

Klick statt Code – Effizienz für Fachbereiche

Rike Kouba & Martin Berndt

HSD

 IDABUS®

 NEXIS

 TD SYNnex



Warum Klick statt Code heute entscheidend ist

- Zeitersparnis – Ideen schneller umsetzen
- Kosteneffizienz – weniger Entwicklerkosten
- Barrierefreiheit & Empowerment von Fachbereichen
- Produktivitätssteigerung – unabhängig agieren vs. warten
- Fehlerreduktion & weniger technischer Aufwand
- Agilität & Anpassbarkeit - dynamisch



USE CASE: HR User

mehrere Verträge, Autocreate von Usern

- Ein neuer **SF Employee** kommt ins System, aber hat **mehrere Beschäftigungsverhältnisse (Employments)**.
- Ziel: Immer das **relevanteste Employment** auswählen und automatisch dem **User (Person Object)** zuordnen.
- Herausforderung: Nicht alle Employments sind gleichzeitig gültig – es gibt **aktuelle, zukünftige und vergangene Jobs**.



USE CASE: HR User

mehrere Verträge, Autocreate von Usern

Entscheidungslogik Employments:

1. Alle Employments abrufen
2. Employments filtern → Enddatum in der Zukunft
3. Employments finden → Startdatum vor heute, Enddatum nach heute → Aktueller Job
4. Zukünftiges Employment finden → Startdatum nach heute
5. Fallback letztes Employment in der Vergangenheit



USE CASE: HR User

mehrere Verträge, Autocreate von Usern

- **Trigger:**
 - SF erkennt aktive Employment-Objekte → /ocgsfemployment
- **Workflow:**
 - Employment wird in **SFUser Object** geschrieben
- **Autocreate User:**
 - Automatische Verknüpfung von **Person Object** ↔ **Employment**

Zur Demo →



USE CASE: HR User

mehrere Verträge, Autocreate von Usern

- **Automatische Auswahl** des relevanten Jobs verhindert Fehler
- **Eindeutige Logik** bei mehreren Beschäftigungen
- **Transparenz:** immer nachvollziehbar, warum ein Job gewählt wurde
- **Sauberer Datenbestand:** keine doppelten oder falschen User



USE CASE: Integration von ServiceNow

■ Useranlage

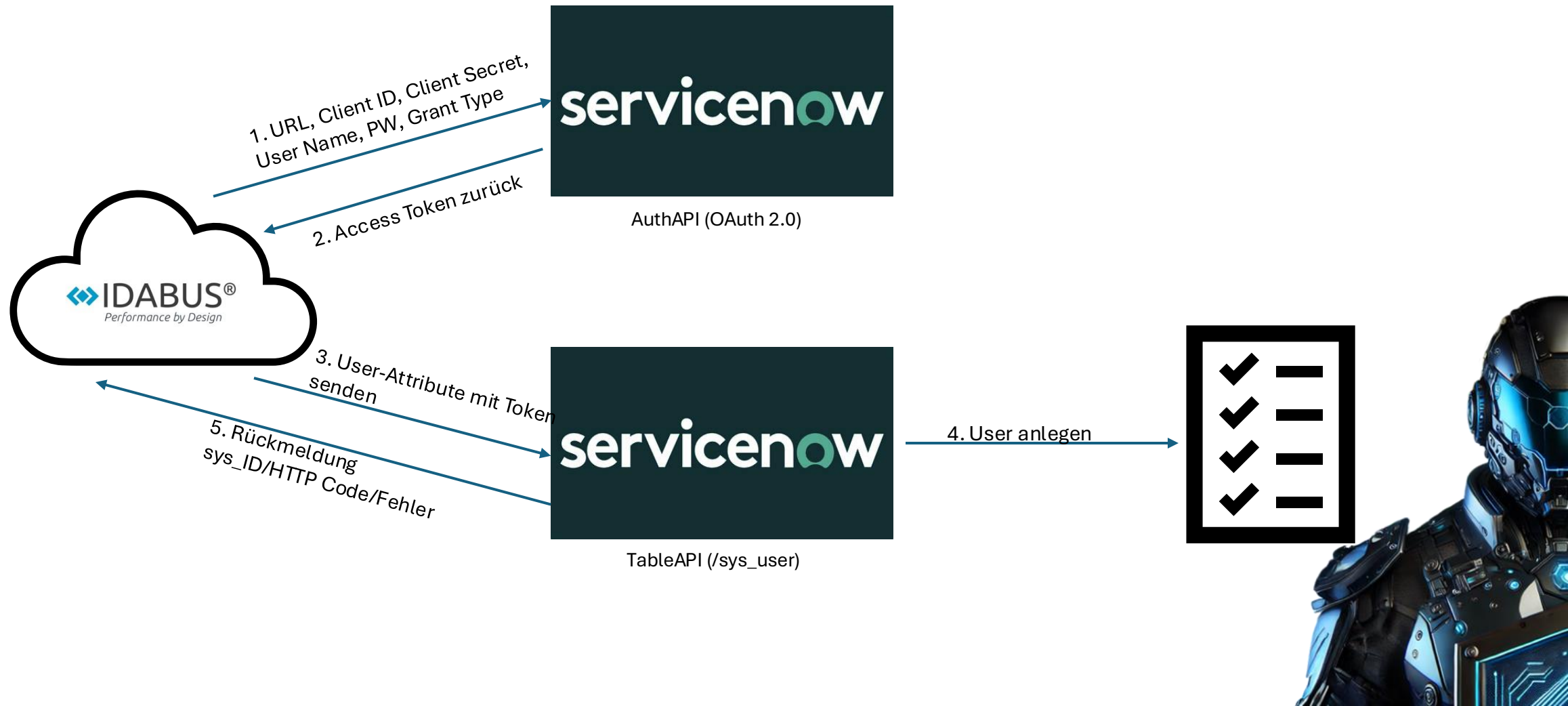
1. Ansprechen der ServiceNow-Auth-API mit Übergabe der Daten
2. User anlegen in SNOW
3. Opt. Flag am User setzen, dass User angelegt wurde

■ Ticketanlage

1. Ansprechen der ServiceNow-Auth-API mit Übergabe der Daten
2. Ticket eröffnen in SNOW



USE CASE: Integration von ServiceNow



USE CASE: Integration von ServiceNow

- Useranlage

1. Ansprechen der ServiceNow-Auth-API mit Übergabe der Daten
2. User anlegen in SNOW
3. Opt. Flag am User setzen, dass User angelegt wurde

- Ticketanlage

1. **Ansprechen der ServiceNow-Auth-API mit Übergabe der Daten**
2. **Ticket eröffnen in SNOW**

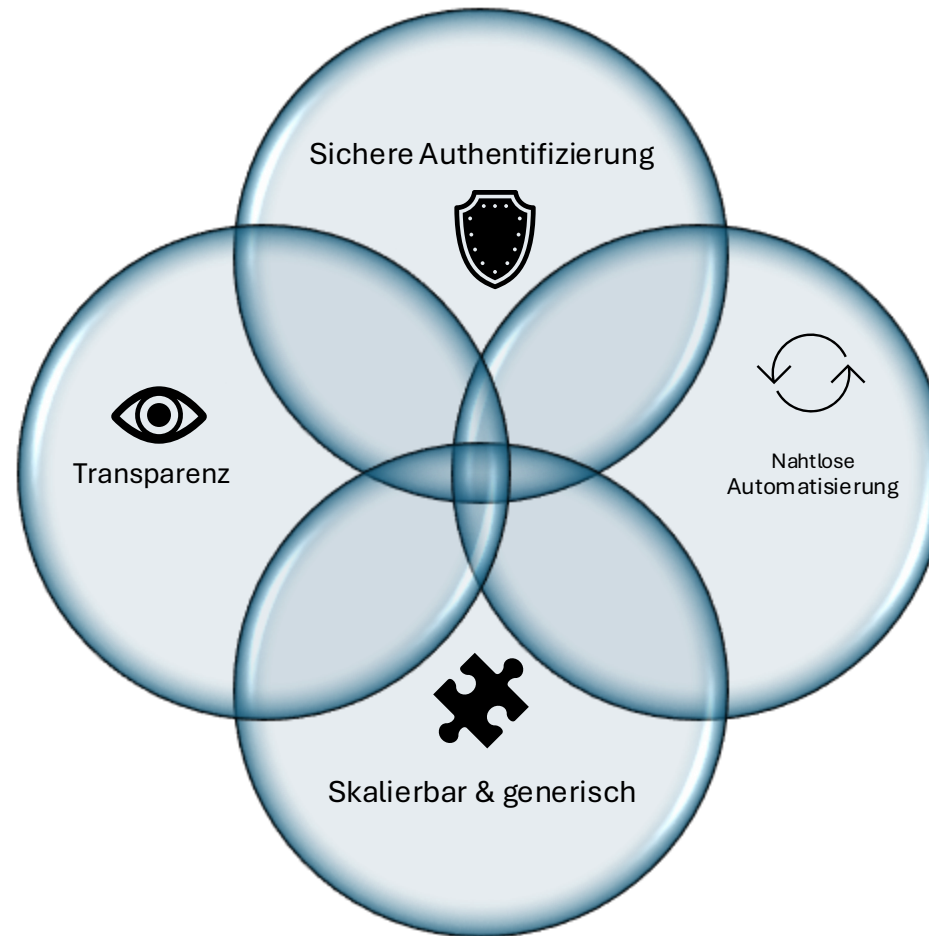
- Umsetzung in IDABUS:

- XPath Template
- Trigger
- Workflow

→ DEMO



USE CASE: Integration von ServiceNow



USE CASE: OU – Move with Delay

- **Scenario – User soll ...**
 - in der Zukunft in eine **neue OrgUnit** wechseln
 - temporär in **zwei OrgUnits gleichzeitig** sein
 - nach definierter Zeit aus der bisherigen OrgUnit entfernt werden
- **Rollenzuweisungen & Gruppen**
 - Alle **direkt vergebenen Rollen** und **Gruppen** werden gleich behandelt
 - Rollen und Gruppen können ein **Enddatum** bekommen



USE CASE: OU – Move with Delay

Ablauf

1. „Move to OU“ für User wird ausgelöst
2. Neue OU wird über Baumstruktur im Wizard ausgewählt
3. Start- und Enddatum wird festgelegt
4. Rollen- und Gruppenzuweisungen mit Enddatum auswählbar

Zur Demo →



USE CASE: OU – Move with Delay

Neue Features

- **Seitenmenü** triggert Wizard
- Wizard triggert **Workflow Template**
- Weitere Optionen:
 - Seitenmenü → Workflow Template mit **Warn- und Bestätigungsmeldung**
 - Button → Workflow Template oder Wizard



USE CASE: OU – Move with Delay

Sicherheits- und Nutzwert

- **Kontrollierter Wechsel** in neue OrgUnits
- **Fehlervermeidung** durch Zeitsteuerung und Bestätigung
- **Transparenz** durch klaren Ablauf und Meldungen
- **Flexibilität** durch verschiedene Kombinationen (Wizard/Workflow/Buttons)



USE CASE: Account-Rollen

Userprovisionierung für beliebige Systeme

- Ziel: automatisierte Useranlange durch Rollenzuweisung in Zielsysteme wie AD oder SAP – direkt aus IDABUS heraus
- Evolution zu MIM: Die Logik zur Steuerung der Provisionierung liegt nicht mehr in der Sync Engine sondern zentral in IDABUS
- Dataflow-basiertes Provisioning



USE CASE: Account-Rollen

Userprovisionierung für beliebige Systeme

- Umsetzung in IDABUS
 1. Rollen-Flag in IDABUS „Target System“ = AD/SAP/..
 2. Generische Komponente – per Dataflow Rule wird das Attribut auf das multivalue-string Attribut „Target Systems“ des Users geschrieben
 3. Sync Engine übernimmt – liest das Attribut aus und erzeugt im Zielsystem (z.B. AD) den entsprechenden Benutzeraccount
- DEMO



USE CASE: Account-Rollen

Rollenprovisionierung für beliebige Systeme

Consistency



Reusability



USE CASE: Kritische Rollenänderungen

Ausgangssituation:

Ein User wird im IDABUS einer kritischen Rolle **hinzugefügt** oder **entfernt**.

Risikobewertung:

Jede Rolle erhält einen **Risk Level (0–10)**.

Ab einem Wert von ≥ 7 wird automatisch eine Meldung generiert.

Benachrichtigung:

- Standard: Der **betroffene User** wird informiert.
- **Anpassbar**: Je nach Kundenfall können zusätzlich **Sicherheitsbeauftragte, Compliance-Verantwortliche oder andere Rollen** benachrichtigt werden.

Zur Demo →



USE CASE: Kritische Rollenänderungen

Transparenz:

Meldung enthält klare Information, **welche Rolle betroffen** ist.

Sicherheitsnutzen:

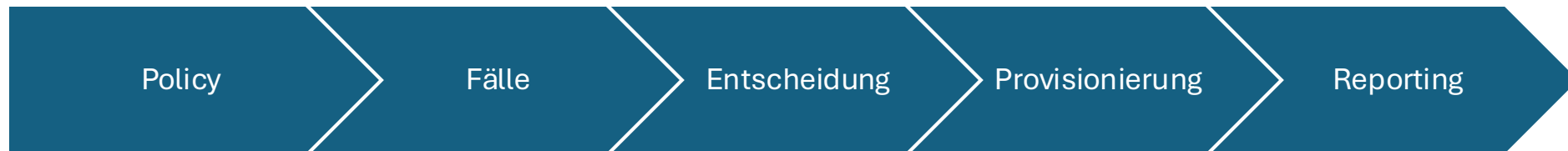
- **Frühzeitige Erkennung** kritischer Änderungen
- **Reduzierung von Missbrauchsrisiken**
- **Stärkung der Compliance** durch Nachvollziehbarkeit
- **Erhöhte Eigenverantwortung** der Nutzer
- **Flexibilität** in der Anpassung an **individuelle Sicherheits- und Compliance-Anforderungen**



USE CASE: Attestierung von Rollen

Sicherheit | Compliance | Effizienz

- Was ist Attestierung?
- Wie läuft es ab?



USE CASE: Attestierung von Rollen

Umsetzung in IDABUS

- XPath Template "Roles for attestation"
- Triggers:
 - Role Attestation with MT
 - Role Attestation with MT (in progress)
 - Role Attestation MT
- Workflows:
 - Attestation of roles via MT
- DEMO



USE CASE: Attestierung von Rollen

Sicherheit | Compliance | Effizienz

Warum regelmäßig prüfen?

- Verhindert unnötige Zugriffe („Privilege Creep“)
- Unterstützt Compliance & Audits
- Beschleunigt und sichert Prozesse durch Automatisierung

