



# SUN IDENTITY MANAGEMENT

Ausgewählte Kunden und  
Anwendungsbeispiele

**Hans Wieser**

Product Marketing Manager

Sun Microsystems

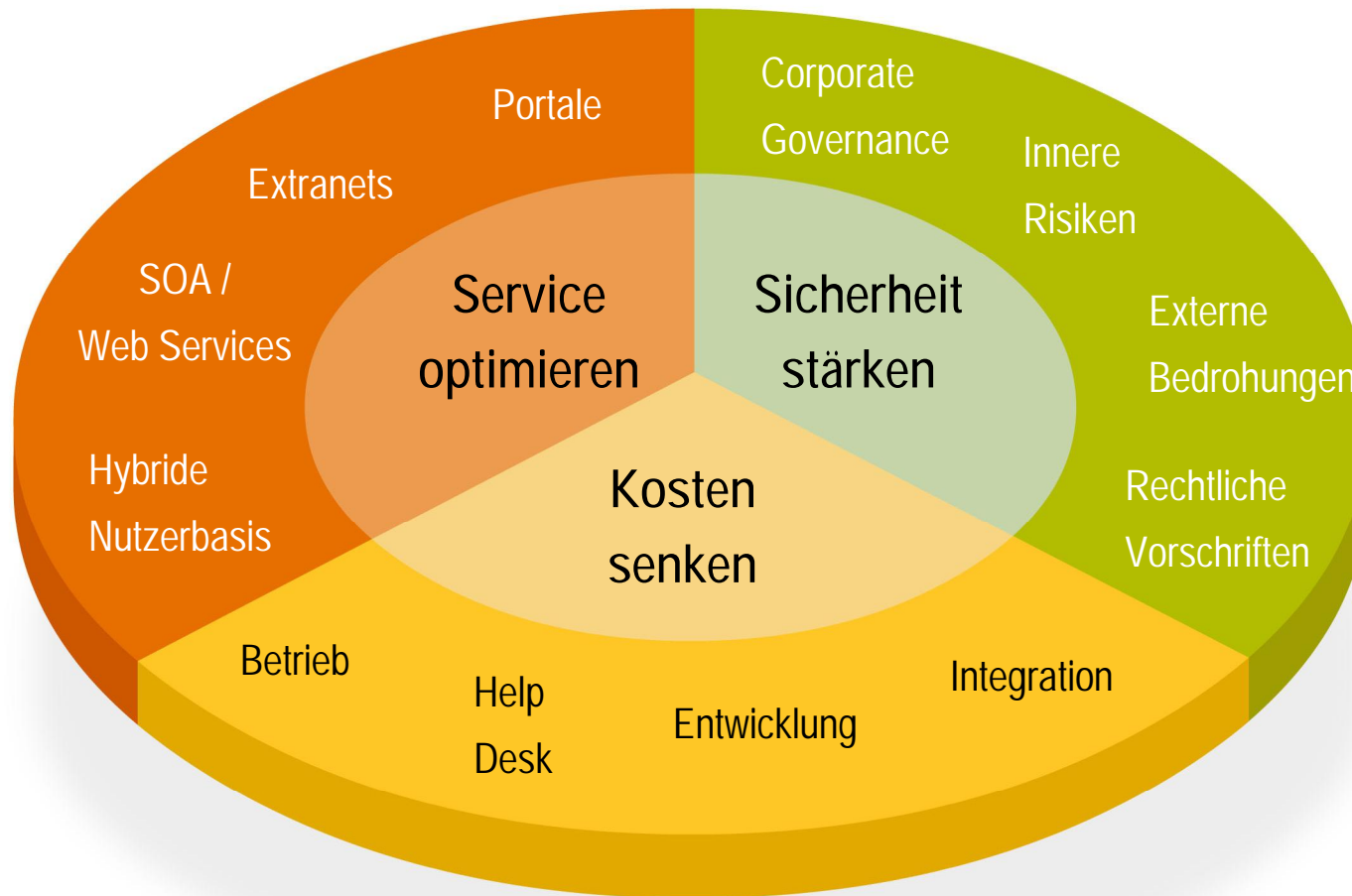


# Agenda

- Identity Management Taxonomie
- Kundenbeispiele
- Use Cases
- Fazit & Empfehlung

# Fachliche Anforderungen

Identity Management Lösungen adressieren konkurrierende Ziele



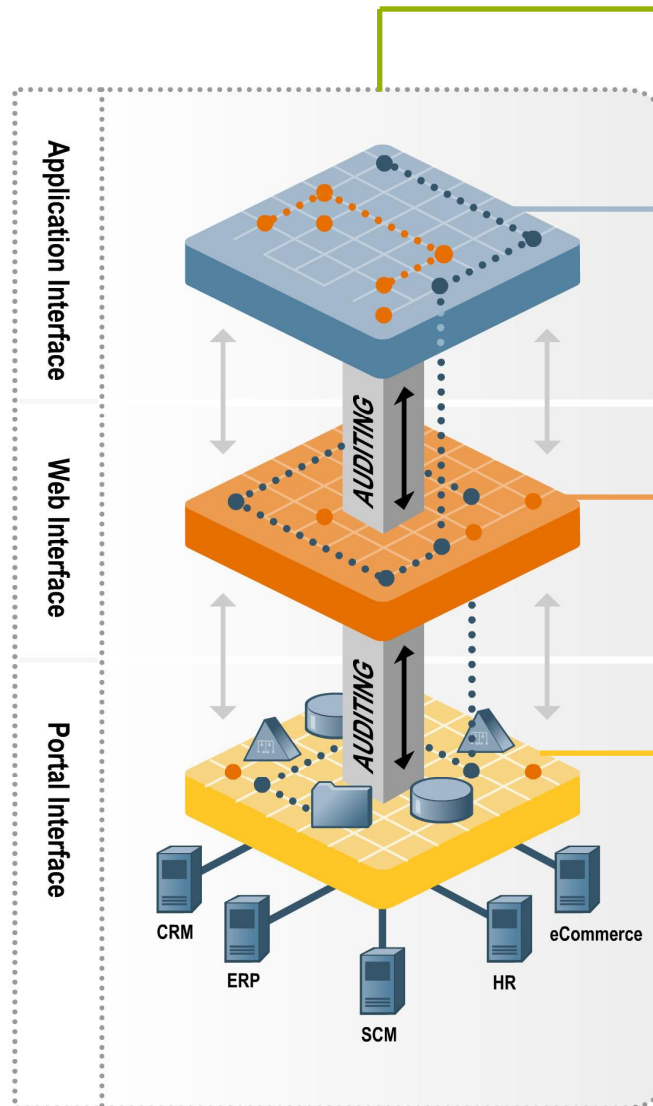
# Identity Grid

  
IT Administratoren

  
Mitarbeiter

  
Partner

  
Kunden



## Audit Dienste

- Richtlinien forcieren
- Konformität dokumentieren
- Abweichungen korrigieren
- Verknüpfungen prüfen

## Administrationsdienste

- Konten bereit stellen
- Kennwörter verwalten
- Nutzer verwalten
- Profile synchronisieren
- Richtlinien verwalten
- Verknüpfte Konten bereit stellen

## Transaktionsdienste

- Daten sicher transportieren
- Nutzer anmelden
- Nutzer sutorisieren
- Extranet Single Sign-On
- Konten verknüpfen

## Datenspeicher

- Verzeichnisse
- Datenbanken
- Dateien

# Sun Identity Management

**Innovativ. Integriert. Integrierbar.**

Wertschöpfungskette



**Federation Manager**



**Identity Manager SPE**



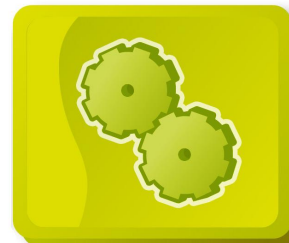
**OpenSSO**



**Directory Server  
Enterprise Edition**



**Access Manager**



**Identity Auditor**



**Identity Manager**

Unternehmen

Alle Module zur Verwaltung von Nutzern im Unternehmen und der Wertschöpfungskette — vollständig integrierbar in dynamische, heterogene IT Umgebungen.

**Mehr als 100 Millionen verwaltete Identitäten**

# General Electric



- **Anforderungen**
  - > Identitäten für 450.000 Nutzer in 11 Geschäftsbereichen sicher verwalten
- **Lösung: Sun Identity Manager**
  - > Automatische sichere Aktivierung und Deaktivierung von Nutzerkonten nach Rolle, Region und Aufgabenbereich
  - > Einhaltung rechtlicher Auflagen durch leichtere Audits
  - > Zentrale Verwaltung globaler Nutzerkonten und Zugriffsrechte

- **Nutzen**
  - > Höhere Sicherheit bei leichteren Audits
  - > Neue Mitarbeiter sind schneller produktiv
  - > Operative und Helpdesk-Kosten gesenkt\*

\*ROI rechnet sich bereits durch die effizientere Verwaltung nichtdigitaler Geräte wie Tankkarten, Kreditkarten, Telefone etc.

# Merrill Lynch

- **Anforderungen**
  - > Große, heterogene Nutzerbasis mit einheitlichem Single Sign-On
  - > Effizientere Bereitstellung von Diensten
  - > Erfüllung wachsender Anforderungen von Sicherheit und Regulierungen
- > **Lösung:** Sun Identity Manager
  - > Standardbasierte Architektur
  - > Konsistentes Branding über Partnersites
  - > Verwaltung von Millionen Identitäten
  - > Flexible Plattform für interne und externe Projekte



- **Nutzen**
  - > Identity Management als Bestandteil des ML Portals sichert Service für direkte und Partnerkunden
  - > Flexible, offene Lösung ermöglicht Erweiterungen und neue Geschäftsansätze
  - > Sicherheit stärkt Kundenvertrauen und senkt Haftungsrisiken

# ADP/ProBusiness\*



- **Anforderungen**

- > Erfüllung von Auflagen durch Sarbanes-Oxley
- > Supportkosten senken, HelpDesk Personal anderweitig einsetzen
- > Schnelle Aktivierung / Deaktivierung von Mitarbeitern
- > Datenqualität verbessern

- **Lösung:** Sun Identity Manager

- > Einheitlicher Prozess für Nutzung, Transport, Weitergabe und Verwaltung von Identitätsdaten in und zwischen Organisationen und Anwendungen

- **Nutzen**

- Reduziertes Risiko, leichtere Revisionsicherheit im Sinne von Sarbanes-Oxley
- Höhere Sicherheit durch transparente Nutzeridentität
- Geringere Kosten durch effizientere Automatisierung

\*Einer der weltweit größten HR-Outsourcer, mit mehr als 550000 Kunden weltweit, ca. 16% Marktanteil in den USA, etwa wie die deutsche Datev

# Burlington Northern and Santa Fe Railway\*

- **Anforderungen**
  - > Schnellere Nutzerregistrierung bei besserer Sicherheit. Die Ziele beinhalteten:
    - > Schnellere Antwortzeiten
    - > Geringere Kosten
    - > Höhere Produktivität
- **Lösung: Sun Identity Manager**
  - > Automatische Nutzerverwaltung
  - > Heterogene Umgebung kein Problem
  - > Microsoft interoperabel

\*Eine der größten US-Bahngesellschaften, mit mehr als 300 Niederlassungen in 28 Bundesstaaten und 2 kanadischen Provinzen



- **Nutzen**
  - > Identität und Zugriffsrechte für Nutzer in Hunderten von Orten in Nordamerika verwalten
  - > Die erste Phase des Roll-Outs (40.000 Nutzer) konnte in 45 Tagen abgeschlossen werden.
  - > Mehr als 100.000 Nutzerkonten mit einer Vielzahl von Anwendungen und Ressourcen

# Pepsico

- **Anforderungen**
  - > Ablösung der halbautomatischen Eigenentwicklung für Workflow/Provisioning
  - > Befüllen des neuen Verzeichnisses mit HR, AD und Lieferantendaten
- **Lösung:** Sun Identity Manager/Directory Server
  - > Virtuelle Identität
  - > Kennwortsynchronisierung
  - > Kennwortwechsel
  - > Führende Systeme



- **Nutzen**
  - > Zentrales führendes System für Nutzerinformationen
  - > Weniger Helpdesk-Anfragen
  - > SOX Konformität
  - > Mehr als 100.000 Nutzerkonten mit Zugriff auf viele verschiedene Ressourcen

# T-Mobile\*

- **Anforderungen**
  - > Sicherer Zugang zu Multimediadiensten für Kunden über t-zones (T-Mobile Portal)
- **Lösung:** Sun Identity Manager/Directory Server
  - > Inhalte von T-Mobile für ca. 20 Millionen Kunden
  - > Mehr als 10 Millionen Kundendateien und 1000 Lieferantendefinitionen



- **Nutzen**
  - > Bessere Nutzererfahrung und reduzierte Kosten
  - > Schnellere Bereitstellung neuer Dienste mit zusätzlichem Umsatzpotenzial
- Einfachere Skalierung

# Wells Fargo

- **Anforderungen**

- > Kundenerfahrung verbessern
- > Schnell wachsende Kundenbasis bedienen
- > Maximale Sicherheit bei Verbindung von Inhalten aus Intranet und Extranet

- **Lösung:** Sun Access Manager

- > Single Sign-On und Verknüpfung
- > Entscheidend für Sun war die maßgebliche Position in Definition und Entwicklung von Industriestandards



- **Nutzen**

- Kundenzufriedenheit als Wettbewerbsfaktor
- Lösung erlaubt extrem große und wachsende Nutzerpopulation
- Effektives Sicherheitsmodell für Identitätsverknüpfung
- Standardlösung erlaubt beschleunigtes Roll-Out von Partnerschaften

# Henkel

- **Anforderungen**

- > Ablösung einer hostbasierten Nutzeradministration
- > Unterstützung für 50.000 Nutzer weltweit
- > Kennwort-Selbstverwaltung, Audit, dezentralisierte Administration

- **Lösung:** Sun Identity Manager

- > Nutzung von Standards erlaubt Einsatz in Fremdunggebung
- > Delegierte Administration und flexible Web-Formulare ermöglichen optimale Anpassung an Kundenbedarf



- **Nutzen**

- > Schnellere und sicherere Administration
- > Einfache Bedienung (web)
- > Transparente Forcierung der Sicherheitsrichtlinien
- > Senkung der Helpdesk-Kosten
- > Zukunftssichere Softwarearchitektur

# Automobilzulieferer

- **Anforderungen**

- > Durchsetzung der konzernweiten Sicherheitsrichtlinien
- > Zentrale Administration für 200.000 Mitarbeiter weltweit
- > Verwaltung von SAP Enterprise Portal und NetWeaver Anwendungen

- **Lösung:** Sun Identity Manager

- > Zentrale Verwaltung für alle Anwendungen
- > Active Directory Administration ermöglicht Abschalten der lokalen Admins

- **Nutzen**

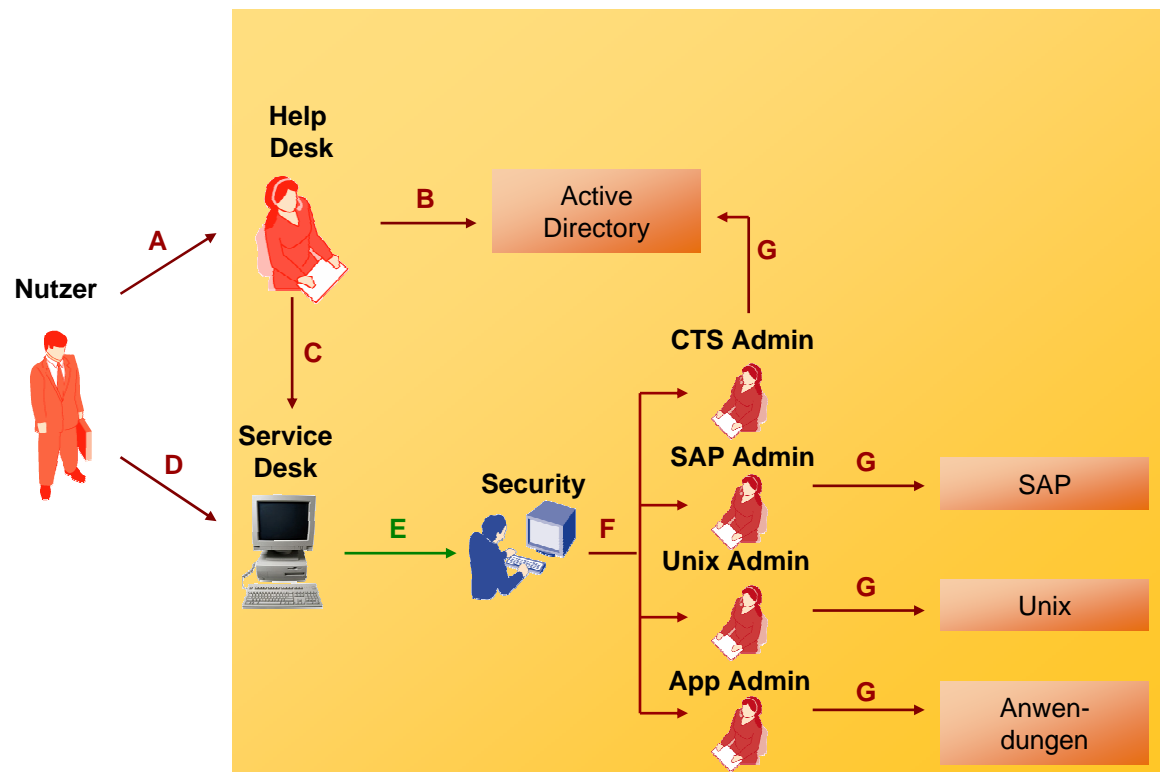
- > Sicherheit forciert und zentral protokolliert
- > Erste Phase (Deutschland) für 20.000 Nutzer erfolgreich abgeschlossen

## Kennwort zurücksetzen - vorher

Der bestehende Prozeß zum Zurücksetzen eines Kennworts benötigt eine Vielzahl manueller Eingriffe und kostet wertvolle Arbeitszeit.

### PROBLEM:

- Zu viele Anfragen im zentralen Helpdesk zum Zurücksetzen von Kennwörtern
- Zu viele manuelle Eingriffe und Produktivitätsverluste der Systemadministratoren, die Kennwörter manuell über native Nutzeroberflächen der Anwendungen zurücksetzen



- Der Nutzer kontaktiert den Helpdesk wegen eines vergessenen Kennworts. Der Helpdesk verifiziert die Identität des Nutzers durch eine Reihe von Kontrollfragen.
- Der Helpdesk-Mitarbeiter meldet sich in einer angepassten Active Directory MMC an, um das Kennwort zurückzusetzen.
- Der Helpdesk Mitarbeiter kann das Kennwort nicht zurücksetzen und eröffnet ein Service Ticket im Service Center
- Der Nutzer eröffnet ein Service Ticket um ein neues Kennwort zu bekommen.
- Das Service Center beauftragt die Arbeitsgruppe Informationssicherheit (Security) per E-Mail.
- Die Security leitet das Ticket an die Bearbeitungsqueues der jeweiligen Systemadministratoren weiter.
- Der Sysadmin setzt das Kennwort über die native Nutzeroberfläche zurück und schließt das Service Center Ticket.

**Rot: Manueller Prozess**  
**Grün: Automatisierung**

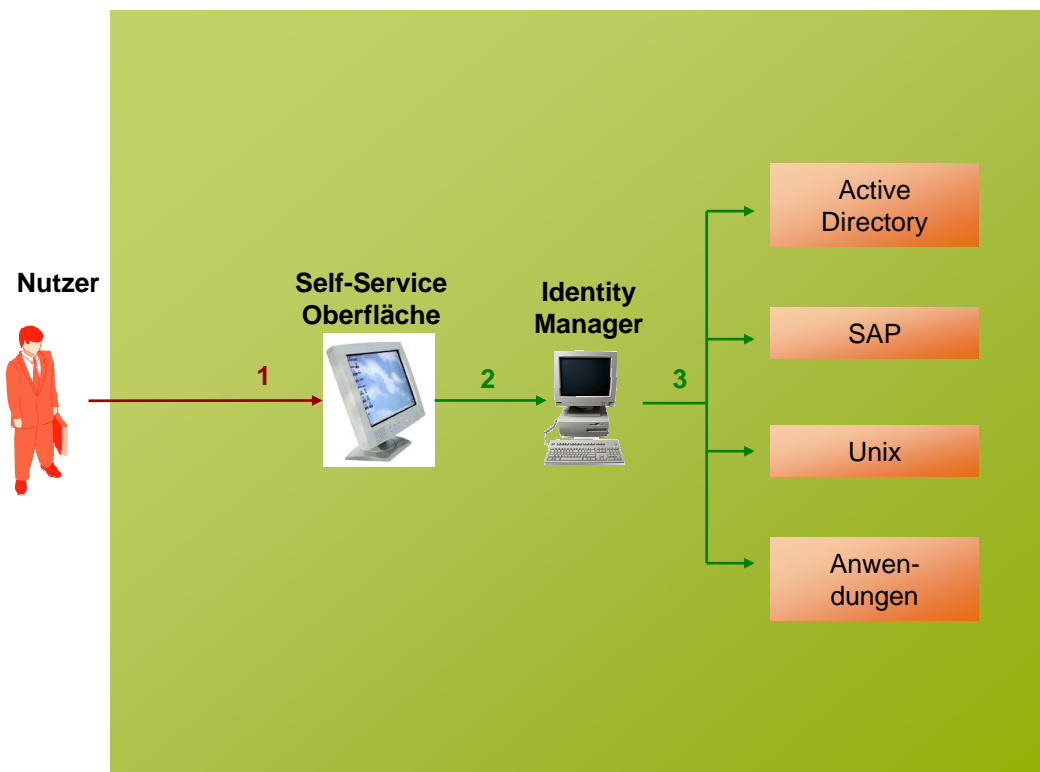
## Kennwort zurücksetzen - nachher

Identity Manager bietet dem Endnutzer eine Oberfläche, von der aus er sein Kennwort zurücksetzen und wählen kann, wohin dieses neue Kennwort propagiert werden soll.

### VORTEILE:

- Weniger Anfragen beim Helpdesk (ca. 33%)
- Bessere Nutzererfahrung durch einheitliche Oberfläche
- Weniger Aufwand für Security im Erfassen und Weiterleiten von Anfragen
- Weniger Aufwand für die Systemadministratoren bei der Kennwortänderung

- 1) Der Nutzer validiert seine Identität durch Antworten auf festgelegte Kontrollfragen. Danach meldet sich der Nutzer bei der Identity Manager's Self-Service Oberfläche an und setzt sein Kennwort zurück.
- 2) Die Nutzerdaten werden an den Identity Manager übermittelt.
- 3) Die neuen Anmeldedaten werden zu den vom Nutzer angegebenen Systemen propagiert.



**Rot: Manueller Prozess**  
**Grün: Automatisierung**

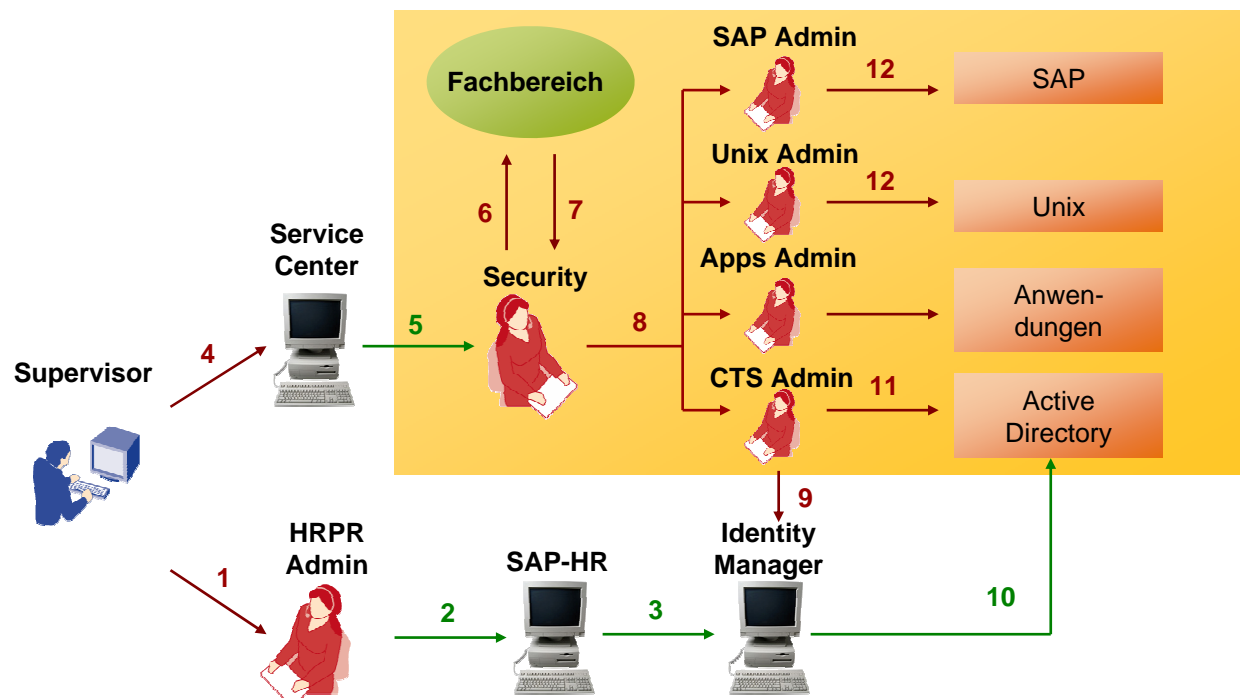
## Neuer Mitarbeiter - vorher

Der bestehende Prozeß zum Anlegen eines neuen Mitarbeiters benötigt eine Vielzahl manueller Eingriffe und kostet wertvolle Arbeitszeit.

### PROBLEM:

- Ein Supervisor muß mehrere Systeme durchlaufen, um einen neuen Nutzer anzulegen.
- Der Nutzer wartet auf mehrere manuelle Prozesse zwischen Security, Fachbereichsleiter und Sysadmins, bevor er Zugang zu den Systemen erhält.
- Die Aktivitäten sind der bestehenden Kommunikation anhand einer Reihe von E-mails schwer nachzuvollziehen.
- Die Berechtigung der Zugangsanfragen läßt sich im Nachhinein schwer überprüfen.

- 1) Supervisor benachrichtigt HR
- 2) HR Admin gibt Daten in SAP HR ein
- 3) Nutzerdaten werden an Identity Manager propagiert
- 4) Supervisor öffnet Service Center Ticket für Anwendungszugriff
- 5) Service Center sendet Anfrage per E-mail weiter an Security
- 6) Security e-mailt Freigabeanfragen an Manager im Fachbereich
- 7) Manager e-mailen Freigabe an Security
- 8) Security vermerkt Freigabe im Ticket und gibt Anfrage frei. Das Ticket geht in die Queue im Service Center zurück
- 9) CTS Admin erzeugt Active Directory Konto via Identity Manager
- 10) Identity Manager propagiert Nutzerdaten nach Active Directory
- 11) CTS Admin bearbeitet Nutzerprofil im Active Directory & schließt Ticket
- 12) Sysadmin erzeugt Nutzerkonto und schließt Service Ticket



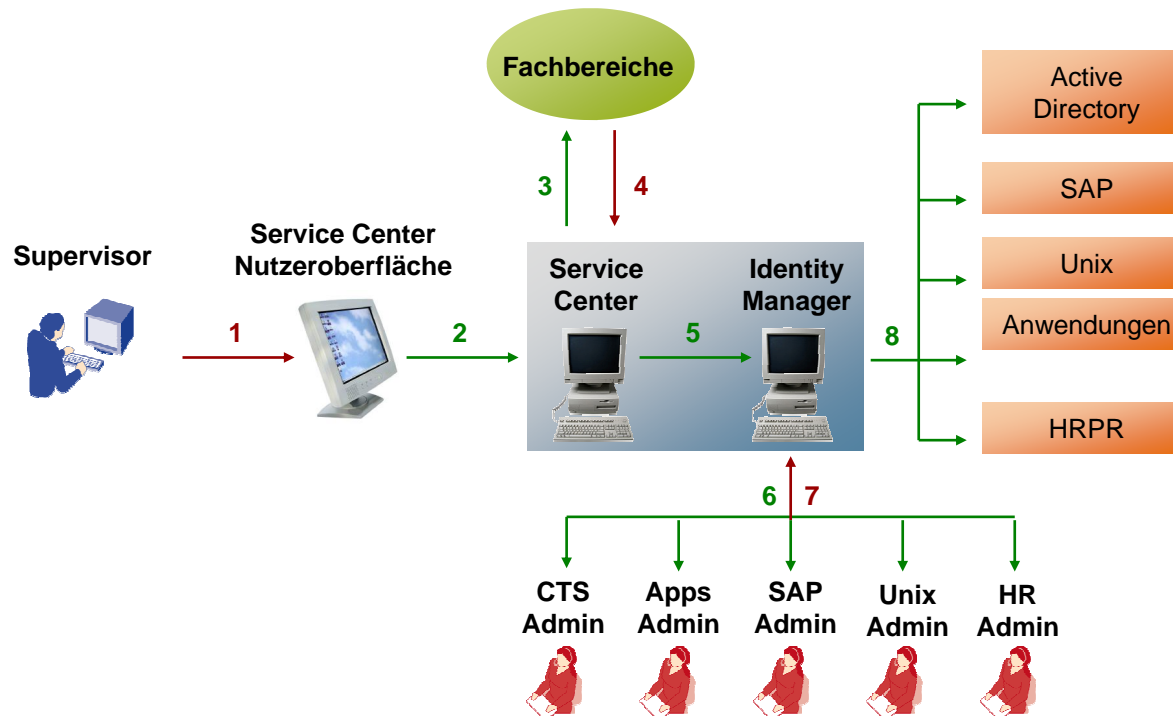
**Rot: Manueller Prozess**  
**Grün: Automatisierung**

## Neuer Mitarbeiter - nachher

Die IAM Lösung beschleunigt die Nutzererstellung und erleichtert Kontrollen der Zugriffe und Freigabeprozesse.

### VORTEILE:

- **Bessere Nutzererfahrung:** Supervisor muß nur auf ein System zugreifen
- **Effizienterer Freigabeprozess** beschleunigt Abarbeitung von Tickets
- **Workflow verbleibt im Service Center** und ist damit einfacher kontrollierbar – Welche Person hat auf welche Anwendungen Zugriff erhalten
- **Identity Manager** verfügt über die komplette Liste aller individuellen Berechtigungen



- 1) Supervisor meldet sich beim Service Center an & beantragt Nutzererstellung für erforderliche Systeme
- 2) Anfrage erreicht Service Center System
- 3) Service Center sendet Fachbereichen Anfrage per E-Mail
- 4) Verantwortliche melden sich beim Service Center an & genehmigen Zugriff
- 5) Service Center sendet Genehmigungsinformation an Identity Manager
- 6) Identity Manager sendet E-Mail an System Admin, erbittet Bereitstellung des Zugangs
- 7) System Admin meldet sich bei Identity Manager an & initiiert Bereitstellungsprozess
- 8) Identity Manager propagiert Nutzererzeugung an Zielsystem

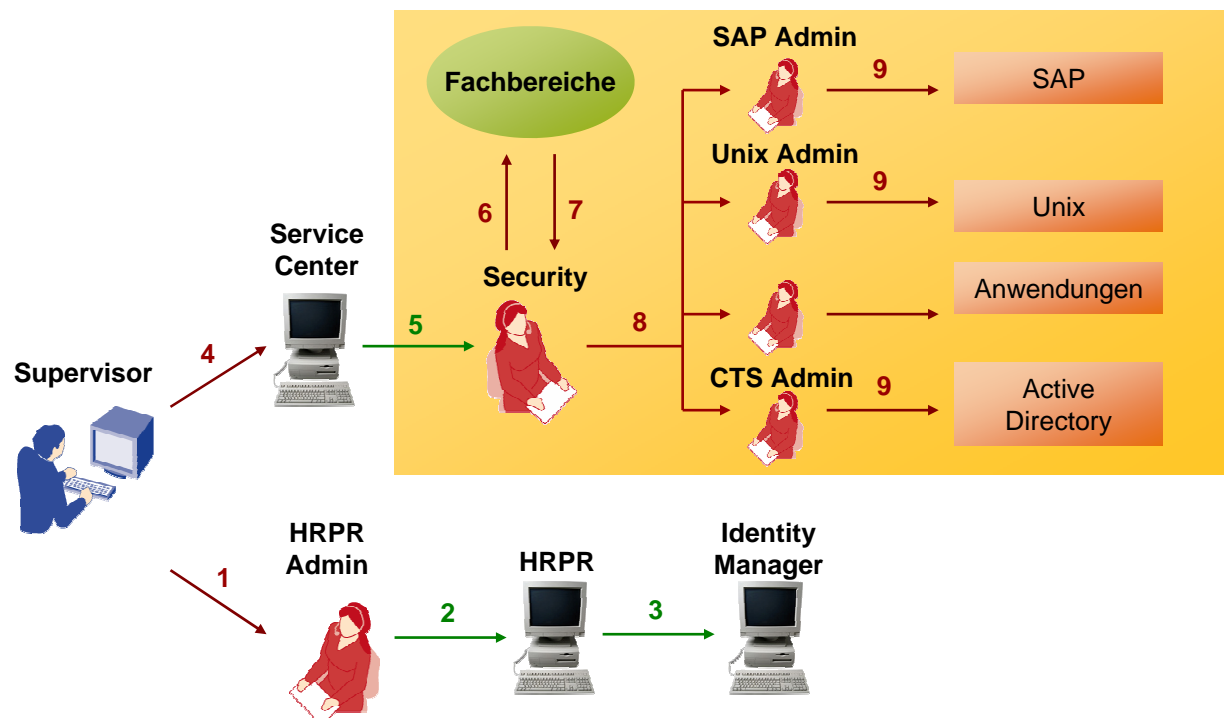
**Rot: Manueller Prozess**  
**Grün: Automatisierung**

## Mitarbeiter Ausscheiden - vorher

Der bestehende Deaktivierungsprozess ist intransparent, da vorhandene Berechtigungen schwer nachzuvollziehen sind.

### PROBLEM:

- Supervisor muß zur Deaktivierung mehrere Systeme durchlaufen.
- Nutzerdeaktivierung dauert zu lange, weil zwischen Security, Fachabteilung und Sysadmins mehrere Manuelle Prozesse ablaufen müssen.
- Tatsächliche Berechtigungen des Nutzers sind nicht einsehbar. Da der Supervisor für jede Deaktivierung explizit ein Ticket eröffnen muß, werden wahrscheinlich nicht alle Rechte entzogen



- 1) Supervisor sendet Formular an HR
- 2) HR Admin setzt Mitarbeiterstatus auf inaktiv in HR. Dieser Prozeß kann bis zum Ende des laufenden Gehaltszahlungszyklus andauern.
- 3) Die Statusänderung wird im IMS reflektiert und der Nutzer dort deaktiviert
- 4) Supervisor erzeugt ein Serviceticket um den Zugriff auf Anwendungen zu entziehen
- 5) Service Center benachrichtigt Security
- 6) Security informiert zuständige Personen per E-Mail
- 7) Fachbereiche genehmigen Deaktivierung
- 8) Security vermerkt Genehmigungen und gibt Anfrage zur Ausführung frei. Das Ticket wandert in die Bearbeitungsqueue des Service Center
- 9) System Admin entfernen Nutzerzugriff auf ihre Systeme

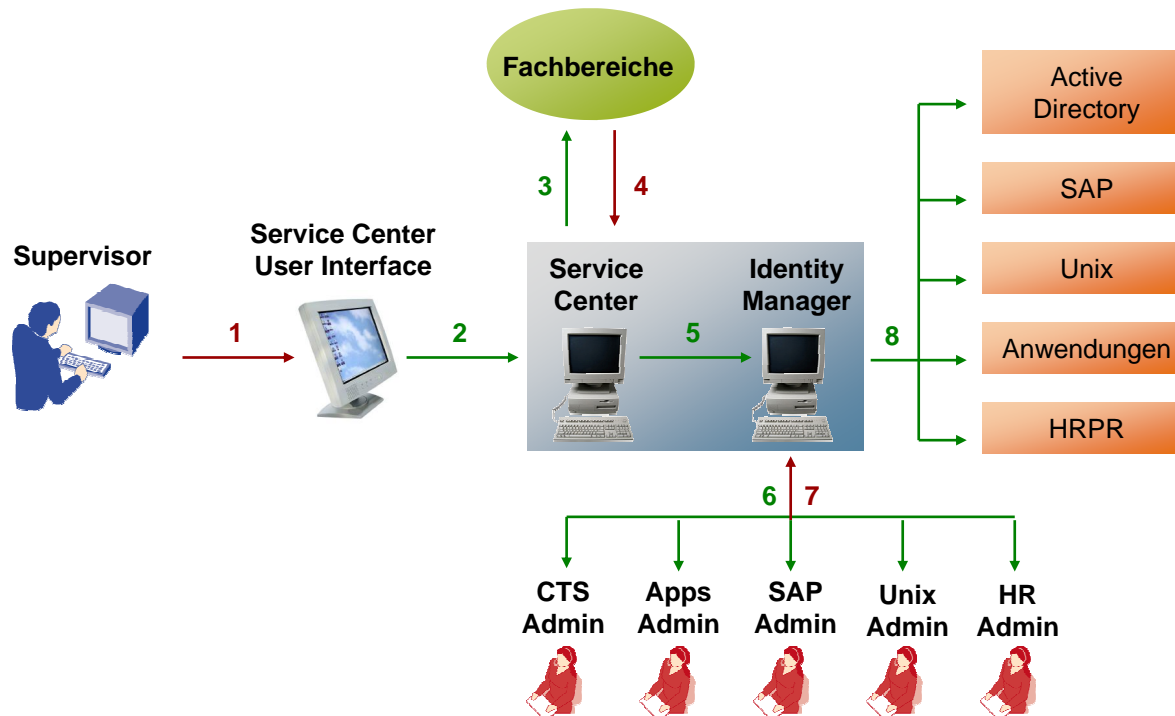
**Rot: Manueller Prozess**  
**Grün: Automatisierung**

## Mitarbeiter Ausscheiden - nachher

Die IAM Lösung beschleunigt die Nutzerdeaktivierung und den nachvollziehbaren Entzug der Zugriffsrechte.

### VORTEILE:

- **Bessere Nutzererfahrung:** Supervisor muß nur auf ein System zugreifen
- **Effizienterer Genehmigungsprozess** beschleunigt Abarbeitung von Tickets
- **Workflow verbleibt im Service Center** und ist damit einfacher kontrollierbar – Welcher Person wurde der Zugriff auf welche Anwendung entzogen
- **Identity Manager** verfügt über die komplette Liste aller individuellen Berechtigungen



- 1) Supervisor meldet sich beim Service Center an und beantragt Deaktivierung
- 2) Anfrage wird an Service Center System gesendet
- 3) Service Center erbittet Genehmigung der Fachabteilungen per E-Mail
- 4) Fachbereiche genehmigen Deaktivierung über Self Service
- 5) Service Center sendet Genehmigungsinformationen an Identity Manager
- 6) Identity Manager sendet E-Mails an System Admins und erbittet Deaktivierung zu starten
- 7) System Admin meldet sich bei Identity Manager an & initiiert Deaktivierung
- 8) Identity Manager deaktiviert Nutzerzugriff auf Zielsystem

**Rot: Manueller Prozess**  
**Grün: Automatisierung**

# Wie geht Sun vor ...

- Systematisches Vorgehen nach Sun Implementation & Development Methodology - SIDM
- Sun's weltweiter IdM Standard basierend auf Waveset Implementierungsmethode
  - > Fokussierung auf "Requirement Definition" and "Signoff" *vor* der Implementierung
  - > Definition der erforderlichen Aufgaben, Ergebnisse, involvierten Rollen und Verantwortlichkeiten
  - > Bereitstellung von Vorlagen, Modellen, ... und "Best Practices"
- ... analog schult Sun seine Partner

# Erfahrungswerte für erfolgreiche Identity Management Projekte

1. Greifen Sie nach tief hängenden Trauben
2. Glauben Sie nicht bunten Anbieterfolien
3. Definieren Sie vorab klare Erfolgskriterien
4. Schränken Sie den Zeitplan ein
5. Begrenzen Sie die Ressourcen





# FRAGEN?

[Hans.Wieser@Sun.COM](mailto:Hans.Wieser@Sun.COM)

