifizierungsinfrastruktur nicht notwendig
  - Kennt in der Grundform nur den Identity Provider

# Circle of Trust (CoT)

## → Schema



- Definitionen
- Notwendigkeit
- Key Concepts
- IdMS-Lebenszyklus
- Single Sign-On
- Circle of Trust
- **Zusammenfassung**

# Identity Management

## → Zusammenfassung

- Identity and Access Management Systeme (IAMS) vereinfachen den Umgang mit **digitalen Identitäten**, ihren **Attributen** und **Berechtigungen** enorm
- IAM ist ein **sehr komplexes Thema** – Ein **Modell** bringt unterschiedliche Module in Einklang
- *Zunehmend wird es wichtiger, Authentikationsverfahren zu verwenden, die in der globalen handelnden Gesellschaft über staatliche Grenzen und Verantwortungsbereiche hinaus verwendet werden können.*  
→ Dieser Anspruch aus der Vorlesung Authentikation wird durch IdMS unterstützt
- Die Einführung und der Ausbau von IAMS und Ihrer Konzepte, wie **Single Sign-On**, sind aufgrund der stetig steigenden Anzahl von Identitäten unausweichlich
- **Identitätsföderation** ermöglicht sicheres organisationsübergreifendes Arbeiten von digitalen Identitäten
- Der **Reifegrad** des IAMS muss beachtet werden



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **(Enterprise) Identity and Access Management**

**Vielen Dank für Ihre Aufmerksamkeit  
Fragen ?**

Prof. Dr. (TU NN)  
**Norbert Pohlmann**

Institut für Internet-Sicherheit – if(is)  
Westfälische Hochschule, Gelsenkirchen  
<http://www.internet-sicherheit.de>

**if(is)**  
internet-sicherheit.