SAP Cloud Identity Service
Secure Authentication, Single Sign-On and User Management in the Cloud

December 2015
Introduction
SAP Cloud Identity Service
In the SAP IT application security product portfolio

- SAP Single Sign-On
  - Make it simple for users to do what they are allowed to do.

- SAP Identity Management
  - Know your users and what they can do.

- SAP Access Control
  - Ensure corporate compliance to regulatory requirements.

- SAP Cloud Identity Service
  - Manage the identity life-cycle in the cloud.

- SAP Enterprise Threat Detection
  - Counter possible threats and identify attacks.

- Add-On for Code Vulnerability Analysis
  - Find and correct vulnerabilities in customer code.

Platform Security
- Make sure that SAP solutions run securely

SAP HANA Platform

SAP NetWeaver Application Server

- SAP Business Suite
- SAP Cloud Applications
- SAP Mobile Applications
- 3rd Party Systems
SAP Cloud Identity Service

In the SAP HANA® Cloud Platform landscape

On-Premise / Managed Cloud

- SAP S/4HANA
- SAP Business Suite
- SAP Business Warehouse

SAP HANA® Cloud Platform (PaaS)

Runtimes
- Java
- HANA XS
- HTML
- node.js

Capabilities
- Integration
- User Experience (UX)
- Analytics
- Internet of Things
- Security
- Collaboration
- Mobile
- Business Services
- Data & Storage
- Dev & Ops

SAP Data Centers

HCP Servers (IaaS)

SaaS

- SAP S/4HANA
- SuccessFactors
- SAP Cloud for Customer
- Ariba
- Hybris
- Concur
- ...

1) beta functionality  2) planned innovations / future direction

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
Today’s world is...
Today

...anytime and anywhere, business people....
Today

present  share  decide  review  purchase
learn  approve  write  read  negotiate
view  sell  travel
Today

...need access to many applications...

...at their workplace or outside

"80% of employees report needing access to work documents from outside the office"¹

¹ BusinessWire.com “New Survey Finds Over Half of Employees Use Unauthorized Consumer Based File-Sharing Apps at Work” (SkyDox survey)
Today

...how many times a day

... how many passwords to remember?
Today

“2014 is the first year when the majority of workloads (51%) shift to the cloud”


Tomorrow

Cloud applications bring competitive advantage to businesses

“By 2018, at Least Half of IT Spending Will Be Cloud Based, Reaching 60% of All IT Infrastructure and 60-70% of All Software, Services, and Technology Spending by 2020”

Product Overview
SAP Cloud Identity Service
Product overview

SAP Cloud Identity service:
- Secure access via the internet
- Web & mobile Single Sign-On
- Identity Federation and Authentication
- Social and strong authentication
- Central User Store
- Branding and policies
- User self-services
- On-premise integration
SAP Cloud Identity Service
Business-to-Consumer scenario

- Secure access and Single Sign-On across sites (based on SAML)
- User self-services
  - Configurable User Registration form
  - Account activation with email verification
  - Password reset
  - User Profile page
- Social Logon - Account linking/unlinking
- Unified user experience optimized for all devices
- Flexibility out-of-the-box
  - Configurations per web application
  - Branding (logo and colors)
  - Own Privacy Policy and Terms of Use
  - Password Policy
- Central User Management
  - Import existing users
SAP Cloud Identity Service
Business-to-Employee scenario

- Secure access and Single Sign-On across cloud or on-premise web applications (based on SAML)
- Central User Management
- Rich choice of authentication methods:
  - Two-factor Authentication and Mobile SSO
  - Authentication against
    - Corporate User Store (LDAP, NW)
    - Other Identity Provider
  - SPNEGO authentication - no login required after authentication in the corporate domain
- User self-services
  - Account activation via email
  - Password reset
  - User Profile page
- Unified user experience optimized for all devices
- Flexibility of configurations per application
- Branding and Policies
Secure Access and Single Sign-On
Access to cloud and on-premise web applications
Secure Access and Single Sign-On
Web Single Sign-On

Identity Federation and Authentication
- User credentials give access to multiple applications
  - Users have one username and password to remember
  - Customers/Partners register once
- Developers don't need to build user management for each in-house built application
- IT does not need to manage disconnected silos of users for each application
- Based on industry standard – SAML 2.0
- Authentication mechanisms applied centrally

Web Single Sign-On
- Improved user productivity
Authentication Methods and User Store Variants

1. SAP Cloud Identity as a cloud user store

**Cloud User Store**

- Suitable for all scenarios B2E, B2B, B2C
- Secure authentication and SSO for cloud and on-premise web apps
- Self-services as registration, forgot password, User Profile page
- Social logon and Two-Factor Authentication
- Branding and policies per application
- Web User Management
- User groups
- Logon credentials
  - email/userID/username
  - password
Authentication Methods and User Store Variants
1. SAP Cloud Identity as a cloud user store - Logon
Authentication Methods and User Store Variants

1. SAP Cloud Identity as a cloud user store – Registration

or direct Register link

Registration

User Store Variants

Account Successfully Activated

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
2. Social Authentication

Social Media Authentication

✓ Suitable for B2C, B2B scenarios
✓ Enabling per application
✓ Linking and unlinking of Social accounts possible
✓ Logon credentials
  - Social Media username
  - Social Media password
Authentication Methods and User Store Variants

2. Social Authentication – Logon

For Business-to-Consumer or Business-to-Partner Scenarios

if logged in into Social media site
Authentication Methods and User Store Variants

3. Two-Factor Authentication with SAP Authenticator

Two-Factor Authentication with One-Time Passwords

- Provides two means of identification
- Second factor required for high security scenarios (HR, Bank, sensitive data access, apps for power users)
- Configurable per application
- Mobile SSO with SAP Authenticator
- Logon credentials
  - email/userID/username
  - Password
  - 6 digit One-Time Password generated on a mobile device
Authentication Methods and User Store Variants

3. Two-Factor Authentication with SAP Authenticator

Based on SAP Authenticator (free) Mobile App

- Generates 6-digit One-Time Passcodes
- Available for iOS and Android
- RFC 6238 compatible
- Enables Mobile SSO
Authentication Methods and User Store Variants

3. Two-Factor Authentication with SAP Authenticator

For Business-to-Partner or Business-to-Employee Scenarios

SAP Authenticator
(free app - iOS and Android)
3. Mobile Single Sign-On for applications with Two-Factor Authentication

Onetime setup:
1. Add a web application to SAP Authenticator
2. Open the application from the SAP Authenticator – enter password and optionally mark Remember me
3. Subsequent Logons to this application via SAP Authenticator won’t require entering Username, One-Time Passcode and Password (if Remember me marked)

Prerequisites:
The user has activated the mobile device for Two-factor Authentication on SAP Authenticator
The application has Two-Factor Authentication enabled and IdP-Initiated SSO is enabled on Tenant level
Authentication Methods and User Store Variants
4. SAP Cloud Identity as a proxy to a Corporate Identity Provider

SAML Identity Provider Proxy
- Authentication to cloud applications is redirected to corporate Identity Provider login
- Reusing existing corporate identity infrastructure
- Easy and secure authentication for externalized Business-to-Employee (B2E) scenarios
- Identity Provider options:
  - SAML 2.0 compliant IDP
  - SAP SSO(benefit from native apps, web and mobile SSO)
  - Microsoft ActiveDirectory FS 2.0
- Logon credentials
  - IDP username
  - IDP password
Authentication Methods and User Store Variants

5. Corporate on-premise user store

- Users Credentials from:
  - MS Active Directory
  - Different User Stores – via SAP NetWeaver AS JAVA
    - with SAP SSO -> to SAP NetWeaver AS ABAP
    - multiple Microsoft Active Directories
- Replication and synchronization of user records to the cloud not required
- Internal network ports do not need to be exposed to the Internet
- External users can register and can be stored in the cloud
- All SAP Cloud Identity features can be used: Branding, customizations and policies, 2FA

Prerequisites
- SAP HANA ® Cloud Platform Account
- SAP Cloud Connector
Authentication Methods and User Store Variants

5. Corporate on-premise user store - Logon

LDAP credentials or cloud credentials
Authentication Methods and User Store Variants

6. SPNEGO Authentication

SPNEGO* Authentication
- Users authenticated with Corporate LDAP Credentials on their Desktops are getting Single Sign-On to cloud applications without the need to enter their credentials
- Reusing existing corporate identity infrastructure
- Secure authentication and SSO for cloud and on-premise web apps
- Increase user productivity in B2E Scenarios

*Simple and Protected GSSAPI Negotiation Mechanism
Authentication Methods and User Store Variants

6. SPNEGO Authentication

For Business-to-Employee Scenarios inside Corporate Network
User Self-Services

- Forgot password
- Configurable self-registration
- User Profile page
  - Mobile device activation (for 2FA)
  - Change password
- Account activation
- Upgrade account
- Invitation and on-behalf registration (via REST API)
Branding and Customization
Configurable per application

- Logo and Colors
  - On UIs
  - In e-mails
- Terms of Use & Privacy policy
- Password policy
- Multi-language support
  DE, EN, ES, FR, JA, KO, NL, PL, PT, RU, ZH

Responsive UIs
Branding and Customization
Configurable Registration Form per application

More info: Documentation
Access Levels and Authentication Methods
Configurable per application

Private Access

Public Access + Social Logon for Customers/Partners

Strong Authentication with a second factor - One-Time Passcode

SAP Authenticator (free app - iOS and Android)
Administration Console Functionality

Overview

Applications Configurations
- Identity Provider and SAML settings
- Application access
- Authentication options
- Policies – ToU, Privacy, Password
- Branding (logo and colors)
- Email templates
- Registration form (add fields)

User Management
- Administrators (users and admin roles)
- User administration
- User groups
- Users Import per application
- Users Download
- APIs – SCIM User Search, Invite, Register

Usage Reporting

Change Logs
- CSV download
Administration Console Functionality

User Management
Administration Console Functionality

User Management
Administration Console Functionality

Administrators Roles

User Details

Add user profile details

E-Mail:
First Name:
Last Name:

Configure Authorizations

ON  Manage Applications
    Authorizations to configure applications

ON  Manage Corporate Identity Providers
    Authorizations to configure corporate identity providers

ON  Manage Users
    Authorizations to manage, export, and import users

ON  Manage Groups
    Authorizations to manage user groups

ON  Manage Tenant Configuration
    Manage tenant configuration and authorization assignment to users
SAP HANA® Cloud Platform and SAP Cloud Identity Integration
Easy SAML Trust configuration with just a click of a button

Trust configuration integration:
✓ The Trust can be easily configured in the SAP HCP Cockpit Trust section - SAP Cloud Identity will be added as default Trusted IDP just by clicking a button
✓ In SAP Cloud Identity Admin Console – the SAP HCP account is added as an application (SP)
✓ Customers have Login out-of-the-box to protected SAP HCP applications and other SAP HCP services

*For customers using SAP Cloud Identity and SAP HANA® Cloud Platform
Enterprise Aspects
SAP Cloud Identity Data Center Presence

SAP Cloud Identity runs in SAP managed datacenter infrastructure

- World-class data center located in:
  - St. Leon-Rot (2) and Walldorf
- Advanced network security
- Reliable data backup
- Built-in compliance, integrity, and confidentiality

http://www.sapdatacenter.com/
SAP Cloud Identity Security Aspects

**Authenticate**
Various authentication methods possible

**Centralize**
Manage centrally user profiles and the user access to applications

**Protect**
Password policies and option to use strong authentication

**Encrypt**
Data encryption for data-in-motion and sensitive data-at-rest
SAP Cloud Identity Enterprise Service Levels

24/7 Global Support

99.9% Service Availability

2 weeks Release Cycle
SAP Runs SAP: Enabling Simple and Secure Authentication and Identity Management with SAP® Cloud Identity

Company
SAP SE

Headquarters
Walldorf, Germany

Industry
High tech

Products and Services
Enterprise software and services

Employees
74,000

Revenue
€16.82 billion

Web Site
www.sap.com

Objectives
- Offer single sign-on (SSO) to applications for SAP employees for things like HR tasks, external cloud applications like the SAP® Jam™ social software platform, and public Web sites like www.sap.com
- Avoid disconnected silos of users for every site or application
- Strengthen security by unifying authentication across the enterprise
- Avoid multiple logins for employees and multiple registrations for external users
- Reduce total cost of ownership (TCO)

Resolution
- Developed a central authentication and SSO software-as-a-service based on open industry standards and protocols
- Created a universal user interface that supports all devices, from smartphones to desktop computers
- Authenticated external users through a cloud user store and SAP employees through an on-premise corporate user store
- Onboarded more than 1,000 applications with SAP’s tenant of the SAP Cloud Identity service
- Offered SAP Cloud Identity as the authentication, SSO, and user management security service for SAP HANA® Cloud Platform

Benefits
- Improved internal and external user productivity and the user experience through uniform logon and SSO to cloud applications
- Simplified access via social logon and self-services like registration and password reset for SAP customers and partners
- Increased security through centralized user management and password policy enforcement
- Lowered TCO and reduced risks with a single authentication and user management system that replaced the various systems across the enterprise and cloud

“SAP Cloud Identity service is a great catalyst for our transition to a cloud company. It combines secure authentication and efficient identity management for all of our target groups: employees, customers, partners, and public users.”

Charles Carney, Project Lead, SAP IT, SAP SE

>8.5 million
Registered users

~1,000
Applications onboarded

~150,000
Active users every week

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
SAP Runs SAP: SAP Cloud Identity Service @SAP
Secure logon and SSO for internal and external websites and apps

http://sap.com

>8,5 mil registered users

~1000 applications

~150,000 active users/week

Community Network

https://www.sapstore.com/

+ many others
Further Information
SAP Cloud Identity Service
Useful Information

SAP Cloud Identity on hcp.sap.com
SAP Cloud Identity on SCN
SAP Cloud Identity Service - Solution Brief
SAP Cloud Identity Roadmap on SAP Service Market Place (SMP)

Video Tutorials via SAP HANA Academy Series
SAP Cloud Identity online help
SAP Cloud Identity How-to Guides on SCN
SAP Cloud Identity Demo in SAP Demo Store
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.

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. Please see http://global12.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.

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 SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE 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 platform 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, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.