

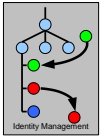
Identity-Management in der NOW IT

Volker Bertermann

Informationsveranstaltung Atos

Online, 23.03.2023

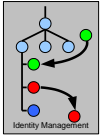
Inhaltsverzeichnis



- 1. Vorstellung der NOW IT GmbH**
- 2. Kurze Einsatz-Historie**
- 3. Aktuell genutzte Funktionen**
- 4. Nutzen für die Unternehmen**
- 5. 6 Kunden – ein IdM**
- 6. Ausblick**

Die Deutsche Rentenversicherung

Bestandteil der Sozialversicherungen in Deutschland



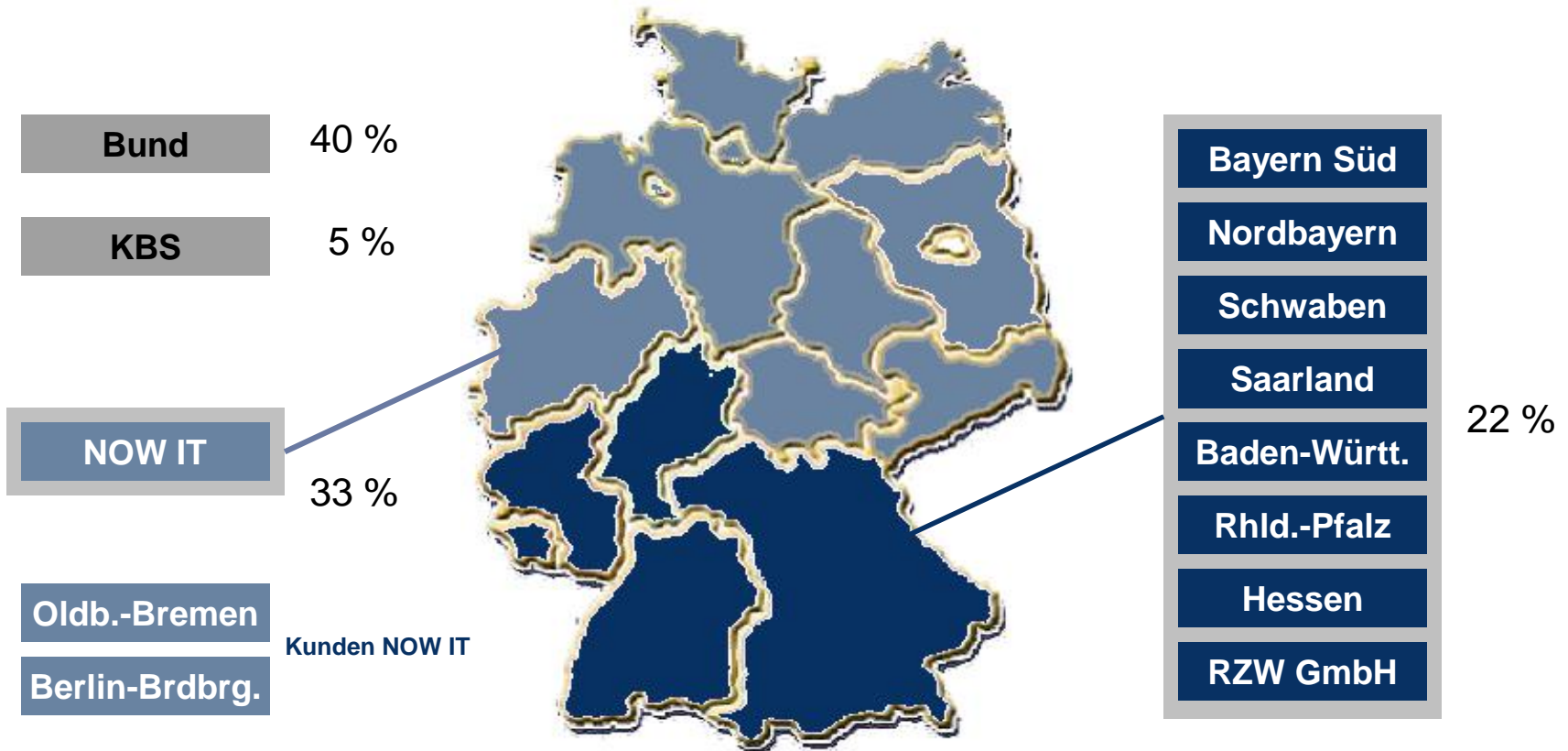
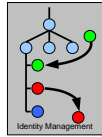
Deutsche
Rentenversicherung
Sicherheit
für Generationen

- 16 Rentenversicherungsträger betreuen

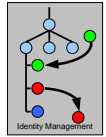
56 Mio. Versicherte und 21 Mio. Rentner

- Rente und Rehabilitation

Die IT-Landkarte der Deutschen Rentenversicherung



Ganzheitliche Steuerung



Aufstellung in Standortprofilen

Hamburg/Lübeck

- Rechenzentrum
- Teilprofil Entwicklung

Münster

- Rechenzentrum
- Betrieb
- Teilprofil Entwicklung

Düsseldorf

- Dokumentenzentrum
- Teilprofil Entwicklung



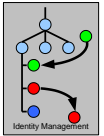
Braunschweig/ Hannover

- Betriebswirtschaft
- Teilprofil Entwicklung

Leipzig mit Standorten

- Betrieb
- Aus-, Fort-
und Weiterbildung
- Teilprofil Entwicklung

Die NOW IT GmbH in Zahlen



Eckdaten Kunden

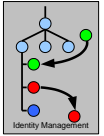
Kunden	5 (+13)
Beschäftigte	17.600
Lokationen	rund 130

Eckdaten NOW IT GmbH

Beschäftigte	~ 670
Betriebsstätten	10
Hostsysteme	2
Serversysteme	~ 3.000
Speicher in TB	~ 3.100

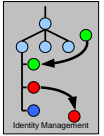
Die NOW IT GmbH

Full service provider für...



- Entwicklung und Betrieb des Kernsystems der Rentenversicherung
- Archiv und Druckzentrum
- Entwicklung und Betrieb von SAP-Systemen (~70)
- Großrechner, Netz, Server, Storage, Telefonie
- IT-Arbeitsplätze mit mehreren hundert Anwendungen
- Dienstleistungen für andere Rentenversicherungsträger

Einsatz-Historie

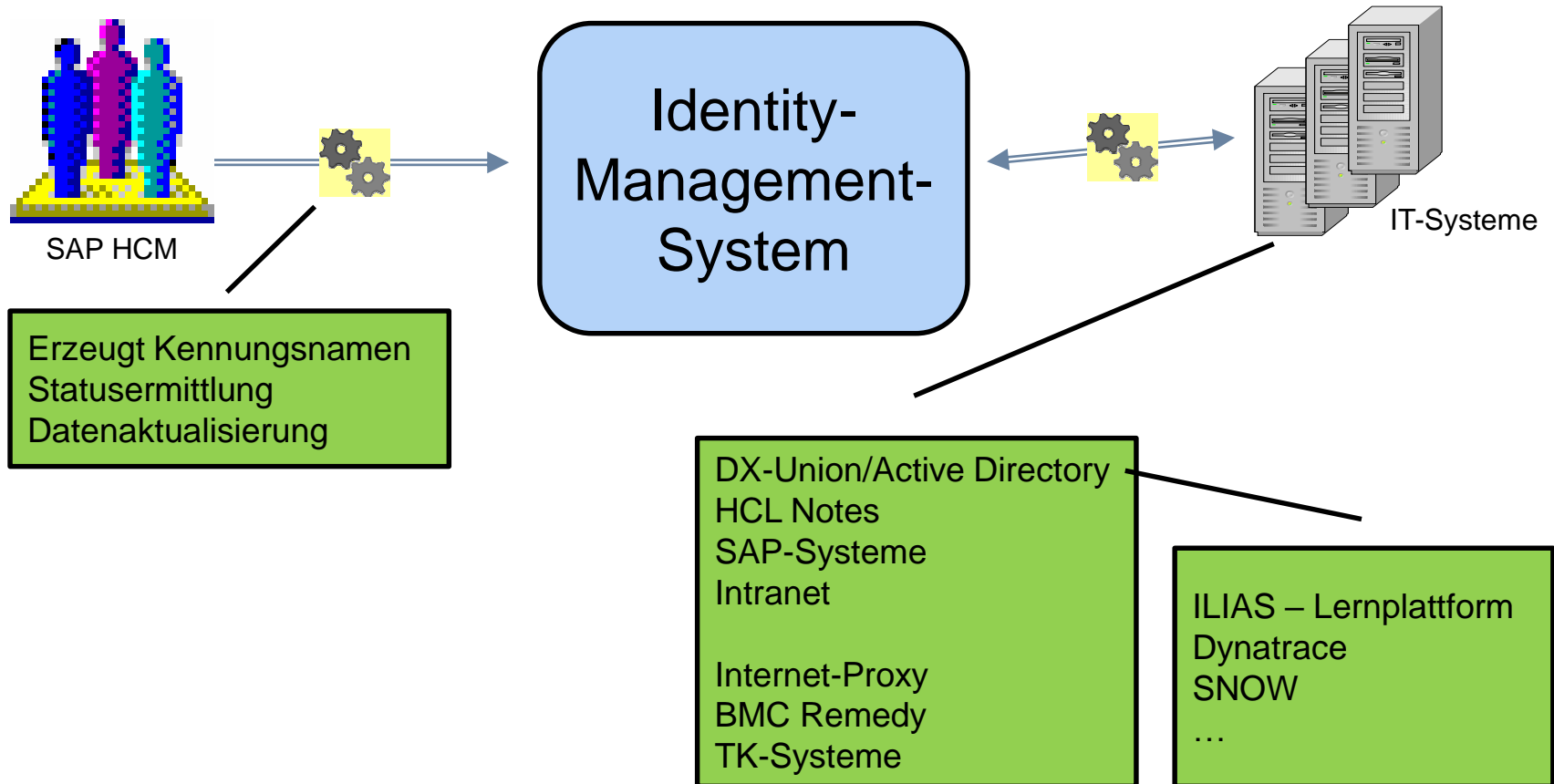
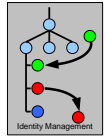


Produkt und Mitarbeiter...

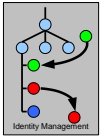
- Einsatz seit 2001 als DirX Metahub -> DirX Metarole ->
- IdM Workflow aus 2001 für die Siemens-TK-Anlage in 2022 abgeschaltet...
- DirX Identity Version 8.7 -> 8.10
- Betrieb auf Linux und Windows VM
 - SLES als primäres System mit DirX Directory und WebCenter
 - Win Server als sek. System mit Notes-, ODBC- und AD-Agenten
- 5 IdM-Kolleginnen und -Kollegen

Funktionsumfang IdM

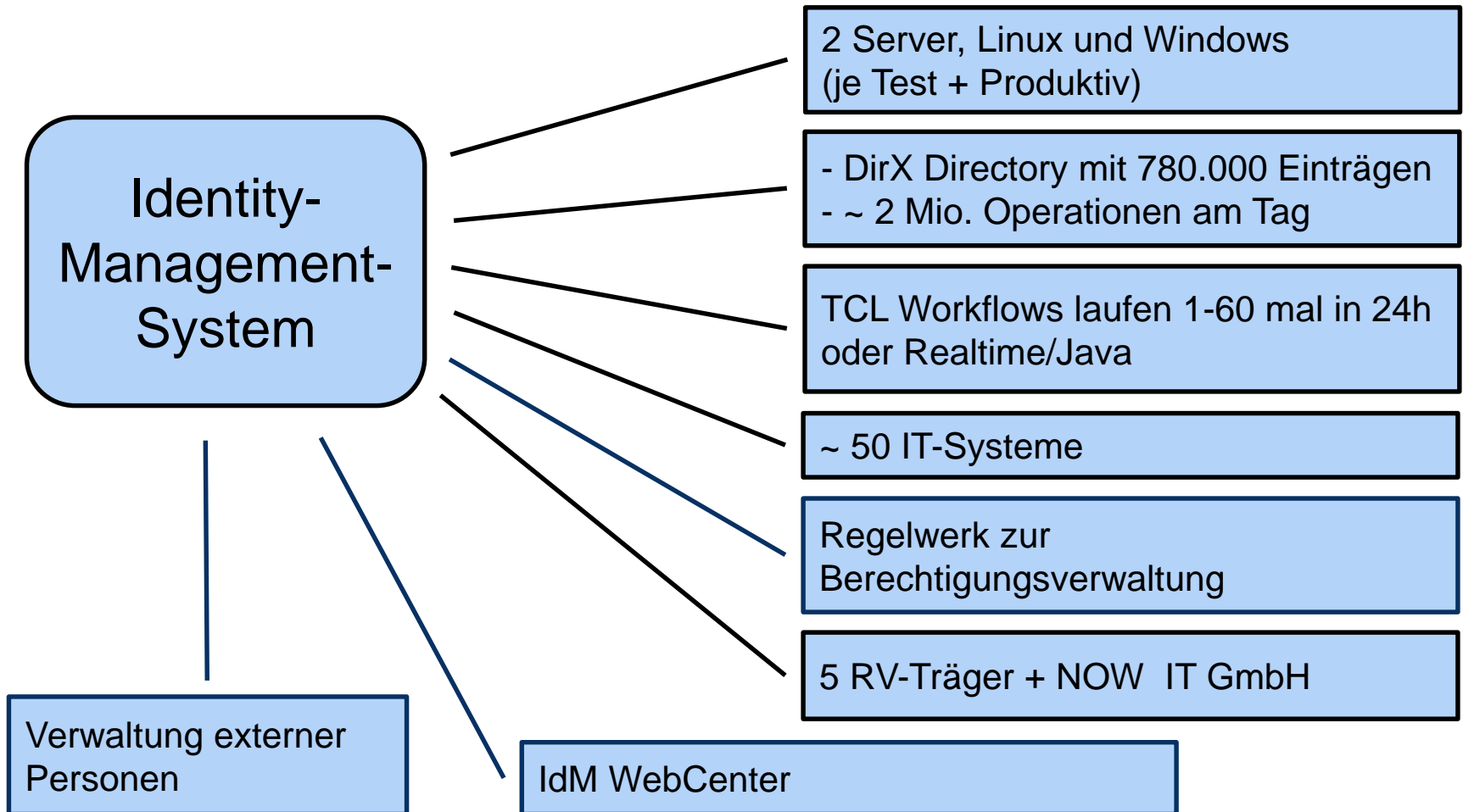
Wesentliche IT-Systeme



Funktionsumfang IdM

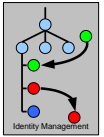


Interne Betriebsaspekte



Nutzen

Für unsere Kunden



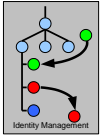
Delegierte Administration via WebCenter durch Kunden

Umsetzung von Standardberechtigungen schneller als Aufträge

Auditierbarkeit der Account- und Rechtevergabe

Daten mit hoher Qualität für Betriebs- und Planungszwecke

Nutzen

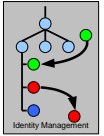


Rentenversicherung ist eine kritische IT-Infrastruktur

- Kerngeschäft und dazugehörige Geschäftsprozesse: KRITIS-Verordnung
- Betrieb nach BSI IT-Grundschutz und KRITIS
- IT-Grundschutzbaustein „Identitäts- und Berechtigungsmanagement“
- Einsatz eines Identity-Managements zwingend erforderlich

- Nachweis über BSI-Audits und BSI Grundschutz-Checks
- Trend zu „Zero-Trust“ dank Log4j

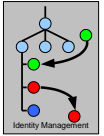
Nutzen



IT-Grundschutz: ORP.4: Identitäts- und Berechtigungsmanagement

- Klare Identifikation: Person <-> Kennung
- Klare Prozesse zur Verwaltung von Zutritts-, Zugriffs- und Zugangsrechten
- Daten sind immer aktuell
- Zentrale Deaktivierungsmöglichkeit
- Dokumentation der Berechtigungen (ITIL Access Management)
- ...

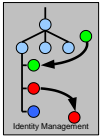
Nutzen



IT-Grundschutz: OPS.1.1.2: Ordnungsgemäße IT-Administration

- Einschränkung des Missbrauchs von administrativen Berechtigungen
- Dokumentation von IT-Admin-Tätigkeiten
- Aufklärungsmöglichkeit bei Sicherheitsvorfällen
- ...

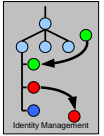
Nutzen



Einsparungen im IT-Betrieb – verbesserte Sicherheit

- Berechtigungsänderungen sehr schnell, besonders der Rückbau
- Keine Aufträge für Standard-Berechtigungen mehr
- Personendaten immer aktuell, auch der Status!
- Online-Dokumentation der Berechtigungen
- IdM ist Basis für Berechtigungs-Audit
- Delegierte Administration möglich
- ...

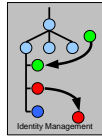
6 Kunden – ein IdM



Ein einziges DirX Identity-System

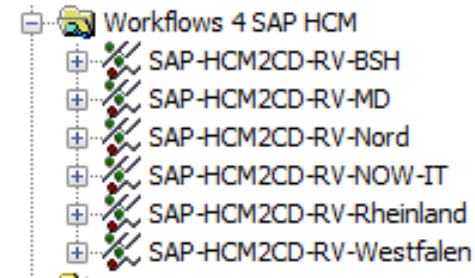
- 6 Quellen für Personendaten (SAP-HCM)
- Trennung der Personendaten im DXI-User-Store
- IdM-Unterstützung für
 - gemeinsam genutzte IT-Systeme
 - gleichartige IT-Systeme für alle Kunden
 - individuelle IT-Systeme am Active Directory
- Kundenindividuelles IdM-Regelwerk

6 Kunden – ein IdM



Was bedeutet das?

→ 6 Quellen für Personendaten (SAP-HCM)

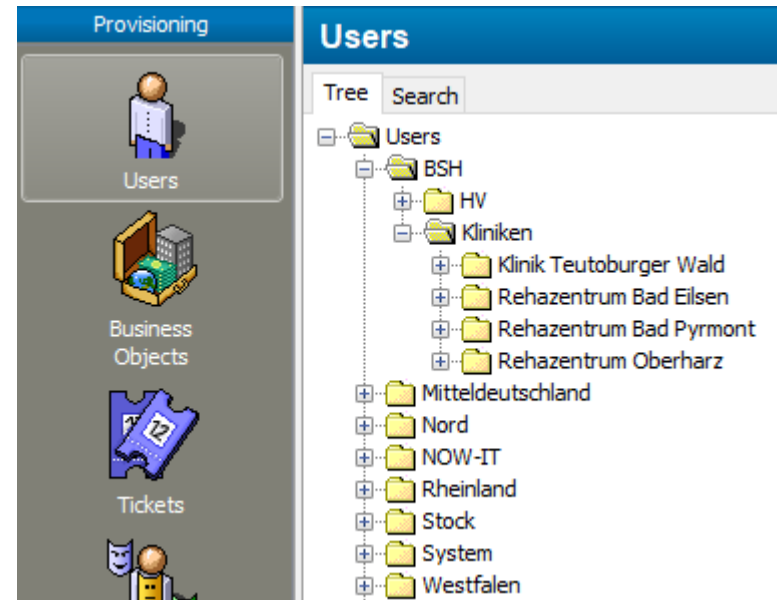


→ Trennung der Personendaten

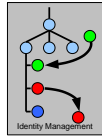
im DXI-User-Store durch

- Baumstruktur
- Sync-Ids, ...
- Kundenmerkmale

- Access Policies im WebCenter
- ~ 50 allgemeine
- ~ 10 je IT-System



6 Kunden – ein IdM

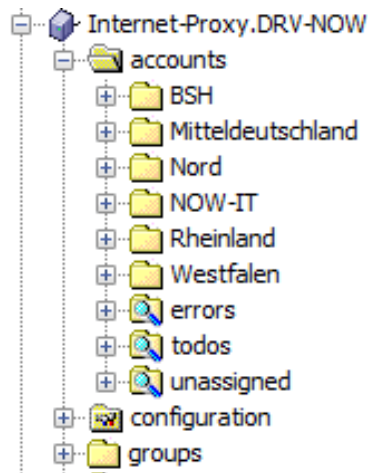


Was bedeutet das?

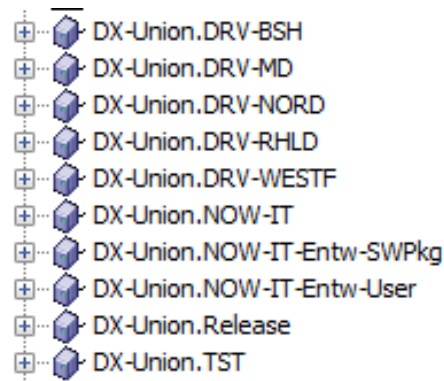
→ IdM-Unterstützung für

1. gemeinsam genutzte IT-Systeme
2. gleichartige IT-Systeme für alle Kunden
3. individuelle IT-Systeme z.B. am Active Directory

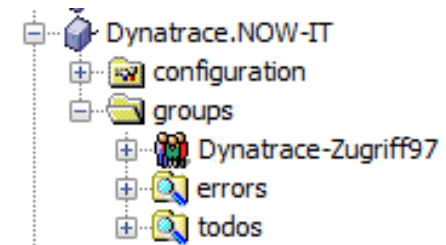
1.



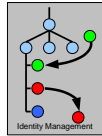
2.



3.



6 Kunden – ein IdM

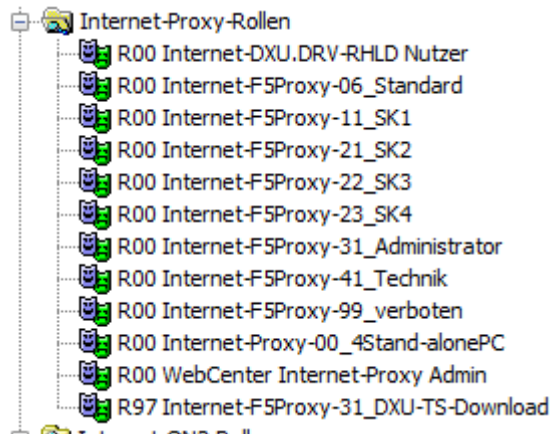


Was bedeutet das?

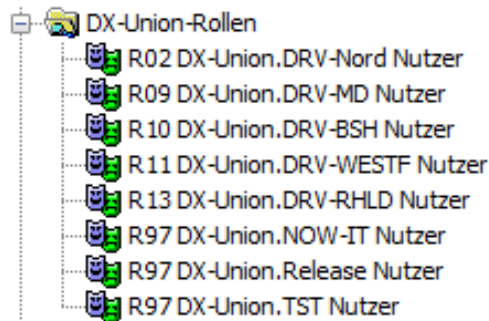
→ Kundenindividuelles IdM-Regelwerk

1. gemeinsam genutzte IT-Systeme
2. gleichartige IT-Systeme für alle Kunden
3. individuelle IT-Systeme z.B. am Active Directory

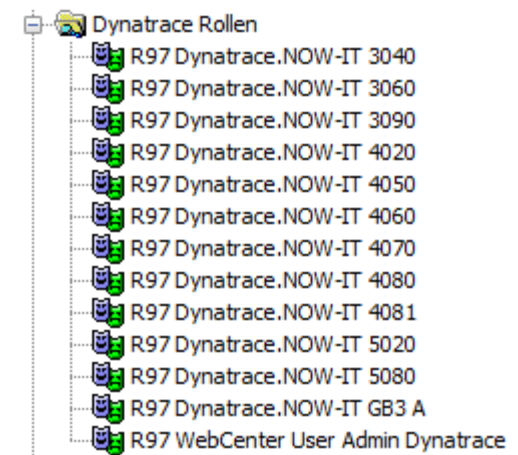
1.



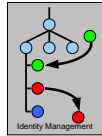
2.



3.



6 Kunden – ein IdM



Was bedeutet das?

→ Kundenindividuelles IdM-Regelwerk

- 1 allgemeine Rolle je Kunde
- Steuern 500 – 800 Gruppen

- Anwendungsspezifische Rollen
25 – 50 je Kunde
- ~100 Permissions je Kunde

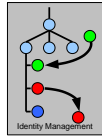
R11 Interner MA DRV Westfalen

General Approval Certification Details Role Parameters Assigned J

Assigned Permissions:

Permission ^
P00 Notes MailExtern Interner MA - o employeeType dxrEndDate
P11 DX-Union.DRV-WESTF - departmentNumber
P11 DX-Union Interner MA - employeeType dxrEndDate
P11 Framework.DRV Anwender
P11 ILIAS Globale-User-Gruppe Nutzer - departmentNumber
P11 ILIAS Lokale-User-Gruppe WzG - departmentNumber
P11 Interner MA DRV Westfalen
P11 Interner MA DRV Westfalen - NEW
P11 Notes.DRV-WESTF - depNo function mail
P11 Notes.DRV-WESTF - depNo function Planst mail
P11 Notes.DRV-WESTF - depNo mail drvSAPPlanst
P11 Notes.DRV-WESTF - depNo o
P11 Notes.DRV-WESTF - depNo o l
P11 Notes.DRV-WESTF - depNo o mail
P11 Notes.DRV-WESTF - function mail
P11 Notes.DRV-WESTF - o BusinessCategory Mail
P11 TK-HiPath-Manager.DRV-ZRWest Nutzer - l

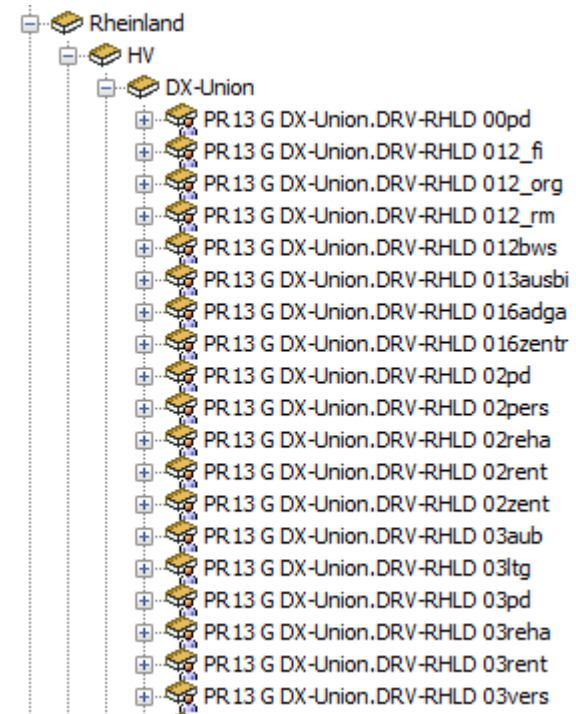
6 Kunden – ein IdM



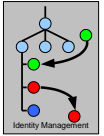
Was bedeutet das?

→ Kundenindividuelles IdM-Regelwerk

- Zusätzlich Provisioning-Rules mit Matchingrules mit Verneinung



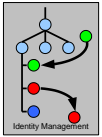
6 Kunden – ein IdM



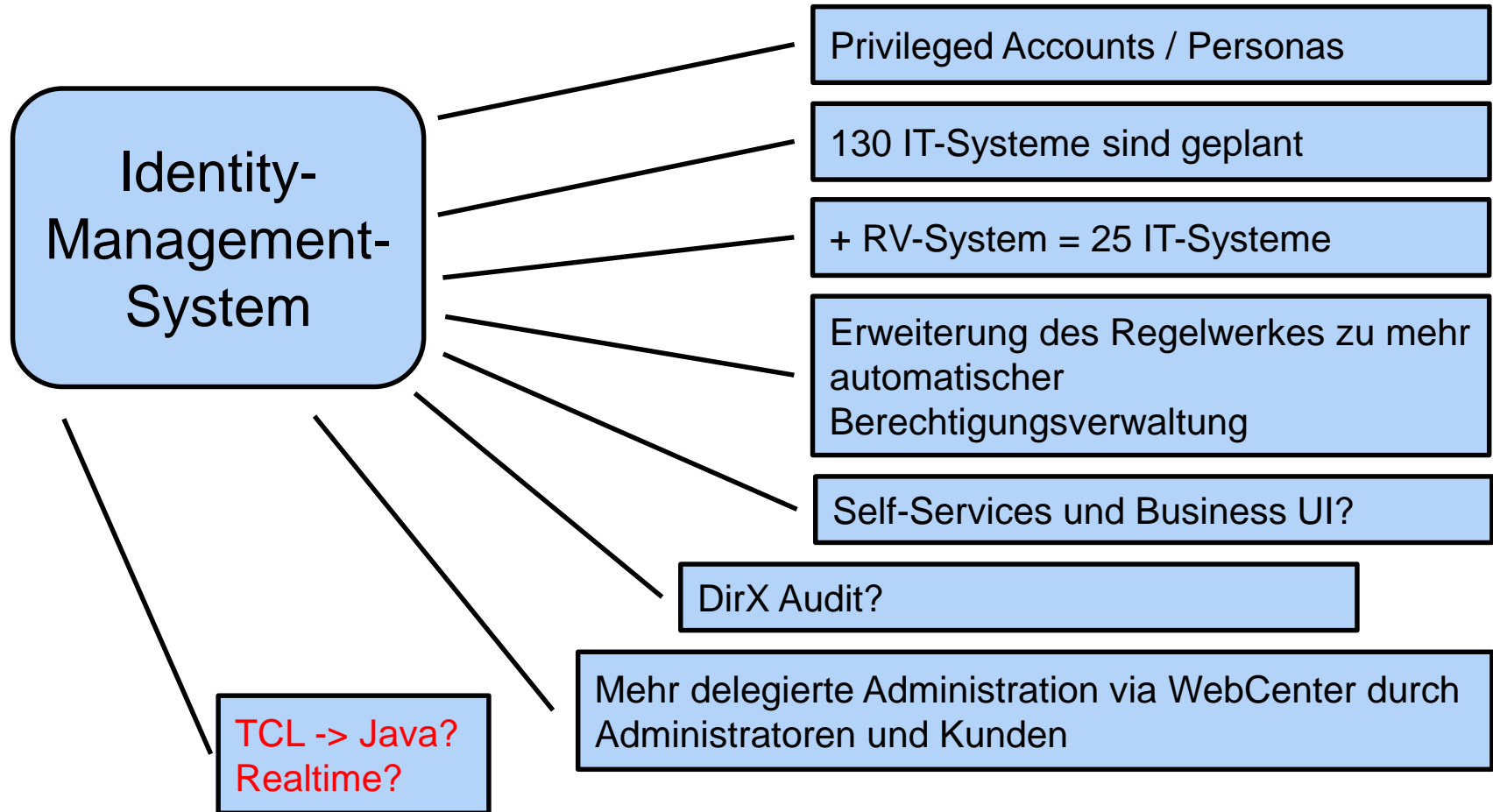
Fertig sind...

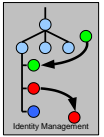
- 14 x SAP Benutzer- und Rollenverwaltung
- 5 x Intranet ON2
- 4 x TK-Systeme
- 6 x HCL Notes
- ITSM-Framework - Anwenderdaten
- Internet-Proxy für alle Mandanten
- 8 x DX-Union
- 6 x ILIAS
- 5 x Facility-Mgmt
- Verwaltung externer Mitarbeiter
- Für NOW IT: Dynatrace, SNOW
- ...

Ausblick



Wie entwickelt sich das IdM weiter?





**Vielen Dank
für Ihre
Aufmerksamkeit**