

Identity Management

10 Schritte auf dem Weg zum
effektiven Identity Management

Oliver Nyderle
SEN SER PS CNS

Siemens Enterprise
Communications GmbH & Co. KG



Kernbotschaften

4 Punkte die Sie mitnehmen sollten

- Identity Management ist kein einmaliges Projekt sondern ständige Verbesserung
- Die richtige Planung entscheidet über den Erfolg bei der Umsetzung.
- Eine stufenweise Einführung sichert den Erfolg und erhöht die Akzeptanz.
- Die Verbesserung bestehender Prozesse und die Erhöhung des Automatisierungsgrades beginnt schon mit der ersten Applikation.

Der Zweck eines Identity Management ist die Vielzahl der Kennungen und personenbezogenen Informationen welche die Anwender für den Zugriff auf Applikationen, Ressourcen und IT-Systeme benötigen, zu reduzieren und nach Möglichkeit in einer einzigen digitalen Identität zusammenzufassen.

<http://www.iam-wiki.org>

Herausforderungen an Identity & Access Management

SIEMENS

Einhaltung v. Gesetzen und Richtlinien sicherstellen

Sicherheitslücken vermeiden

Administrationskosten senken

Effizienz steigern

Datenqualität verbessern

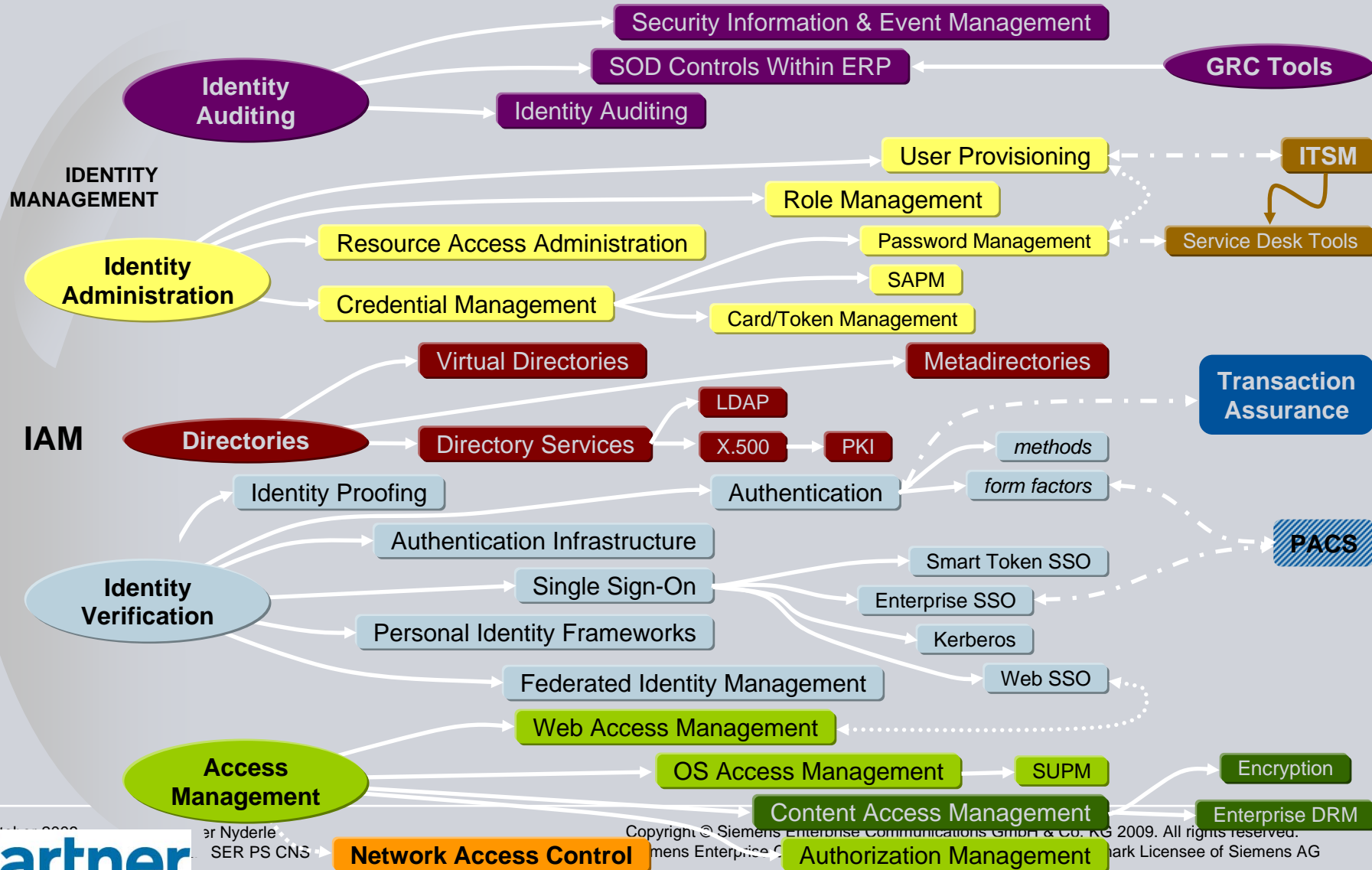
Insellösungen vermeiden



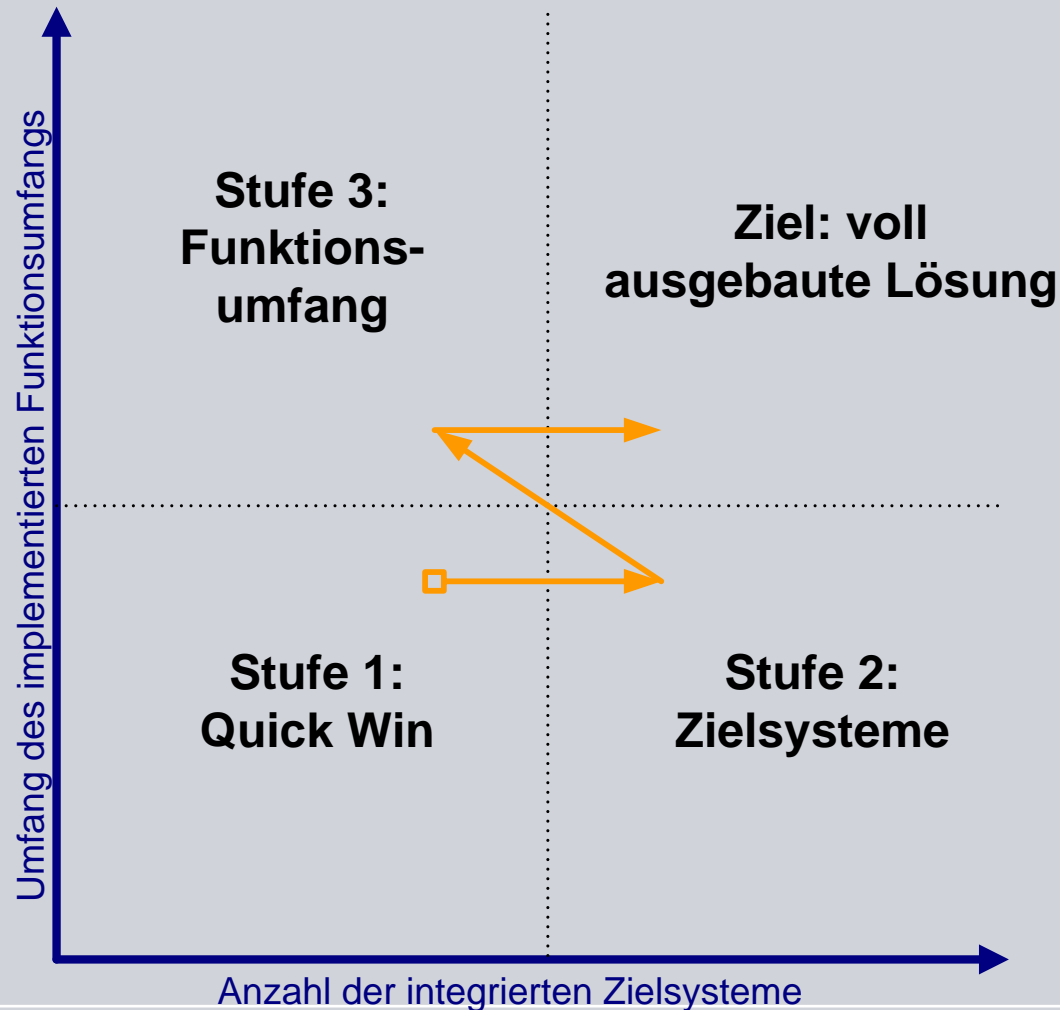
Identity & Access Management

Die Themenvielfalt im Gartner Jellyfish

SIEMENS



1. Vorbereitung Der Stufenplan



2. 10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten
- Schritt 2: **Überprüfen** - Integration von Zielsystemen
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe
- Schritt 7: **Verwenden** - Identity Management für die Benutzer
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht
- Schritt 10: **Verändern** - Rollenmodellierungsprozess

Übersicht - Komponenten

Quellen (z.B. HR)

internal

external

partners

customers

Mitarbeiter



Zielsysteme

accounts

membership

groups/roles

Zusatzinformationen

organizational

geographical

commercial

life cycle

Identity Store

Compliance

security policy

revision department

laws / regulations

10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten
- Schritt 2: **Überprüfen** - Integration von Zielsystemen
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe
- Schritt 7: **Verwenden** - Identity Management für die Benutzer
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht
- Schritt 10: **Verändern** - Rollenmodellierungsprozess



Schritt 1: Integrieren - Integration von Identitäten

Herausforderungen, Aufgaben, Vorteile

Herausforderungen

- verschiedene Quellen
- unterschiedliche Verantwortlichkeiten
- Mengengerüste, Aktualität
- Verfügbarkeit von Organisations-Daten

Aufgaben

- Klassifizierung von Identitäten
- Spezifikation des Lebenszyklus
- Integration von Organisations-Daten

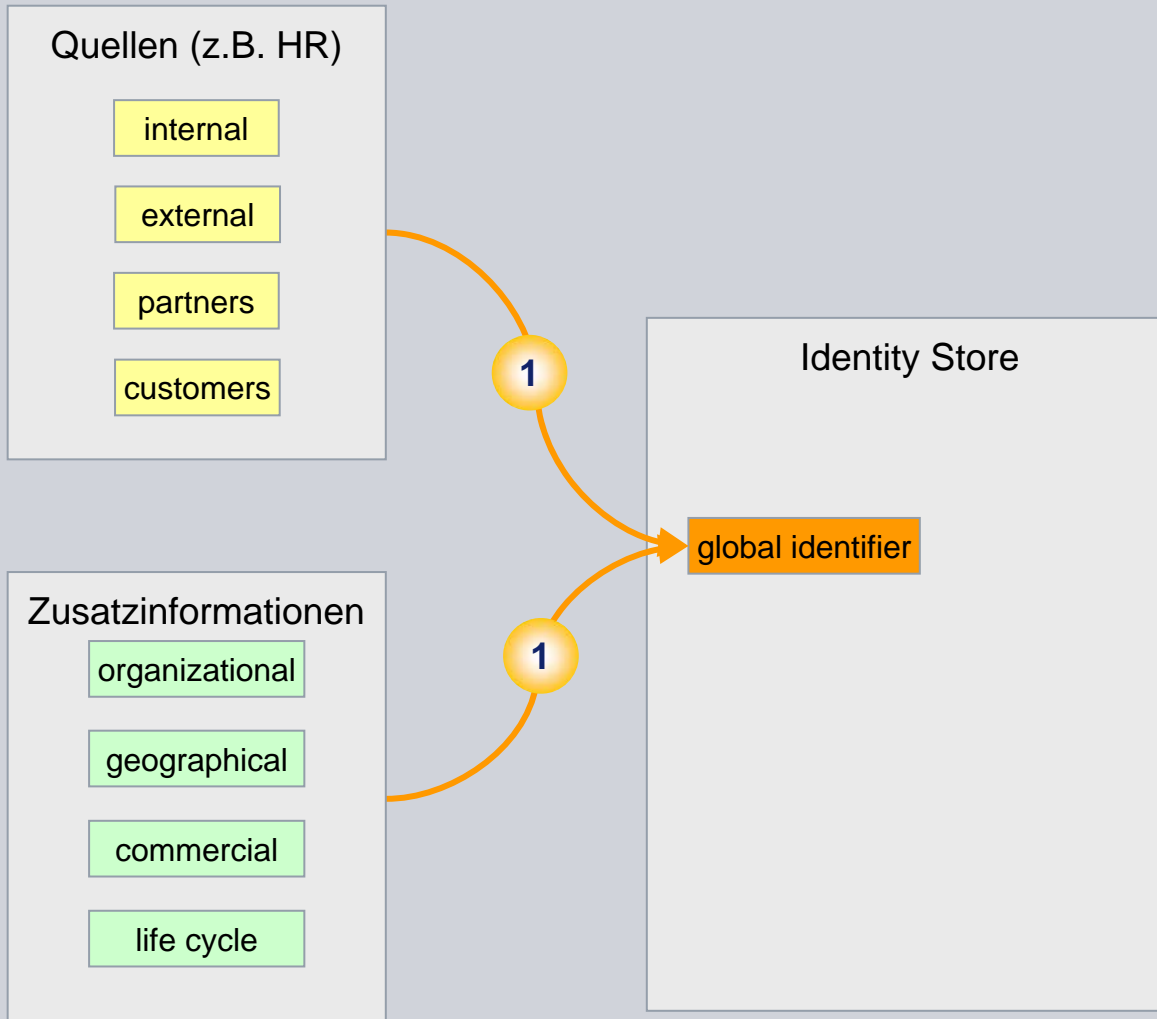
Nutzbare Vorteile

- Zentraler Identitätsspeicher
- Nutzbarkeit als Identity-Provider in einer Service Orientierten Architektur
- konsistente Stammdaten für die Einführung neuer Systeme




Schritt 1: Integrieren

Integration von Identitäten



10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen 
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe
- Schritt 7: **Verwenden** - Identity Management für die Benutzer
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht
- Schritt 10: **Verändern** - Rollenmodellierungsprozess

Schritt 2: Überprüfen - Integration von Zielsystemen

Herausforderungen, Aufgaben, Vorteile

Herausforderungen

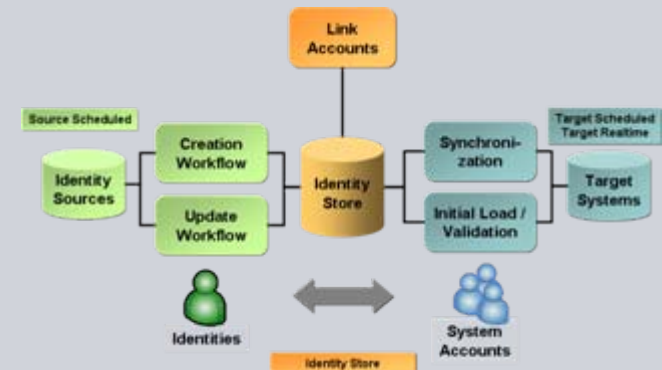
- unterschiedliche Verwaltungsprozesse
- Namesregeln
- Verfügbarkeit geeigneter Schnittstellen

Aufgaben

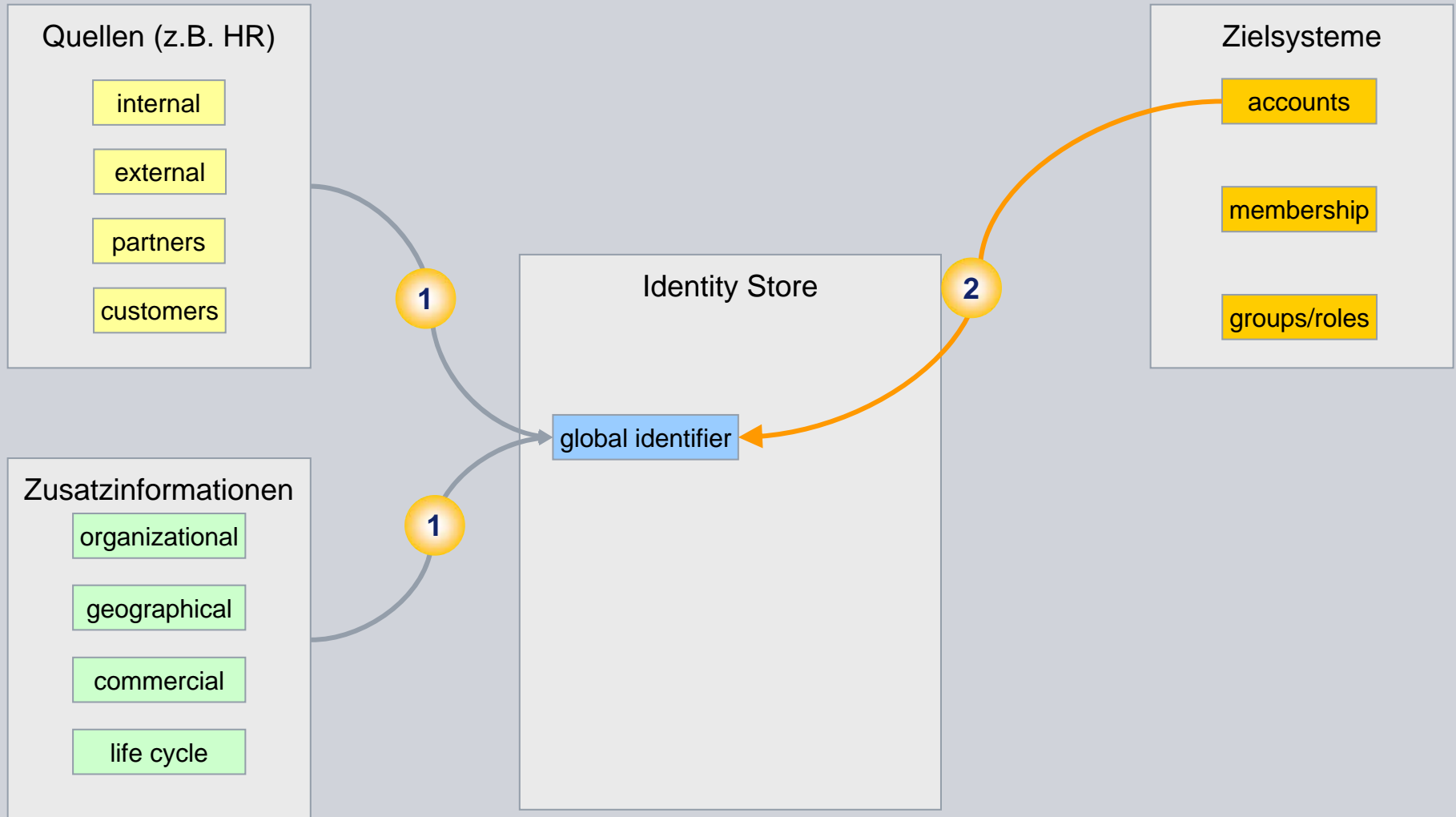
- Zusammenführung von Systemkennungen
- Einführung eines globalen Identifiers
- Durchführung von Datenkonsolidierungen

Nutzbare Vorteile

- Überprüfung der Zielsysteme möglich
- Verhinderung unberechtigter Zugriffe
- Zusammenführung nutzbar für Lizenzkostenberechnung



Schritt 2: Überprüfen Integration von Zielsystemen



10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen ✓
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen ←
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe
- Schritt 7: **Verwenden** - Identity Management für die Benutzer
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht
- Schritt 10: **Verändern** - Rollenmodellierungsprozess

Schritt 3: Analysieren - Analyse der bestehenden Berechtigungsstrukturen

Herausforderungen, Aufgaben, Vorteile

Herausforderungen

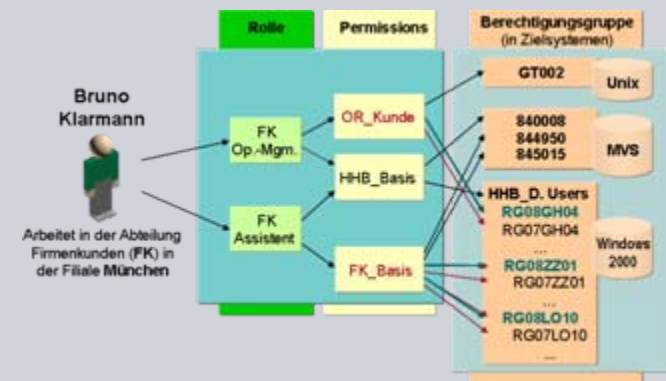
- vorhandene Rechtestrukturen müssen berücksichtigt werden
- Systeme mit komplexen Rechtestrukturen
- Datenleichen verschleiern das tatsächliche Bild

Aufgaben

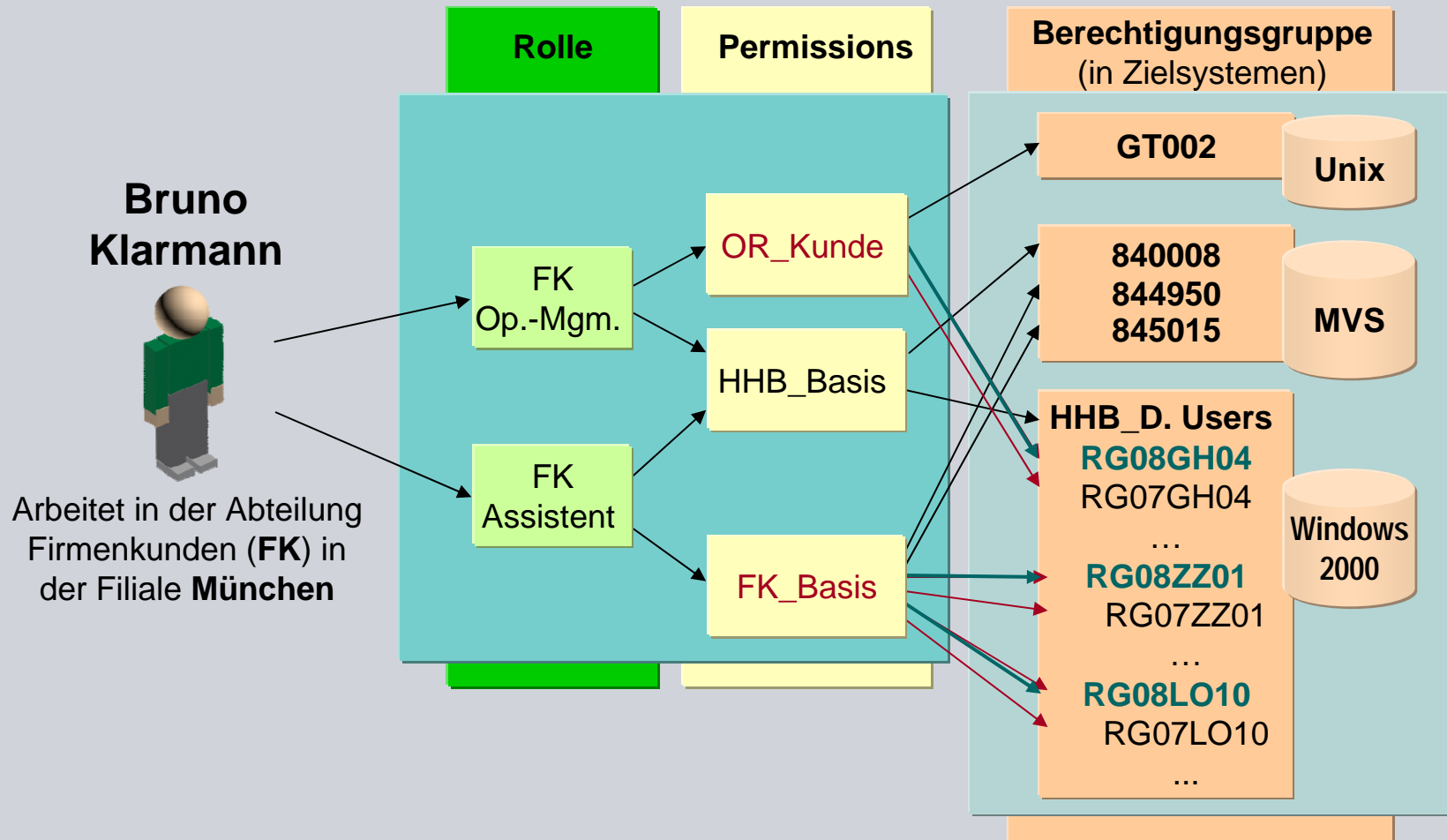
- Analyse der Berechtigungsstrukturen
- Strukturierung der Zielsystemrechte
- Entfernen von veralteten Zuweisungen

Nutzbare Vorteile

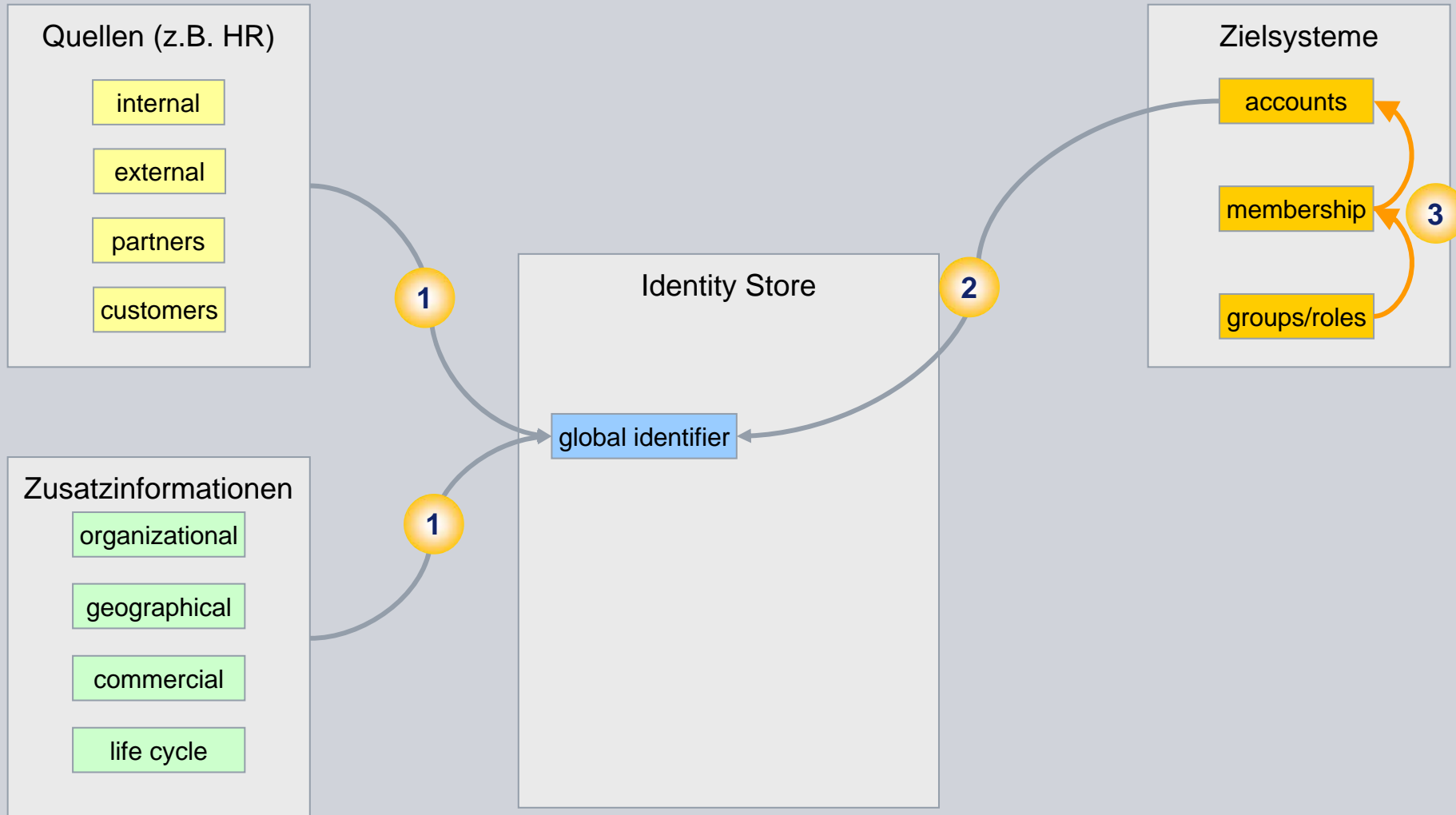
- Nutzung des bestehenden Wissen zur Rechtestrukturierung
- Identitätszuordnungen können die Auswertung verbessern (Schritte 1,2)
- Vereinfachung der Zuweisung durch Strukturierung




Schritt 3: Analysieren - Analyse der bestehenden Berechtigungsstrukturen (Role Mining)



Schritt 3: Analysieren - Analyse der bestehenden Berechtigungsstrukturen



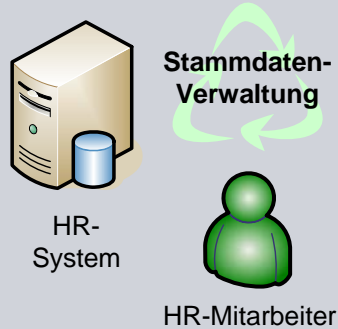
10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen ✓
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen ✓
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge 
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe
- Schritt 7: **Verwenden** - Identity Management für die Benutzer
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht
- Schritt 10: **Verändern** - Rollenmodellierungsprozess

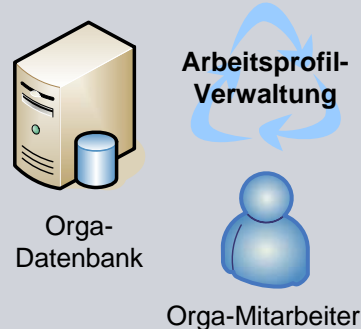
Schritt 4: Automatisieren - Steuerung der Berechtigungszugänge

Aktivieren und Deaktivieren von Systemzugängen

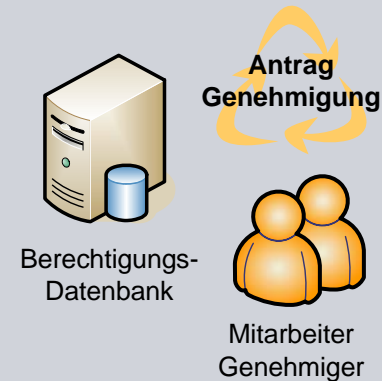
Personal-prozesse



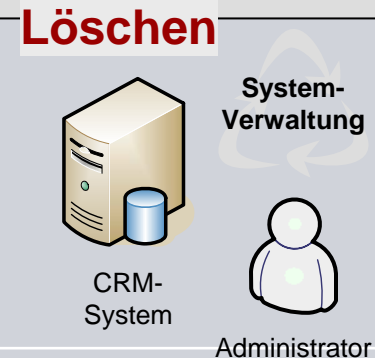
Organisations-prozesse



Berechtigungs-prozesse



Systemverwaltungs-prozesse



Schritt 4: Automatisieren - Steuerung der Berechtigungszugänge

Herausforderungen, Aufgaben, Vorteile

SIEMENS

Herausforderungen

- verschiedene Prozessebenen
- Verantwortlichkeiten innerhalb der Organisation
- Budget für übergreifende Projekte

Aufgaben

- Prozesse Zusammenführen
- Aufgabentrennung zwischen Benutzer- und Systemverwaltung
- Trennung zwischen Systemzugang und Detailrechten

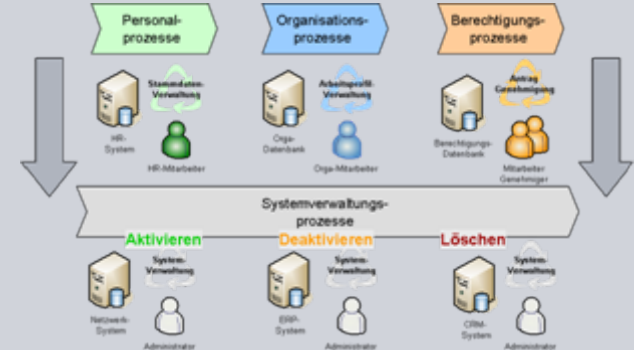
Aktivieren

Deaktivieren

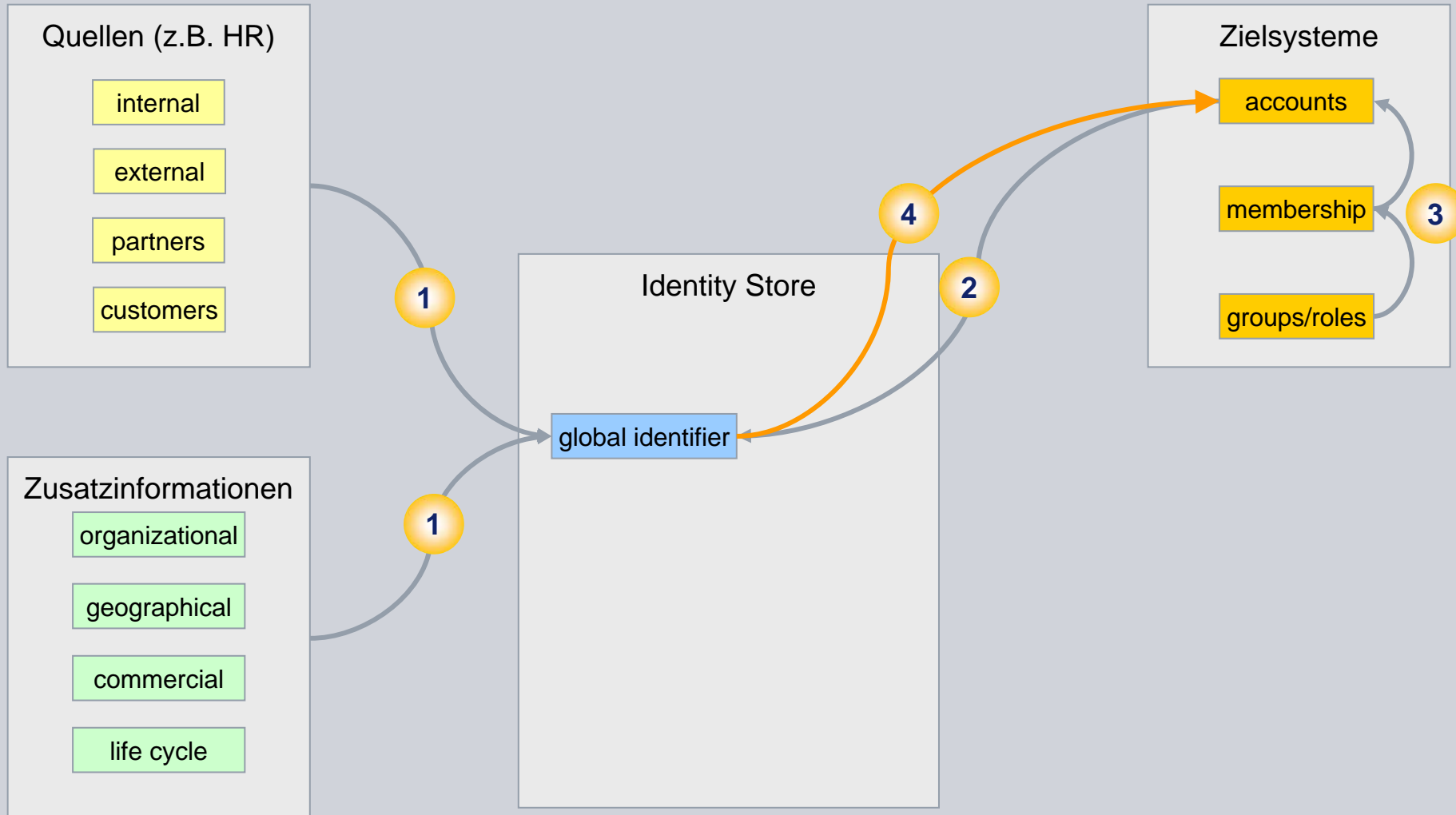
Löschen

Nutzbare Vorteile

- Erhöhung des Automatisierungsgrades
- Erhöhung des Sicherheitslevels
- Entlastung der Systemadministratoren bzgl. manueller Prüfungen



Schritt 4: Automatisieren Steuerung der Berechtigungszugänge



10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen ✓
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen ✓
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge ✓
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe ←
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe
- Schritt 7: **Verwenden** - Identity Management für die Benutzer
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht
- Schritt 10: **Verändern** - Rollenmodellierungsprozess

Schritt 5: Bereitstellen - Regelbasierte Automatisierung der Rechtevergabe (Provisionierung)

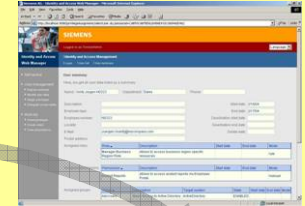
Mitarbeiter wird eingestellt

HR-Verwaltung

- Die Stammdaten werden im Personalwesen erzeugt und automatisch an den zentralen Identity Store übergeben

Identitätsverwaltung

- Über die IAM Plattform werden Identitäten unterschiedlicher Herkunft zentral bereitgestellt.
- Regeln sind auf Basis der Sicherheitsrichtlinien (Policies) des Unternehmens hinterlegt



Einführung von Regeln

- Zuweisung
- Validierung
- Konsistenz

Identity & Access Management

Berechtigungen

- Entsprechend den definierten Regeln werden Berechtigungen automatisch gesetzt
- Individuelle Kriterien: z.B. Laufzeit werden im IAM eingetragen

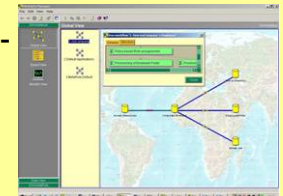
Produktivität

- Mitarbeiter verfügt über die in den Regeln vereinbarten Zugänge und Berechtigungen

In Minuten

Provisioning Prozess

- In den Zielsystemen werden Intranet-/Extranetzzugang, Email-Account, (...und andere) automatisch erzeugt
- Individuelle Berechtigungen in Portale werden gesetzt



SIEMENS

Herausforderungen, Aufgaben, Vorteile

Herausforderungen

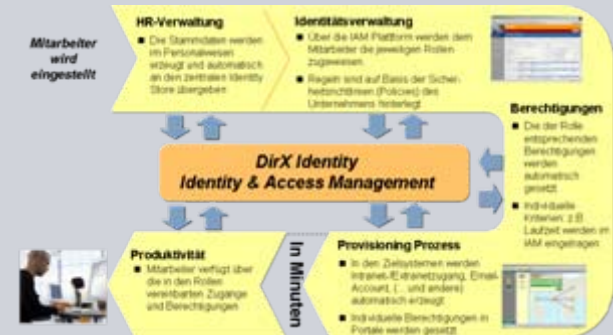
- Organisationsdaten für Regeldefinitionen
- Ausnahmeregelungen
- Komplexe Rechtestrukturen in Zielsystemen

Aufgaben

- Implementierung von Regeln
- Behandlung von Ausnahmen
- Anpassung der Prozesse für notwendige Organisationsdaten

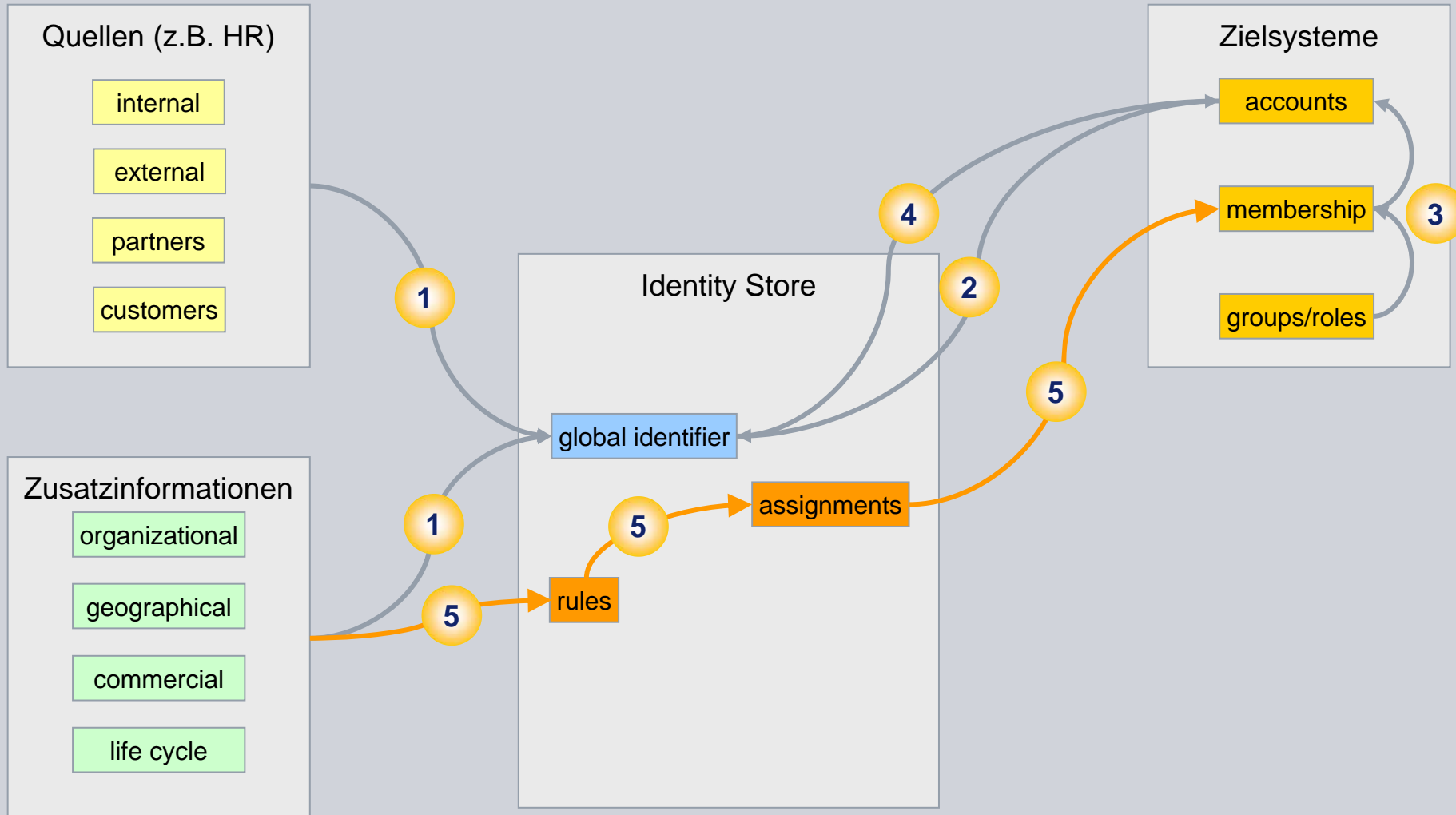
Nutzbare Vorteile

- Erhöhung des Automatisierungsgrades
- Berechtigungen entsprechend der Sicherheitspolicy
- Beschleunigung von Entitlements




Welche Grundlagen existieren für die Definition von Regeln?
Die Organisationsdaten müssen verfügbar sein!

Schritt 5: Bereitstellen – Regelbasierte Automatisierung der Rechtevergabe

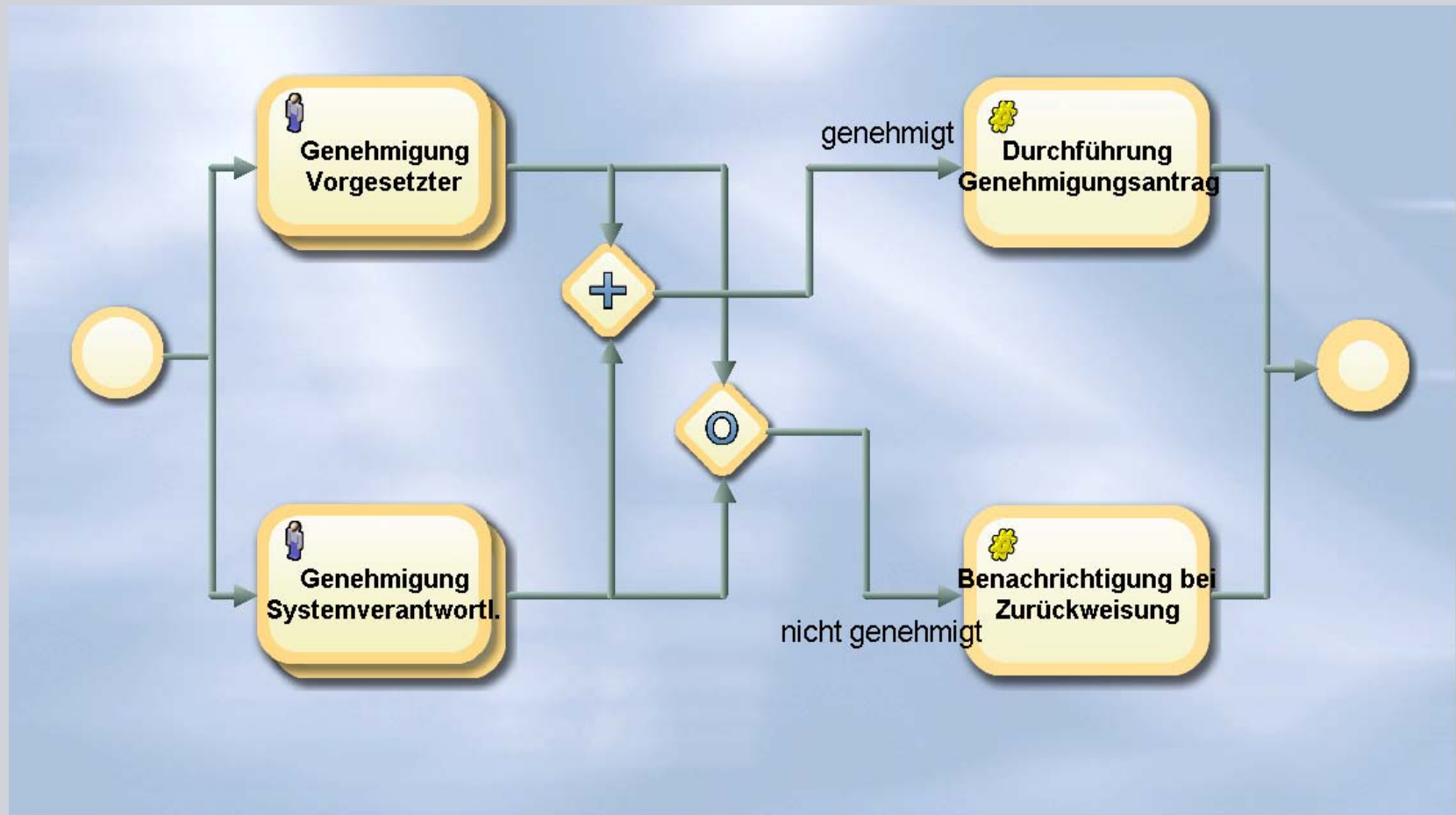


10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen ✓
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen ✓
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge ✓
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe ✓
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe 
- Schritt 7: **Verwenden** - Identity Management für die Benutzer
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht
- Schritt 10: **Verändern** - Rollenmodellierungsprozess

Schritt 6: Absichern - Absicherung der Berechtigungsvergabe

Genehmigungsprozesse



Schritt 6: Absichern - Absicherung der Berechtigungsvergabe

Herausforderungen, Aufgaben, Vorteile

Herausforderungen

- Weitere Rollen für Approvals notwendig
- Prozesse müssen angepasst werden
- Prozessrollout notwendig

Aufgaben

- Definition von Genehmigungsprozessen
- Einbindung der Prozessbeteiligten

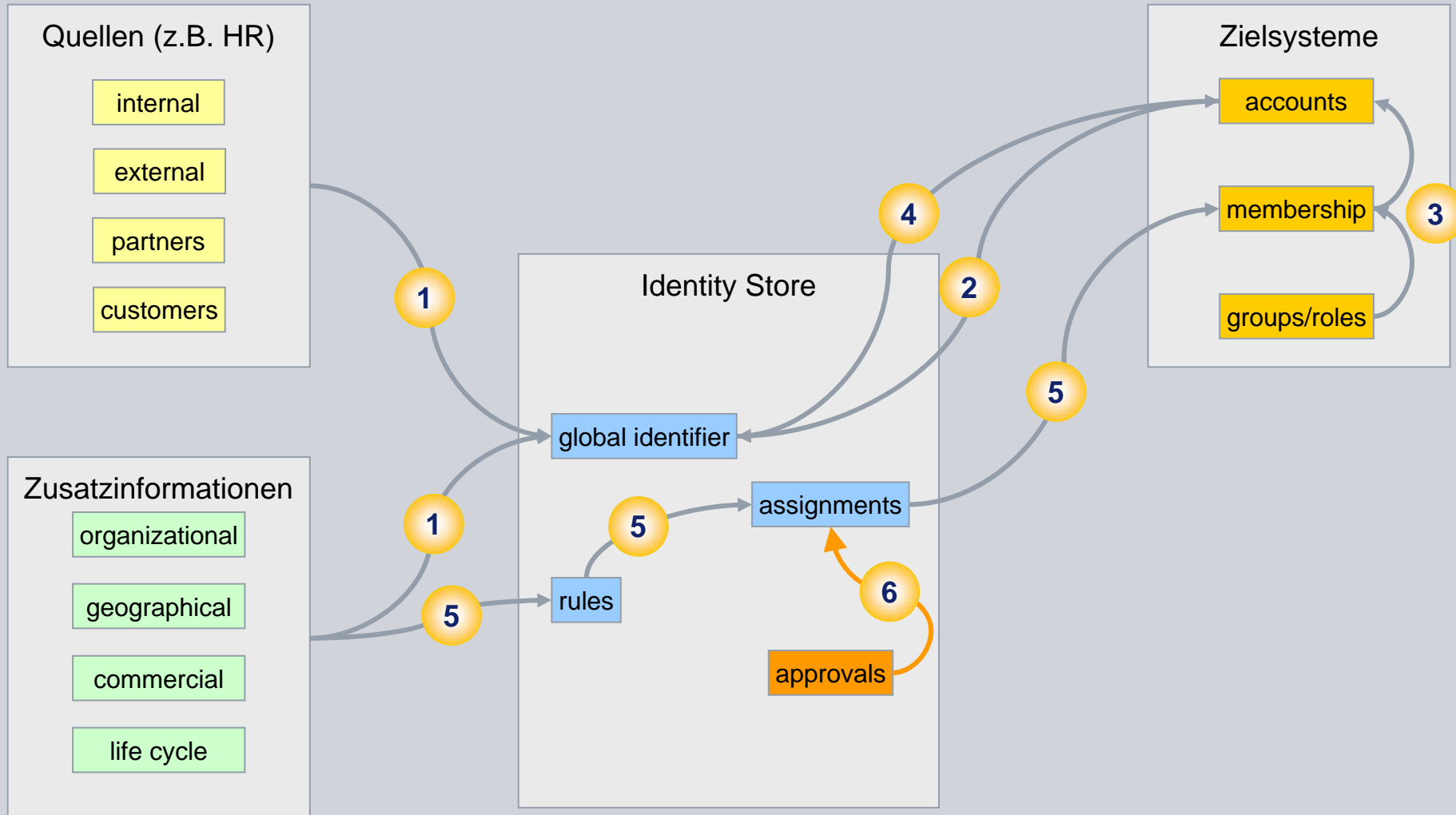
Nutzbare Vorteile

- Absicherung von manuellen Zuweisungen möglich.
- Die Entscheidungen werden durch die Verantwortlichen getroffen.
- kein Medienbruch bei der Umsetzung.




Schritt 6: Absichern

Absicherung der Berechtigungsvergabe



10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen ✓
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen ✓
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge ✓
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe ✓
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe ✓
- Schritt 7: **Verwenden** - Identity Management für die Benutzer 
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht
- Schritt 10: **Verändern** - Rollenmodellierungsprozess

Schritt 7: Verwenden - Identity Management für die Benutzer Self-Service

Siemens AG - DirX Identity Web Center - Microsoft Internet Explorer

Address: http://localhost:8080/webCenter/showUserData.do

Logged on as: Taspach Nik

Language

DirX Identity Web Center

User Management with DirX Identity

Logout

Self service

- Change password
- Add authentication questions
- Modify user data
- Subscribe privileges
- Show subscription status

Delegation

- Show access rights
- Delegate access rights
- Show delegated access rights

User Management

- Add new user
- Display summary
- Modify user data
- Reset password
- Assign privileges
- Copy privileges
- Show subscription status

Administration

- Manage password policies

Work list

- Grant privilege
- View orders

Welcome Retha Wagner

Web Center

Self Service | Delegation | Users | Work List | Rules | Roles | Permissions | Groups | Password Policies

Display summary

History | Back | Forward

Detailed Navigation

- Select user
- Add new user
- Display summary
- Modify user data
- Reset password
- Assign privileges
- Copy privileges
- Show subscription status

User summary

Here, you get all user data listed as a summary.

Name: Bellosa Marco Organizational unit: Proc 12 Phone: +39 6 2345-4657

Description: Procurement Europe

Employee type: Customer Employee number: 5476 Start date: End date:

Country: Italy Locality: Rome Deactivation start date: Deactivation end date: Delete date:

E-Mail: Marco.Bellosa@Mercato-Aurum.com

Postal address: Mercato Aurum, Avenida Diagonale, 00186 Roma, Italy

Fax: +39 6 2345-8873 Mobile: Password policy:

Assigned roles:

Name	Description	State	Start date	End date	Parameters	Mode
Platinum Customer	Platinum customer (excellence bonus program)	ENABLED				rule
Silver Customer	Standard customer	ENABLED				rule

Assigned permissions:

Name	Description	State	Start date	End date	Mode
Platinum Customers	Permission for platinum customers (excellence bonus program)	INHERITED			
Silver Customers	Permissions for standard customers	INHERITED			

Assigned groups:

Name	Description	Target system	State	Start date	End date	Mode
Platin Customers	Excellent customers to be handled with Excellence Bonus Program	Extranet Portal	ADD			
Platin Customers	Excellent customers to be handled with Excellence Bonus Program	Extranet Portal	ADD			
Silver Customers	Standard customer group	Extranet Portal	ADD			
Silver Customers	Standard customer group	Extranet Portal	ADD			

Accounts:

Name	Description	State	Target system	State in TS
Marco Bellosa 5476	Account for Marco Bellosa	ENABLED	Extranet Portal	NONE

- Self-Service
- Stellvertreter-Verwaltung
- Delegierte Administration
- Anträge und Genehmigungen
- Passwort-Management

Schritt 7: **Verwenden** - Identity Management für die Benutzer

Herausforderungen, Aufgaben, Vorteile

Herausforderungen

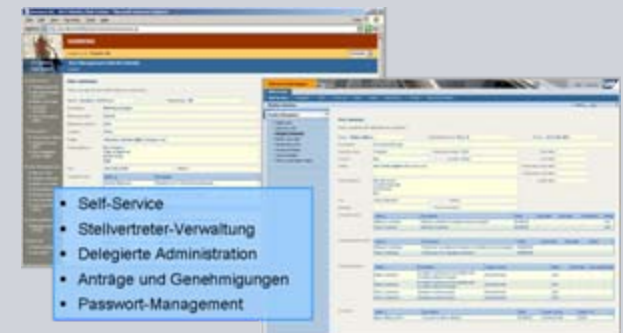
- Endnutzer verwenden das IdM-System
- Antrags- und Genehmigungsprozess

Aufgaben

- Rollout einer Endnutzer-Oberfläche für das IdM-System
- Schulungen für die Endbenutzer
- Implementierung des Antrags- und Genehmigungsprozesses

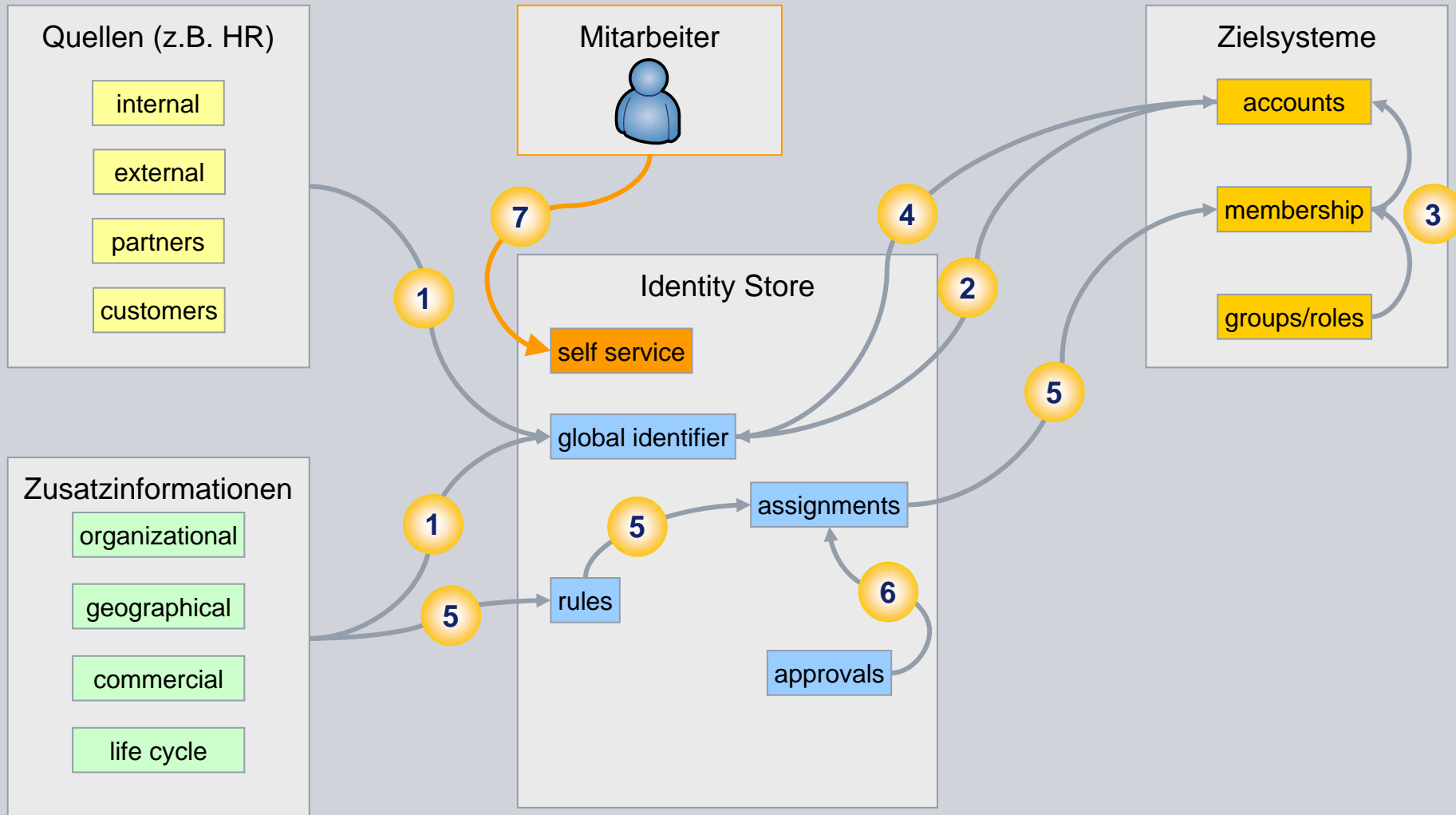
Nutzbare Vorteile

- Reduktion von Hotline-Kosten
- Reduktion papiergestützter Prozesse
- Kostensenkung der administrativen Kosten



Schritt 7: Verwenden

Identity Management für die Benutzer



10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen ✓
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen ✓
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge ✓
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe ✓
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe ✓
- Schritt 7: **Verwenden** - Identity Management für die Benutzer ✓
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht
- Schritt 10: **Verändern** - Rollenmodellierungsprozess



Das Compliance-Problem und die Rolle von IAM



Regulatory Compliance – Was ist zu tun ?

Klare Definition der Zugriffsrechte /
Umsetzung / Überwachung / Reporting



Welche Hindernisse müssen beseitigt werden ?

manuelle Rechteverwaltung /
Intranspatentes Rechte- und Rollenkonzept /
Geringe Datenqualität / Einmal-Aktionen



Source: Gartner 2006,
Identity and Access
Management Today



Die Lösung: Identity und Access Management automatisieren

Prediction: By 2008, investments in identity management solutions will increase 60 percent in order to address regulatory compliance requirements (0.8 probability).

Schritt 8: Nachweisen - Nachweisbarkeit der Rechtevergabe

Herausforderungen, Aufgaben, Vorteile

Herausforderungen

- Rechtliche Rahmenbedingungen
- Security-Policy der Organisation
- zielsystemübergreifende Auswertungen

Aufgaben

- Regelmässige Auswertungen
- Sicherungskonzept für Zuweisungsoperationen
- Erstellung von für die Organisation geeigneter Berichten

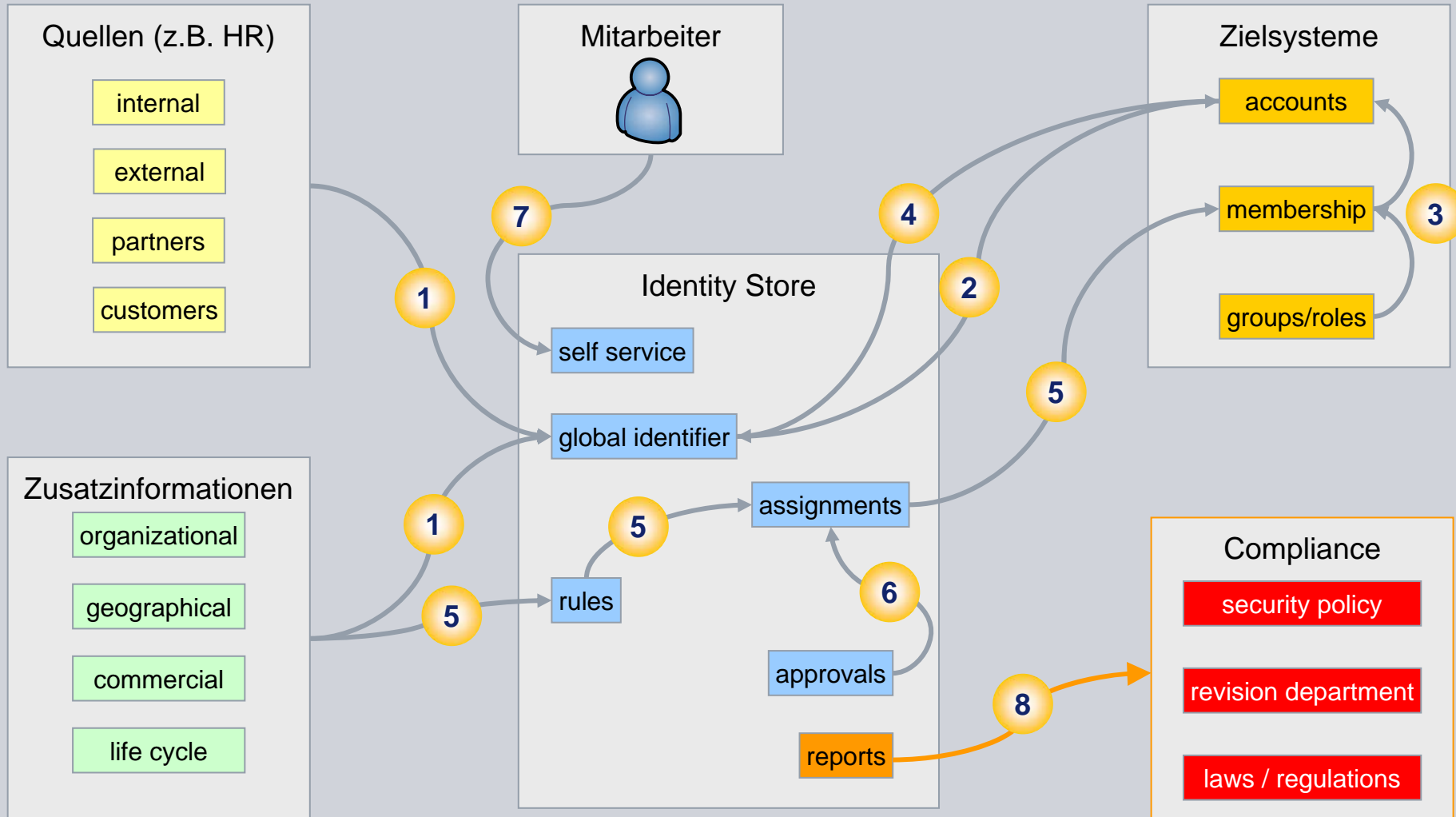
Nutzbare Vorteile

- Erfüllung der Compliance-Anforderungen
- Nachweisbarkeit für Revisionsanforderungen
- Risikominimierung
- Reports auf Basis realer Identitäten


DirX Identity Standard Report:	Auswertungszeitpunkt:	7/17/07 5:20:17 PM CEST
	Auswertungsbasis:	globaler Rollenkatalog
Anzahl der Identitäten pro Rolle	Auswertungsbereich:	alle Identitäten
	Anzahl der Identitäten	direkte Zuweisungen
Standardrollen		
interne Mitarbeiter	1000	1000
externe Mitarbeiter	150	150
Organisations-Rollen		
Vorstand	2	
Landesleitung Vertrieb	1	
Landesleitung Finanzen	1	
Vertrieb	200	
Kaufmannschaft	100	
Produktion	500	
Partnerrollen		
Lieferant	50	
Projektbezogenen Rollen		
Projektmanager	10	
Projektmitarbeiter Entwicklung neue Produktreihe	25	

Schritt 8: Nachweisen

Nachweisbarkeit der Rechtevergabe



10 Schritte im Überblick (Identity Management)

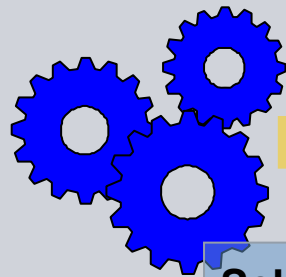
- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen ✓
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen ✓
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge ✓
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe ✓
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe ✓
- Schritt 7: **Verwenden** - Identity Management für die Benutzer ✓
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe ✓
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht 
- Schritt 10: **Verändern** - Rollenmodellierungsprozess

Schritt 9: Konstruieren - Rollenmodellierung aus Unternehmenssicht (Role Engineering)

Zusammenwirken von Role Finding und Role Mining im Role Engineering Prozess

Organisationsstruktur

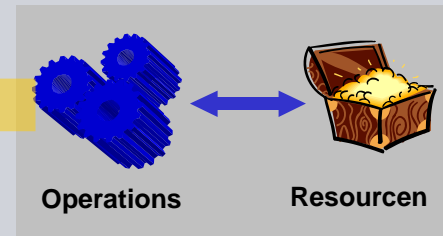
Zielsysteme



Schritt 9

Role Finding
(top down)

Role Mining
(bottom up)



Schritt 3

Policies, Prozesse
Tätigkeiten

Berechtigungsstruktur

Durch Zusammenwirken von Role Finding und Role Mining entsteht schrittweise ein unternehmensweites, systemübergreifendes Rollenmodell

Schritt 9: Konstruieren - Rollenmodellierung

Herausforderungen, Aufgaben, Vorteile

Herausforderungen

- Einführung eines Rollenbegriffs
- Voraussetzungen in der Organisation
- Prozessveränderungen (Verantwortlichkeiten)

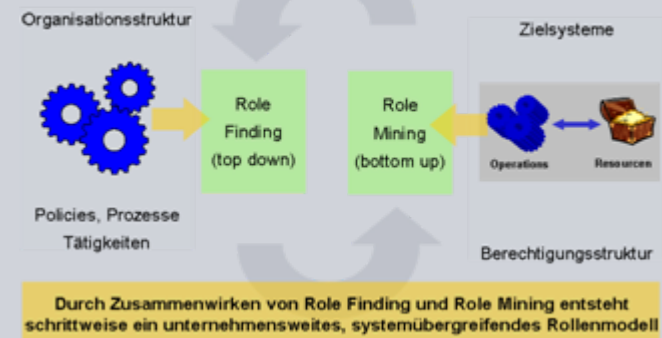
Aufgaben

- Einführung eines Rollenbegriffs für die Organisation
- Geschäftsprozessmodellierung
- Organisationsdaten bereitstellen (Organisation, Kostenstellen, Standorte, ...)

Nutzbare Vorteile

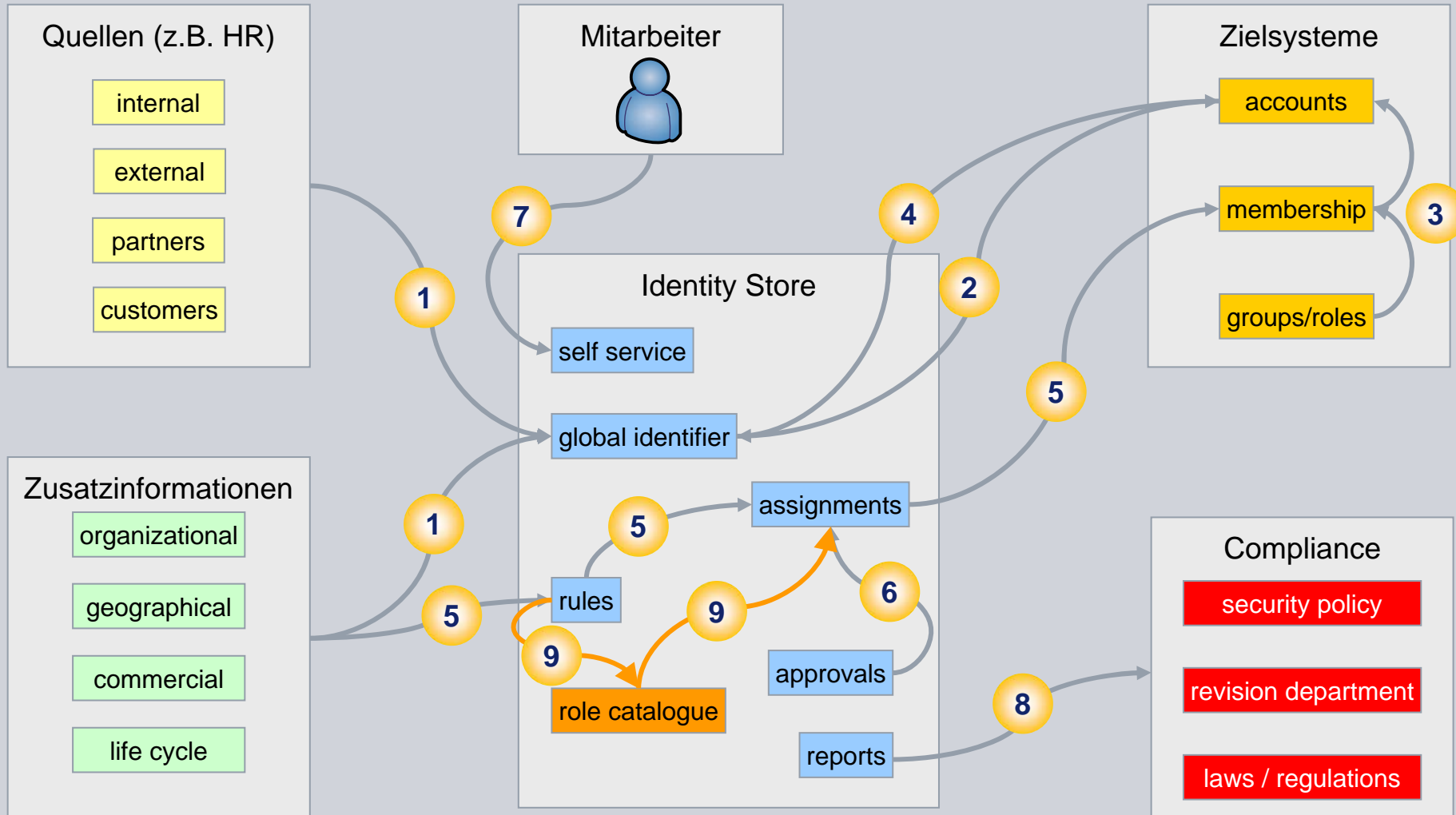
- Zuordnung von Berechtigungen auf fachlicher Ebene (Verständnis)
- Zusammenführung von Zuordnung und technischer Umsetzung
- Übertragung von Rechten (Vertretungen)
- Anzahl der Rechtezuweisungen sinkt

Zusammenwirken von Role Finding und Role Mining im Role Engineering Prozess



Schritt 9: Konstruieren

Rollenmodellierung aus Unternehmenssicht



10 Schritte im Überblick (Identity Management)

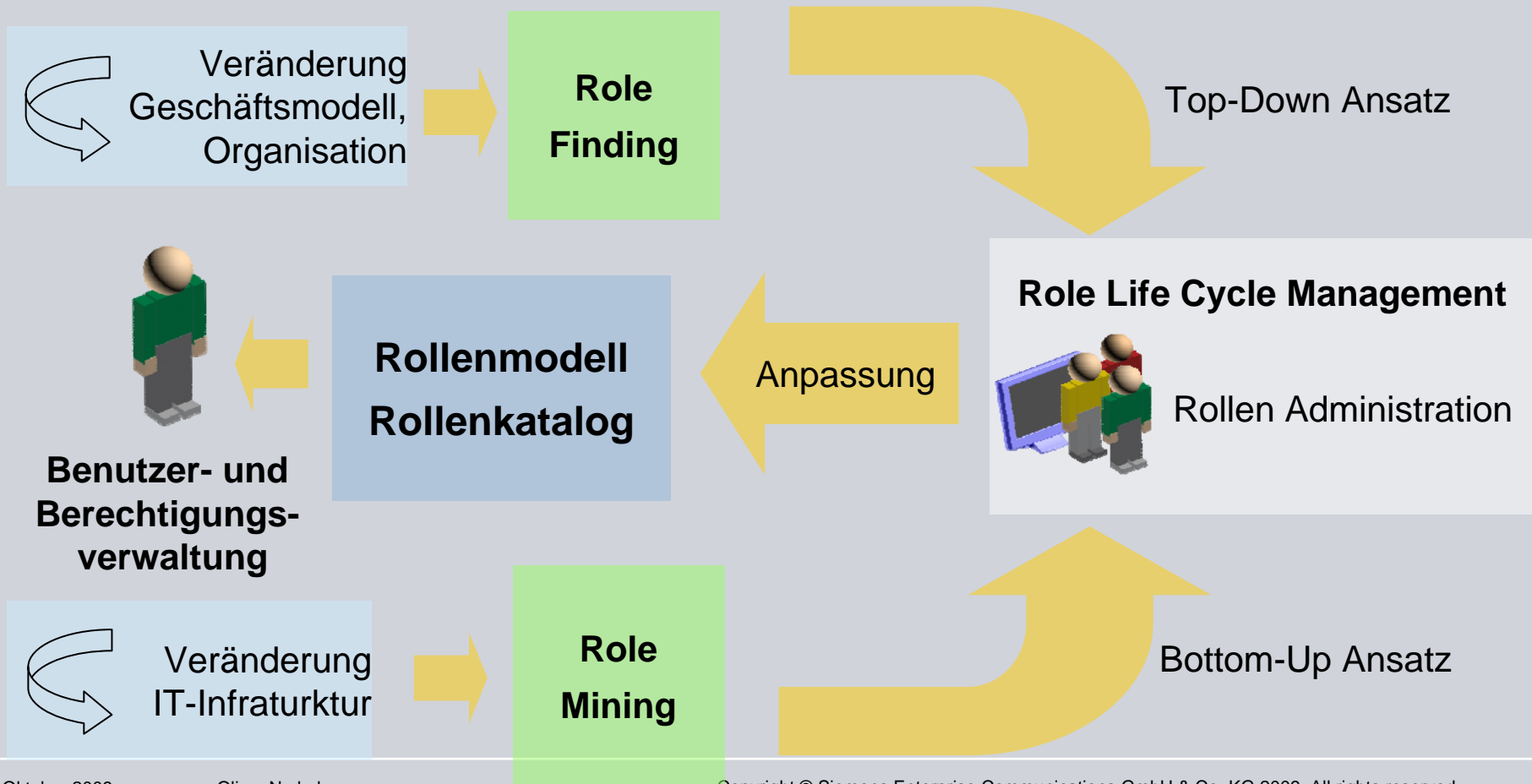
- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen ✓
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen ✓
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge ✓
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe ✓
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe ✓
- Schritt 7: **Verwenden** - Identity Management für die Benutzer ✓
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe ✓
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht ✓
- Schritt 10: **Verändern** - Rollenmodellierungsprozess



Schritt 10: **Change** – Rollenmodellierungsprozess

Aktualisierung des Rollenmodells

Durch die Veränderungen in der Organisationsstruktur, den Geschäftsprozessen und der IT-Infrastruktur ist auch das Rollenmodell einem kontinuierlichen Veränderungsprozess unterworfen.



Schritt 10: **Change** – Rollenmodellierungsprozess

Herausforderungen, Aufgaben, Vorteile

Herausforderungen

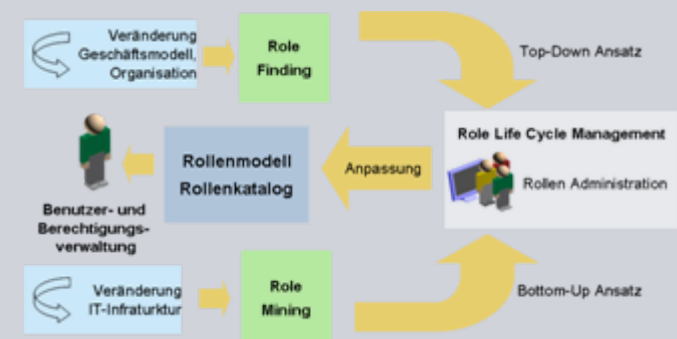
- Veränderungen in der Organisation
- Veränderungen in der Technik
- Lösungen entwickeln sich
- Simulation von Anpassungen
Testmöglichkeiten

Aufgaben

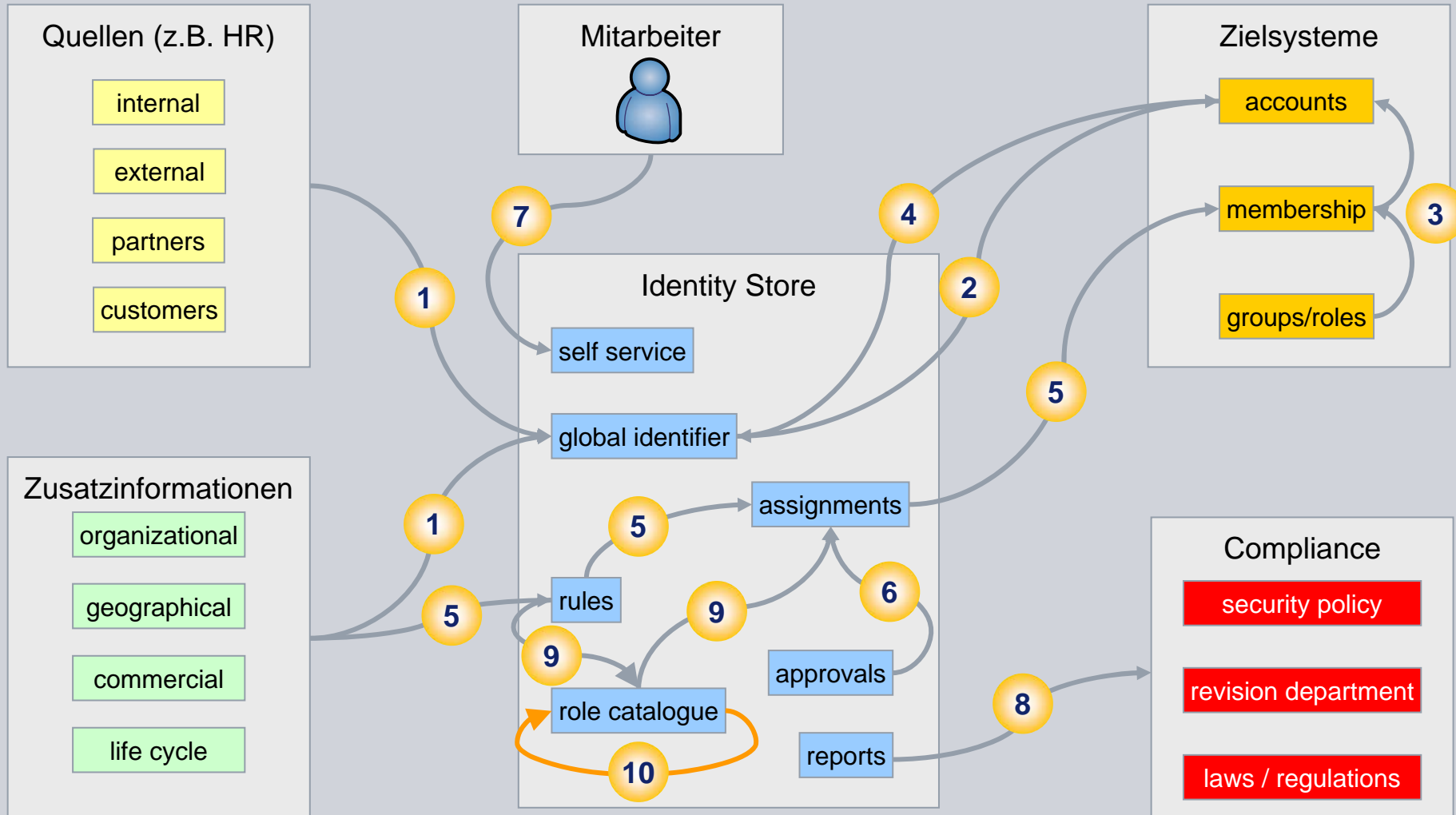
- Definition von Rollen für die Rollenmodellierung
- Erstellung von Testmodellen
- Änderungs- und Freigabeprozess implementieren

Nutzbare Vorteile

- Identity Management Lösung wird vervollständigt
- Änderungen auf Basis von Umstrukturierungen werden einfacher durchführbar



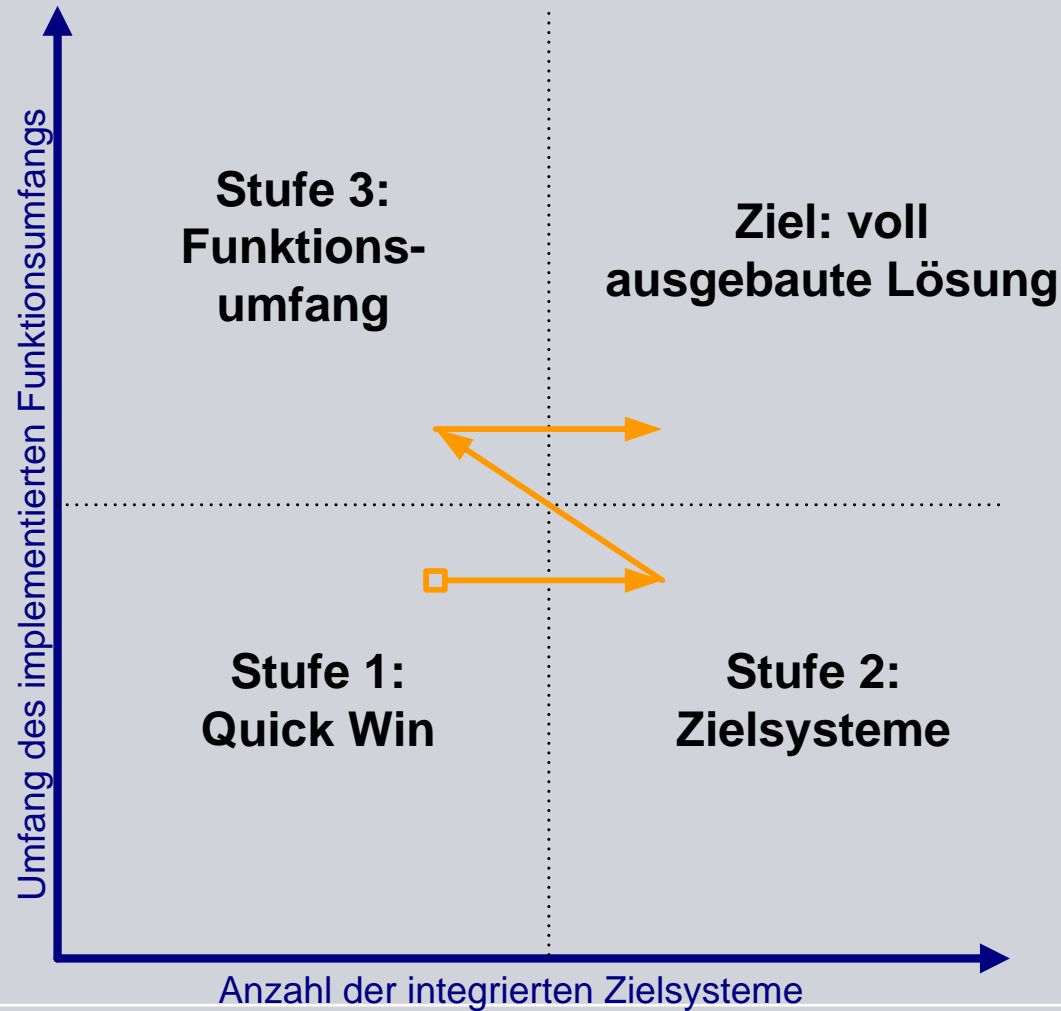
Schritt 10: Change Rollenmodellierungsprozess



10 Schritte im Überblick (Identity Management)

- Schritt 1: **Integrieren** - Integration von Identitäten ✓
- Schritt 2: **Überprüfen** - Integration von Zielsystemen ✓
- Schritt 3: **Analysieren** - Analyse der bestehenden Berechtigungsstrukturen ✓
- Schritt 4: **Automatisieren** - Steuerung der Berechtigungszugänge ✓
- Schritt 5: **Bereitstellen** - Regelbasierte Automatisierung der Rechtevergabe ✓
- Schritt 6: **Absichern** - Absicherung der Berechtigungsvergabe ✓
- Schritt 7: **Verwenden** - Identity Management für die Benutzer ✓
- Schritt 8: **Nachweisen** - Nachweisbarkeit der Berechtigungsvergabe ✓
- Schritt 9: **Konstruieren** - Rollenmodellierung aus Unternehmenssicht ✓
- Schritt 10: **Verändern** - Rollenmodellierungsprozess ✓

Der Stufenplan



Kernbotschaften

4 Punkte die Sie mitnehmen sollen

- Identity Management ist kein einmaliges Projekt sondern ständige Verbesserung
- Die richtige Planung entscheidet über den Erfolg bei der Umsetzung.
- Eine stufenweise Einführung sichert den Erfolg.
- Die Verbesserung bestehender Prozesse und die Erhöhung des Automatisierungsgrades beginnt schon mit der ersten Applikation.



Der Zweck eines Identity Management ist die Vielzahl der Kennungen und personenbezogenen Informationen welche die Anwender für den Zugriff auf Applikationen, Ressourcen und IT-Systeme benötigen, zu reduzieren und nach Möglichkeit in einer einzigen digitalen Identität zusammenzufassen.

<http://www.iam-wiki.org>

Siemens Enterprise Communications delivers the complete value chain for IAM



Identity Management

Management of complete user life cycle to provide efficient and secure user administration for heterogeneous IT infrastructures.

- (De-)Provisioning
- Approval and Validation
- User Self Service
- Certified SAP Integration

Access Management

Reliable protection for applications in the web environment through authentication, single sign-on and access control.

- Password Management
- Identity Federation
- Audit and Reporting

Role engineering

Bottom-up and/or top-down analysis of business processes, deduction of business and/or technical roles and their compliant implementation.

- Need-to-know and least-privilege
- Delegated Administration
- Regulatory Compliance

Professional Services

Profound consulting, integration and operations know-how based on numerous projects and deep knowledge of businesses and IT.

- Consult, Design, Build and Integrate
- Operate and Maintain
- Technical Project Management

Siemens provides an integrated product suite for Identity and Access Management

SIEMENS

Services



Products

DirX Identity

Comprehensive **Identity Management** for automated user and entitlement management



DirX Audit

Sustainable compliance through continuous **Identity Auditing** of user access and entitlements



DirX Directory

High-end **Directory Server** for enterprise and e-Business environments



DirX Access

Secure and reliable **Access Management** and **Federation** for Web and SOA environments

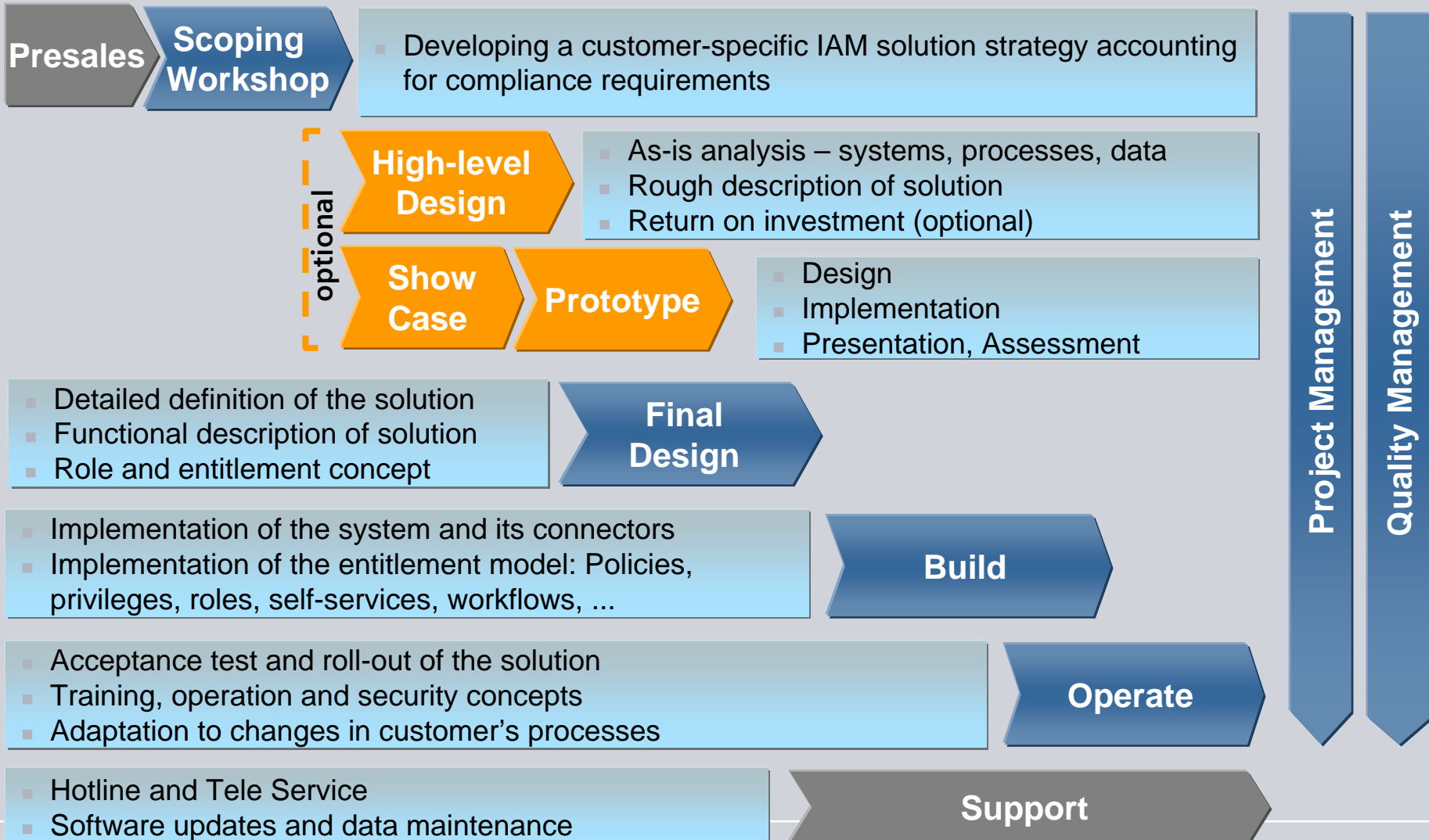


ID Center

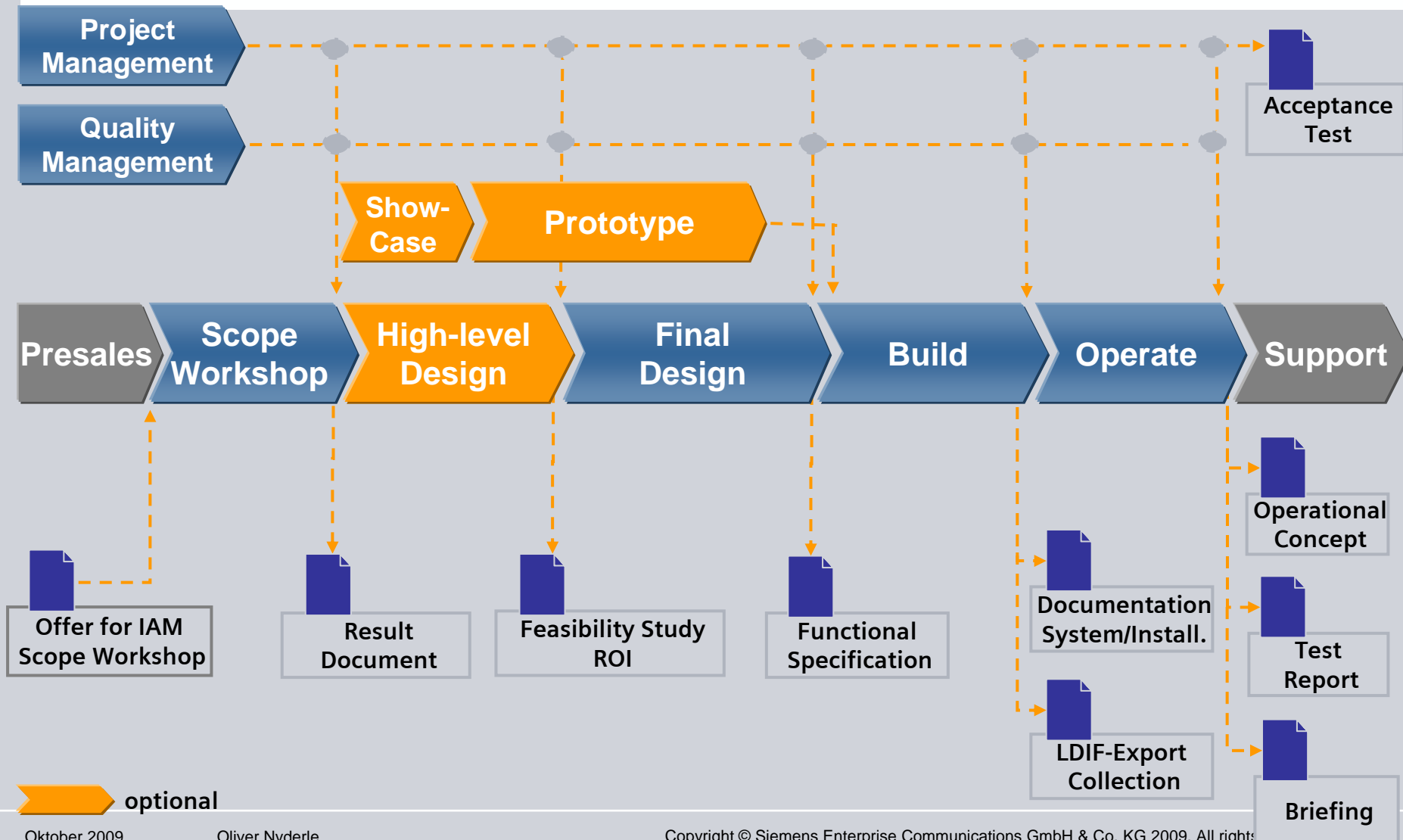
Biometric identification for secure and convenient authentication



Standard Process Model for Identity and Access Management Projects (1)



Standard Process Model for Identity and Access Management Projects (2)



Siemens Enterprise Communications GmbH & Co. KG

**Oliver Nyderle
SEN PSM SEC**

Danke!



Kontakt



Oliver Nyderle

Solution Line Manager
Identity & Privacy

Siemens Enterprise
Communications GmbH & Co

+49 (151) 1083 4640

oliver.nyderle@siemens-enterprise.com