SAP’s Bring Your Own Identity (BYOI)

Introduction at the SAP Security Webcast Call

SAP SE - Cüneyt Çam, Viacheslav Romanov

January 22, 2026

Agenda

01 Introducing bring your own identity

- What is BYOI?
- Benefits for your Company and Employees

02 Implementation Strategy

- Program methodology
- Roadmap and Timeline

03 Technical Overview

- BYOI Layers, BYOI Flavors
- Architecture at a Glance

04 Interactive Session

- Top Questions and Answers
- Our Feedback channel

1. Introducing Bring Your Own Identity

- What is BYOI?
- Benefits for your Company and Employees

Introducing Bring Your Own Identity
Challenges of Modern Authentication Systems

Attacks growth stats 2023-2024

+202%

Phishing Attacks

+703%

Credential Attacks

User Experience

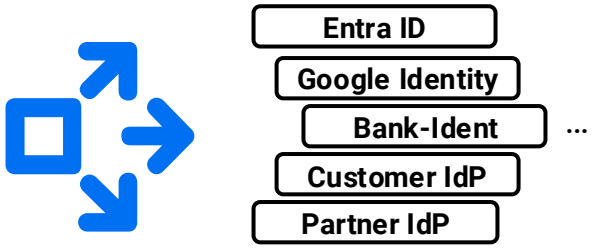
76%

Companies have no uniform login experience

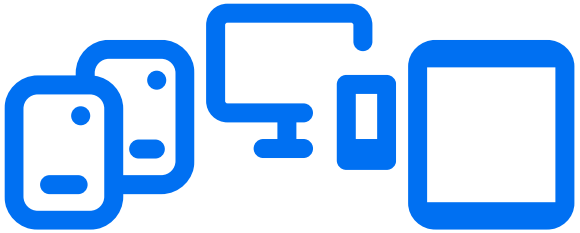
56%

Login attempts fail due to forgotten passwords

Usage of multiple different IdP's leads to disharmonized login experience



Extended hardware also requires secure and user-friendly authentication methods for each



Source: https://www.airlock.com/die-puzzleteile-moderner-authentifizierung (Whitepaper, LinkedIn)

Introducing Bring Your Own Identity
What is BYOI?

Bring Your Own Identity (BYOI) is an **innovative transformation** designed to enhance interactions with SAP's digital platforms by allowing customers and partners to **connect their Corporate Identity Providers (IdPs) with SAP**. Our vision is to enable straightforward digital interactions from initial contact to known user status, consistent across all touchpoints and cloud products. This initiative aims to meet the growing expectations for a **modern**, **secure**, and **compliant** digital experience. SAP is going to be the first one to adapt to BYOI.

What

- **Integrate** customers Identity and Access Management (IAM) solution into SAP's ecosystem
- **Harmonized** identity management for SAP products and ecosystems with seamless navigation across SAP platforms
- **Transforming** SAP's identity management into state-of-the-art infrastructure

Why

- **Allow** customers to manage their users' identities centrally, using their existing identity management systems
- **Enable** customer to manage authorizations across digital and product in a compliant and secure way
- **Onboard** customer identities once and use them across products and digital services
- **Enable** users to manage multiple user identities

How

- **Utilizing** SAP Cloud Identity Services for a harmonized login experience
- **Delivering** an open IAM platform for customers to bring their own Corporate Identity
- **Sunsetting** SAP Customer Data Cloud (formally known as Gigya) as authentication stack
- **Improving** user management backend processes

BYOI Program Overview

Benefits for your Company and Employees

Streamlined User Management:

Centrally manage user identities with your existing systems, simplifying onboarding and permissions management.

Enhanced Security:

Leverage your trusted identity providers to meet your security standards, ensuring compliance with strict industry requirements.

Cost Savings:

Minimize operational expenses by streamlining identity management processes, reducing manual tasks, and enhancing overall efficiency.

Benefits for the company

Benefits for the individual user

Improved User Experience:

Consistent and familiar login across services enhances user engagement and adoption.

Convenience:

Users log in to multiple services with one set of credentials, reducing the hassle of managing multiple usernames and passwords.

Reduced Friction:

Users start using new services instantly with their existing credentials, skipping lengthy registration and boosting adoption.

Unlock Total User Management Freedom:
Empowering Your Organization with Seamless Control, Compliance & Security

Customers gain **comprehensive control over their user management**, including identities, roles, and authorizations. They can leverage **their preferred Identity & Access Management (IAM) solution to ensure secure and compliant access** across all SAP cloud services and products.

This approach **addresses significant challenges** present in the current S-user Management system.

Customers have the **option** to upgrade to **BYOI** or continue using the existing S-user Management system.

Please note: once the decision to adopt BYOI is made, it cannot be reversed.

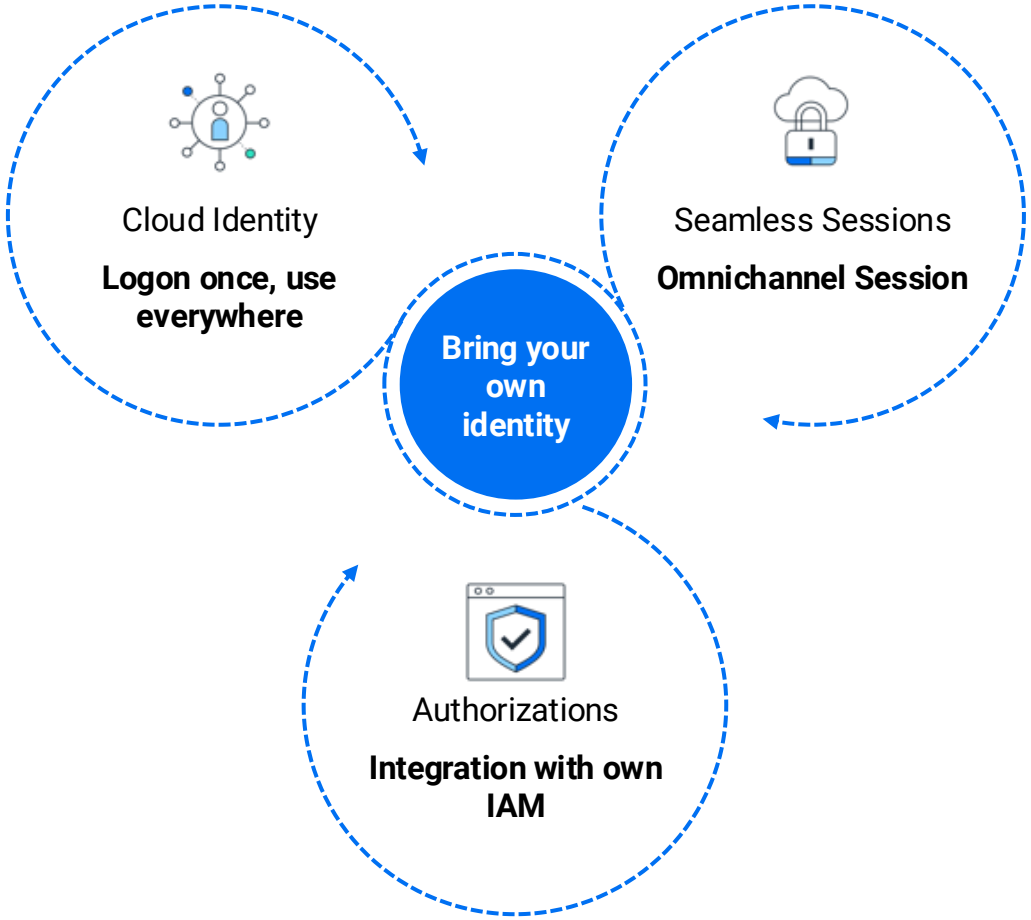
Future Hybrid Scenario

	Classic: S-User Management	Modern: Bring Your Own Identity
User Experience	○ Multiple logins depending on SAP touchpoints, more related issues (e.g., passwords, resets etc.)	✓ Seamless SSO, less login issues
Security	○ Weaker authentication, decentralized security, MFA setup by Super Admins enabled since Jan 2026	✓ MFA possible as you want, centralized security policies, monitoring by your ”own IT Security”
Compliance	○ Fragmented compliance management, manual auditing	✓ Easier compliance, centralized audit logs
User Management	○ Manual user management, potential for errors, dependency from SAP	✓ Automated provisioning and entitlement, centralized role management “at home”
Cost Efficiency	○ Higher support costs (due to incidents/ticketing), infrastructure redundancy	✓ Lower IT support and infrastructure costs
Operational Efficiency	○ Slower onboarding, more manual processes, incidents/ticketing needed in certain cases	✓ Faster onboarding/offboarding of users, automated processes ”as you want”

2. Implementation Strategy

- Program methodology
- Roadmap and Timeline

Implementation Strategy
Program methodology



Logon once, use everywhere:
Setup your identities and authentication once for all SAP digital services and products. After onboarding the first cloud solution, use these credentials for all future interactions with SAP - no S-user restriction.

Omnichannel Session:
With BYOI, every user interaction is a single, continuous session across all touchpoints. Switch channels/platforms seamlessly, with consistent security and compliance throughout.

Integration with own IAM:
Manage authorizations using your own Identity and Access Management solution, with SAP Identity Provisioning fully integrated across SAP cloud products and digital touchpoints.

Implementation Strategy
Roadmap and Timeline

Q2 2025

- **Identity Renovation as an official SAP program**
  Set the right priorities, supported by leadership.
- **Announcement of upcoming changes**
  Introduction to the new authentication method and what it means for you.
- **Invitation to join Pilot Phase**
  Secure your spot if you want to be one of the first customers/partners invited to use and test the new authentication process.

Q3 2025

- **Retirement of SAP Universal ID (UID) as an authentication stack**
  Ready for switching to SAP IDS.
- **Selection of early adopters for the Pilot Phase**
  Strengthening next level engagement and collaboration, incl. communication and next steps.

Q4 2025

- **Start of First Pilot Phase Engagements**
  Reach out to pilot candidates and start first engagements,

Getting ready for Jan 2026:

- **Prepare for ending the UID Password Migration**
  Customers and Partners to review & reset their passwords for their users and migrate them accordingly
- **Prepare to Introduce the IDS Account Selector**
  Allow users to select between their different identities that share the same email.

2026

- **Finalization of the UID password migration, removal of UID as authenticator & introduction of IDS Account Selector (Q1)**
- **Start of Pilot Phase & Later Evaluation of results**
  Pilot phase to be started and findings as potential enhancements. (Q1-Q3)
- **SAP as First Customer**
  Migrated to the new concept as SAP runs SAP. (Q1-Q3)
- **BYOI Migration Concept**
  Guidance and documentation provided for easier adoption (Q3)
- **General Availability of BYOI**
  Gradual onboarding opens for customers & partners (End of 2026)

3. Technical Overview

- BYOI Layers
- BYOI Flavors
- High-level Architecture

Technical Overview
BYOI Layers

Authentication

Users with company domain emails are redirected to the customer's CIS tenant upon login (SAP ecosystem only, not cloud products)

Customers control & decide on employee access and authentication methods for SAP digital touchpoints (e.g., FaceID, fingerprint, MFA)

User Data in SAP ID:
Added *manually* by the customer admin via S-User creation in User Management Tool (UMT within SAP for Me).

Data Provisioning

- Customer explicitly flags users for S-User or P-User creation.
- Prevents automatic user creation for the entire user base.

- Real-time data provisioning includes updates (email, name changes).
- Multiple S-Users (different company IDs) but only one P-User per account.

User Data in SAP ID:
Added via data provisioning from customer CIS tenant *automatically*.

Authorization Management

Process:
- Authorization objects bundled into packages in SAP4Me (UMT side).

- New packages automatically transferred to customer CIS tenant as user groups.
- User groups ready for assignment to users.

Fully controlled by the customer:
- Permissions assigned by adding users to groups.
- Groups represent sets of authorizations.

Technical Overview
BYOI Flavors

Authentication: Customer´s SAP Cloud Identity Services (CIS) tenant: Users with onboarded customer domain emails are forwarded to the customer CIS tenant for authentication.
Requirements: User must exist in SAP ID; no automatic provisioning.
Admin Tasks: Customer admin creates S-User in UMT (SAP4Me).
Notes: Passport creation deactivated; customer identity provider provides certificates if needed.

Authentication Only

Full BYOI

Includes: Authentication, data provisioning, and authorization management.
Authentication: Same process as 'Authentication Only'.
Data Provisioning:

- Users flagged by customer for special permissions (S-User) or community/learning access (P-User).
- Flagged user data provisioned to SAP; S/P-User created and stored in SAP ID.

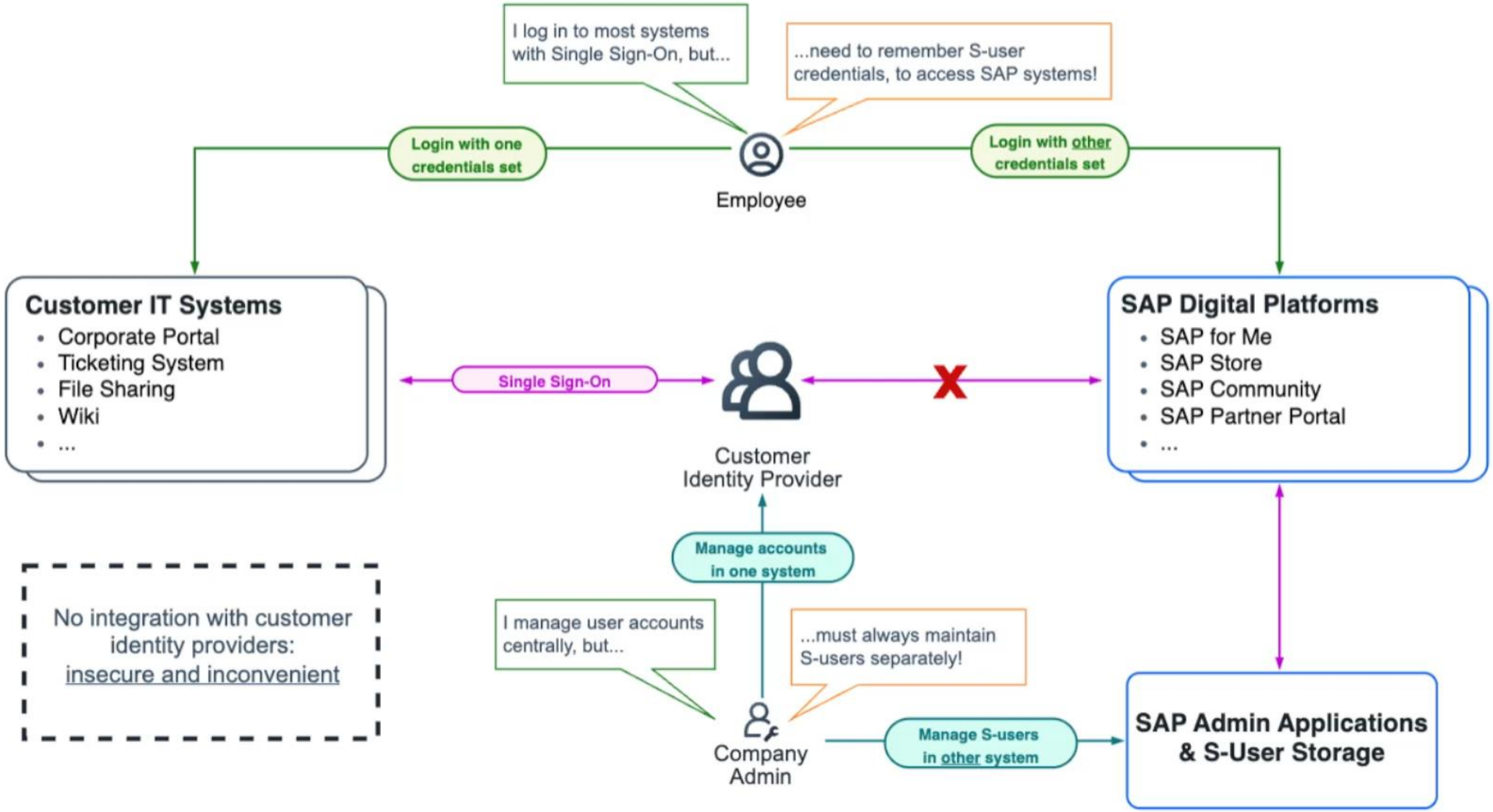
Authorization Management:

- S-User assigned authorizations based on role.
- Admin creates authorization packages in UMT; mirrored as groups in customer CIS tenant.
- Users assigned to groups receive corresponding permissions.
- Multi-group assignment possible; permissions revoked upon unassignment or unflagging.

Changes: S-User creation and permission assignment in UMT replaced by group assignment and user flagging on customer side.

Technical Overview

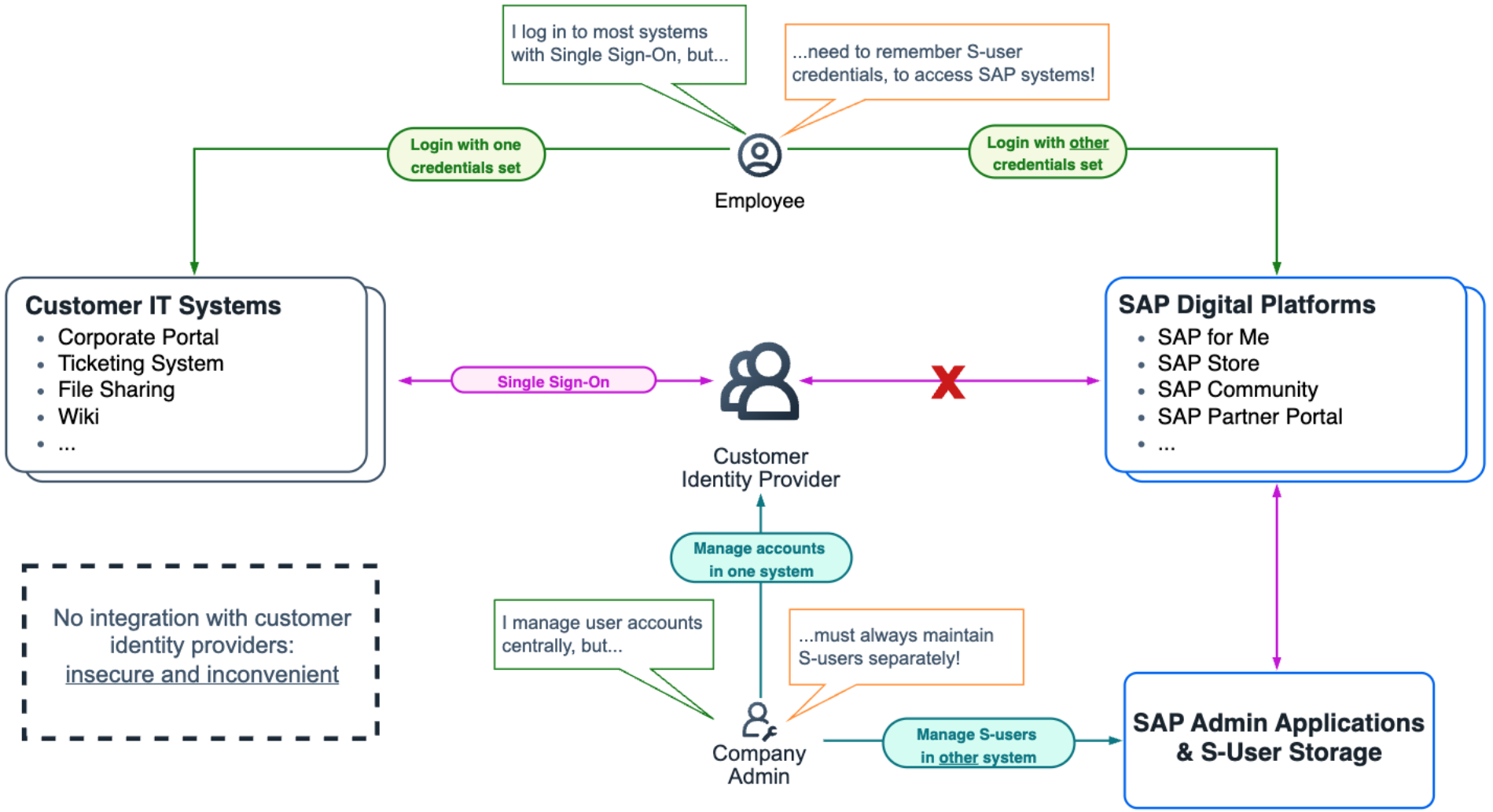
Architecture at a Glance: Customers managing identities - Current state



Demo

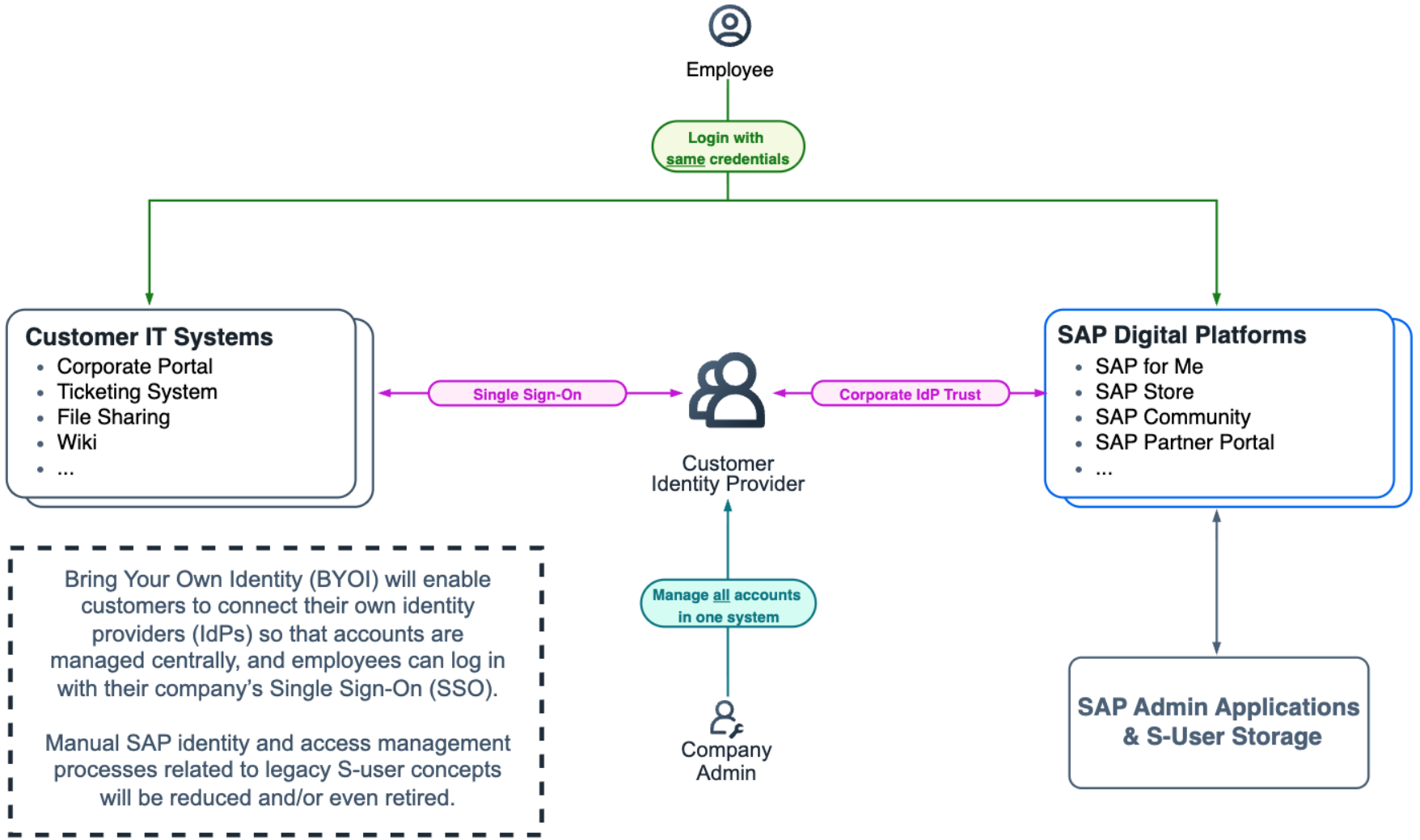
Technical Overview

Architecture at a Glance: Customers managing identities - Current state



Technical Overview

Architecture at a Glance: Customers managing identities - Target state

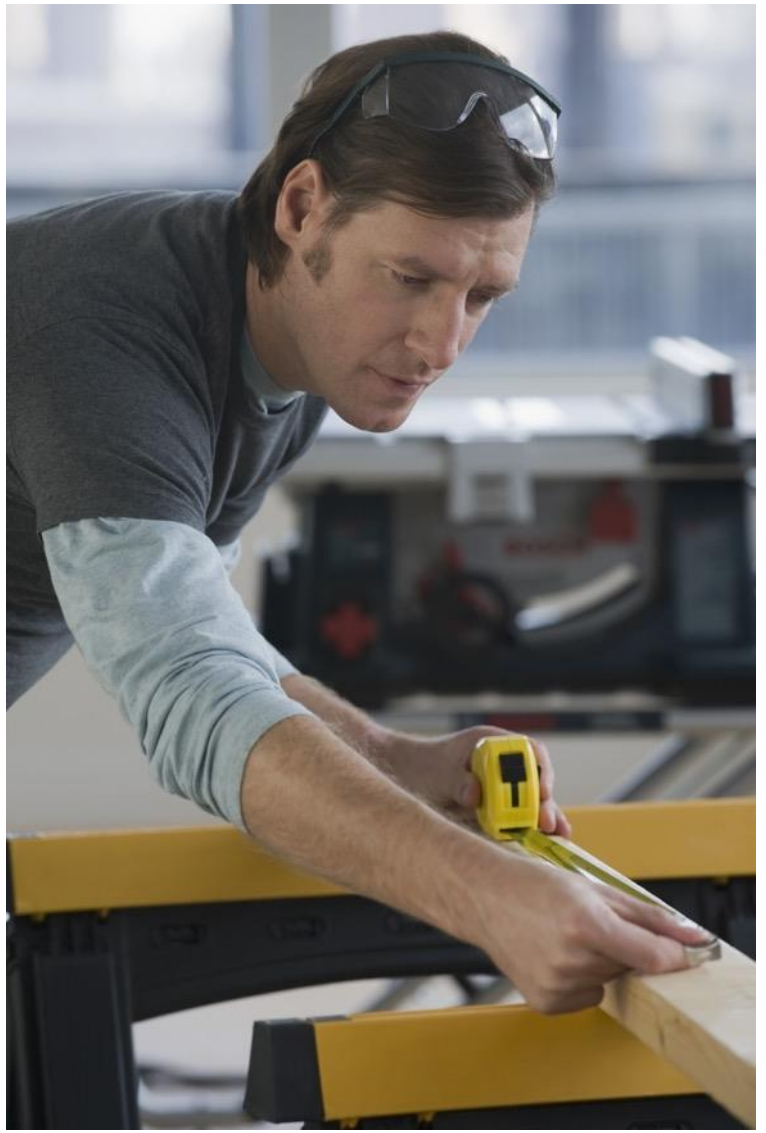


4. Interactive Session

- Our feedback channel
- Top Questions and Answers

Use our Continuous Influence Session – your voice counts!

1. **Access & check existing requirements** in the Continuous Influence Session at https://influence.sap.com/sap/ino/#campaign/3831
2. **Assess their relevance and vote for already existing and relevant ones** for you instead of composing new requirements for the same.
   Info: 10+ votes lead to a first review by SAP.
3. If none match, **submit your own** and ensure getting support through voting by others. **It matters!**
4. **Select the appropriate category** to ensure it lands at the right SAP team:
   - Identity Renovation/BYOI
   - S-user Management
   - SAP Universal ID
5. **Send in your requirement(s)** and wait for qualification by votes. SAP monitors this channel frequently and will contact you accordingly.



Top Questions & Answers

What is bring your own identity (BYOI)?

- BYOI means that customers and partners can log in to SAP's digital platforms (e.g., SAP Signavio, SAP4Me, etc.) using their own company login system instead of creating a separate SAP account. In other words, SAP "trusts" the customer's existing identity provider (IdP) to authenticate the user.

What are the benefits of adopting the Bring Your Own Identity approach?

- Bring Your Own Identity allows customers to onboard users through their enterprise identity provider and enables seamless, secure access across SAP products and digital services. Because authentication is managed on the customer's side, it reduces the need to maintain separate user credentials, lowering maintenance effort of user identities and improving compliance.

How does authentication work today and what will change with BYOI?

- SAP performs all the identity management work (S-user accounts creation, identities verification, access management when users change companies), while users log in with SAP credentials (email + password, MFA if applicable). SAP will move from being the "guard" (for authentication) and "guest list manager" (for account management) to the "access gatekeeper". The BYOI program will enable Customers who already have their own Identity Providers (IdP) manage user account logins, password resets, MFA, while SAP will be checking the "access ticket" sent by the customer's system and provide users the right access inside SAP. With BYOI in place, SAP will still be responsible for:
  - ✓ Defining what roles, permissions, and data a user can access inside SAP tools
  - ✓ Keeping audit logs and ensuring compliance
  - ✓ Maintaining the connection ("trust") between SAP and each customer's IdP

Will it be possible to use our own Corporate IdP for login? Can we choose to log-in with S-users or our corporate ID? Or will it be with Corp ID only?

- With the BYOI principle, you will connect your Corporate IdP with SAP and establish full control over all facets of your user management including access to several SAP touchpoints. As this innovation is optional, you may still decide to stay within the current framework and continue to use your S-users as is. If you decide to adopt the BYOI, you will need to use your own corporate identities for logging into SAP touchpoints in future.

When will the option to bring your own identity be available for customers and partners? What are the prerequisites?

- The BYOI Go-Live with first customers is planned until the end of 2026. The pilot phase with selected customers is planned to take place in H2/2025. It will not be mandatory as a first step, which means you can decide whether to accept this innovation or remain with the current S-user Management. The major prerequisite is that your company has its own IdP provider running to manage your own corporate users and identities. Your own Identity and Access Management (IAM) solution can bring more possibilities but is not a must. Other aspects depend on your IT landscape which needs to be investigated specifically.

Top Questions & Answers

Will Bring Your Own Identity lead to any modifications in the authorization system?

- If you opt for BYOI program, you'll be connecting your own corporate Identity Provider (IdP) to SAP. This requires establishing a new user and authorization management system on your end which aligns with SAP for user verification purposes. In general, if your company already has an IAM system active, most essential structures would be already set. However, in the absence of a separate IdP that you don't own, you need to remain within the classic S-user Management framework.

Will new permissions/authorizations or authorization packages be able to be added on different levels such as enabling separation between customer/installation number and even tenants?

- This is one of the major requirements of our big-sized customers having complicated structures in place. The introduction of a new tenant level is already in our roadmap. New authorization objects may then potentially be introduced as well.

How are permissions assigned in SAP for Me for users authenticating through their corporate Identity Provider (IdP)?

- If your company has opted for BYOI and is using its own IdP, the responsibility of managing and assigning permissions falls under your own responsibility and control. In this case, everything is managed within your IAM solution, and it simply needs to be replicated with SAP to interact accordingly.

How will the Functional User in the BTP work?

- The "BYOI by Identity Renovation" is a project driven solely by SAP's internal IT, focusing exclusively on authentication topics and corresponding IAM scenarios at our central, customer-facing SAP touchpoints, such as SAP for Me, SAP Community, SAP.com, etc. BTP (Business Technology Platform) and any other application-specific IAM scenarios are not the focus of this project and will be handled by the respective application/platform, so there are no direct dependencies between us. In such cases, these requests should be discussed directly with the affected application/platform.

Why is SAP enhancing IAM authentication and access infrastructure?

- SAP is modernizing its authentication and access management approach with state-of-the-art technology to improve security, reduce complexity, and create a more seamless experience for customers and partners—both on SAP's digital platforms and throughout their SAP journey.

Your Perspective Matters

Join the Conversation

You Ask, We Answer.

Thank you.

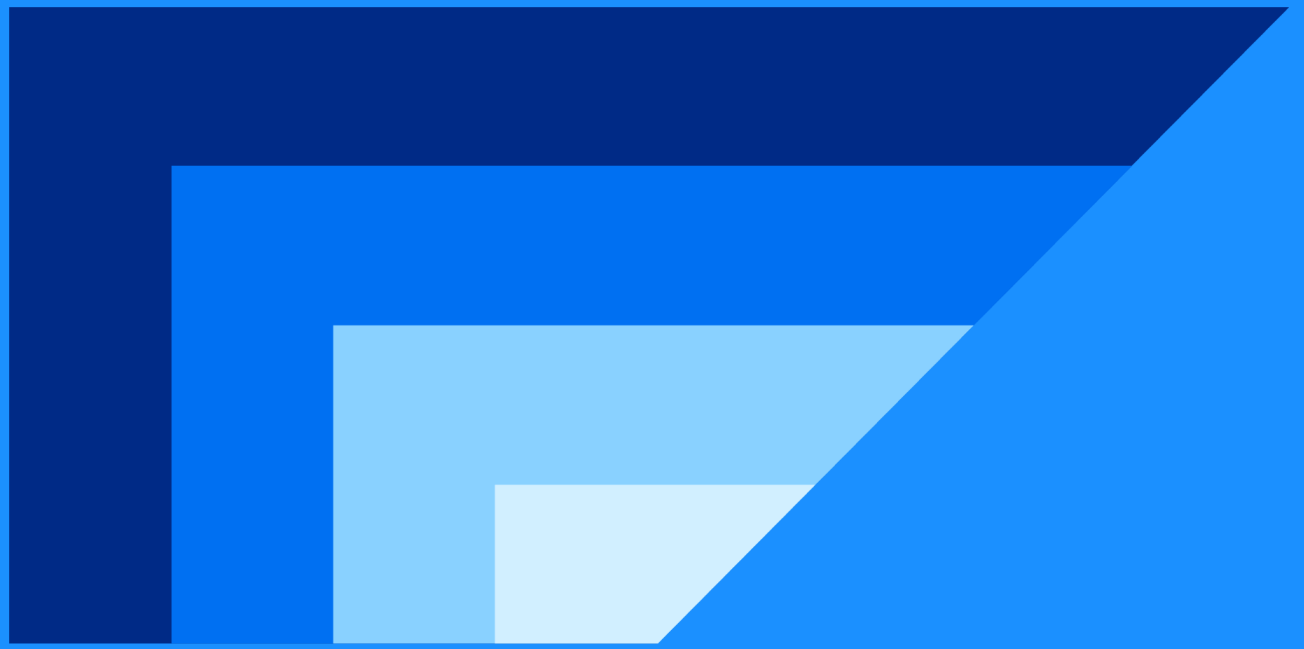
Contact information: customer-identity-management@sap.com

Cüneyt Cam
Senior Program Director, Bring Your Own Identity by SAP Identity Renovation
SAP SE

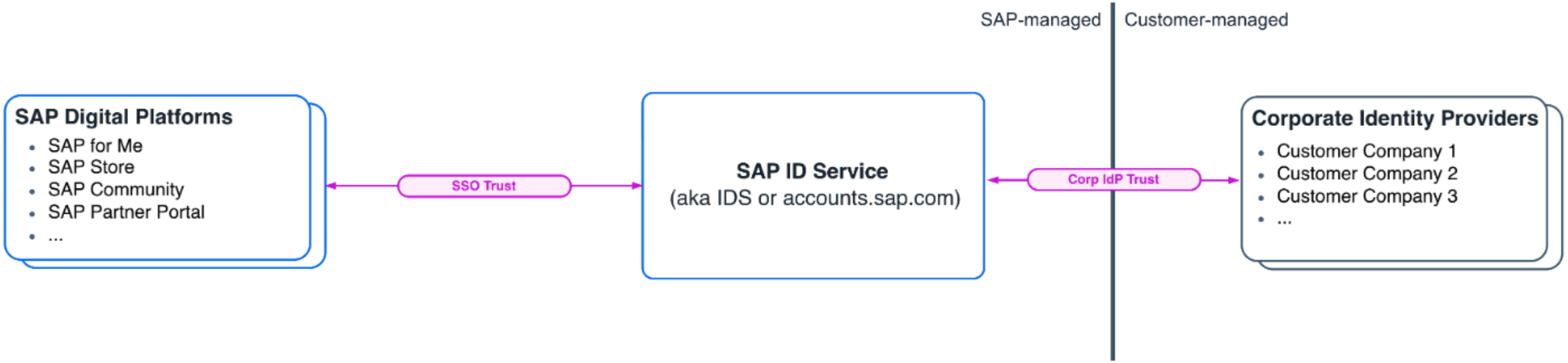
Viacheslav Romanov
Solution Architect, Identity Renovation Program
SAP SE

SAP Bring out your best.

Appendix

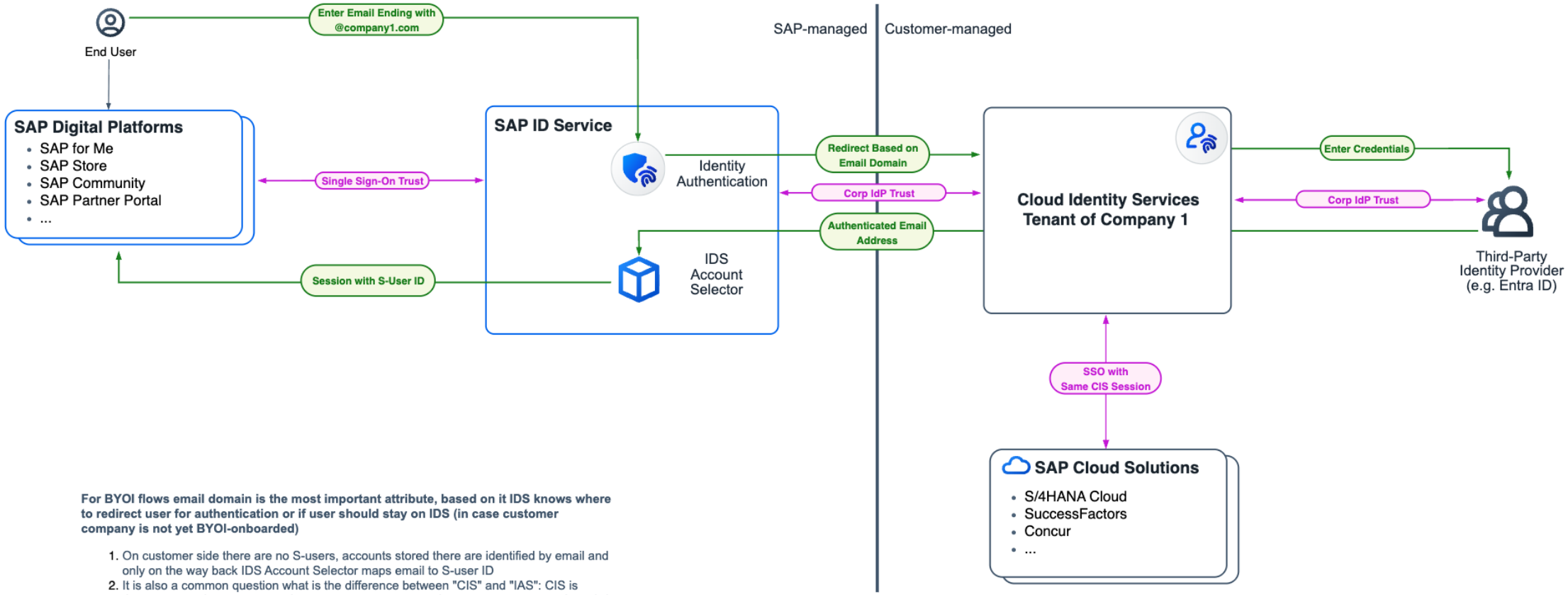


BYOI Architecture: Single Sign-On for SAP Digital Platforms



With BYOI customers will be able to connect their own corporate IdPs.
Those IdPs are operated not by SAP, but by customers directly.

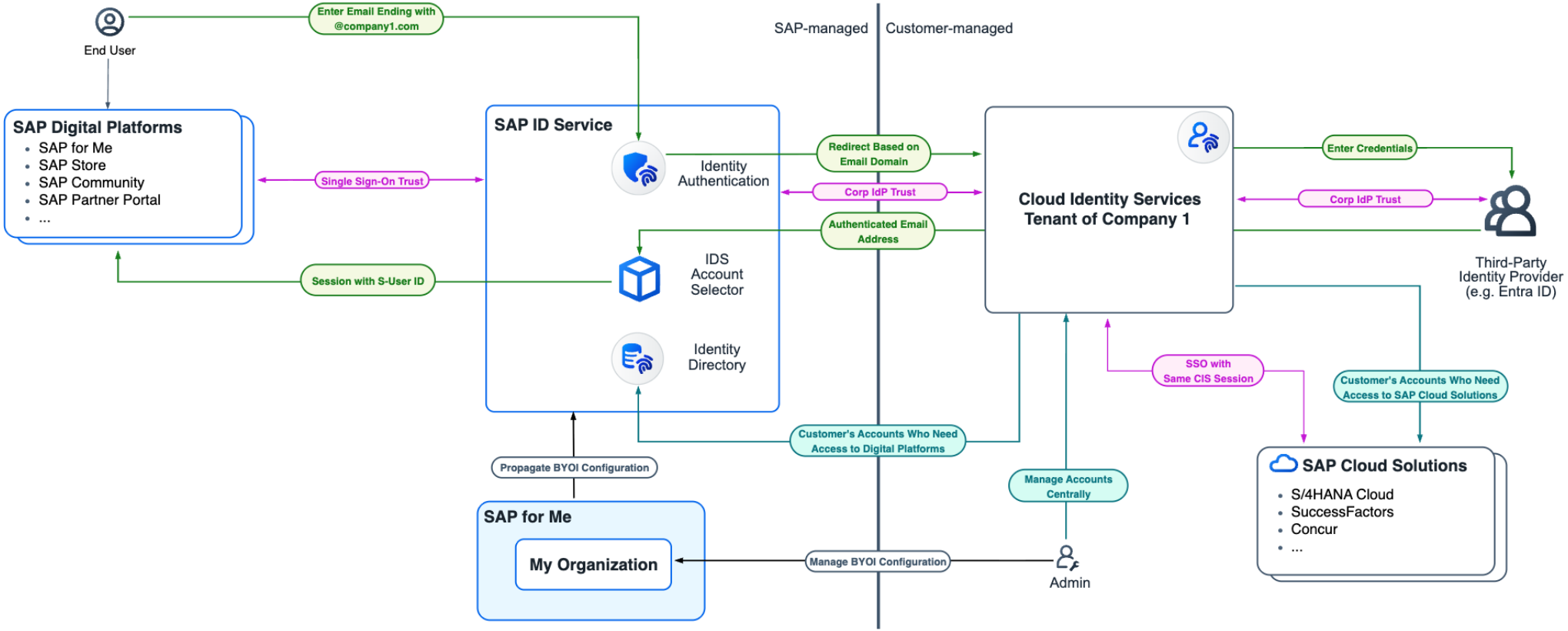
BYOI Architecture: Authentication



For BYOI flows email domain is the most important attribute, based on it IDS knows where to redirect user for authentication or if user should stay on IDS (in case customer company is not yet BYOI-onboarded)

1. On customer side there are no S-users, accounts stored there are identified by email and only on the way back IDS Account Selector maps email to S-user ID
2. It is also a common question what is the difference between "CIS" and "IAS": CIS is Cloud Identity Services and IAS is Identity Authentication Service, which is part of the CIS and when we say "CIS tenant" or "IAS tenant" it means exactly the same thing
3. IDS is not connected directly to third-party IdP, rather CIS tenant acts as an entry point for us on customer side and customer can define conditional rules or even connect several third party IdPs as needed
4. Third-party identity provider is optional, small companies that don't have it, can manage user accounts in CIS directly
5. It might be confusing that CIS tenant or SAP Cloud Solutions are marked as "Non-SAP" (black color), even though those are SAP products, but here the color is representing who owns/operates a system and not who is developer of software

BYOI Architecture: Identity Lifecycle Processes



While SAP source systems themselves and most of the internal IAM processes stay the same, the way how admin of customer company manages accounts changes significantly

1. Instead of interacting with applications on SAP side (UMT, MMU), admin will manage accounts and assign permission in own CIS tenant. Those changes will be provisioned to SAP Digital Platforms infrastructure in the background.
2. To do the initial BYOI onboarding, verify email domain and configure connection between IDS and CIS tenant, customer will use a new application named My Organization (My Org). UI of this application will be accessible via SAP for Me
3. Propagate BYOI configuration is primarily about creating conditional rule for onboarded domain
4. Admin can manage accounts in CIS tenant manually, but it can also be that customer infrastructure is advanced so they have automated processes or approval tool which will provision users to CIS tenant