SAP Cloud Platform Identity Authentication
Solution Overview

February 2020
Agenda

Introduction

Technologies and capabilities

Further information

Appendix
SAP Identity Management and Access Governance Solutions
Overview

<table>
<thead>
<tr>
<th>Identity Management</th>
<th>Governance, Risk &amp; Compliance</th>
<th>Authentication &amp; Single Sign-on</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP CP Identity Provisioning</td>
<td>SAP Cloud Identity Access Governance</td>
<td>SAP CP Identity Authentication</td>
</tr>
<tr>
<td>SAP Identity Management</td>
<td>SAP Access Control</td>
<td>SAP Single Sign-On</td>
</tr>
</tbody>
</table>

Setting the stage

Accessing the applications
Authentication and provisioning services

End User

Secure Authentication & Single Sign-On

SAP Cloud Platform

Identity Authentication

Identity Provisioning

Corporate Identity Provider

Identity Store, e.g. HR
- Users, Groups, Roles
- Cloud or On-Premise

Management of Identities and Authorizations

SAP Customer Experience
SAP Concur
SAP Fieldglass
SAP SuccessFactors
SAP S/4HANA
SAP Ariba
Google Cloud Platform
Microsoft Azure
Technologies and capabilities
SAP Cloud Platform Identity Authentication
Identity provider for SAP’s cloud-based business applications

SAP Cloud Platform Identity Authentication enables single sign-on for SAP’s cloud-based business applications, with two usage options

1. As IdP proxy for a seamless, flexible integration with customers’ existing IAM infrastructure
   - Simple central configuration
   - Flexible configuration options

2. As the landscape-wide identity provider
   - Secure authentication with multiple factors
   - User management and self-services
   - Pre-configured trust configuration

SAP Cloud Platform Identity Authentication

Secure authentication & single sign-on

Customers

Authentication

Username/password
X.509
Kerberos/SPNEGO
2FA (TOTP, RSA, SMS, ...)

Partners

SAML
OpenID Connect

Employees

Identity Authentication

On-Premise User Store

Corporate Identity Provider

SAP Ariba
SAP Concur
SAP SuccessFactors
SAP S/4HANA Cloud
SAP Fieldglass
SAP Cloud Platform

SAML / OpenID - enabled 3rd Party Application

employees

Single Sign-On
MS ADFS / Azure
3rd Party SAML IDP

SAP® C/4HANA

© 2020 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
Based on open security standards

Interoperable

with all applications supporting SAML* 2.0 standard

or OpenID Connect (OIDC)

*SAML = Security Assertion Markup Language
Delegated authentication
IAS as a proxy to a corporate identity provider (IdP)

Identity provider proxy
- Authentication is delegated to corporate identity provider login
- Reuse of existing single sign-on infrastructure
- Easy and secure authentication for employee scenarios
- Federation based on the SAML 2.0 standard
- System applications supported as well
Delegated authentication
Federation, proxy or both?

Enriching the assertion

- Original assertion from the corporate identity provider is enriched with additional attributes
- Mix of attribute values coming from the corporate IdP and the local user store
- Users don’t need to exist in local user store
- Enables hybrid scenarios such as authenticate via corporate IdP but manage groups via IAS
Delegated authentication
Authentication with an on-premise user store

On-premise user store
- Users credentials from:
  - Active Directory (through LDAP)
  - AS ABAP (through SCIM*)
- No user replication to the cloud required
- Internal network ports do not need to be exposed to the Internet
- In addition: usual IAS product features can be used:
  - UI configuration, policies, two-factor authentication

* requires AS Java + SAP Single Sign-On (which enables SCIM interface)
Delegated authentication
Re-use of Windows Domain Authentication (SPNEGO)

SPNEGO* authentication

- Users authenticated with Microsoft Active Directory enjoy single sign-on to cloud applications without re-authentication
- Reuse of existing corporate identity infrastructure
- Secure authentication and SSO for cloud and on-premise web applications

*SPNEGO: Simple and Protected GSSAPI Negotiation Mechanism
Delegated authentication towards multiple identity providers

Conditional authentication
Delegated authentication towards multiple identity providers
IdP-initiated authentication

IAS as a proxy to multiple IdPs

- Secure your business network and allow partner users to login via their corporate IdP
- Authentication is initiated by the corporate IdP
- Upon successful authentication, a check for correct user group assignment can be configured (optional)
  - Sync of users from IdPs to groups in IAS is required
Delegated authentication
Benefits of Identity Authentication Service in proxy mode

Central SSO endpoint for all SAP cloud applications
- Single trust configuration to customer’s corporate identity provider
- Easy to set up for customers
- Pre-configured or semi-automated trust configuration for SAP cloud applications
- Choice between SAML and OpenID Connect, incl. protocol conversion towards SAP applications
- One SSO session for all SAP cloud applications with the option to enforce separate access control policies
- Single audit log for authentication/SSO for all SAP cloud applications

Extended configuration and security settings
- Service provider specific attribute mapping/rewriting and assertion enrichment without the need to adjust the corporate identity provider
- Easy separation mechanism for multiple user stores (internal, external users, employees)
- Flexible configuration where to validate user’s credentials
- Risk-based authentication with the option to enforce stronger means of authentication
Authentication options

Basic authentication
- User ID / email and password

Re-use of Windows Domain logon
- Use of Kerberos token for single sign-on

Two-factor authentication
- Second factor via soft-tokens
- Second factor via Radius*
- Second factor via SMS**

Delegated logon
- Social IdPs
- Corporate IdP

*Radius support enabled upon request
**SMS requires the license of SAP Authentication 365
Custom password policies can be configured
Two-factor authentication options

Authentication with one-time passwords (OTP)
- Provide two means of identification
- OTP required for login in addition to password or security token
- Second factor for high security scenarios

Via soft tokens
- OTP (6-digit) created on mobile device
- SAP Authenticator – Available for iOS, Android, and Windows
- RFC 6238 compatible (compatible with Authenticator apps from Google and Microsoft)

Via SMS
- OTP sent as a message to the mobile phone of a user
- Requires SAP Authentication 365

Via Radius
- Code generated via Radius-supported devices
- Activation upon request
Control access to the application – risk-based authentication

- User
- Authentication Method
- IP-Address Range
- User Type
- Assignment to Application
- Self-registered?
- Email verified?
- Member of User Group
- Allow
- Deny
- 2-factor Authentication
- IAS

Supports both local authentication and IdP proxy
Control access to the application

- User
- Authentication Method
- Member of User Group
- IP-Address Range
- User Type
  - "employee"
- Assignment to Application
- Self-registered?
- Email verified?
- IAS
- Allow
- Application
Control access to the application

- User
- IAS
- Application
- User Type
- IP-Address Range “10.55.0.0/16”
- Authentication Method
- Member of User Group “Admin”
- Assignment to Application
- Self-registered?
- Email verified?
- 2-factor Authentication

© 2020 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
Protecting self-registration with Google reCAPTCHA / phone verification

Access protection for applications

- Protect the registration to applications from spam and abuse
- Prevent bots from automated fake user registrations to your websites
- Further information
  - Google reCAPTCHA
  - Phone verification
Branding and customization

Customization features
- Company logo
- Application name and logo
- Color style
- Full customization via CSS
- Terms of use & privacy policy, incl. IdP proxy
- Adjust UI texts via API
- Email templates

Product features
- Responsive UIs
- Multi-language support
Logon overlays in customer applications

Logon screen as an overlay (compared to a browser redirect to navigate away from application)

- Can programmatically be integrated by the application
- Out-of-the-box integration for SAP Cloud Portal
How can users be created?

1. Self-registration
2. Sync through IPS*
3. CSV-upload
4. Manual creation
5. Programmatically through SCIM

* IPS: SAP Cloud Platform Identity Provisioning
User & group management

User administration
- Web based user management
- User search
- Mass user import/export
- Monitor user access

User groups administration
- Define user groups
- Assign users to groups

Integration
- Programmatic integration via SCIM REST APIs
Further information
Where to find more information

Security software
https://community.sap.com/topics/security

SAP Cloud Platform Identity Authentication Service
https://community.sap.com/topics/cloud-platform-identity-authentication
Product strategy for IAM & CIAM

General direction

*SAP Cloud Platform Identity Authentication service* and *SAP Customer Identity* are complementary side-by-side solutions:

- **SAP CP Identity Authentication service addresses mainly B2E-scenarios** with focus on employee and contractor users.
- **SAP Customer Identity addresses mainly B2C-scenarios and B2B-scenarios** with focus on consumer (end customers and businesses) and prospect-users.

Integration between the two products for authentication can be established by delegating authentication requests to the ‘other’ IdP.
Product strategy for IAM & CIAM

Focus areas

SAP Cloud Platform Identity Authentication service
- Integration with a corporate SSO infrastructure / federation capabilities
- Support for various standards to delegate authentication
- Stronger means of authentication (2FA/MFA)
- Support for managed identity lifecycle via IDM solutions

SAP Customer Identity
- User self-registration scenarios and progressive profiling
- Enterprise consent management
- Integration with social IdPs
- Sophisticated branding capabilities
- Seamless integration of IdP functionality directly into customer’s sites (‘native integration’)
Secure authentication and single sign-on
How to decide on the right solution

SAP Single Sign-On and SAP Cloud Platform Identity Authentication both support secure authentication and single sign-on. While SAP Single Sign-On focuses on employee scenarios, and on-premise, the Identity Authentication service targets cloud applications beyond the corporate user base.

<table>
<thead>
<tr>
<th>Solution</th>
<th>Supported SSO technologies</th>
<th>Supported clients</th>
<th>User types in focus</th>
<th>Specific capabilities</th>
<th>Consumption model</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Single Sign-On</td>
<td>• Kerberos/SPNEGO</td>
<td>• Browser</td>
<td>• Employee</td>
<td>• Risk-based authentication</td>
<td>• On-premise</td>
</tr>
<tr>
<td></td>
<td>• X.509 certificates</td>
<td>• Desktop clients</td>
<td></td>
<td>• Digital signatures</td>
<td>• Some capabilities require SAP AS Java</td>
</tr>
<tr>
<td></td>
<td>• SAML</td>
<td></td>
<td></td>
<td>• Certificate lifecycle management</td>
<td>• Some capabilities require a desktop client</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP CP Identity Authentication</td>
<td>• SAML</td>
<td>• Browser</td>
<td>• Employee</td>
<td>• Self-registration</td>
<td>• Cloud subscription</td>
</tr>
<tr>
<td>Service</td>
<td>• SPNEGO</td>
<td></td>
<td>• Partner</td>
<td>• User management</td>
<td>• Run by SAP</td>
</tr>
<tr>
<td></td>
<td>• Social IdP</td>
<td></td>
<td></td>
<td>• Branding</td>
<td>• Zero footprint on desktop</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Risk-based authentication</td>
<td></td>
</tr>
</tbody>
</table>
# Acronym glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Text</th>
<th>Acronym</th>
<th>Full Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2B</td>
<td>Business to Business</td>
<td>OTP</td>
<td>One-time password</td>
</tr>
<tr>
<td>B2C</td>
<td>Business to Consumer</td>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>B2E</td>
<td>Business to Employee</td>
<td>RSA</td>
<td>RSA is a public-key cryptosystem</td>
</tr>
<tr>
<td>C4C</td>
<td>SAP Cloud for Customer</td>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>CP</td>
<td>SAP Cloud Platform</td>
<td>SCIM</td>
<td>System for Cross-domain Identity Management</td>
</tr>
<tr>
<td>HR / HCM</td>
<td>Human Resources, Human Capital Management</td>
<td>SF / SFSF</td>
<td>SuccessFactors</td>
</tr>
<tr>
<td>IAM / IDM</td>
<td>Identity Access Management / Identity Management</td>
<td>SPNEGO</td>
<td>Simple and Protected GSSAPI Negotiation Mechanism (GSSAPI: Generic Security Service Application Program Interface)</td>
</tr>
<tr>
<td>IBP</td>
<td>SAP Integrated Business Planning</td>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>IdP / SP</td>
<td>Identity Provider / Service Provider (SAML)</td>
<td>TCO</td>
<td>Total Cost of Ownership</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td>TFA / 2FA</td>
<td>Two-factor authentication</td>
</tr>
<tr>
<td>OAuth</td>
<td>Open Authorization Framework</td>
<td>X.509</td>
<td>in cryptography, X.509 is a standard for a public key infrastructure (PKI)</td>
</tr>
</tbody>
</table>
Thank you.

Contact information:

Marko Sommer
Product Expert
SAP SE
69190 Walldorf, Germany
marko.sommer@sap.com