

Let's nighti facune secure digital authentication

This ceale remcation insights knowling nor. bung its authentitw. ons secure identity is proviers of the comming and thie digitl provicers (we use) charning to you whdoes to and feahing from imaan authentication of the secure, popal., and the your fin your provider in.



Authentication Scenarios in SAP BTP

Herem, we'll explore the different authentication scenarios supported by SAP BTP. Understanding these scenarios is crucial for implementing secure and efficient user authentication in your SAP BTP environment.

por Mayko Silva



Overview of Authentication Scenarios

1 Standard Identity Federation

Authentication through the SAP ID service, which comes preconfigured by default on SAP BTP, requiring no additional setup.

2 Identity Authentication Tenant

Uses your instance of the Identity Authentication service to integrate your enterprise user base with SAP BTP applications.

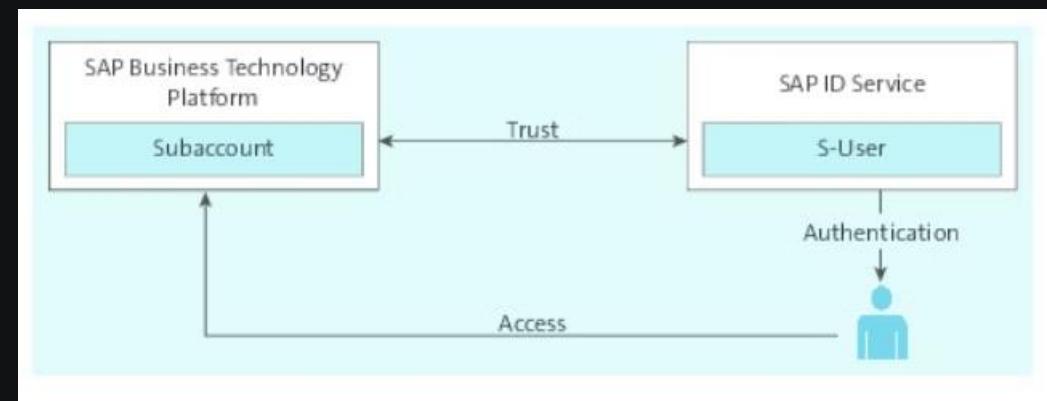
3 Corporate Identity Provider

Delegates authentication to an existing identity provider within your company, allowing employees to use their regular credentials.

Standard Identity Federation

The SAP ID service serves as the default identity provider for SAP BTP. This trust relationship is preconfigured, making it immediately available without any additional setup required.

When users attempt to access SAP BTP, they are authenticated through the SAP ID service. SAP BTP recognizes this authentication as trustworthy based on the established trust relationship, granting access once the SAP ID service confirms successful authentication.



Authentication Process with SAP ID Service

User Access Request

When a user attempts to gain access to SAP BTP, they initiate the authentication process.

SAP ID Authentication

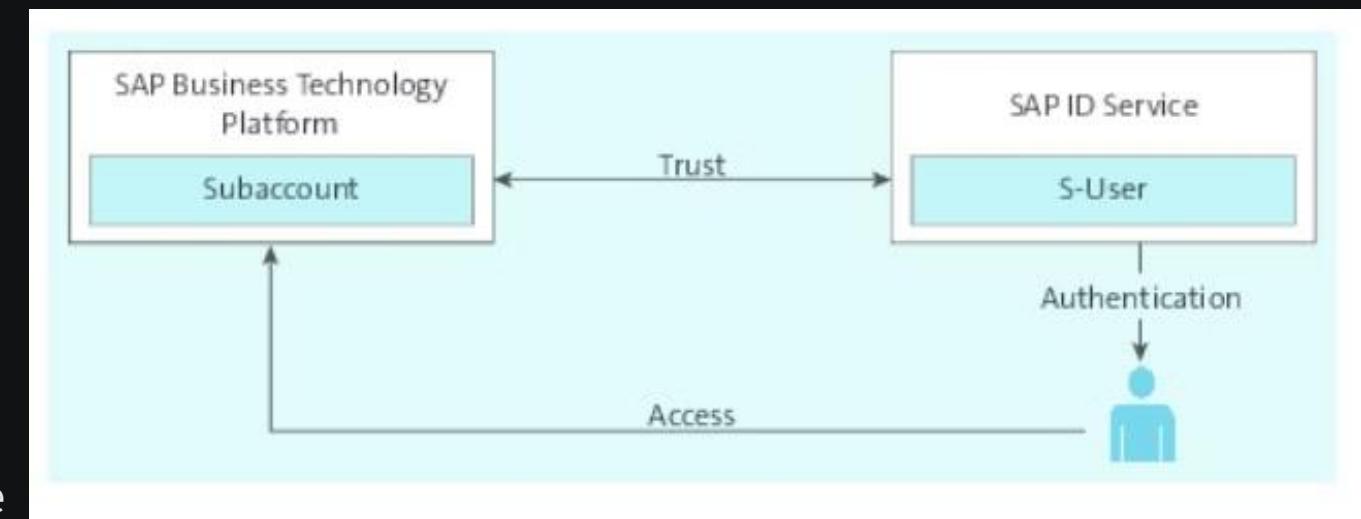
Authentication is performed via the SAP ID service, where the user provides their credentials.

Trust Verification

SAP BTP classifies this authentication as trustworthy based on the established trust relationship.

Access Granted

Access is granted if the SAP ID service confirms positive authentication of the user.





When to Use Standard Identity Federation

Quick Setup

The standard identity federation is the quickest way to get up and running with SAP BTP, making it ideal for environments that need rapid deployment.

Development Environments

Particularly well-suited for development and testing environments where simplicity and speed of setup are prioritized over complex authentication requirements.

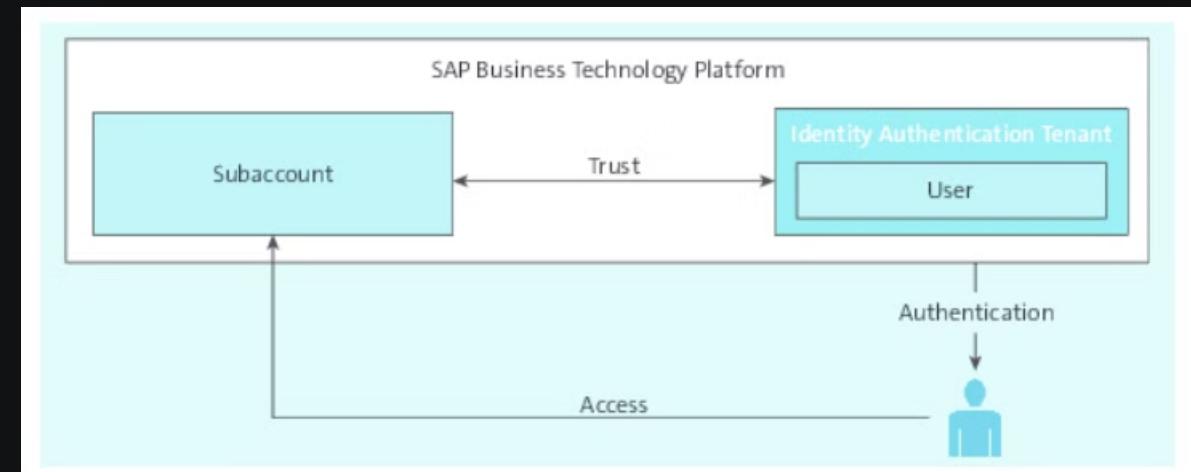
Limited Production Use

While functional for production, other authentication scenarios may be more appropriate for enterprise-level production environments with specific security requirements.

Identity Authentication Tenant

The Identity Authentication tenant provides a more customized approach to authentication. Instead of creating S-users, you can integrate your enterprise user base directly with SAP BTP applications.

This approach allows you to leverage your existing user management systems while providing a seamless authentication experience for your users. It's particularly valuable for organizations that want to maintain control over their user identities.



Benefits of Identity Authentication Tenant



User Base Integration

The Identity Authentication tenant gives you the ability to seamlessly integrate your own user base with SAP BTP, eliminating the need for separate user management.



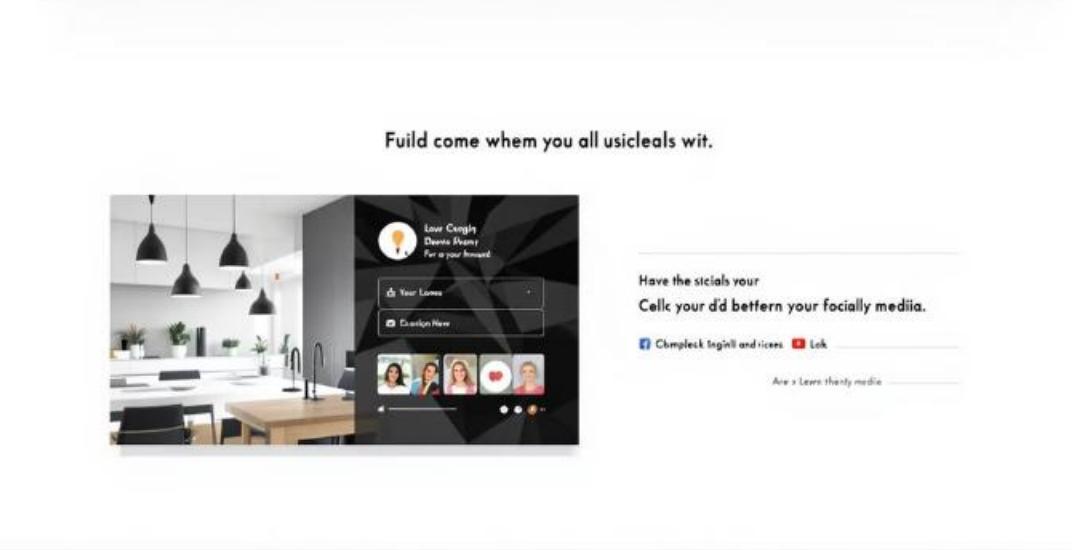
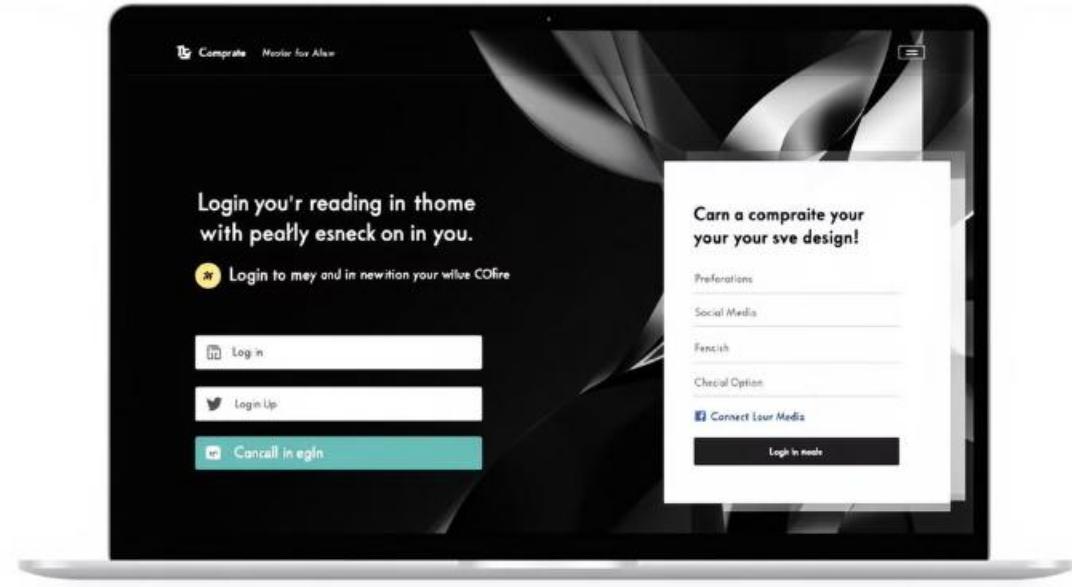
Corporate Branding

You can apply your corporate branding to the authentication experience, providing a consistent look and feel that aligns with your organization's identity.



Social Media Integration

The service allows you to leverage identity providers from social media sites, offering additional authentication options for your users.



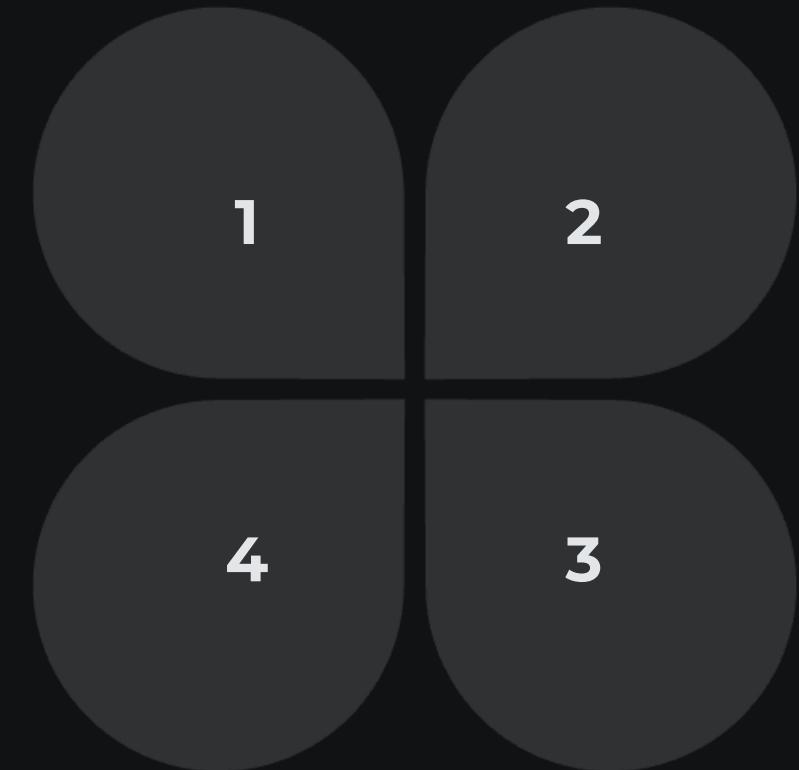
Global Availability of Identity Authentication

Global Account

The central administrative entity in SAP BTP that contains all your subaccounts.

Subaccount C

Production environment benefiting from the centralized Identity Authentication setup.



Subaccount A

Development environment utilizing the Identity Authentication tenant for user authentication.

Subaccount B

Testing environment sharing the same Identity Authentication tenant configuration.

One of the significant advantages of the Identity Authentication tenant is its availability to all subaccounts within your global account. This means that once you've configured it, all your subaccounts can benefit from the same authentication setup, ensuring consistency across your environments.

Real-World Application of Identity Authentication

1

Integration Challenge

On-premise SAP systems isolated from cloud applications

2

Identity Authentication Solution

Implementation of Identity Authentication tenant

3

Seamless User Experience

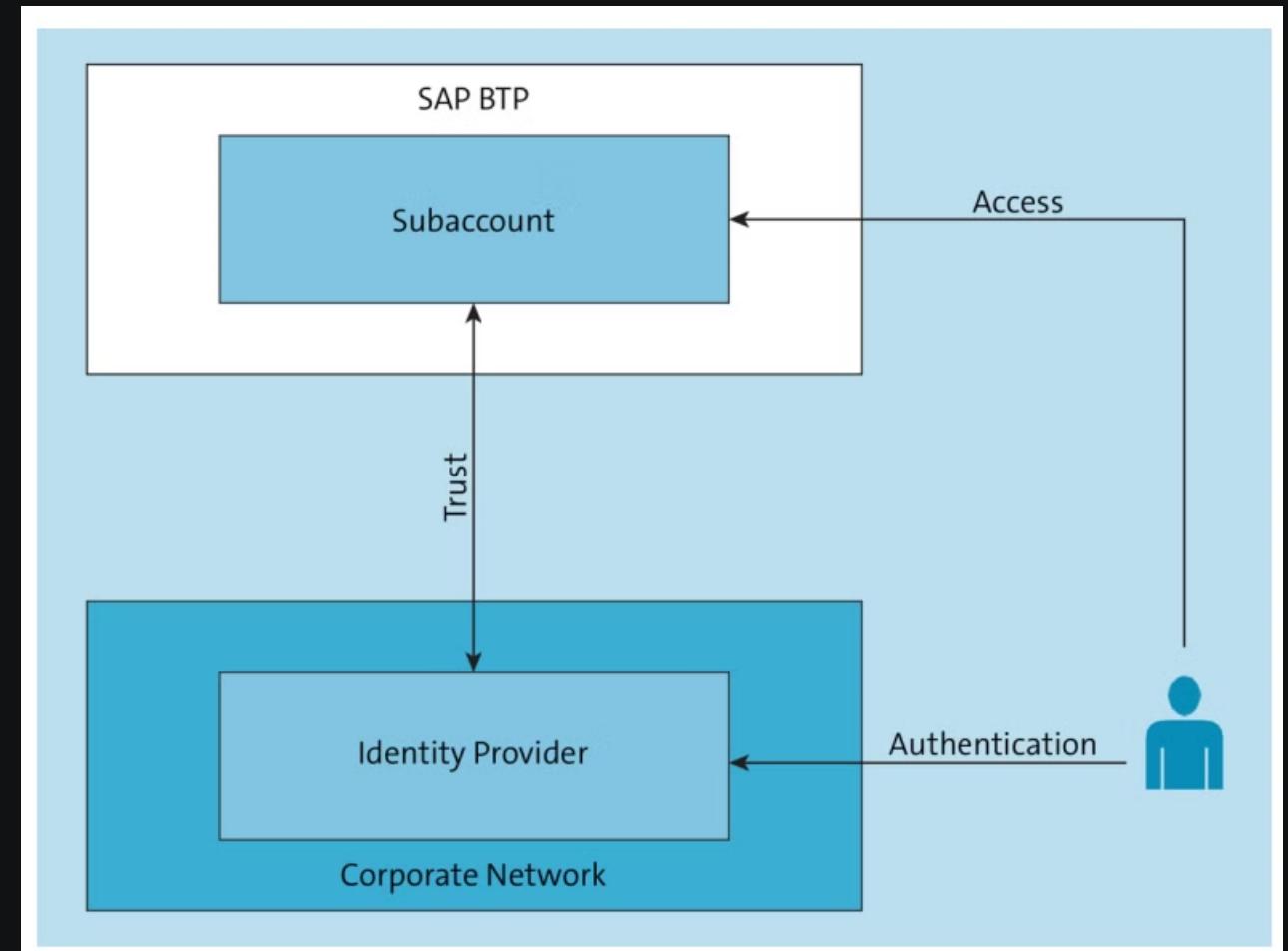
Single sign-on across all systems

A client successfully used the Identity Authentication tenant to integrate their on-premise SAP systems with their cloud applications. This integration provided a seamless single sign-on experience for their users, significantly improving user satisfaction and productivity by eliminating the need for multiple logins.

Corporate Identity Provider

Beyond the SAP ID service and Identity Authentication service, SAP BTP applications can delegate authentication and identity management to an existing identity provider within your company. This approach leverages your established identity infrastructure.

This scenario allows your company's employees to authenticate against your corporate directory service, enabling them to log on to cloud applications using their familiar user credentials without requiring additional accounts.



Corporate Authentication Process



Employee Access Request

1 Your company's employees attempt to access the SAP BTP cloud application using their regular corporate credentials.

Corporate Directory Authentication

2 SAP BTP authenticates users against your corporate directory service, verifying their identity through your existing systems.

Secure Information Transfer

3 User information required by SAP BTP is securely passed during the logon process using standardized security protocols.

Application Access Granted

4 Upon successful authentication, employees gain access to the cloud application without needing separate credentials.





Security in Corporate Identity Provider Scenario

Standardized Security Protocols

The authentication process relies on proven and standardized security protocols to ensure the secure transmission of user information during the logon process.

Secure Data Transfer

All information about a user required by SAP BTP is securely passed on during authentication, maintaining data integrity and confidentiality throughout the process.

Trust Relationship

The security foundation is built on an established trust relationship between the SAP BTP subaccount running the application and your corporate identity provider.

Advantages of Corporate Identity Provider

No Additional Systems Required

You don't need to manage additional systems for synchronization or provisioning of user accounts between your corporate network and SAP BTP, simplifying your IT landscape.

Simple Trust Configuration

All that's required is establishing a trust relationship between the SAP BTP subaccount running the application and your corporate identity provider, a relatively straightforward configuration process.

Seamless User Experience

Employees can use their familiar corporate credentials to access cloud applications, eliminating the need to remember multiple sets of login information and improving the overall user experience.



Enterprise Preference for Corporate Identity Provider

Large Enterprise Adoption

The majority of large enterprises prefer the corporate identity provider scenario for their SAP BTP implementations.

Existing Investment

Many organizations have already invested significantly in robust identity management solutions.

Integration Complexity

Reduced complexity compared to maintaining multiple identity systems.

Based on experience, this is the preferred option for many large enterprises, especially those that have already invested in robust identity management solutions. It allows them to leverage their existing infrastructure while providing a seamless experience for their users.



Summary of Authentication Scenarios

Authentication Scenario	Key Characteristics	Best For
Standard Identity Federation	Uses SAP ID service, preconfigured by default on SAP BTP	Development environments, quick setup needs
Identity Authentication Tenant	Uses your instance of the Identity Authentication service	Organizations wanting to integrate enterprise users with custom branding
Corporate Identity Provider	Uses your existing corporate identity provider	Large enterprises with established identity management systems

Each authentication scenario has its place in the SAP BTP ecosystem. The right choice depends on your specific requirements, existing infrastructure, and organizational needs. Consider factors like user experience, security requirements, and integration complexity when making your decision.

A AUTHENTICATION METHODS

