IBM Software Partner Academy Program

Telefonkonferenz am 06.11.2009

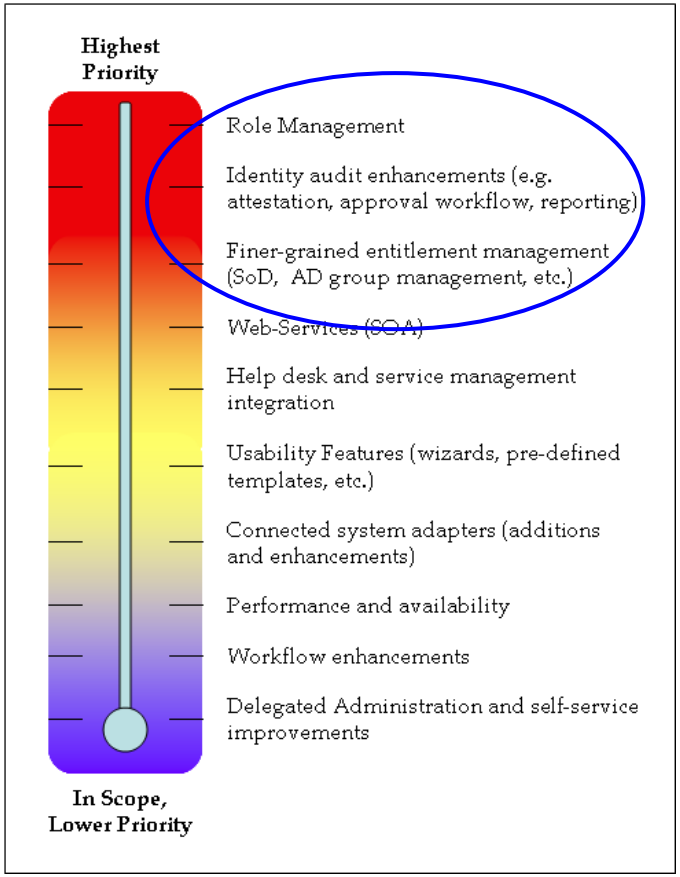
Identitätsmanagement inklusive Single Sign-On - Ein Quick Start Paket für den Mittelstand

Walter Karl
GER SWG Channel Technical Sales (SWIT)

Zahlen zu Identity Management

Marktpotential

Aktuelle Situation im Bereich Identity Provisionierung



Source: Provisioning Market 2009 (Burton Group)

2009 Identity and Access Management Market Opportunity

Category	Sub-Category	Market Data ($M) Market Size	CAGR
User Provisioning		$ 737	13%
Single Sign-On	Web SSO	$ 1,298	16%
	Enterprise SSO	$ 442	6%
Legacy Authorization		$ 289	-2%
Authentication	Advanced Authentication	$ 592	7%
	Traditional Tokens	$ 455	2%
Identity Governance	Role Management & Access Certification	$ 90	40%
	Entitlement Management	$ 140	19%
	Privileged Identity Management	$ 70	46%
	Separation of Duties	$ 300	29%
		$ 4,413	**13%**

Source: 2008 GMV, Forrester & IBM Internal Estimates

Was ist Identity Management?

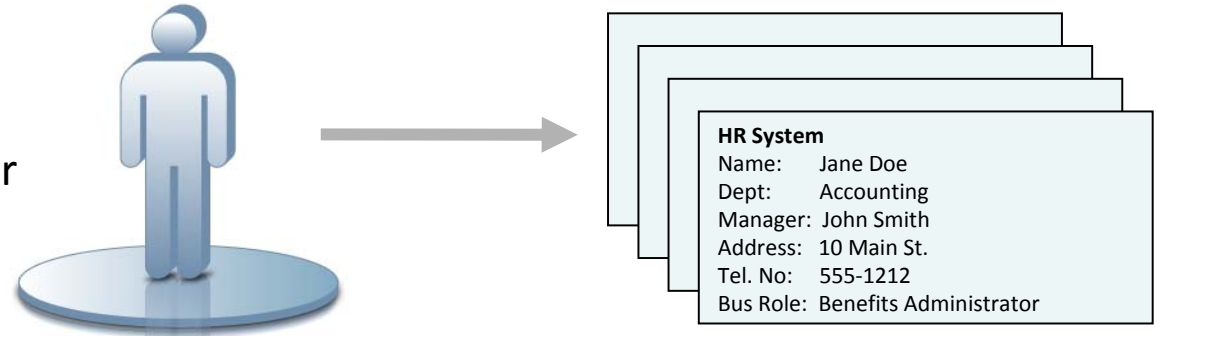
Das '1x1' von Identity Management (IdM)

Management von
WER hat ZUGRIFF auf WAS

People	Policy	Resources

Das WER im Identity Management

- Benutzer benötigt Zugriff auf eine Resource.
- Benutzertyp kann intern als auch extern sein.
  - Angestellte
  - Kunden
  - Business Partner
  - etc



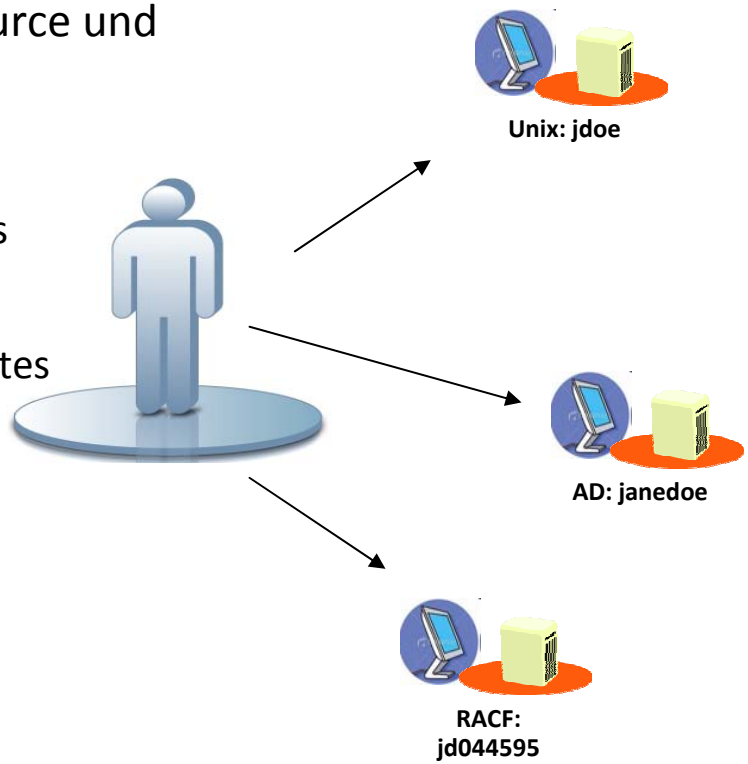
- Jeder Benutzer besitzt eine *Identität* und dazugehörige *Attribute* (-> Rolle).
  - Zugriff auf Resource
  - Berechtigung
- Benutzer unterliegt einem Life-Cycle. Dieser bestimmt ...
  - Zugriff auf Resource
  - Änderungen von Zugriff und Resource
  - Löschen des Zugriffs

Das WAS im Identity Management

- Das WAS ist das Benutzerkonto zu einer IT-Resource und bestimmt die Zugriffsart

  Wie z.B.:

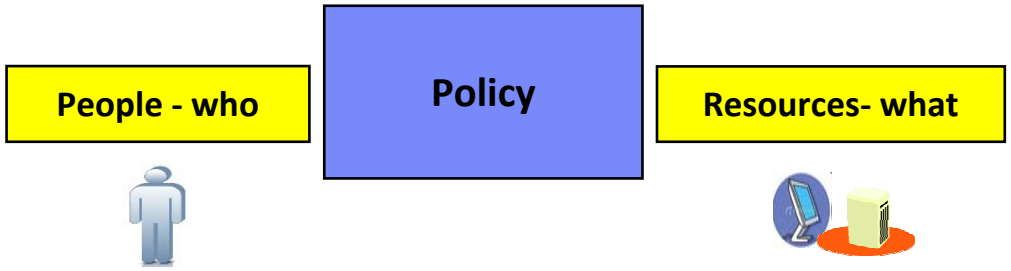
Betriebsysteme	Unix, Windows
Datenbanken	DB2, Oracle
Applikationen	SAP, Lotus Notes
Directories	Active Directory, Ldap



- Attribute des Benutzerkontos
  - Userid
  - Password
  - Gruppe/Rolle
  - etc

Jane's account identity can be different for each of the systems she has access to. It is important to be able to map the account identity back to the owner

Wie wird die Zugriffsart vergeben ...



- Richtinien (Policies) bestimmen *Wer* hat Zugriff auf eine *Resource*.
  - Mitgliedschaft (Rolle)
  - Entitlement
- Workflow und Approvals definieren den Prozess – die richtigen Leute bekommen die richtigen Berechtigungen
- Richtlinien (Policies) – Mitgliedschaft wird durch Rollen definiert
  - Business Role (Job, Verantwortlichkeit, etc)
  - Application Role (Entitlement=IT-Resource+Berechtigungen)

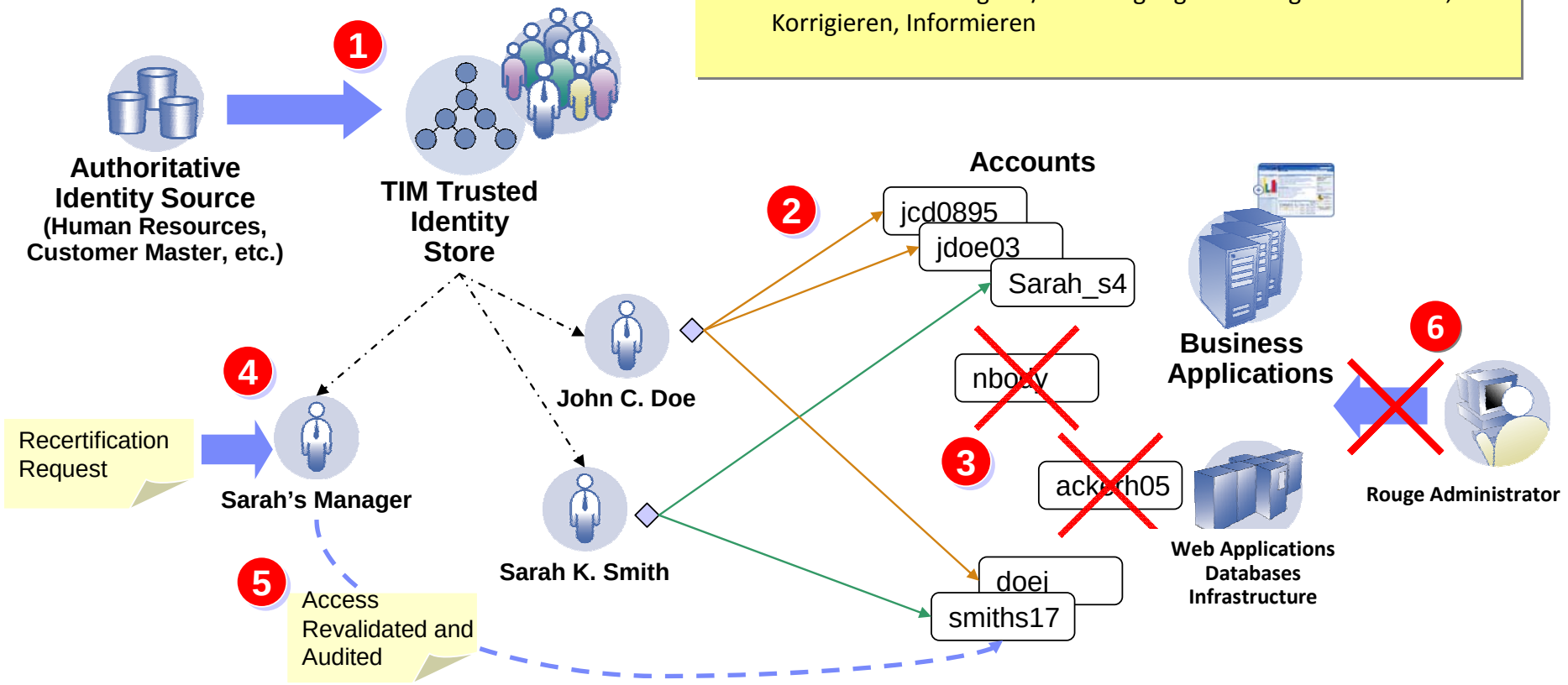
Herausforderungen an Identity Management

IdM - Verbesserung von Sicherheit & Compliance

Mehr als 30% der Benutzerkonten sind verwaist

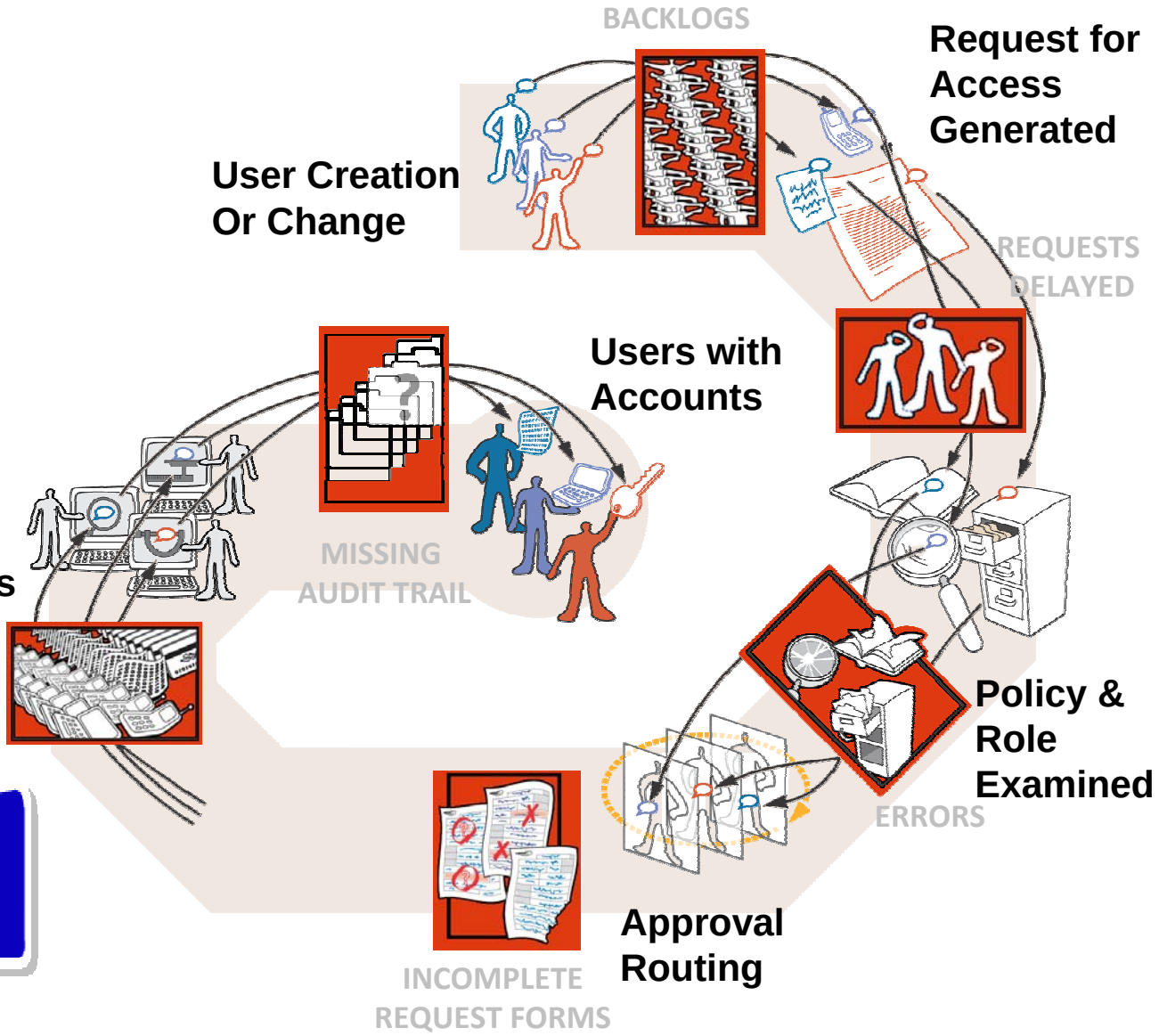
Gartner Group

1. Kenntnis über Benutzer, Geschäftszusammenhang verstehen
2. Wem gehört welcher Account
3. Sperren/Löschen von verwaisten Accounts (Orphants)
4. Überprüfung und Bestätigung von Berechtigungen
5. Korrigieren von Zugriffen/Berechtigungen
6. Unauthorisierte Zugriffs/Berechtigungsänderungen: Erkennen, Korrigieren, Informieren



Manuelle Approvals & Provisionierung

- Zu langsam
- Zu unflexibel
- Fehleranfällig
- Schnell überfordert



Manuelle Provisionierung bedeutet im Schnitt 12 Tage Wartezeit

Gartner Group

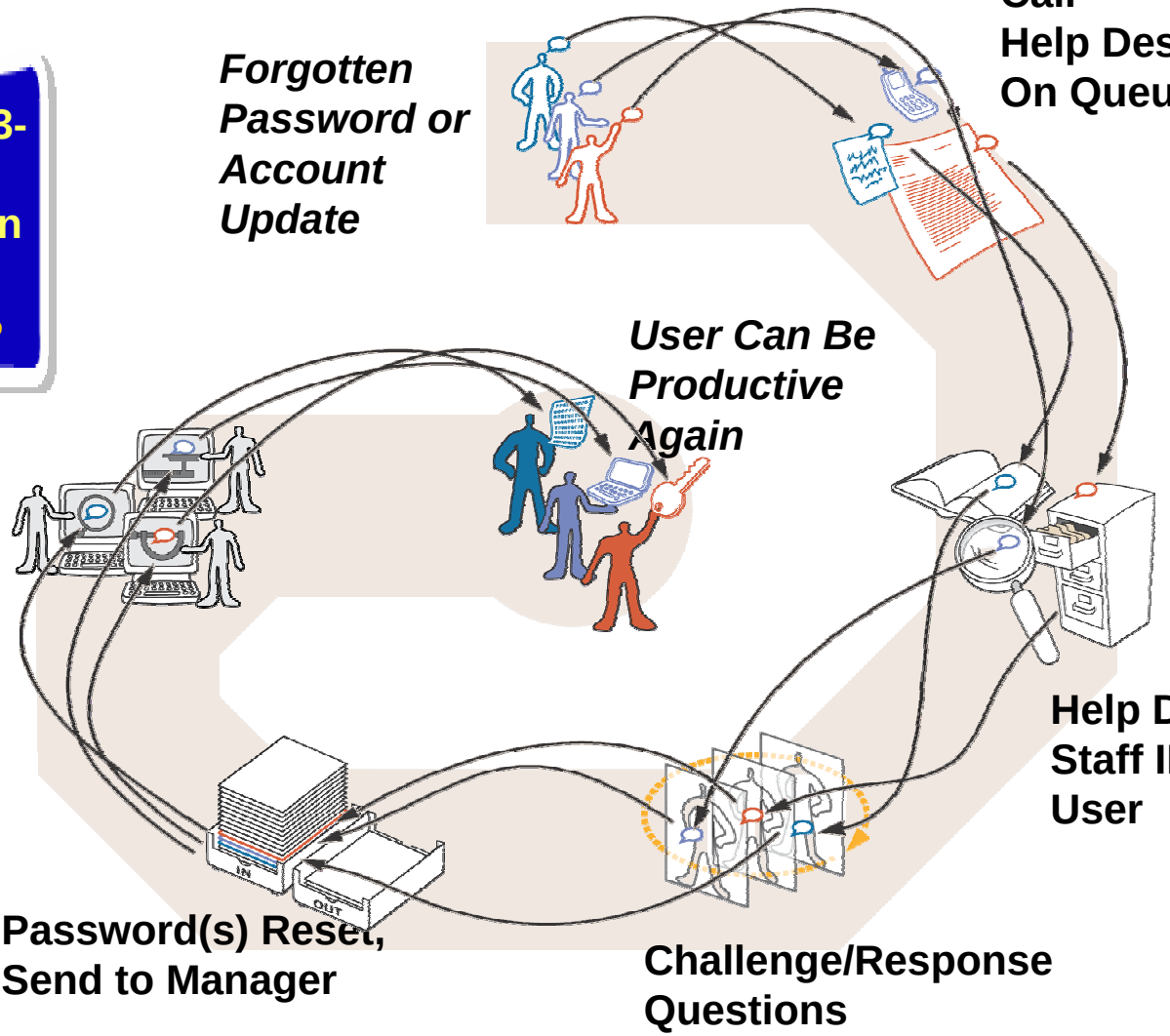
Viele Benutzerkonten, Viele Help Desk Calls

Benutzer ruft im Schnitt 3-4/Jahr den Help Desk wegen Passwort Reset an

IDC/MetaGroup

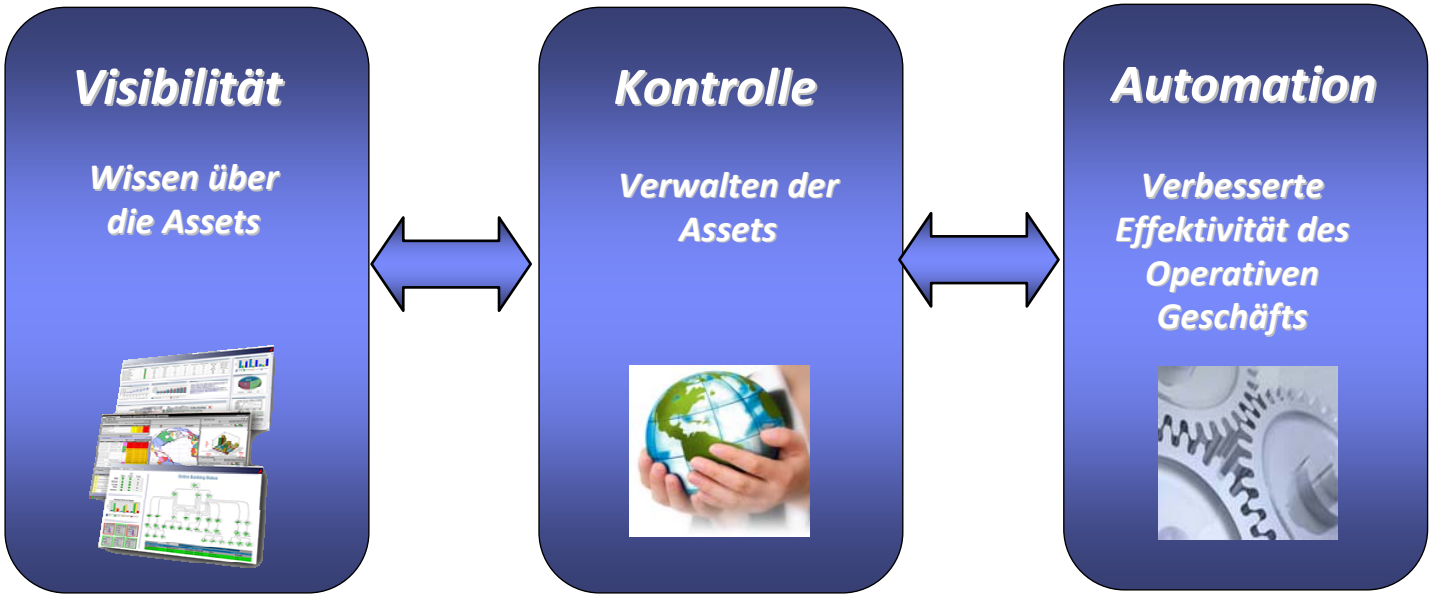
Kosten/Call sind €20,- bis €45,-

IDC/MetaGroup

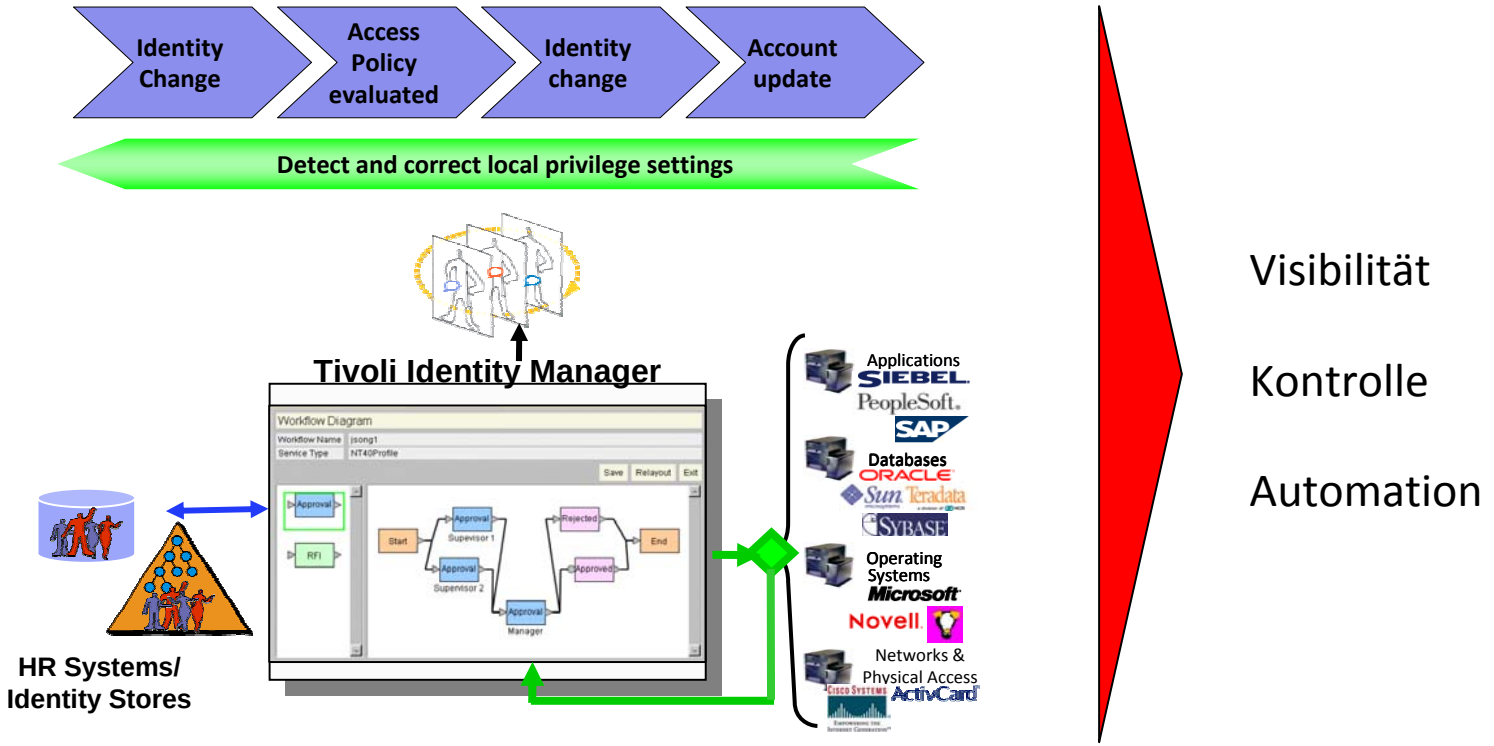


IBM Tivoli Identity Manager

Identity Management & Single Sign-On als Service

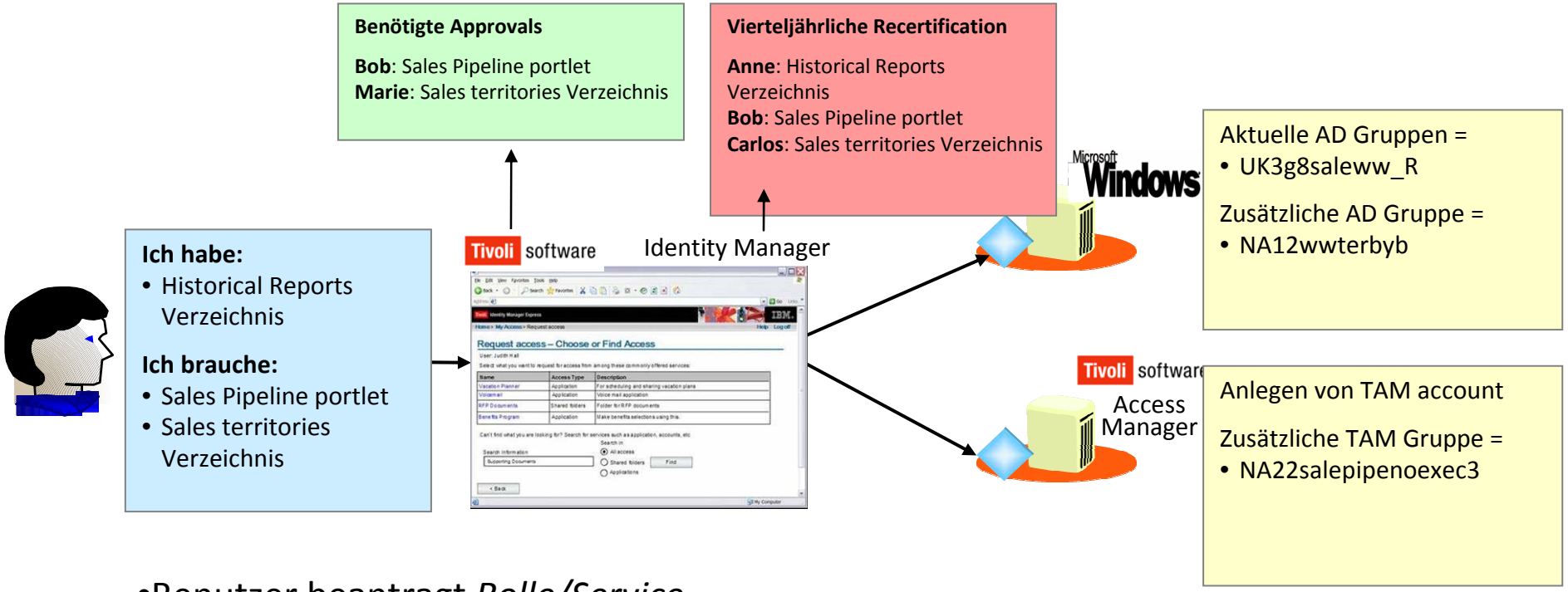


Tivoli Identity Manager – unternehmensweites Live-Cycle Management



- Kenntnis von *Wer, Wo, Warum*
- Einhalten von *Compliance*, Berichtigen von *Non-Compliance*
- Automation von Benutzerberechtigungen unternehmensweit

Self-Service, Life-Cycle, Compliance

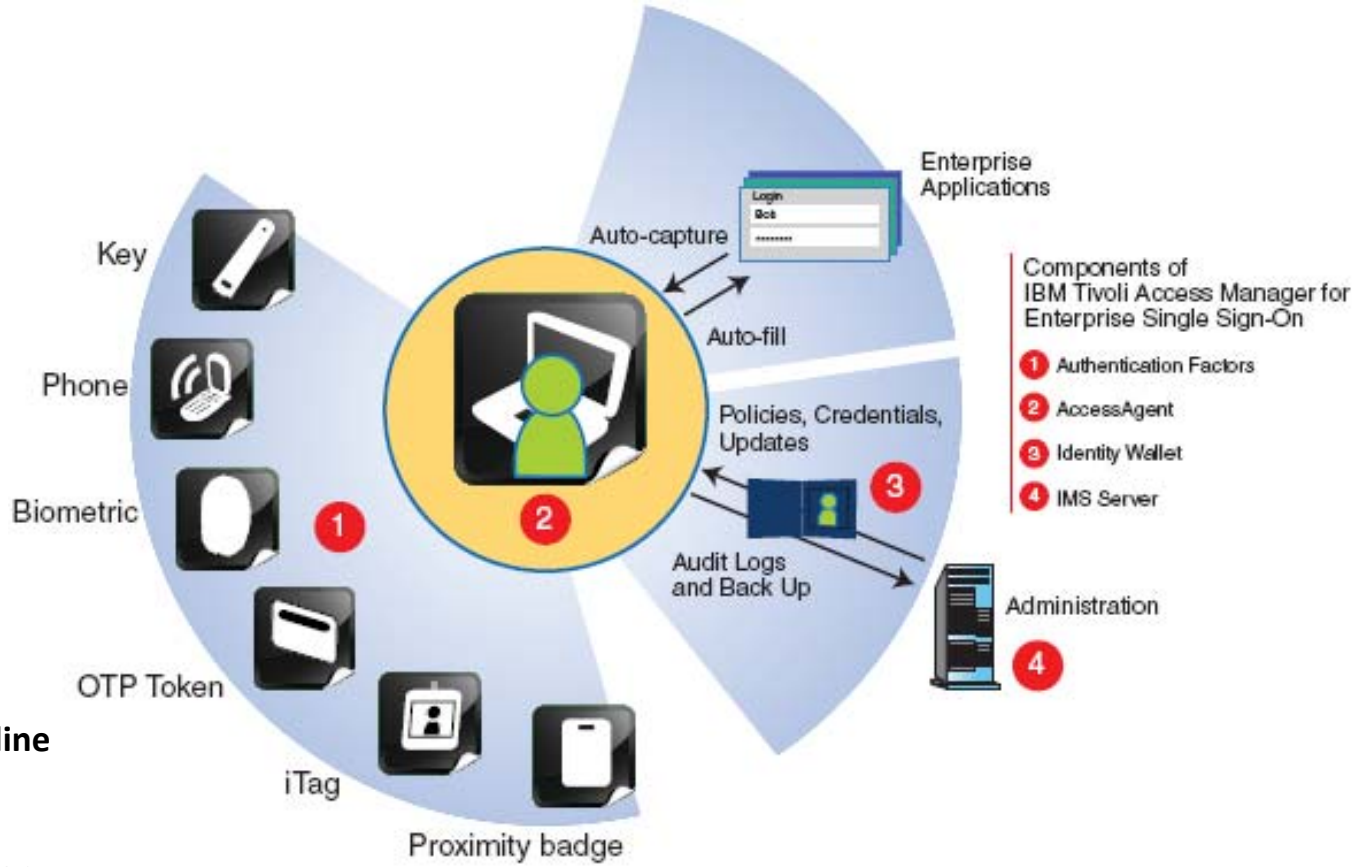


- Benutzer beantragt *Rolle/Service*
- *Automatische* und *kontrolierte* Provisionierung
- Approvals und Rezertifizierung gewährleistet *Compliance*
- *Aussagekräftige Berichte* über IdM

IBM Tivoli Access Manager for Enterprise Single Sign-On

ITAM-ESSO Übersicht

- **Single-Sign-On**
- **Kiosk-Modus**
- **Zwei-Faktor-Authentisierung**
- **Zentrales Management**
- **Passwortreset online und offline**
- **Auditing**
- **Keine Änderungen im zentralen Verzeichnis erforderlich (z.B. Schemaerweiterung)**



ITAM-ESSO Applikationen

- **TAM E-SSO unterstützt viele Webapplikationen mit Hilfe der "web auto-learn" Möglichkeit, gleichzeitig werden die folgenden vorkonfigurierten SSO Templates mitgeliefert:**
  - Windows Logon, Meditech, AOL Instant Messenger, Cisco VPN, Eudora, Windows Explorer, GoldMine, iPass, Intellisync, MSN Messenger, Lotus Notes, Outlook, Outlook Express, PuTTY, Windows RDP Client, Reflection, SecureCRT, Skype, VNC Client, Yahoo Messenger, Novell Logon, Citrix ICA Client
- **Automatisierung von Kennwortwechsel, Logon und Logoff bei den folgenden Applikationstypen:**
  - Web interface (Webformular, Pop-Up Sign-On, Dropdown Listen, Radio Buttons, Pop-Up Dialoge, Checkboxen)
  - MS Windows Fensterdialoge
  - Java-Anwendungen
  - Mainframe und Host mit Emulatoren (EHLLAPI – 3270, 5250, telnet)

ITAM-ESSO – System-Logon, VPN, Terminal-Emulation

- **Das TAM E-SSO Logon kann mit den folgenden System Logon Verfahren kombiniert werden:**
  - Windows Log On, Windows 2000/XP/Server 2003, Active Directory Login, NT Domain, Novell Client, Kerberos/NTLM

- **TAM E-SSO unterstützt SSO bei folgenden Dialup, Networking und VPN Lösungen:**
  - Cisco, Checkpoint, Nortel, Microsoft VPN, Microsoft Dial-Up Networking, iPass, GRIC, Fibrelink, Citrix Nfuse

- **TAM E-SSO bietet SSO zum Host (TTY) und Mainframe Anwendungen mit folgenden Methoden:**
  - Vorkonfiguriert für kommerzielle und kundenspezifische Terminalemulatoren wie Putty, Secure CRT, Reflections, Rhumba, etc.
  - Direkte Unterstützung für kommerzielle Mainframeanwendungen wie Care Manager und Meditech
  - Unterstützung für mehrfache Logon und Passwortdialoge

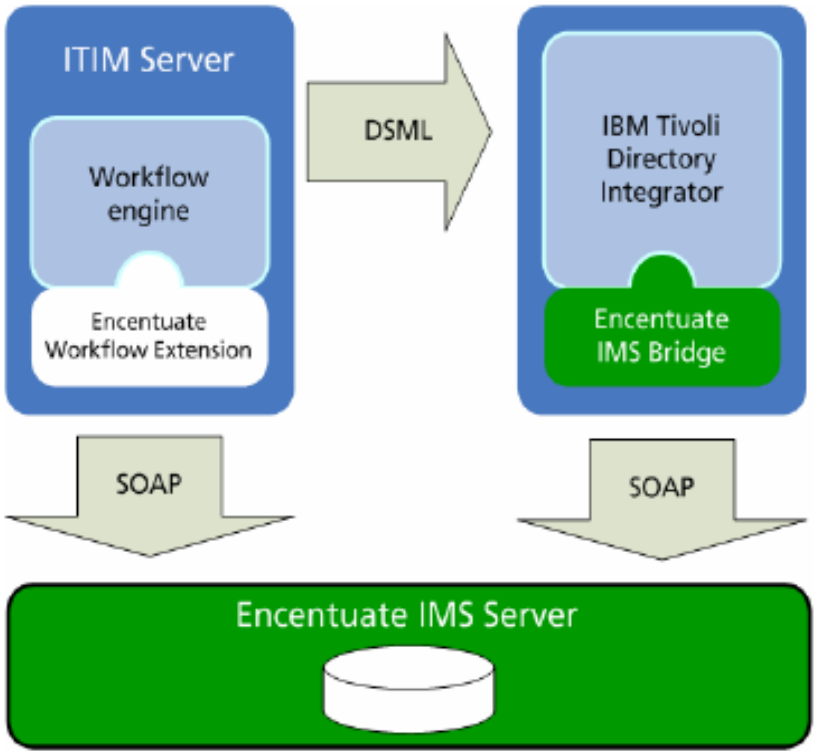
2nd-Factors für höhere Sicherhei

- Smart Cards
- RFID
- USB Token
- Biometric Devices
- One Time Password

Gesamtlösung IdM und SSO

Integration ITIM & ITAM-ESSO

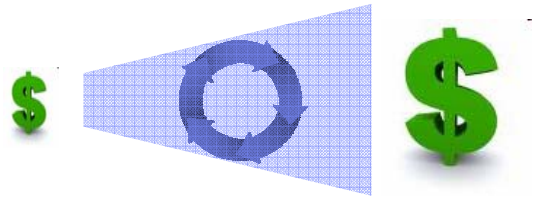
- Benutzer beantragt Rolle/Zugang
- ITIM provisioniert automatisch, kontrolliert
  - Zugang und Berechtigungen für Zielsystem
  - Zugangsdaten Zielsystem zu ITAM-ESSO
- ITAM-ESSO setzt automatisch (optional) beim Erst-Login neues Passwort

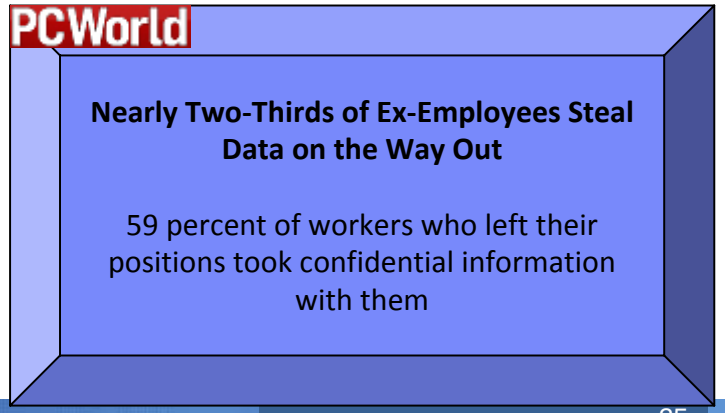


Ergo sum

Was uns treibt ...

- Compliance
  - Audits
  - Regularien
  - Standards
- Kostenersparnisse
  - Automation
  - Self-Service
- Sicherheit
  - Kontrolle
  - Berichte





25

Implementation

ITIM Quickstart

- Mindestanzahl Benutzer: 250
- Service-Leistung: 20MT
  - Kick-Off meeting, Feinkonzept
  - Aufbau Pilot (Anzahlbegrenzung für Zielsysteme, Workflows, Policies)
  - Dokumentation, Schulung, Projektkoordination
- Kosten Lizenz/Service ca. €65000,-

Übersicht ITAM-ESSO Projekt

Test	Deployment and Configuration Planning	Phase 1 rollout	Full Rolluot
▪Softwareinstallation in Testumgebung ▪Einbindung von 5-20 Usern und Computern	▪Koordination der beteiligten Abteilungen wie: Desktop-Verantwortliche Softwareverteilung Application owner ▪Einbindung weiterer Applikationen	▪Schulung des Helpdesk ▪Automatische Softwareverteilung in Pilotumgebung ▪Auswertung Pilotgruppe	▪Automatische Softwareverteilung in Gesamtumge-bung ▪Je nach Strategie entweder mehr Anwender oder weitere Applikationen einbinden

Dienstleistung: ca. 10-20 Servicetage

Kontaktdaten:

Karl Walter
GER SWG Channel Technical Sales (SWIT)
Tel: +49 170 578 2213
Email: wkarl@de.ibm.com

Vielen Dank für Ihre Aufmerksamkeit!