

Eviden DirX Identity Management for hybrid SAP-Environments

Gary Weissenbacher, Eviden

AGENDA

- 1. Introduction**
- 2. Eviden DirX Identity Management for SAP**
- 3. Best Practice: Siemens AG SAP - User Management and Access Governance**
- 4. Best Practice: Kubus IT (AOK) - SAP Interfaces to Identity Management**
- 5. Conclusions**

Today's Presenter

Gary Weissenbacher



Eviden Product Manager

Gary has over 22 years of experience in identity and access management, gained through his work as a consultant, software developer, and architect.

In his current role as Product Manager for DirX, he is responsible for the continuous development and innovation leadership of the Eviden DirX portfolio. His focus is on operational excellence in IAM and the strategic transformation to cloud-based architectures.

📍 Essen, Germany

✉ gary.weissenbacher@eviden.com

🌐 [LinkedIn: Gary Weissenbacher](#)

AGENDA

1. Introduction
- 2. Eviden DirX Identity Management for SAP**
3. Best Practice: Siemens AG SAP - User Management and Access Governance
4. Best Practice: Kubus IT (AOK) - SAP Interfaces to Identity Management
5. Conclusions

DirX - Identity Management for SAP

Why Identity Management? What does Eviden offer?

Identity & Access Management answers the 4 Questions

Who are you ?



Identity Lifecycle

Can you prove it ?



Authentifizierung

Which rights do I have ?



Autorisierung

Who did what, when, why ?



Compliance & Intelligence

Eviden DirX – Product Suite & Services



DirX Identity

User and Access Management aligned with Business Processes



DirX Access

Identity Federation, Access Management, and SSO for the Connected World



DirX Audit

Analytics and Intelligence for Identity and Access Management



DirX Directory

High-end LDAP / X.500 Directory Server and LDAP Proxy



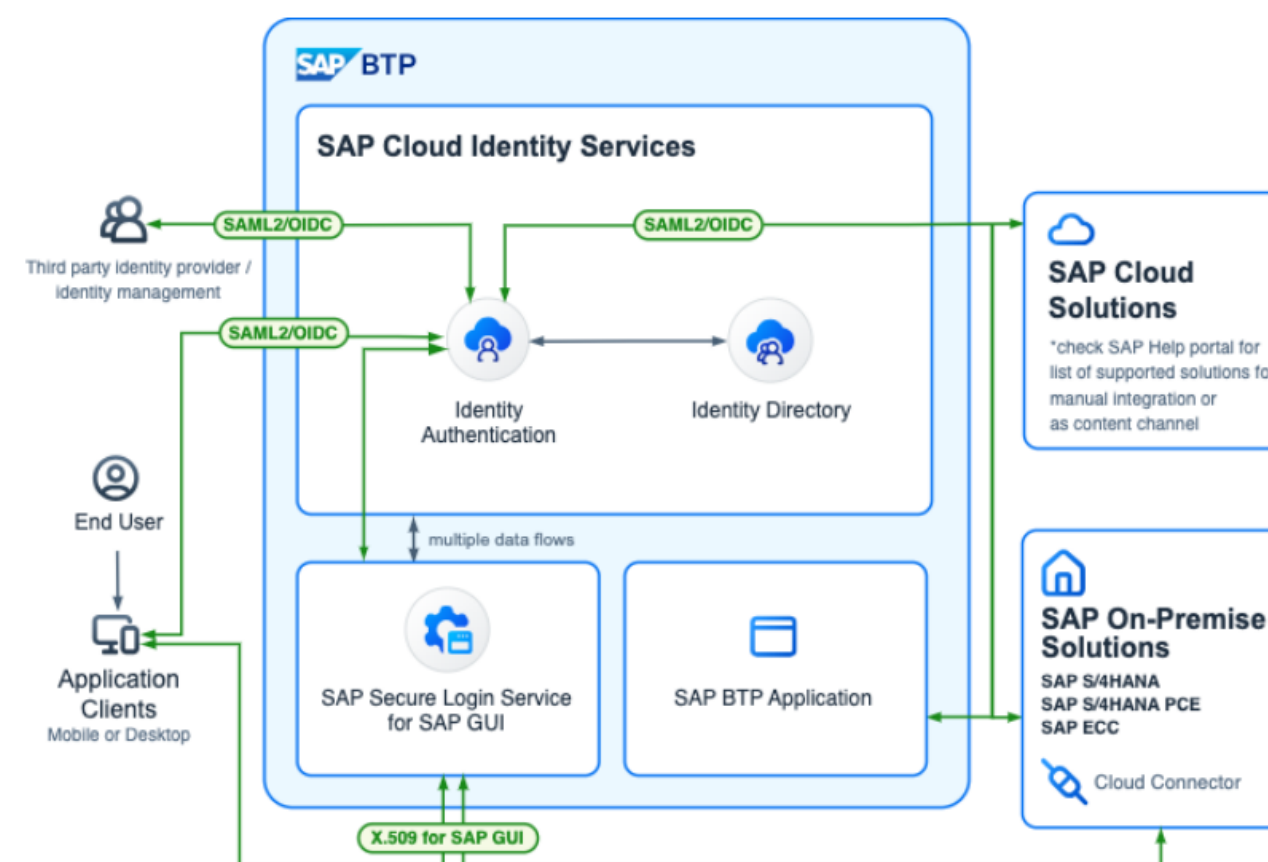
Professional Services & Consulting

DirX - Identity Management for SAP

Why Identity Management? What does Eviden offer?

- SAP is pursuing a cloud-only strategy.
- SAP Identity Management no longer plays a role in the Business Technology Platform.

Reference Architecture - Cloud leading Authentication

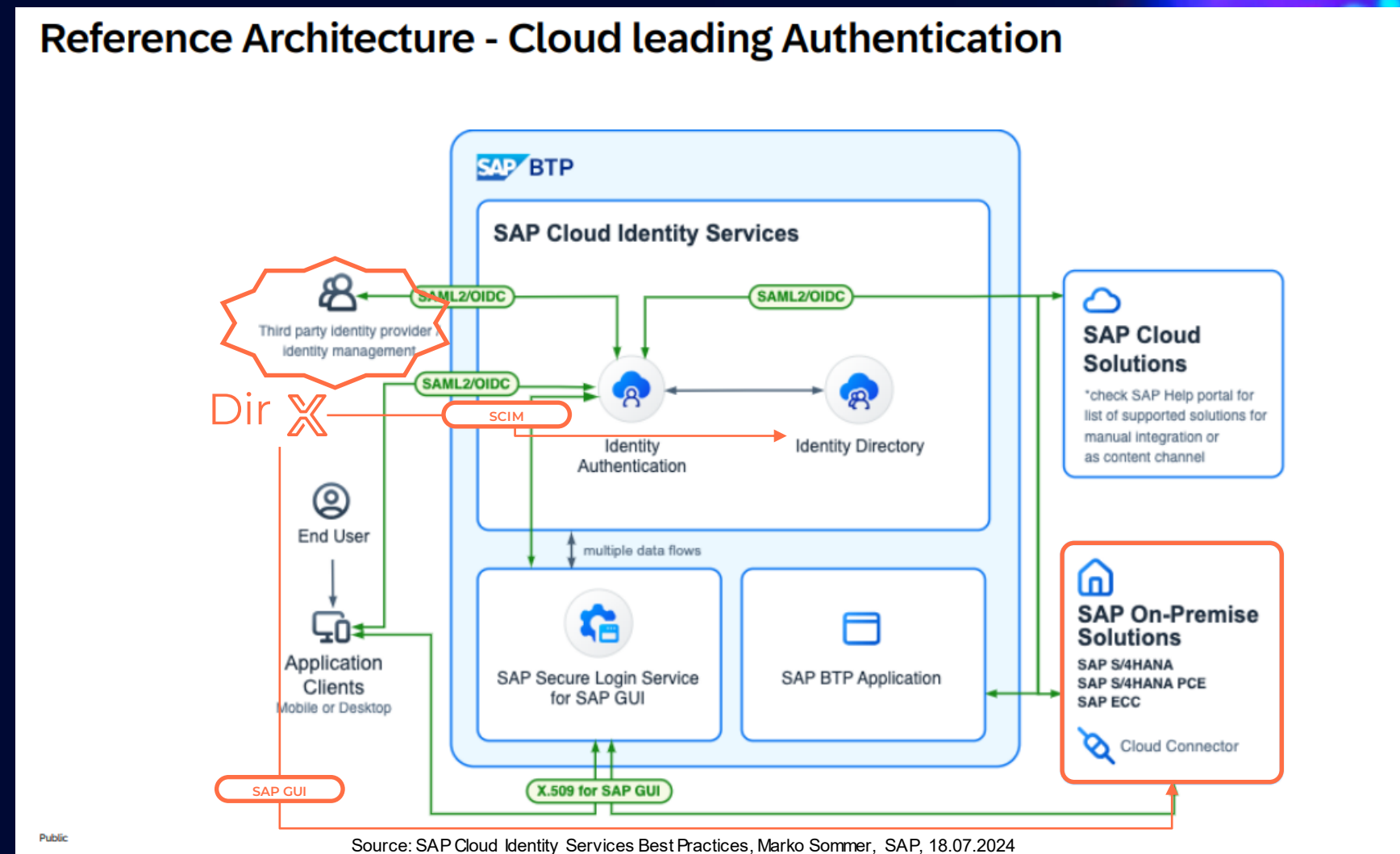


Source: SAP Cloud Identity Services Best Practices, Marko Sommer, SAP, 18.07.2024

DirX - Identity Management for SAP

Why Identity Management? What does Eviden offer?

- SAP is pursuing a cloud-only strategy.
- SAP Identity Management no longer plays a role in SAP cloud strategy
- **Eviden DirX** extends SAP Cloud Identity
- Services with the following capabilities::
 - **Identity Lifecycle**
 - **Role and Authorization Management**
 - Compliance through **Auditing and Reporting**
 - **Single Sign-On**
- **Eviden DirX** already provides these functions for SAP R/3
- **Eviden DirX** can therefore support SAP migration



Provisioning with SCIM

Standardized and extensible

What is SCIM?

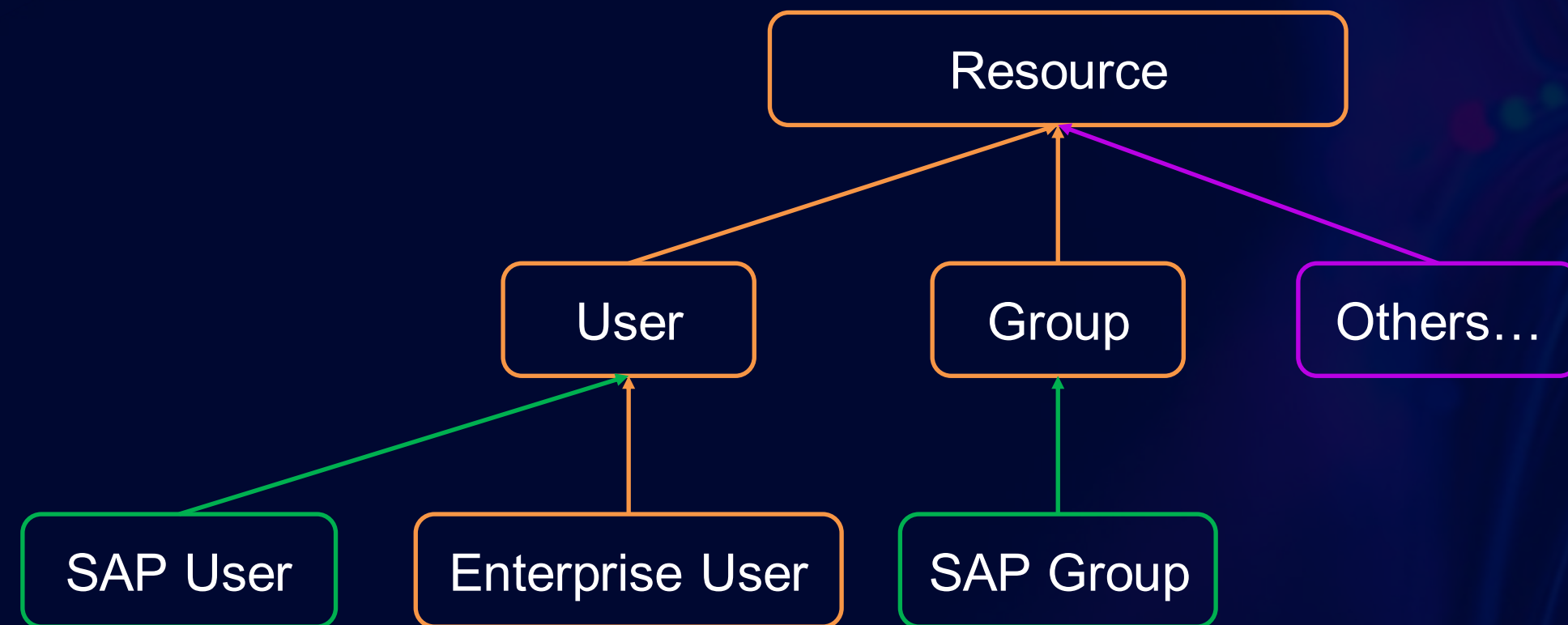
Open standard protocol for identity provisioning based on REST APIs.

SCIM 2.0 defines standard object model for users and groups.

Object model is extensible.

Consistent schema based on JSON.

Eliminating need for custom integrations for every app.



DirX - Identity Management for SAP

Managing daily tasks – The new Business User Interface

Based on

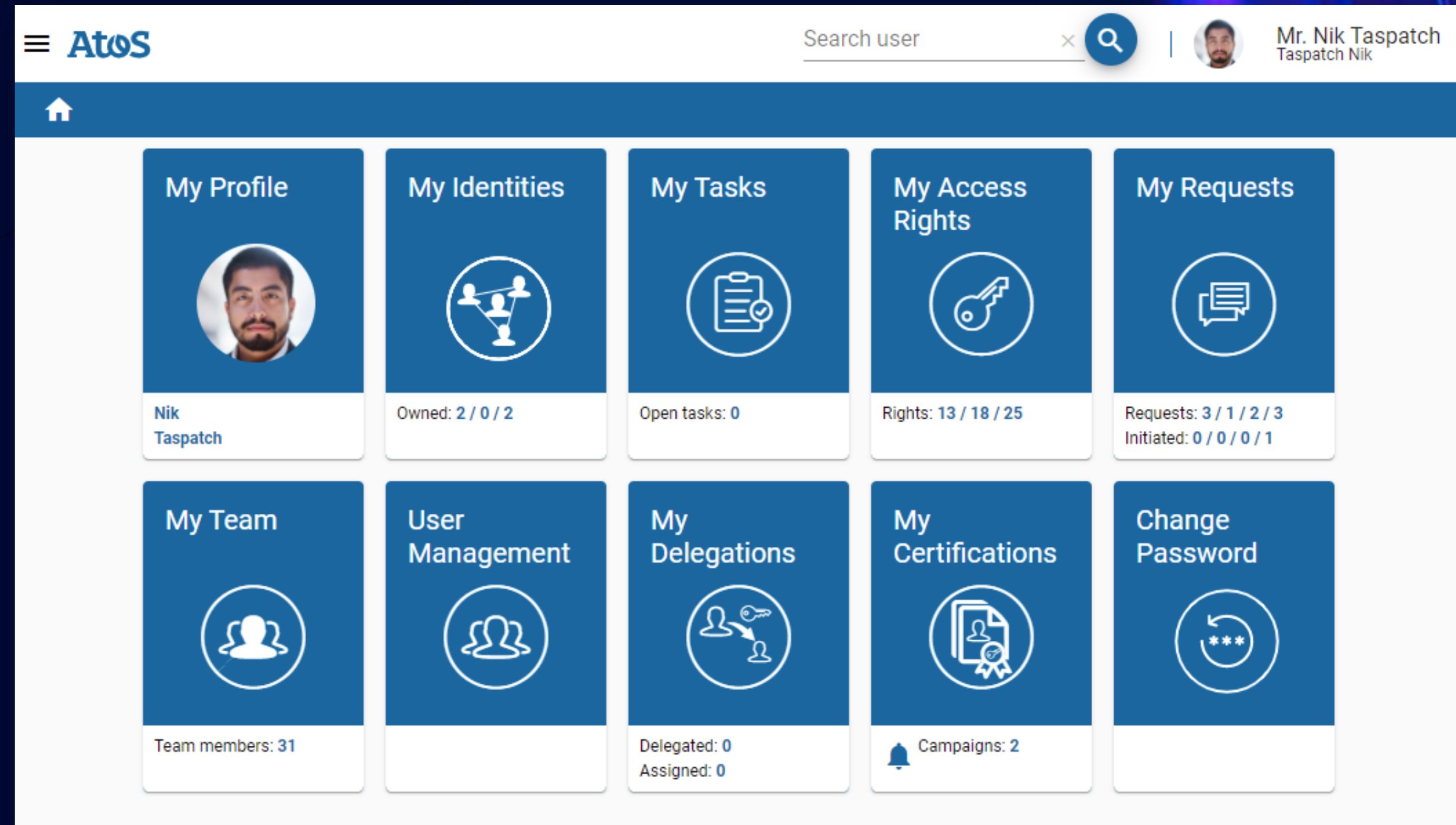
- ✓ HTML5
- ✓ RESTful APIs

Responsive Design

- ✓ Also ideal for Mobile Devices

Supports Accessibility

- ✓ WCAG 2.2 Lvl. AA
- ✓ BITV 2.0
- ✓ EN 301 549 V3.2.1



AGENDA

1. Introduction
2. Eviden DirX Identity Management for SAP
- 3. Best Practice: Siemens AG SAP - User Management and Access Governance**
4. Best Practice: Kubus IT (AOK) - SAP Interfaces to Identity Management
5. Conclusions

Best Practice

SIEMENS

Siemens in figures – as of 2025

318,000 employees, €88.4 billion in order intake

The businesses and services of Siemens AG

The Industrial Business – Digital Industries, Smart Infrastructure, Mobility, Siemens Healthineers and Siemens Advanta

The Services – Siemens Financial Services, Siemens Real Estate, Global Business Services, Foundational Technologies.

Initial situation and challenge

Ensuring compliance for critical applications



Decentralized user rights management led to:

- High manual effort for repetitive administrative tasks
- Error susceptibility due to system- and application-specific user interfaces and heterogeneous processes
- Lack of transparency regarding authorization assignment and individual rights profiles
- Problems with auditing the compliance of critical systems in SAP and other applications



Specifics of Siemens AG

- Complexity due to the business-specific requirements of Siemens divisions and differing role and process requirements
- High scalability requirements: Managing authorizations for **120+ IT systems, 100,000+ end users, 10,000+ roles, 700,000+ permissions**



Implementation Goals

- **Eviden DirX** is used as a central management tool to manage all critical access rights.
- It is designed as a **seamless self-service solution** that enables connected services to automate their processes and allows end users to easily request roles for all major IT systems themselves.

Solution – Functionality, Implementation

The following core processes are implemented based on standard Eviden DirX functions.

Joiner/Mover/Leaver process - automatic deletion of assignments for users who have left Siemens / in the case of transfers, a review of rights is requested.

Request/Approval Processes - Standardized two-stage approval process and dynamically assigned approver roles / Standard emails for open tasks in DirX (approval)

Self-management and delegation - Self-management of role parameters and delegations to manage absences (Approver)

Segregation of Duties - automated avoidance of assigning conflicting business roles

Recertification and audits - automatically triggered approval process to verify roles in a service or application / 8 standard reports per application cover all standard audit requests

Reconciliation in three phases - identify deviations, eliminate known deviations, eliminate unknown deviations

Automatic deactivation and reminder - Automatically deactivate user accounts after a defined period of inactivity (e.g., 90 days) / Reminder for expiring user roles (1/7/14 days before expiry)

Benefits – advantages and outlook

Automation and central control

By implementing **DirX Identity** Management:

- **Quality** was improved **through** the **automation** of manual processes.
- The number of recurring **manual** steps was **reduced**.
- **Transparency** within the company regarding access to IT systems was **increased**.
- The comprehensive standard functions **support compliance with regulatory requirements with minimal effort**.
- End-user **autonomy** was increased (self-service instead of role management by supervisors).
- Role management became more **flexible**, as quick and diverse adjustments to the automated processes are possible.

AGENDA

1. Introduction
2. Eviden DirX Identity Management for SAP
3. Best Practice: Siemens AG SAP - User Management and Access Governance
4. Best Practice: Kubus IT (AOK) – SAP Interfaces to Identity Management
5. Conclusions

Best Practice



kubus IT - IT for AOK health insurance company

Since 2008, kubus IT has been ensuring IT operations for 17,000 AOK users in the German states of Saxony, Thuringia, and Bavaria. Currently there are approximately 700 employees at kubus IT.

The businesses and services of kubus IT

The range of services extends from innovation and consulting to the organization and implementation of customized solutions to support the AOKs in achieving their goals.

Initial situation

The challenge

Manual user maintenance for user master data and groups was previously performed in SAP.

→ This was time-consuming, error-prone, and tied up personnel resources.

→ Due to limited personnel resources, the need arose to implement an automated solution.

The implementation of the IAM interface is being carried out in a "two-person project" with the goal of generating added value, reducing workload, and increasing performance through automation.

Scalability of the solution: kubus IT manages three separate SAP clients with the following systems and users:

- kubus IT itself with three CUA and five non-CUA systems and approximately 1,400 identities.
- AOK Bayern with five CUA systems and approximately 1,800 identities.
- AOK PLUS with three CUA and five non-CUA systems and approximately 7,800 identities.

Target Configuration

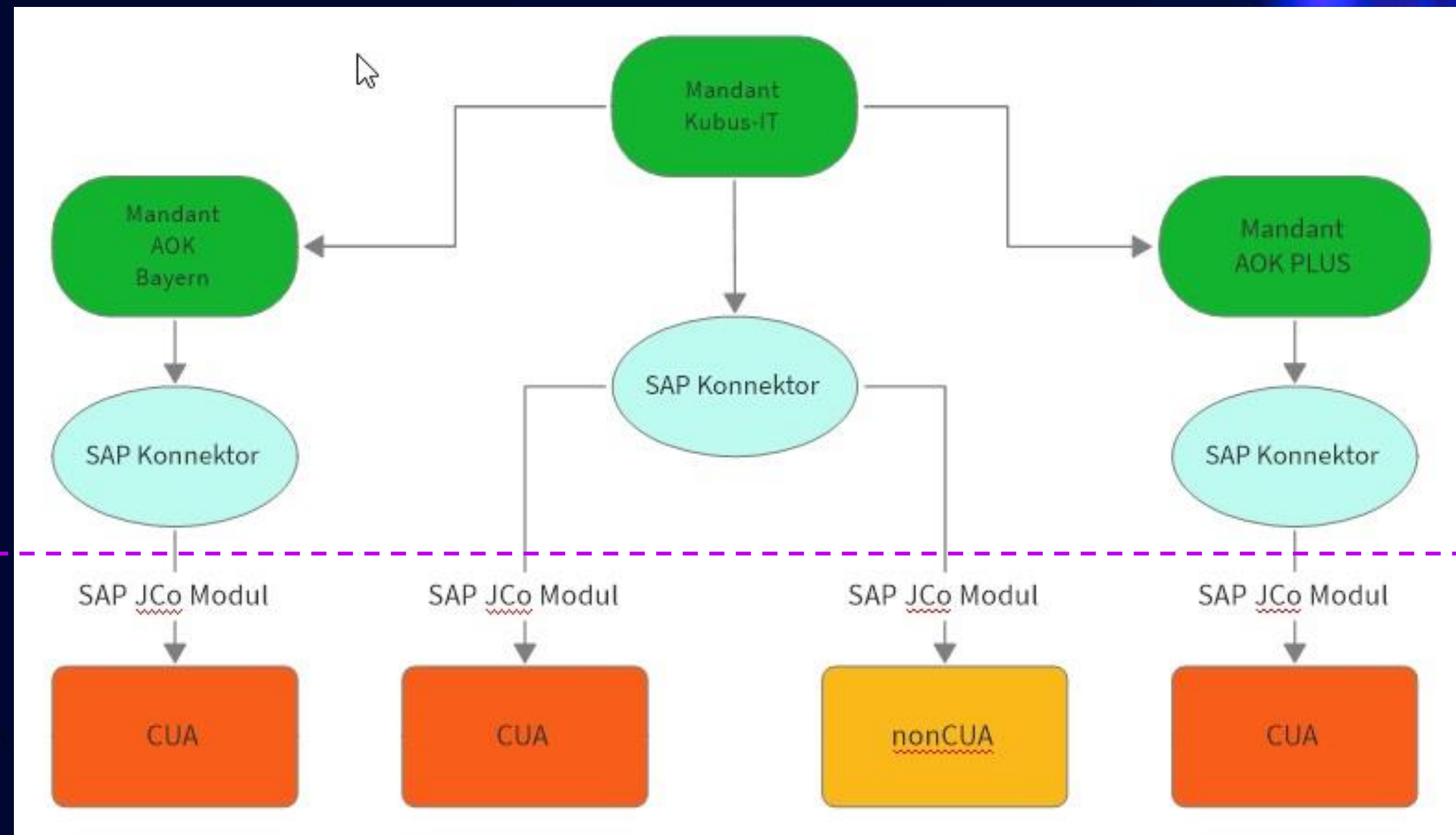
The solution

Identity Management

- **DirX Identity**
- **DirX Directory**
- **DirX Audit**

with SAP Connectors

SAP Tenants



Implementation and Next Steps

The solution

These points were particularly challenging during implementation

1. Setting up a cluster workflow for CUA and non-CUA
2. Correctly mapping attributes to SAP e.g., separating phone numbers
3. Creating **complex test procedures** to capture and test all use cases in the QA phase.
Example: Testing the interface and writing the set value to the SAP account during provisioning.

Outlook: further expansion phase

- kubus IT is currently developing the SAP connector with EVIDEN to provision the start and end dates for roles in the SAP systems.
- When importing SAP roles back from the target SAP system into the IDM system, the date values should also be transferred.
- Unfortunately, the planned implementation is delayed due to a lack of internal resources.

Benefits

Automation, Transparency and Auditability

30 Datensatz(-sätze) gefunden

Wann ▼	Ergebnis ▾	Quelle ▾	Wer ▾	Typ ▾	Operation ▾	[Objekt] Typ ▾	Details
20.2.2026 11:58:18	Erfolg	DirX Identity		manual	Update Object	Account	Account = ' (TargetSystem =
20.2.2026 11:50:29	Erfolg	DirX Identity		manual	Update Object	Account	Account = ' (TargetSystem =

Complete lifecycle of SAP accounts

- Ensuring the creation, modification, and deactivation of SAP accounts

Position-based permission with SAP groups

- Provisioning and deprovisioning are automated for each SAP system. This is essential for setting up the external identities required by SAP accounts, as the setup occurs in real time.

Audit-proof authorization

- Access rights management in SAP is auditable and transparent with DirX Audit.

Relieving SAP user administration of manual tasks



DirX Audit

AGENDA

1. Introduction
2. Eviden DirX Identity Management for SAP
3. Best Practice: Siemens AG SAP - User Management and Access Governance
4. Best Practice: Kubus IT (AOK) – SAP Interfaces to Identity Management
5. Conclusions

Conclusion

Eviden is a major player in the identity and access management market and offers standard-based leading-edge technology for scalability, reliability, and high availability

The **DirX** products help customers to ensure regulatory compliance, support business agility, and provide a proven return on investment

Eviden has a long track record of successful customer solutions implementation and is a reliable and globally acting partner for international enterprises and organizations

Questions?

Gary Weissenbacher, Eviden

gary.weissenbacher@eviden.com