

# PRIVIUS MEETS SAP

---

EINE ERWEITERUNG DES SAP BERECHTIGUNGSMANAGEMENTS



# WIR STELLEN UNS VOR



**Dennis Westers**

Teamleiter Business Automation



**Manuel Müller**

Automation Consultant

# AGENDA

**01** Privius – Die Story

---

**02** Fallbeispiel (1): User Onboarding

---

**03** Security by Design & Wissenswertes

---

**04** Privius SAP Berechtigungsmanagement

---

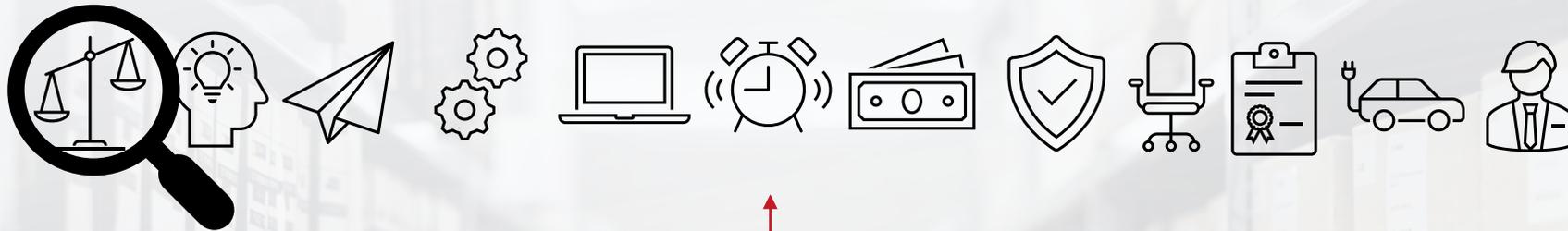
**05** Fallbeispiel (2): Externen Mitarbeiter für einen begrenzten Zeitraum auf SAP-System anlegen

---

**06** Roadmap & Release Date

# 01 | PRIVIUS – DIE STORY





Eigenentwicklung mit dem Fokus auf Sicherheit, Flexibilität & Usability

...

Fehlender Überblick

Unklare  
Eigentümerschaften

Missverständnisse  
bei Anforderungen

Zu lange  
Bearbeitungsdauer

Komplexe  
Genehmigungsverfahren

Nicht standardisierte  
Berechtigungen

Identity und Access Management sind komplexe Themen mit vielen Prozessen und einer hohen Fehleranfälligkeit

Flexible Anpassung an vorhandene Infrastruktur

Keine vollumfänglichen Tools am Markt oder Nachteil des Vendor Lock-ins



### Ziel 1: Hoher Automatisierungsgrad



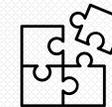
- Reduzierung menschlicher Aufwände & Fehler
- Schnelle Umsetzung von Berechtigungsvorgängen ohne lange Wartezeiten

### Ziel 2: Klarheit



- Überblick über Zuständigkeiten
- Alle Berechtigungen auf einen Blick
- Ablösung des Vorgesetzten als Genehmiger für Alles

### Ziel 3: Nahtlose Integration



- Einfache Integration in bestehende IT-Infrastruktur
- API Led Connectivity
- Manuelle Pflege weiterhin möglich

# PRIVIUS MODULE



## Privius User- & Fileservice Management

### Benutzermanagement

Onboarding    Offboarding

### Verzeichnismanagement

Fileserver    Data Ownership



## Privius Access Management

### JiT - Access

Privileged User

### Application Membership

AD-Groups    Exchange



## SAP Berechtigungsmanagement

### SAP Benutzer

Lifecycleprozesse

### SAP Rollenmanagement

Inventarisierung    Rollenpflege

## Privius Pakete

Privius Basic

Privius Access Management

(+) „SAP Berechtigungsmanagement“

Privius Advanced \*

\* „Privius Advanced“ wird aktuell im vergünstigten Set-Preis angeboten

02

# FALLBEISPIEL USER ONBOARDING



# Beispiel 1: User Onboarding

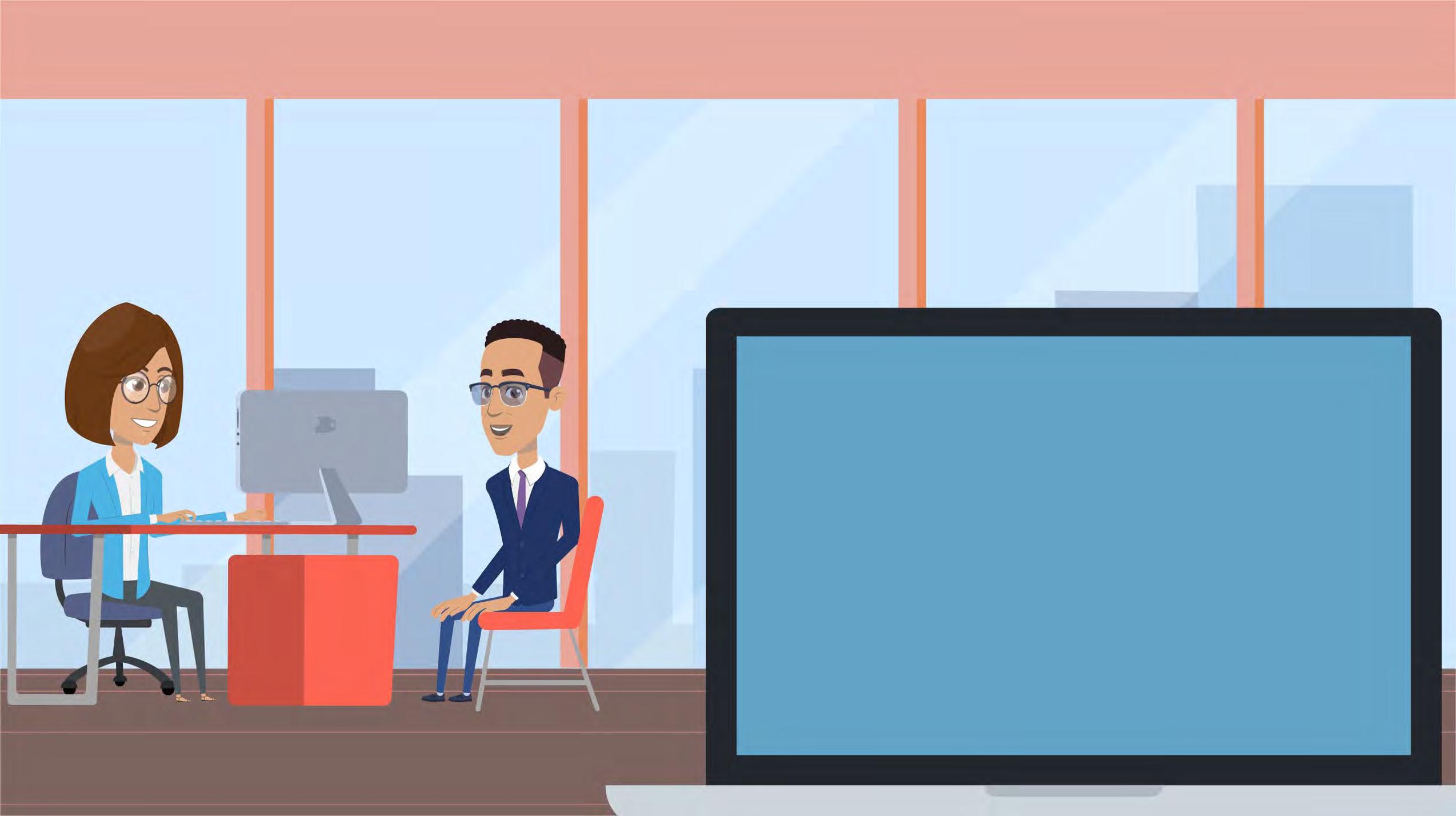
## DIE STORY

### Ausgangslage / Auslöser

Bei Eintritt eines neuen Mitarbeiters dauert es häufig mehrere Tage, bis er alle seine notwendigen Berechtigungen hat.

### Die Lösung

Geführter Prozess für neuen Mitarbeiter in Privivus



# 03 | SECURITY BY DESIGN



# SECURITY BY DESIGN

- ✓ Security By Design
  - ✓ Security als Priorität
  - ✓ In jeder Phase, vom Konzept über Entwicklung bis hin zum Betrieb
- ✓ Sichere Multi-Faktor-Authentifizierung
- ✓ Super-User Prinzip
- ✓ Automatisierte Sicherheitsprüfung des Quellcodes und der Abhängigkeiten auf Schwachstellen
- ✓ Architektonische Trennung der Berechtigungsvergabe von der Privius Applikation
  - ✓ Dedizierter Prozess mit erweiterter Absicherung
  - ✓ Eigene Laufzeitumgebung inklusive separatem Group Managed Service Account



# SECURITY BY DESIGN

## PRIVACY ALS SICHERE UMGEBUNG FÜR SENSIBLE BERECHTIGUNGEN

- ✓ Hohe Ausfallsicherheit und Datentrennung durch Containerisierung
- ✓ Schnelle Behebung von Sicherheitsproblemen durch Continuous Integration & Deployment (CI/CD Pipelines)
- ✓ Instanzendesign für einfache Mandantentrennung
- ✓ In der Praxis
  - ✓ Nur notwendige Berechtigungen vergeben
    - ✓ Zugriff auf Daten und Systeme auf geringsten Berechtigungen reduzieren
    - ✓ Berechtigungen nur vergeben wenn sie für den Moment benötigt werden
  - ✓ Von Kompromittierung ausgehen
    - ✓ Ausbreitung vermeiden und Ausmaß reduzieren
    - ✓ Ende zu Ende Verschlüsselung

# EINGESETZTE PLATTFORMEN

- Einsatz von Open Source Software
  - NodeJS (OpenJS Foundation)
  - ReactJS (Meta)
  - PostgreSQL (PostgreSQL Global Development Group)
  - Docker (Docker)
  - Kubernetes (Google / Cloud Native Computing Foundation)
  - git (Linus Torvalds / Junio Hamano)
  - Visual Studio Code (Microsoft)
- Orientierung an modernen Branchen-Standards wie
  - ESLint (OpenJS Foundation)
  - Airbnb Style Guide (Airbnb)
  - Material Design (Google)

- Light und Dark Mode
- Responsive Design
  - Vom kleinen Smartphone bis zum 32" Desktop
- Single Sign-On zusätzlich zur Anmeldung mit Passwort
- Benachrichtigungen in Privius und per E-Mail
  - Pro Kategorie deaktivierbar
- Abspeicherung von persönlichen Tabelleneinstellungen wie Filter, Sortierung, Spaltenauswahl, ...
- Unternehmensbezogene Einstellungen
- Pflege der Genehmiger auf jeder Ebene



04

# PRIVIUS SAP BERECHTIGUNGSMANAGEMENT



# WAS IST PRIVIUS ?

## SAP BERECHTIGUNGSMANAGEMENT

### SAP ROLLENPFLEGE

Inventarisierung aller SAP Rollen sowie bei Bedarf um Genehmigungsworkflow erweiterbar

### SAP ROLLENMANAGEMENT

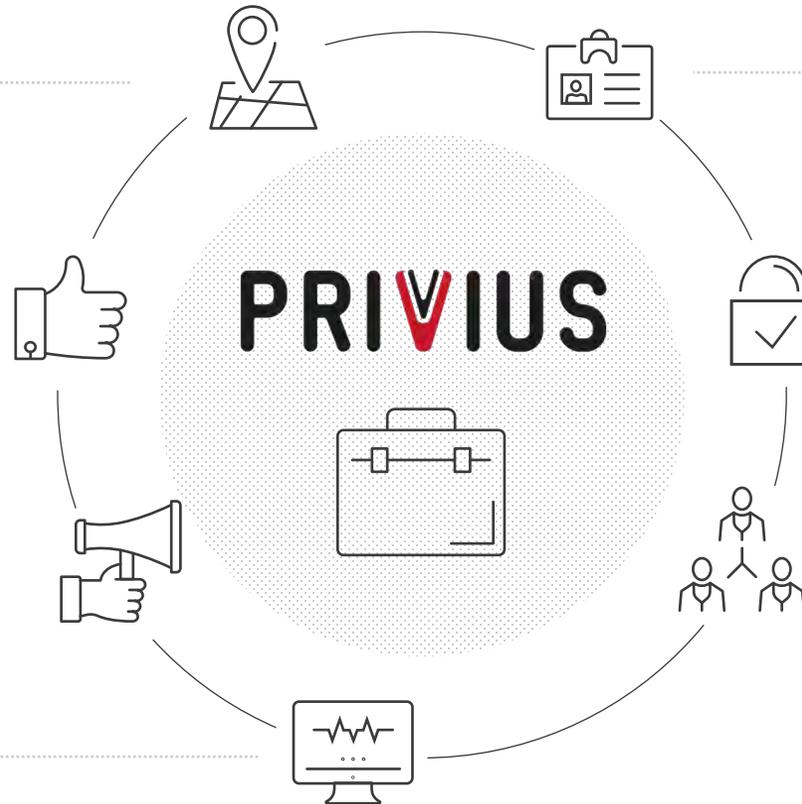
Zuweisen / Entfernen von SAP Rollen für einen Benutzer im definierten Tochtersystem

### PRIVIUS BUSINESSROLLEN

Design & Festlegung von definierten SAP Rollen zu Businessrollen zur vereinfachten Vergabe von Berechtigungen

### ÜBERBLICK

Übersicht über alle relevanten SAP – Berechtigungsrollen inkl. lesbarer Beschreibung



### INVENTARISIERUNG

Inventarisierung und Darstellung aller SAP Benutzer (in CUA & verwalteten Tochtersystemen)

### SAP ON-/OFF BOARDING

SAP-Benutzer anlegen & Löschen (in SAP CUA)

### SAP-BENUTZERPFLEGE

SAP-Benutzer sperren/entsperren, Pflege des Gültigkeitsdatum

## Beispiel 2: Temporäre SAP- Berechtigung

### DIE STORY

#### Ausgangslage / Auslöser

Für die Unterstützung in einem Projekt soll ein externer Mitarbeiter zeitlich begrenzten Zugang zu einem SAP-System erhalten.

#### Die Lösung

Geführter Prozess für die Beantragung & Genehmigung des externen Zugriffs



**PRIVIUS** 🔔<sup>7</sup> ⚙️ 👤

---

  
**Manuel Müller**

Startseite  
**Willkommen**

**Willkommen auf deinem Dashboard, Manuel!**

Startseite

- 🏠 Willkommen
- 📁 Berechtigungen
  - 📄 App-Berechtigungen ▾
  - 📁 Verzeichnisse ▾
  - 📁 Business-Rollen ▾
  - 👤 Active Directory ▾
  - 📄 SAP ▾
  - 📄 Vorgänge ▾
  - 📄 Audit ▾
- VERSION: DEV

**Vorgänge**

- 👤 Active Directory Benutzer  
Neuen Vorgang starten
- 📄 Active Directory Benutzer  
Veränderung  
Neuen Vorgang starten
- 📄 App-Berechtigungen  
Neuen Vorgang starten
- 🕒 Just-in-Time  
Neuen Vorgang starten
- 📄 Verzeichnisberechtigungen  
Neuen Vorgang starten
- 📄 SAP-Benutzer  
Neuen Vorgang starten

**Offene Genehmigungen**

- 👤 Active Directory Benutzer  
Genehmigung erteilen
- 📄 Active Directory Benutzer  
Veränderung  
Genehmigung erteilen
- 📄 App-Berechtigungen  
Genehmigung erteilen
- 🕒 Just-in-Time  
Genehmigung erteilen
- 📄 Verzeichnisberechtigungen  
Genehmigung erteilen
- 📄 SAP-Benutzer  
Genehmigung erteilen

**Administration**

- 👤 Privius Benutzer  
Benutzerpflege öffnen
- 📁 Abteilungen  
Abteilungspflege öffnen

# ROADMAP

---



# PRIVIUS MEILENSTEINE



# PRIVIUS

2021

2022

2023

2024

2025

Release Just-in-Time

# PRIVIUS

Q4 2023

Q1 2024

Q2 2024

Q3 2024

Q4 2024

SAP Berechtigungspflege Beta

# PRIVIUS ROADMAP

# PRIVIUS

Q1 2023

Q2 2024

Q3 2024

Q4 2024

Q1 2025

Release SAP Berechtigungsmanagement

# HABEN SIE FRAGEN?

(UND / ODER LUST AUF EINEN POC?)

---

## DENNIS WESTERS

items GmbH  
Hafenweg 7  
48155 Münster

+49 251 20 83-24 61  
+49 175 5975052  
d.westers@itemsnet.de

## MANUEL MÜLLER

items GmbH  
Hafenweg 7  
48155 Münster

+49 251 20 83-24 09  
+49 171 2049091  
manuel.mueller@itemsnet.de



# VIELEN DANK

---

[www.itemsnet.de](http://www.itemsnet.de)

 [@items\\_GmbH](https://twitter.com/items_GmbH)

