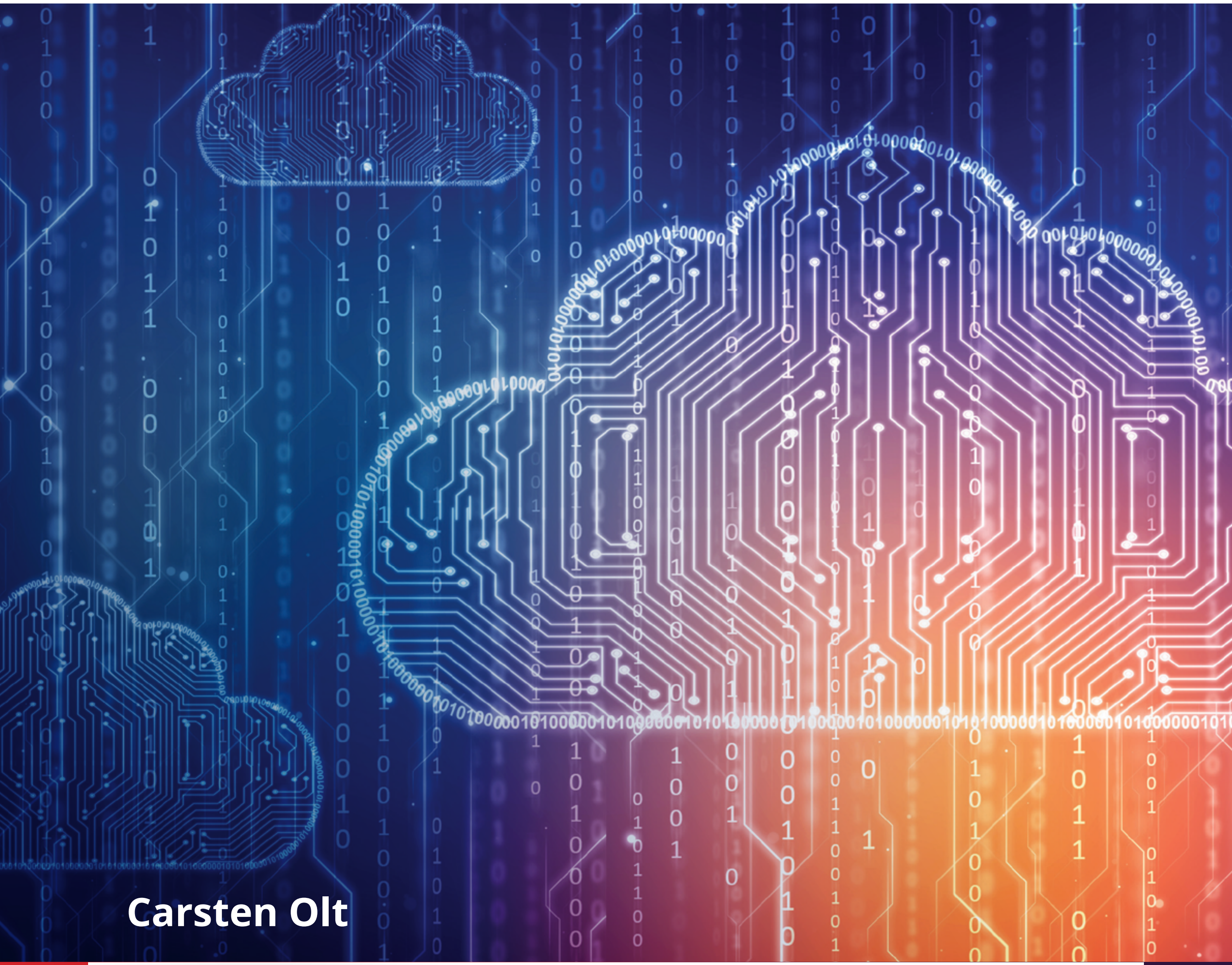


Carsten Olt

Xiting E-Book

# SAP Cloud Identity Services

## Overview, best practices and typical use cases

www.xiting.com

# Tabel of Contents

# Introduction

SAP Cloud Identity Services is a set of services within SAP Business Technology Platform (SAP BTP) that allows for seamless integration of identity and access management (IAM) between systems. The main goal is to provide a secure and seamless single sign-on (SSO) experience across systems.

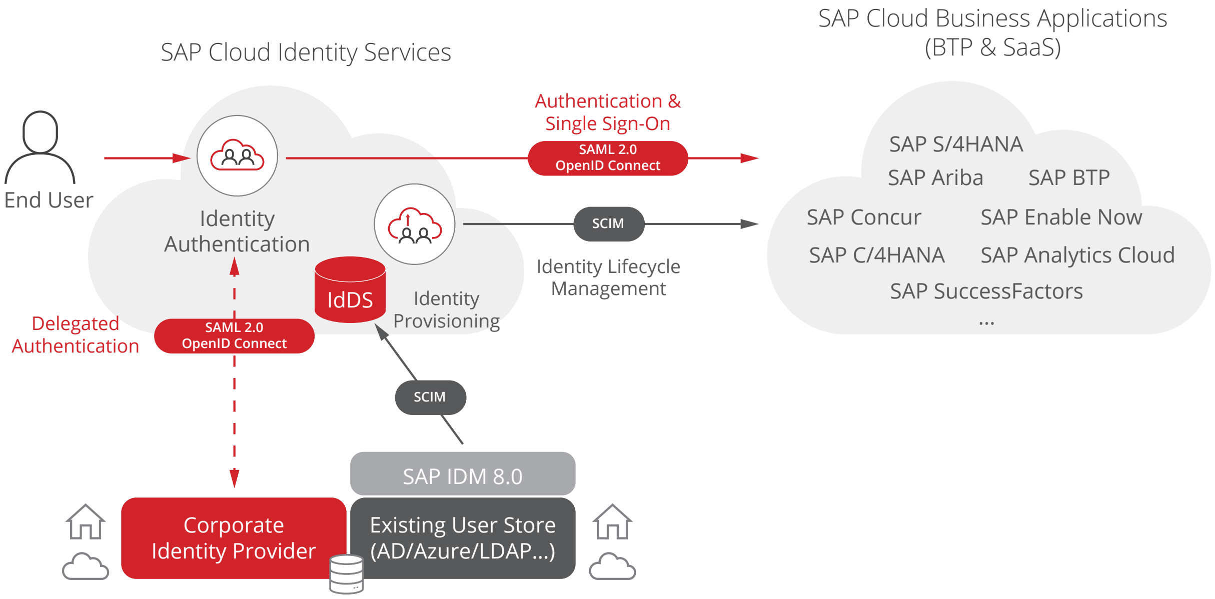
This eBook serves as a condensed overview of SAP Cloud Identity Services and is designed for solution architects, project managers, SAP consultants, and IDM administrators who want to gain a quick understanding of the essentials of the service. Additionally, it includes Xiting best practices for the service and outlines the common use cases for the solution.

SAP Cloud Identity Services provides a standard for authentication and user administration as core services of SAP BTP. It allows for the centralization of user identities to ensure secure access to all applications within the SAP cloud universe and automate user administration.

In a constantly growing hybrid SAP landscape, it is crucial to manage and consolidate all identities in one place. SAP Cloud Identity Services supports industry standards like SCIM, SAML 2.0, OAuth2, and OpenID Connect, which allows for flexible deployment scenarios and integration options into existing IAM systems in a multi-vendor landscape.

Overall, SAP Cloud Identity Services provides a foundation for secure and efficient IAM integration between systems, which is essential for every SAP organization today.

SAP Cloud Identity (SCI) services are public cloud services provided by SAP, available in various regions globally. These services consist of two primary components: **Identity Authentication (IAS)** and **Identity Provisioning (IPS)**, which are essential building blocks for IAM in hybrid SAP landscapes. Both components are built on the same technology stack and are included in many SaaS solutions offered by SAP SE or available as a bundle.



IAS provides authentication services, including secure single sign-on, multi-factor authentication, and social media authentication. IPS, on the other hand, is responsible for provisioning user identities to various SAP applications that have their user store.

Together they enable organizations to streamline IAM processes and improve the user experience by providing a single sign-on experience across systems while ensuring data security. Additionally, these services are built with the flexibility to integrate with existing IAM systems, making them a valuable addition to any SAP organization looking to enhance their IAM capabilities.

The **SAP Cloud Identity Authentication Service (IAS)** represents a central identity provider. Here all SAP cloud applications are connected to consolidate trust management. The aim of this approach is to standardize the onboarding of additional SAP cloud applications. This simplifies the entire onboarding process for new SAP applications. For user authentication IAS uses common standards such as Security Assertion Markup Language 2.0 (SAML 2.0) and OpenID Connect to provide ID-Federation.

The **SAP Cloud Identity Provisioning Service (IPS)** is used to provision user identities from a specific source system to the Identity Directory service based on preferences and filter rules. This component ensures the ID lifecycle.

The **Identity Directory Service (IdDS)** is used by the two services IAS and IPS as a user database in the SAP cloud environment. Using a group concept customers can automate the provision of users and groups to SAP cloud applications. Changes such as the creation of a new employee, adjustments to user data and group assignments or the deactivation of an account are detected and automatically implemented based on jobs running in scheduled intervals.

| Identity Authentication<br>**IAS** | Identity Directory<br>**IdDS** | Identity Provisioning<br>**IPS** |
|---|---|---|
| ■ Serves as the main identity provider for SAP cloud and on-premises applications.<br>■ Consolidates and automates trust management.<br>■ Standardizes the onboarding process of new SAP cloud applications.<br>■ Supports common standards like SAML 2.0 and OpenID Connect.<br>■ Can be easily connected to the existing identity provider supporting proxy-mode and identity federation scenarios. | ■ Central user database used by the SAP cloud services IAS and IPS<br>■ Foundation for identity lifecycle.<br>■ SCIM 2.0 REST API to support programmable access.<br>■ Supports 20 custom schemas with 20 custom attributes each.<br>■ User persistency essential for many features and SAP cloud applications, including SAP SuccessFactors and SAP Task Center.<br>■ Owns attributes like the SAP Global User ID and can be enriched with attributes from other source systems. | ■ ID lifecycle for cloud-based SAP applications.<br>■ Integrates with SAP Identity Management for hybrid landscapes and non-SAP IDM solutions.<br>■ Supports the industry-standard protocol SCIM.<br>■ Dedicated connectors for most important applications - normalizes system interfaces to the SCIM standard.<br>■ Provides a powerful JSON transformation framework.<br>■ Has no feature parity and does not aim to replace IDM solutions. |

## Benefits of using SAP Cloud Identity Services include:

1. **Centralized identity management:** SAP Cloud Identity Services provide a central repository for managing user identities, which makes it easier to manage access rights and privileges across multiple systems.

2. **Improved efficiency:** By using the Identity Directory (IdDS) as a central repository for all SAP user identities, organizations can reduce administrative overhead and automate processes. All users are stored in a central location without having to manage and update user identities in each service.

3. **Single sign-on:** By storing user identities in the identity directory, you can enable single sign-on (SSO) for users across different SAP applications and services. This provides a seamless and secure user experience, as users only need to sign in once to access all the SAP services they need.

4. **Integration with other systems:** By persisting user identities in the identity directory, you can more easily integrate SAP services with other systems, such as authentication providers, security information and event management (SIEM) tools, and identity management solutions.  This reduces the risk of errors or inconsistencies.

5. **Improved user experience:** The SAP Global User ID (UUID) makes it easier for users to access multiple systems with a single sign-on, providing a more seamless and efficient experience.

6. **Improved governance:** SAP Cloud Identity Services combined with other services such as SAP Cloud Identity Access Governance (IAG), provide tools and capabilities for auditing and reporting on user access, helping organizations to meet regulatory and compliance requirements.