Deloitte.

SAP

Towards Risk-Based and Passwordless Authentication in SAP Applications

MAKING AN IMPACT THAT MATTERS since 1845

Executive Summary

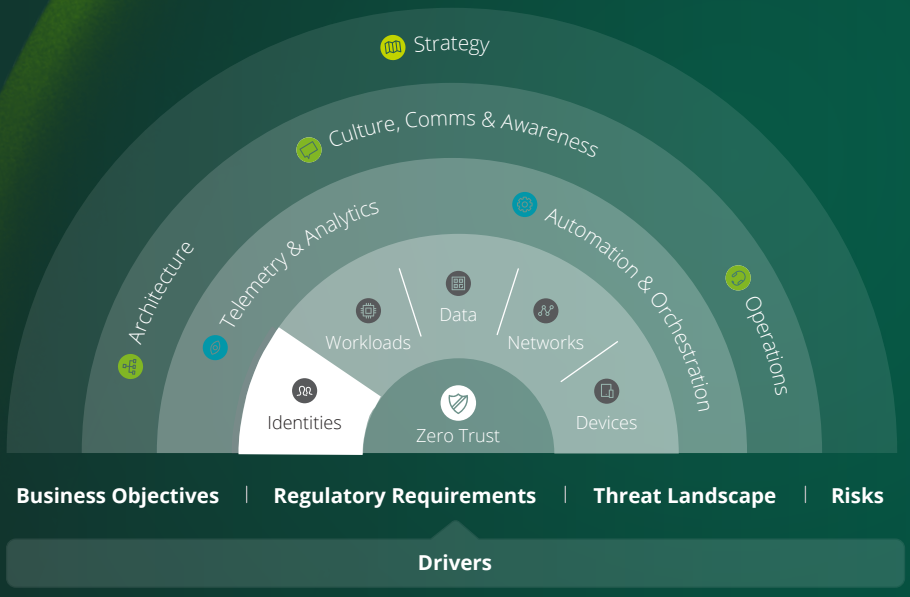
Due to an ever-increasing digitalization of business operations, companies are constantly acquiring and implementing new technologies within their SAP landscape as a means to ensure their competitiveness. These acquisitions, in turn lead to an expanding attack surface and paint a bigger and more vulnerable target to cyber attackers attempting to outmatch their cyber defenses.

Zero Trust posture adopts the moto: “Never trust, always verify” and limits, as much as possible, the access to valuable information in the event of a cyber incident. Passwordless is a cutting-edge feature that actively helps protect the access to SAP information by authenticating services without traditional credentials while improving productivity and security.

Following the series of stories launched by the “Towards a Zero Trust Architecture in SAP Landscapes” paper, this story focuses on Risk-Based and Passwordless Authentication in SAP Applications. Specifically, it reveals which are the currently available methods and the main benefits of using them. It also presents how biometric authentication works when replacing a typical password, leveraging the SAP Identity Authentication Service (IAS).

Executive Summary

This story is focused on the **Identities domain** of the Deloitte's Multidisciplinary Zero Trust Framework :



The Identities domain comprises the integration of centralized and consolidated identity technologies with the digital identity landscape to embrace context aware authentication. Passwordless and Risk-based authentication drives the context aware authentication as different authentication methods can be defined considering the risk based on system and actor characteristics.

STRATEGY LAYER
Zero Trust strategy should be aligned to the business drivers in a way that the journey is supporting the business, ensuring organization-wide adoption, future readiness and agility

GOVERNANCE LAYER
Zero Trust governance ensures a cohesive top-down strategy that considers stakeholders consensus to achieve necessary cultural, architectural and operational changes

ENABLING LAYER
Enabling layers help automate & orchestrate enforcement policies while continually analyzing enforcement decisions to identify Zero Trust violations

CORE DOMAINS
Zero Trust model is built upon strong foundational capabilities across five foundamental domains. The maturity across these domais will utimately determine Zero Trust maturity

Passwordless Authentication

What is it and where does it differ from the typical authentication?

As it can be inferred from its name, passwordless means that no password is used in the authentication mechanism. This alternative strengthens security by eliminating password management practices and minimizes the risk by eradicating various threat vectors (e.g. password spraying, phishing).

Some methods of passwordless authentication include:

One-Time Password

A one-time password (OTP) is a code that is valid only for a specific period of time. It is typically used as Multi-Factor Authentication (MFA) during a login session or a critical transaction. In SAP, this code can be sent to the person being authenticated through a dedicated application, Web, SMS, E-mail or RADIUS.

Although sending the OTP for MFA via SMS is better than not using MFA at all, this method is currently being heavily targeted by attackers and has consequently become more vulnerable as attackers explore it. This growing vulnerability is due to its inherent characteristics such as: lack of encryption, vulnerable to phishing and inoperability due to communications provider outages.

Biometrics

There are unique physical traits than can be leveraged in the authentication process. This method uses the fingerprint to verify a person's identity without requiring any password. This option is very effective as the likelihood of finding two identical fingerprints is 1 in 64 trillion.

What are the main separate benefits and methods that come with it?

Password Re-use

Despite being against the majority of the company policies, many employees use the same password for multiple internal and external applications. If one password is disclosed during an attack such as a phishing campaign, several applications are exposed.

User Experience

Memorizing several different passwords while ensuring the security of each of them, either through complexity requirements or difference compared to other passwords (both current and past passwords), is no easy task. By defining only one strong password user experience is greatly increased.

Productivity

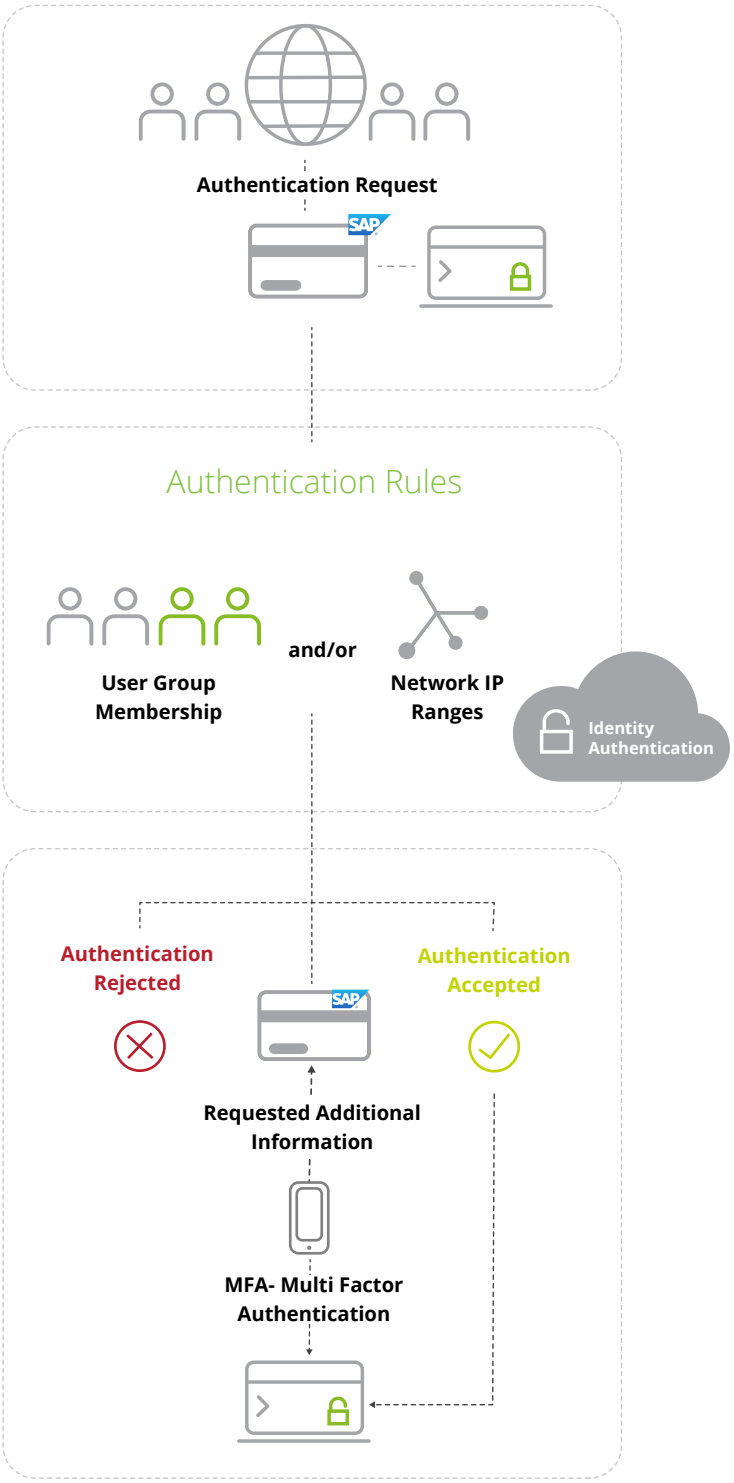
When using one of the passwordless mechanisms, time is saved as the user does not have to remember its different passwords and manually input the correct one. In fact, depending on the mechanism and the configuration, it is even possible for the user to login without any interaction (Single Sign-On). Furthermore, when a password is forgotten, the recovery process will only need to be applied on one password, versus having to do it to a multitude of different passwords. Which, depending on the criticality of each application, may take a long time and require multiple approvals.

Risk-Based Authentication

What is it and where does it differ from the typical authentication?

A Risk-Based Authentication strengthens security authentication by processing the likelihood of the access to a given system is compromised. In fact, leverages the context which a user is trying to log in and decides, based on a predefined set of rules - the risk of that authentication.

Common criteria for assessing risk includes **geographic location** and **IP address.**



Towards Authentication Security in an SAP Environment

On-premises Applications using Single Sign-On (SSO)

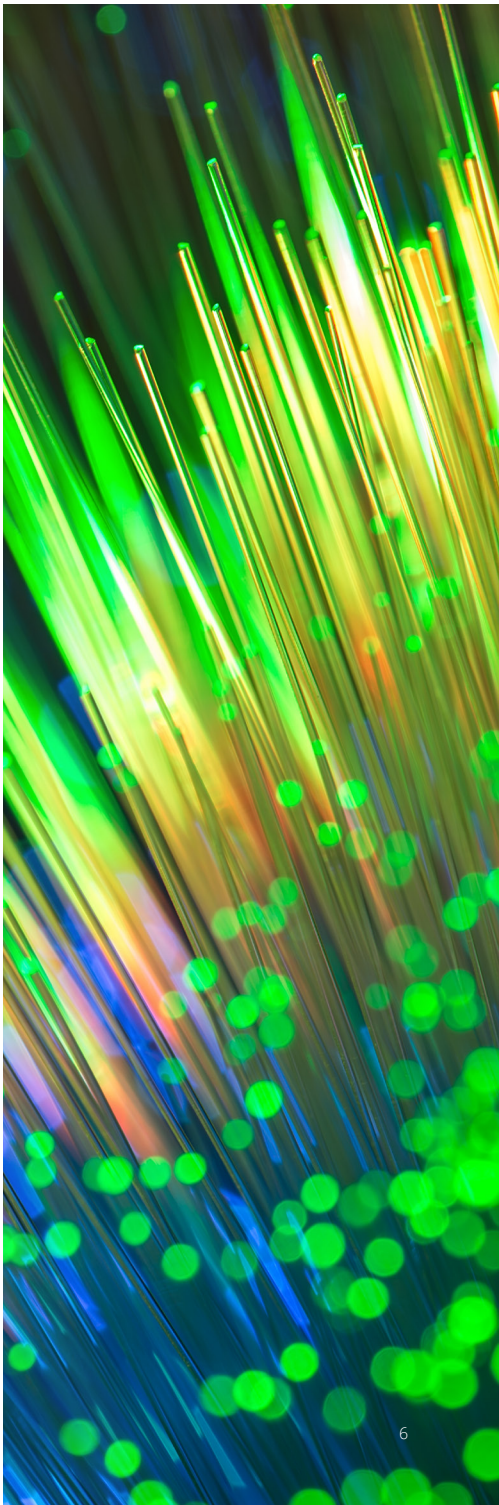
Single Sign-On is a service that allows a user to use one set of login credentials to access across multiple applications. In SAP, this feature is achieved by using the Secure Login software solution and may be used to provide authentication in SAP GUI, HTML-based user interfaces (over HTTPS) and Third-party application servers (with Kerberos or X.509 certificates). In fact, this software may provide authentication with a wide variety of mechanisms:

- Windows Domain (Active Directory Server)
- RADIUS server
- LDAP server
- SAP Single Sign-On 3.0
- Smart card authentication
- RFID identification
- Public-Key Infrastructure (PKI)

Cloud-based Applications using SAP Identity Authentication Service

The SAP Identity Authentication Service provides a controlled cloud-based authentication of users to access the business processes, applications, and data hosted in the cloud. This service provides not only traditional authentication, but also Single Sign-On and Passwordless authentication.

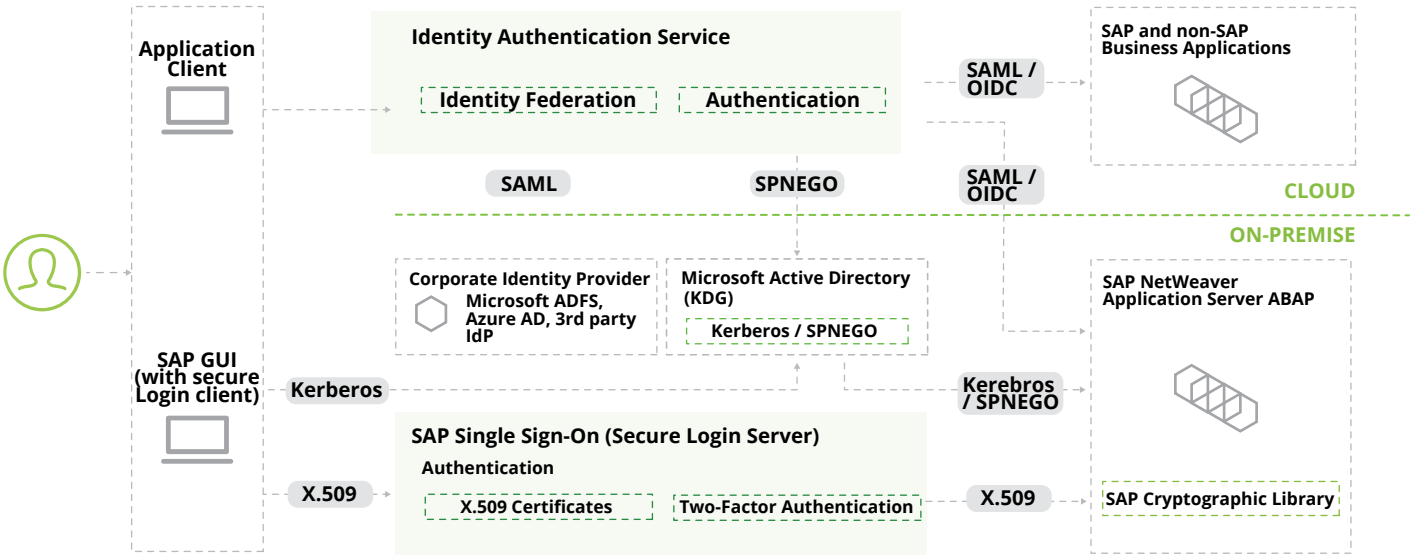
To begin this setup, first an identity authentication tenant must be created. This tenant represents a single instance of a specific configuration within a segregated environment. After the tenant is created, it is possible to configure and perform authentication related actions such as user management and provisioning, password policy definition, authentication method definition, social identity providers definition and integration with external systems.



Towards Authentication Security in an SAP Environment

Hybrid Architecture for Passwordless

The SAP Single Sign-On and the SAP Identity Authentication Service can be used together to accomplish a secure login across all SAP Landscape. While the first service focuses on employee scenarios and on-premises infrastructure, the last one targets cloud applications beyond the corporate user base. The image below illustrates how these can be combined to work together:

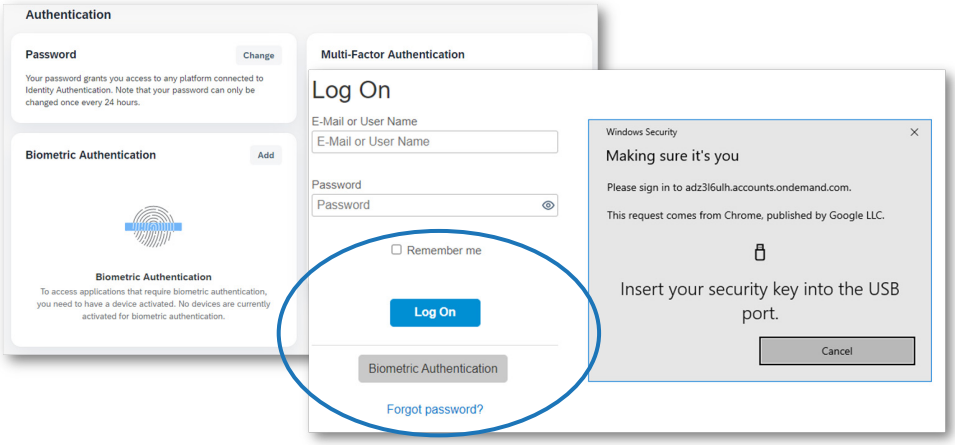


Source: SAP Cloud Identity Services, Identity Authentication - Solution Overview

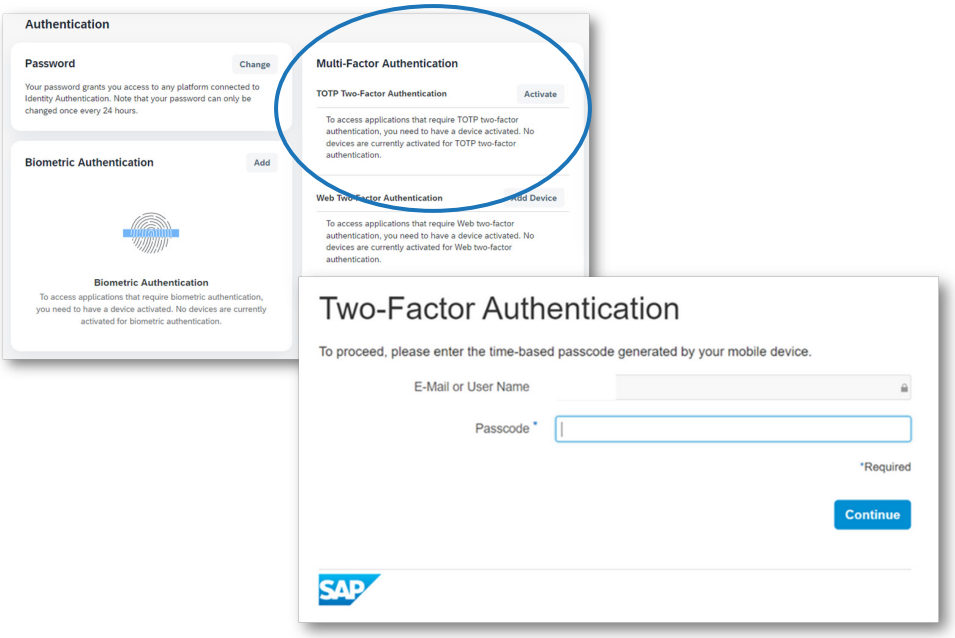
Towards Authentication Security in an SAP Environment

How does it work with the Identity Authentication Service?

After a proper configuration in the Identity Authentication Service tenant and a fingerprint device & identity registration, we are able to successfully login a user in an SAP cloud-based application.



Alternatively, another option would be to setup MFA authentication with TOTP:



Towards Authentication Security in an SAP Environment

Defining Risk-Based Rules to Assess Risk

In administration console for SAP Cloud Identity Services, Risk-Based rules may be defined according with the following factors:

Group Membership

- Cloud user group (defined in the Identity Authentication service)
- On-premise user group (e.g. LDAP User Group)

Condition

Network IP Addresses

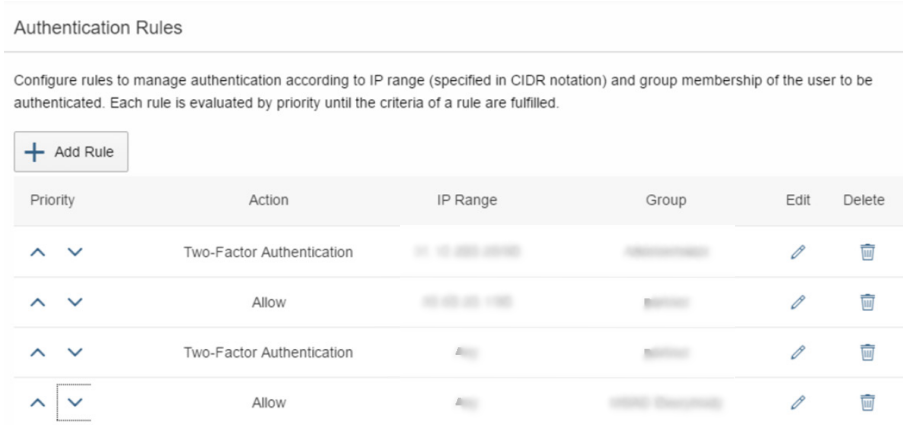
Actions

- Allow access
- Enforce Two-Factor Authentication
- Deny access

Combining these factors, it can be defined different risk-based authentication rules, such as:

- Deny Access from outside corporate network except a certain group of users that are on a remote work model, and it would be asked to authenticate with Two-Factor Authentication
- Apply stronger security for the administrators' access that are on a group of users.
- Enable MFA for specific users of a specific application

If none of the conditions of the defined rules are met, a predefined default action is performed.



Future Challenges

- Implement external MFA in SAP GUI authentication
- Third-Party IAM/PAM integration in the SAP Environment

Authors

Andre Correia Sousa
Portugal SAP Security Expert
andrsousa@deloitte.pt
+351 962753775

Matthias Sill
Germany SAP Security Expert
msill@deloitte.de
+49 15158000306

Contacts

Andre Correia Sousa
Portugal SAP Security Expert
andrsousa@deloitte.pt
+351 962753775

Antony Jose Vallookaran
Poland SAP Security Expert
anvallookaran@deloittece.com
+48 123944429

Fabio Bonanni
Italy SAP Security Expert
fbonanni@deloitte.it
+39 0283326347

Gabriele Piersanti
Spain SAP Security Expert
gpiersanti@deloitte.es
+34 638315587

Hans Peersman
Netherlands SAP Security Expert
hpeersman@deloitte.nl
+31 882887368

Marc Noergaard
Denmark SAP Security Expert
mnoergaard@deloitte.dk
+45 22300140

Marisa Geldenhuys
UK SAP Security Expert
mgeldenhuys@deloitte.co.uk
+44 7552 549146

Matthias Sill
Germany SAP Security Expert
msill@deloitte.de
+49 15158000306

Rajwinder Singh
USI SAP Security Expert
rajwindsingh@deloitte.com
+1 (470) 3624637

Vaibhav Jani
Canada SAP Security Expert
vaijani@deloitte.ca
+1 4167757269

Vikas Bhan
Belgium SAP Security Expert
vbhan@deloitte.be
+ 32 24558752

Deloitte.