

Best Practices to Enable Identity Access Management

Sonia Petrescu, Marko Sommer, SAP SE
June 17, 2025

Public

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Speakers



Sonia Petrescu

Product Manager
SAP Cloud Identity Services

Product Expert
Identity Lifecycle Management



Marko Sommer

Product Manager
SAP Cloud Identity Services

Product Expert
Single Sign-on

Agenda

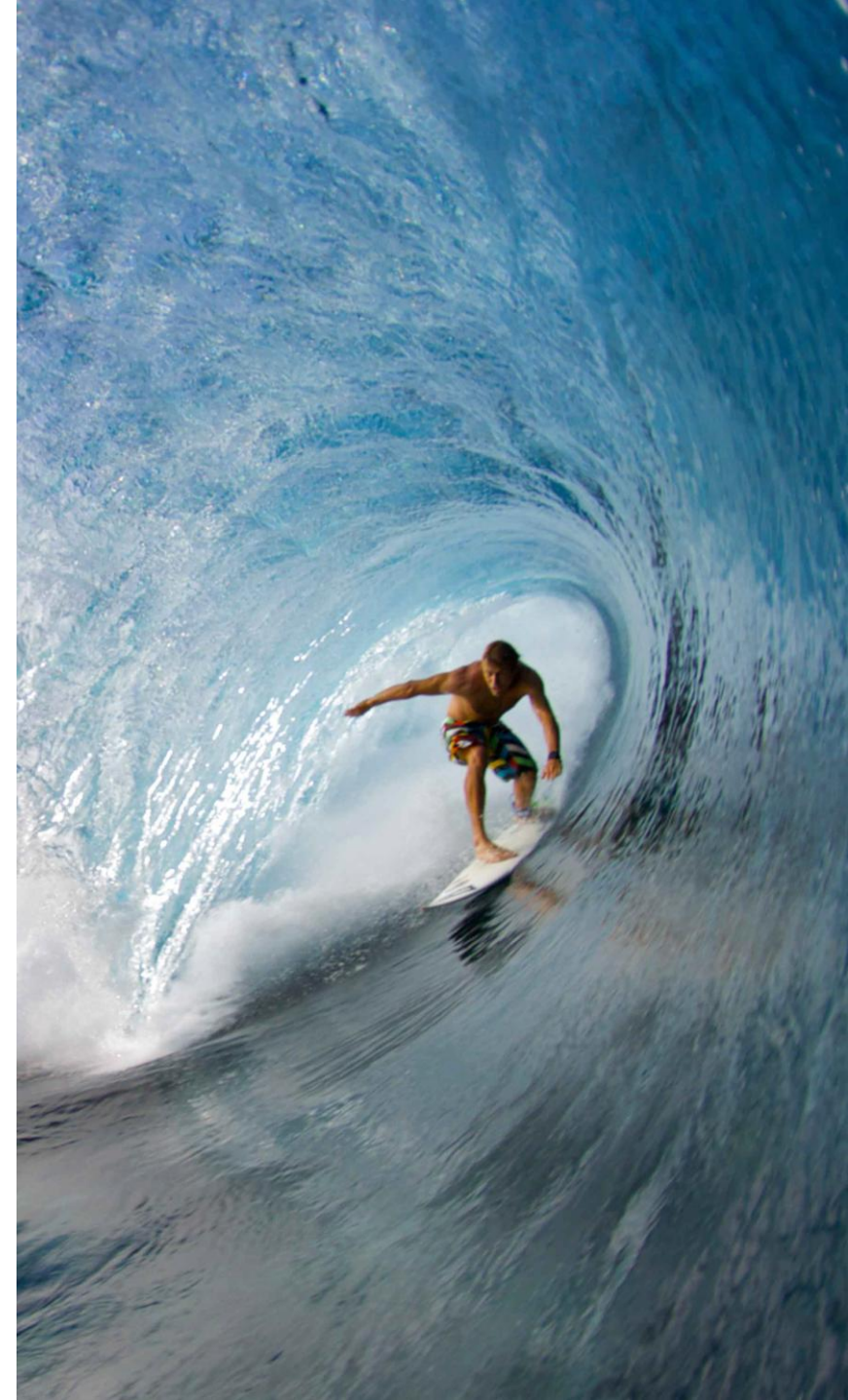
SAP Strategy

Identity Access Management

SAP Cloud Identity Services (SCI)

Best Practices to enable IAM

Demo



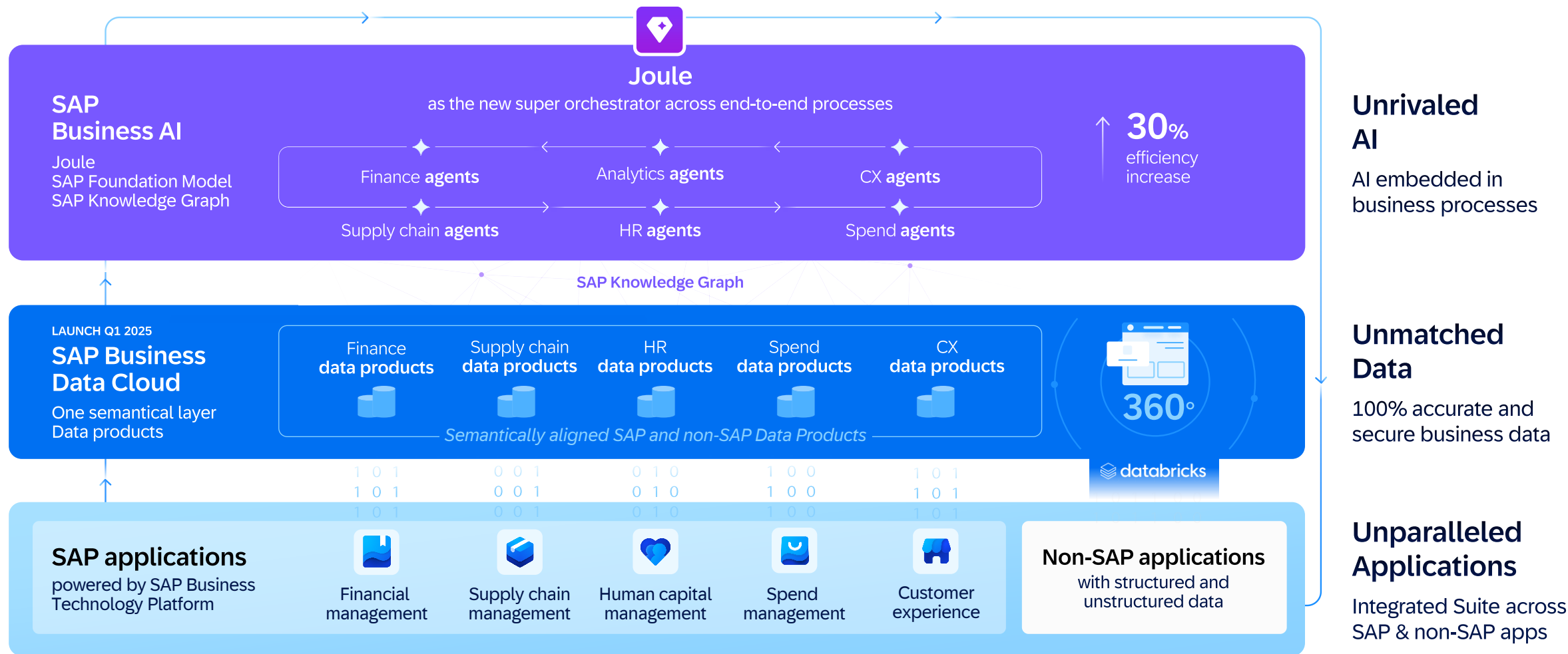
Our purpose

**Help the world
run better
and improve
people's lives**



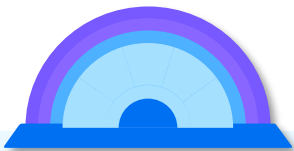
Realizing our vision by bringing together applications, data, and AI

SAP brings all components together to lead the way into the next era of enterprise management



Unparalleled Applications

Most comprehensive and integrated set of applications generating a wealth of business data



Industry-specific • Networked • Sustainable

Financial Management
Record to Report

Providing one view of the
Financials

Spend Management
Procure to Pay

Providing one view of the
Supplier

Supply Chain Management
Design to Operate

Providing one view of the
Product

Human Capital Management
Hire to Retire

Providing one view of the
Workforce

Customer Experience
Lead to Cash

Providing one view of the
Customer

Business Technology Platform

Integration • Extensibility

IAM for end-to-end Business Processes

The SAP Cloud Identity Services are a key component to ensure Consistent Security and Identity Management for SAP solutions with:

- Central user store for SAP cloud applications (Joule!)
- Consistent protocol support for customer IAM (SAML/OIDC, FIDO, SCIM, ...)
- Consistent security feature set for SAP cloud applications
- Authentication broker for multiple IdPs
- Application specific attribute mapping and enrichment of tokens by corporate IdP
- Feature support for non-standard integration scenarios
- Adoption of new technologies
e.g. step-up-authentication, context based authorizations

| Record to report


| Procure to pay


| Design to operate


| Hire to retire


| Lead to cash


Suite qualities


 Seamless user experience


 Consistent security and identity management

 One workflow inbox

 Aligned Domain Models and integration content

 Embedded and cross-product analytics

 Coordinated lifecycle management

 End-to-end process blueprints

Identity Access Management - Domains

IDENTITY LIFECYCLE



How users are being maintained, replicated, authorized from creation until deletion.

AUTHORIZATION



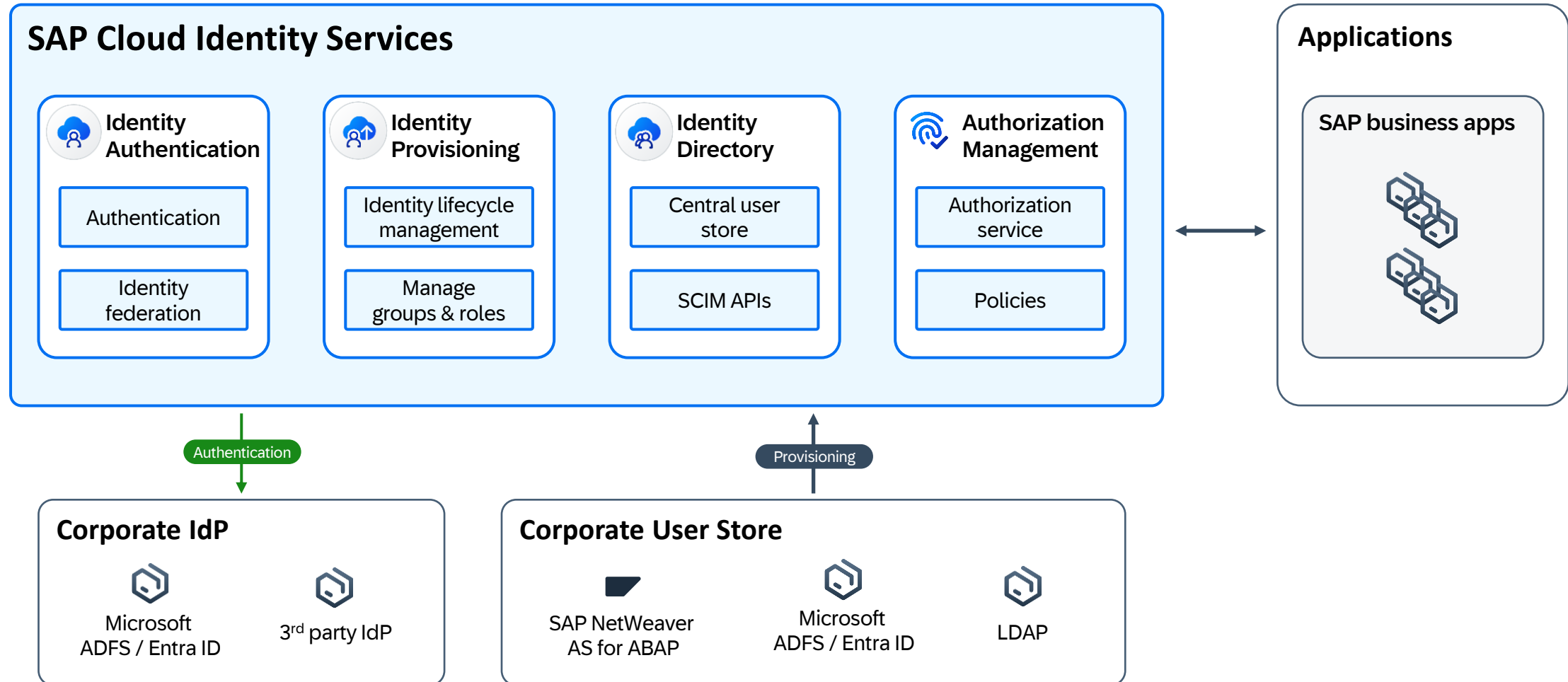
How authorizations are being maintained, analyzed from creation until deletion.

AUTHENTICATION



How users securely authenticate to applications with as few user-interactions as possible.

SAP Cloud Identity Services



Agenda

SAP Strategy

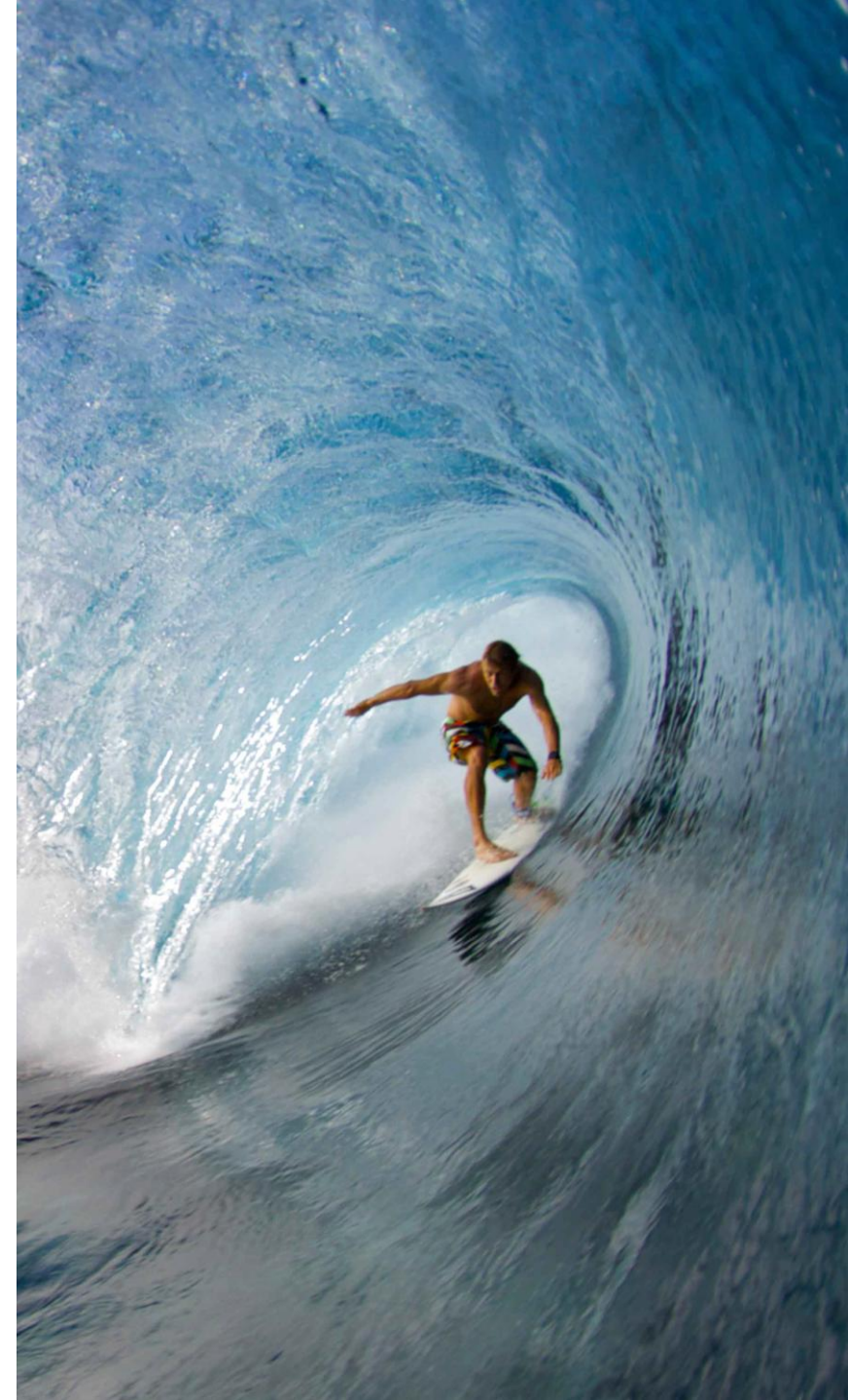
Identity Access Management

SAP Cloud Identity Services (SCI)

Best Practices to enable IAM

- Preparation
- Tenant Delivery & Persistence
- Identity Lifecycle Management
- MFA & Single Sign-on

Demo





Preparation - Checklist I/II

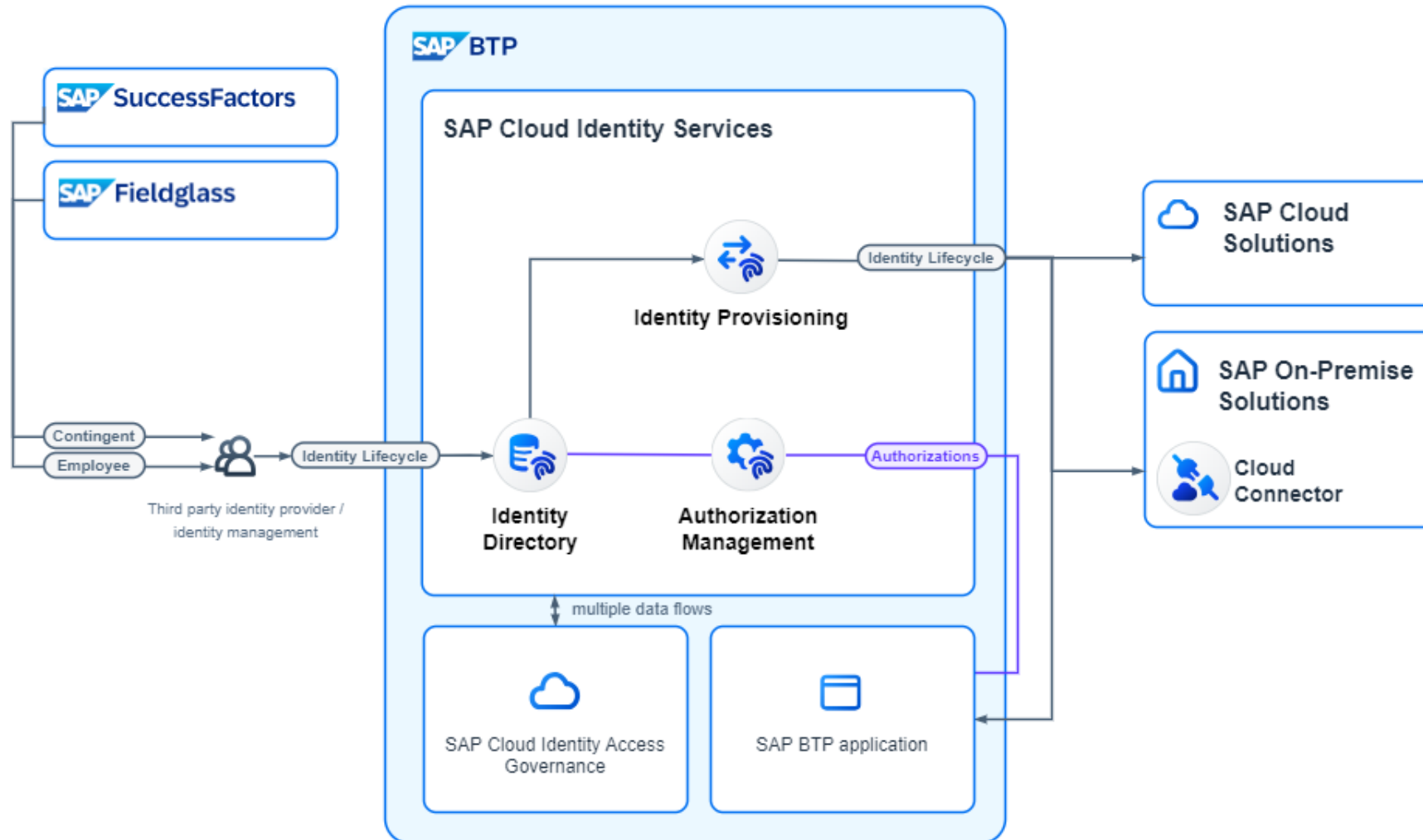
Best Practices – Landscape & Tenant Planning

- ❖ SAP reference architecture: one prod/one test SCI tenant ('default tenants')
- ❖ Lifetime of additional SCI tenants is bound to BTP or SuccessFactors
- ❖ Tenant domain: standard, common super domain or custom domain (3rd party cookie issue)
- ❖ Multi region landscape: beware of latency

Best Practices – User Identifiers

- ❖ Establish a unique user identifier across the SAP cloud landscape;
recommended: SAP Global User ID
- ❖ SAP Global User ID could be replaced with an established identifier, should be realized right from the start

SAP's IAM Reference Architecture - Identity Lifecycle





Preparation - Checklist II/II

Best Practices – Identity Lifecycle

- ↔ Definition of system of origin for each user type (employee/contractor/external/...)
- ↔ Avoid multiple systems of origin per user
- ↔ Holistic concept including access governance
- ↔ Identity Provisioning as the central tool to provision users to SAP (cloud) solutions

Best Practices – Single Sign-On

- ↔ SAML vs. OpenID Connect
 - ↔ In general both SSO protocols are fine, but the ‘trend’ is towards OIDC
 - ↔ OpenID Connect has advantages when it comes to principal propagation
- ↔ whenever possible consider parent-child setup to simplify configuration efforts
- ↔ SSO with SAP GUI should be established with SAP Secure Login Service



Tenant Delivery & Persistence

Best Practices - Tenant Delivery & Integration

↔ Tenant Delivery

- ↔ Fully preconfigured, e.g. for S/4 HANA Cloud, Integrated Business Planning
- ↔ Self-service, e.g. BTP cockpit, BTP boosters, SuccessFactors Upgrade Center, SAP for Me
- ↔ Overview about existing tenants: [help docu - viewing-assigned-tenants-and-administrators](#)

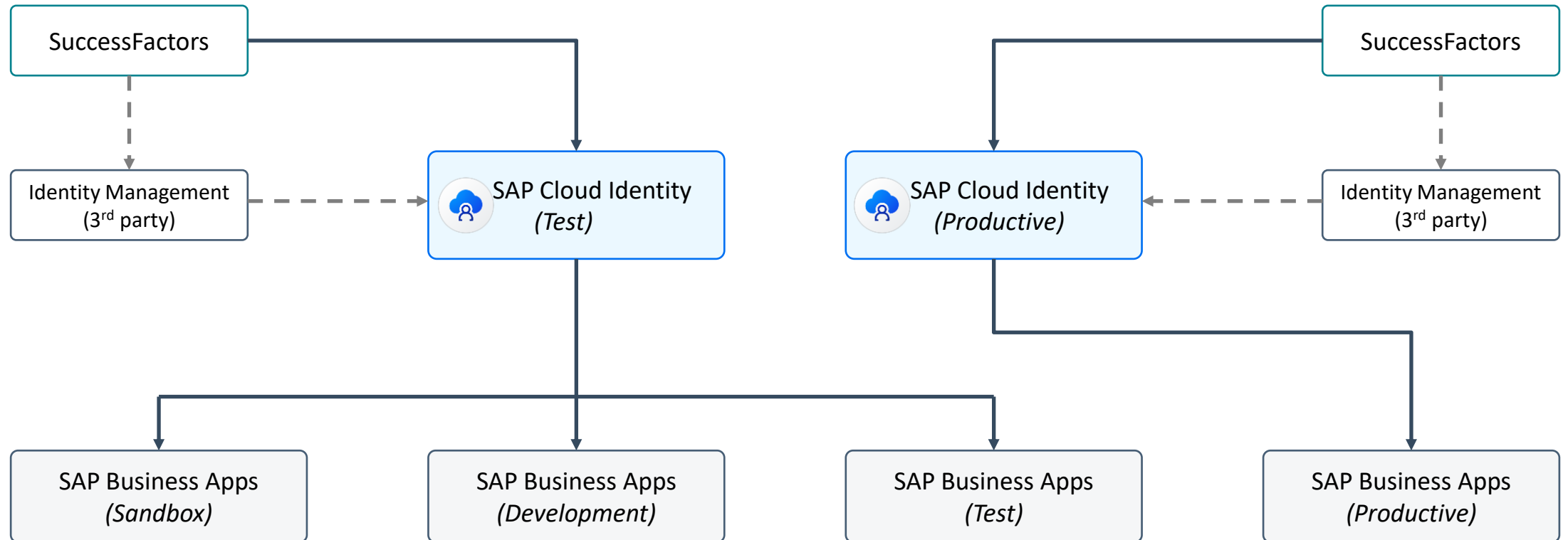
↔ Tier recommendations

- ↔ SCI prod ↔ prod. applications & SCI test ↔ test/QA/sandbox
- ↔ SCI prod ↔ prod/test/QA applications & SCI test ↔ sandbox
- ↔ [3-System Landscape S/4HANA Cloud](#) & [IAM for S/4HANA Cloud](#)

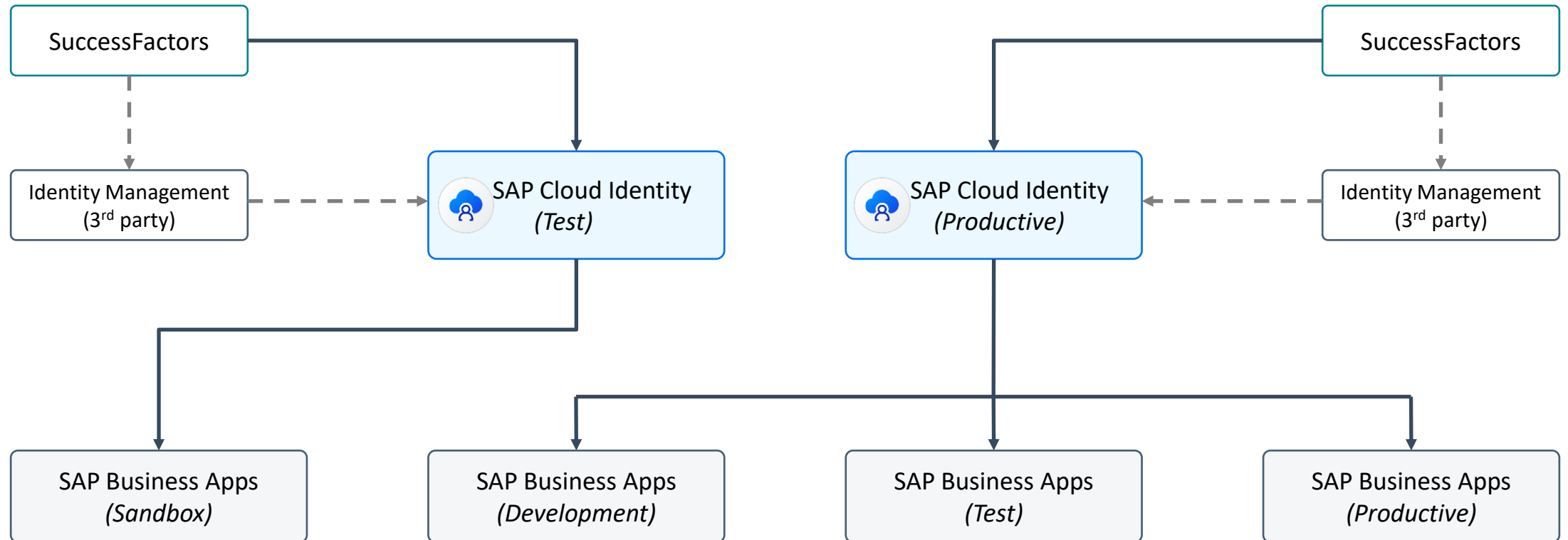
Best Practices - Persistence

- ↔ Identity Directory as central user store for SAP applications
- ↔ User persistence in SCI is a precondition for Joule and applications with embedded Analytics

Tier Recommendations - Productive IAM manages productive Applications



Tier Recommendations - Productive IAM manages dev/test/prod



Agenda

SAP Strategy

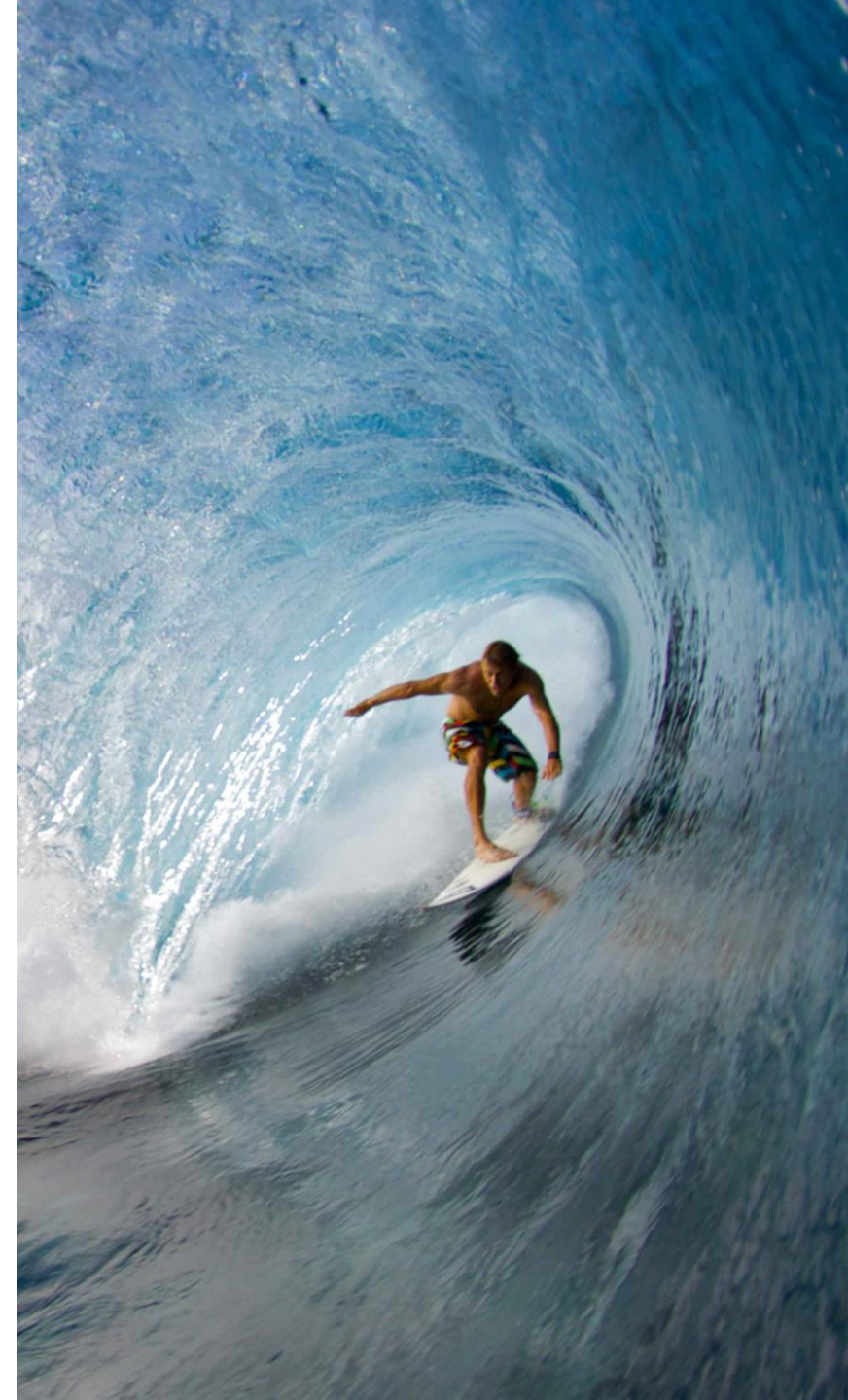
Identity Access Management

SAP Cloud Identity Services (SCI)

Best Practices to enable IAM

- Preparation
- Tenant Delivery & Persistence
- Identity Lifecycle Management
- MFA & Single Sign-on

Demo





Identity Lifecycle & Authorization Management

Best Practices - Identity Lifecycle Management (B2E)

- ↔ use either HCM or an IDM solution as leading system
- ↔ users should be provisioned to Identity Directory and then via IPS to SAP cloud applications
- ↔ 'old' IPS tenants on BTP Neo infrastructure should be migrated to the SCl infrastructure
- ↔ do not use BasicAuthentication for provisioning scenarios in productive landscapes but X.509 based authentication with automatic certificate rotation
- ↔ Large scale user provisioning: use bulk mode whenever possible

Best Practices - Authorization Management (central access governance)

- ↔ Provision approved authorizations from the Identity Access Governance solution via SAP Cloud Identity Directory to SAP cloud solutions



Best Practices – Multi-factor Authentication (MFA) & Single Sign-On

Best Practices - Authentication

- ↔ Consider passwordless authentication methods
- ↔ Configure custom password policies according to corporate security concept
- ↔ Multi-factor Authentication
 - ↔ preferred: WebAuthentication/FIDO or TOTP
 - ↔ SMS and RSA require a license for 3rd party products
- ↔ Troubleshooting: SAML tracer, troubleshooting logs

Best Practices – Single Sign-on with corporate identity provider

- ↔ SAML vs. OpenID Connect: if possible, go for OIDC
- ↔ SSO for one application with multiple identity providers
 - ↔ Use conditional authentication configuration
 - ↔ To avoid (interim) login screen: use IdP initiated SSO or SP initiated SSO with IdP parameter
- ↔ For corporate users both 1st and 2nd factor should be validated with the corporate IdP

Agenda

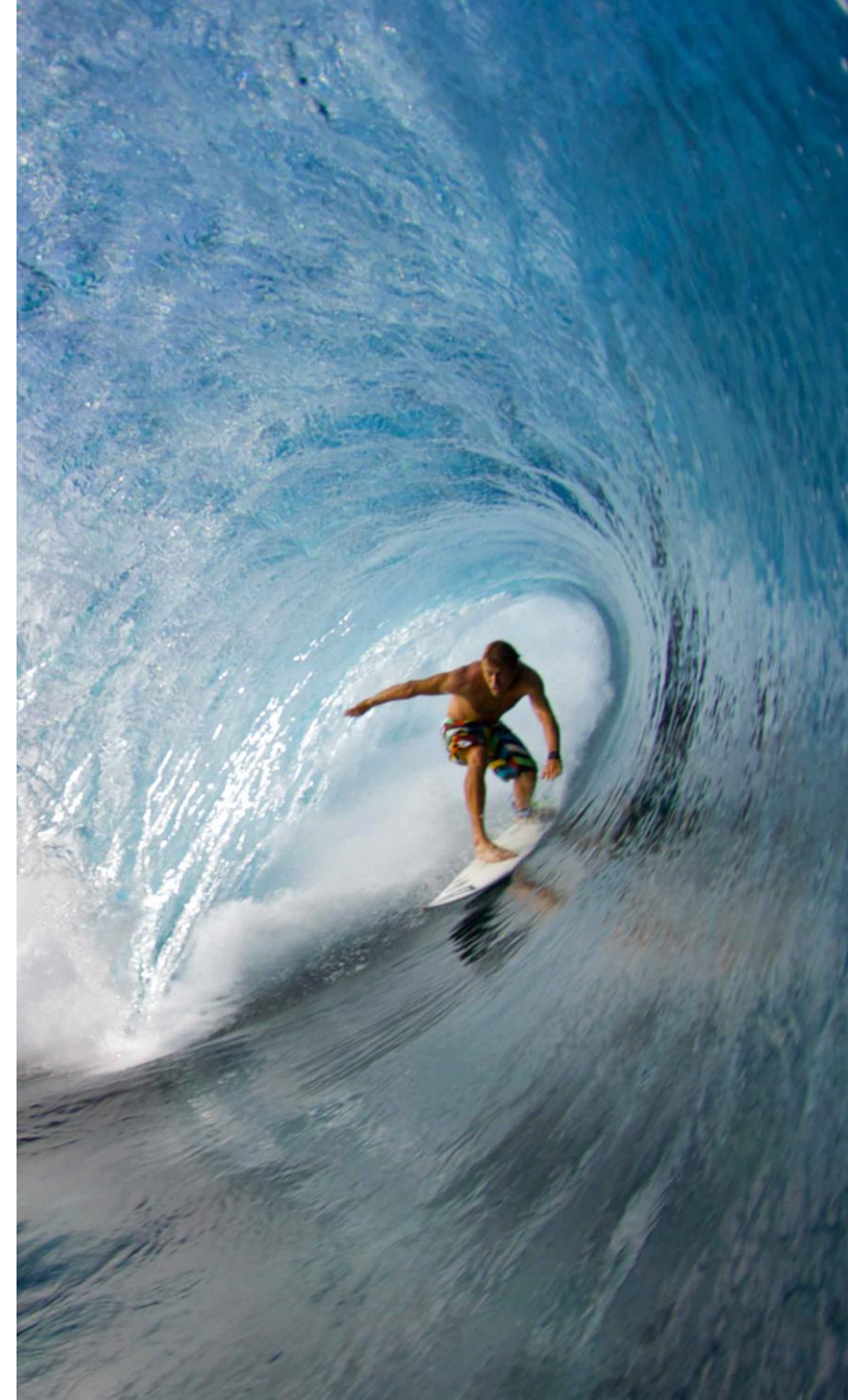
SAP Strategy

Identity Access Management

SAP Cloud Identity Services (SCI)

Best Practices to enable IAM

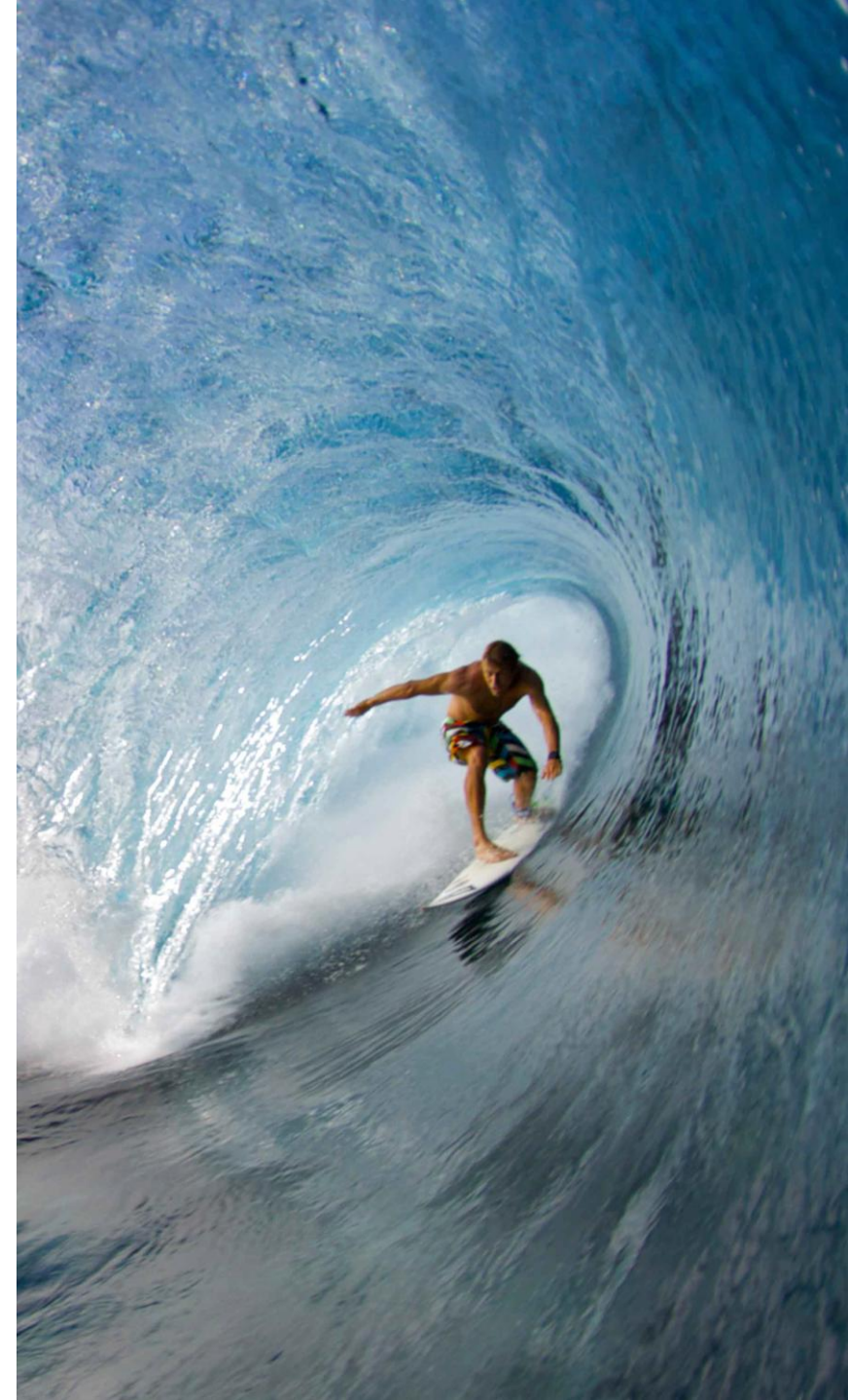
Demo



Further Information

SAP Cloud Identity Services Best Practices

- [CIO Guide: Identity Lifecycle in SAP Landscapes](#)
- [SCI Getting Started - Initial Setup \(SAP Help Portal\)](#)
- [Establish SSO to your cloud solutions \(Discover Center Mission\)](#)
- [Best Practices for BTP - Onboard to SCI \(SAP Help Portal\)](#)
- [Security Recommendations \(SAP Help Portal\)](#)
- [IAM Reference Architectures](#)



Thank you.

Contact information:

Sonia Petrescu

sonia.petrescu@sap.com

Marko Sommer

marko.sommer@sap.com



SAP Bring out your best.

Follow us



www.sap.com/contactsap

© 2025 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/trademark for additional trademark information and notices.