Auth Shield
Multi Factor Authentication

An Authentication Security Organization

Whitepaper

Integration of AuthShield Multi-Factor Authentication with SAP Login Interfaces

By Innefu Labs

Auth Shield
Multi Factor Authentication

Contents

1. Overview

SAP is run by over 250,000 customers worldwide, including 87 percent of Global 2000 companies and 98 percent of the 100 most valued brands. Despite housing an organization's most valuable and sensitive information, SAP systems are not protected from cyber threats by traditional security approaches.

A recent study conducted by the SAP solutions provider revealed that more than 95 percent of enterprise SAP installations are affected by serious security issues that open them to cyber-attacks that could result in a dangerous data breach. The assessment confirmed that more than 250,000 SAP business customers worldwide, including 98 percent of the 100 most valued brands, are potentially exposed to cyber-attacks that could exploit a series of vulnerabilities.

Access to SAP can be used for –

- Espionage
- Stealing financial information
- Stealing corporate secrets
- Stealing supplier and customer lists
- Stealing HR data
- Sabotage

"559 SAP servers worldwide are at risk of the denial of service vulnerability, with a cluster of vulnerable servers located in London and Ireland. Most, however, are located in India, the US or China." - ERPScan

Furthermore, ERPScan suggested that it was able to identify almost 36,000 SAP systems in use worldwide now, which are running services vulnerable to cyber-attacks. Most of those services (69 per cent) should not be exposed directly to the internet.

ERPScan warned that professional hackers are increasingly turning their attention to industry-specific solutions. Hacker could manipulate financial data and change entries to move funds to an outside account. They could:

- Alter the remittance address on vendor records
- Create a new vendor and manual check entry
- Change general ledger accounting records
- Increase customer credit limit
- Credit the balance in a customer account in order to get a refund

"SAP released 36 vulnerabilities in SAP products, most of them are clickjacking. This patch update also contains fixes for several dangerous vulnerabilities".

The SAP threat landscape is always growing thus putting organizations of all sizes and industries at risk of cyberattacks. The idea behind SAP Cyber Threat Intelligence report is to provide an insight on the latest security threats and vulnerabilities.

In such a scenario, to protect themselves, more and more organizations should use Two Factor Authentication system to protect SAP logon credentials.

2. Threats to SAP Accounts

a. Social Engineering or Password Sharing

Most people end up sharing their passwords with their friends or colleagues. The act may be deliberate or accidental. But the fact remains that a user seldom even remembers the number of people the account details may have been shared with. At the same time, passwords are not changed at frequent interval, giving an outsider unlimited access to an account. Occasionally, users also fall prey to common social engineering techniques and end up revealing answers to their security questions thereby providing intruders a chance to gain unauthorized access to the account.

b. Reuse Logins

A user on the net usually has more than one account. Most users end up using same or similar passwords in multiple accounts leading to a possibility where an inadvertent leak may lead to providing access to multiple accounts

c. Identity thefts – Phishing

"One Phishing attack at a Bank / Online Portal / store/ BPO etc can lead to a loss of thousands of accounts in one step. Acquire details such as credentials to SAP and other critical applications etc by masquerading as a trustworthy entity. Such an information breach by authorized personnel either intentionally or accidentally, can cause irreparable damage to an organization.

d. Virus, worms, Trojans

Keyloggers, remote sniffers, worms and other types of Trojans have been used since the evolution of the internet to steal user's identity. Most data is accessed from stolen computers and laptops or by hackers capturing data on unprotected networks.

3. Protecting SAP Accounts

When your organization banks on you, what do you bank on?

Prevention is always better than cure. It is truer today than ever before when the theft is conducted on the net with no physical threats and with less cost to the perpetrator of the crime. The only challenge that remains is to cover ones tracks and considering the massive flow of information on the net almost on a daily basis, it is not much difficult either.

Multi-Factor Authentication: why do you need it?

Phishers try to obtain personal information such as your password or PIN-code by pretending to be a legitimate entity.

Using Phishing, static passwords can be easily hacked providing fraudsters easy access your personal accounts, files and confidential information.

AuthShield - Multi Factor Authentication maps the physical identity of the user to the server and increases the security of financial and other critical systems. Integrating Stronger User Authentication system not only helps prevent Online Credit Card fraud, Card Cloning, Identity theft but also helps in the capture of habitual cyber criminals.

AuthShield authenticates and verifies the user based on –

- ❖ something only the user has (mobile phone/ land line/ hard token)
- ❖ something only the user knows (user id and password)
- ❖ something the user is (Biometrics)

AuthShield technology uses a dual mode of identification where along with the user id and password, client shall be prompted for second factor of authentication check, the second factor of authentication needs to be validated.

One-Touch Authentication

AuthShield One Touch authentication bypasses the entire Concept of One Time Password and replaces it with One Touch Authentication.

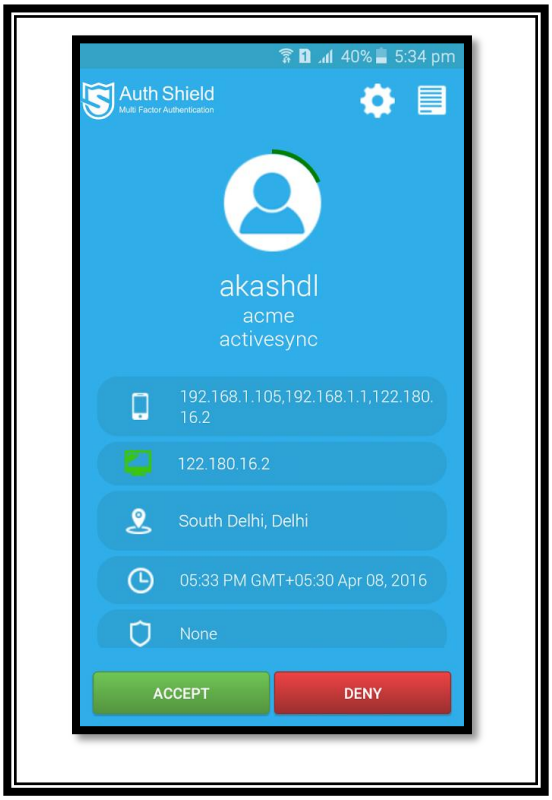
Anytime a user wishes to login using Two- Factor Authentication a 'Push' notification is sent to his smartphone or his desktop with details of the authentication request and an option to approve or deny the request at a click of a button. The token replaces 'Seed' based token with a challenge response architecture based on PKI.

One-Touch Authentication

"With One-Touch Authentication, secure access is just One Click away".

Mobile One Touch Authentication

Mobile One Touch Authentication is a latest Two Factor Authentication mechanism brought out by AuthShield Labs. The authentication mechanism bypasses the entire concept of One Time Passwords by converting the user's handset into a secondary form factor using a challenge Response mechanism. Any time the user wishes to log in, a 'push' notification is sent to the registered handset of the user with the login details including IP address, Time stamp, location (based on IP) etc. The user has to 'approve' or 'deny' the request to login. It's a complete 'Hackproof' token and cannot be compromised even by compromising the server or the device.

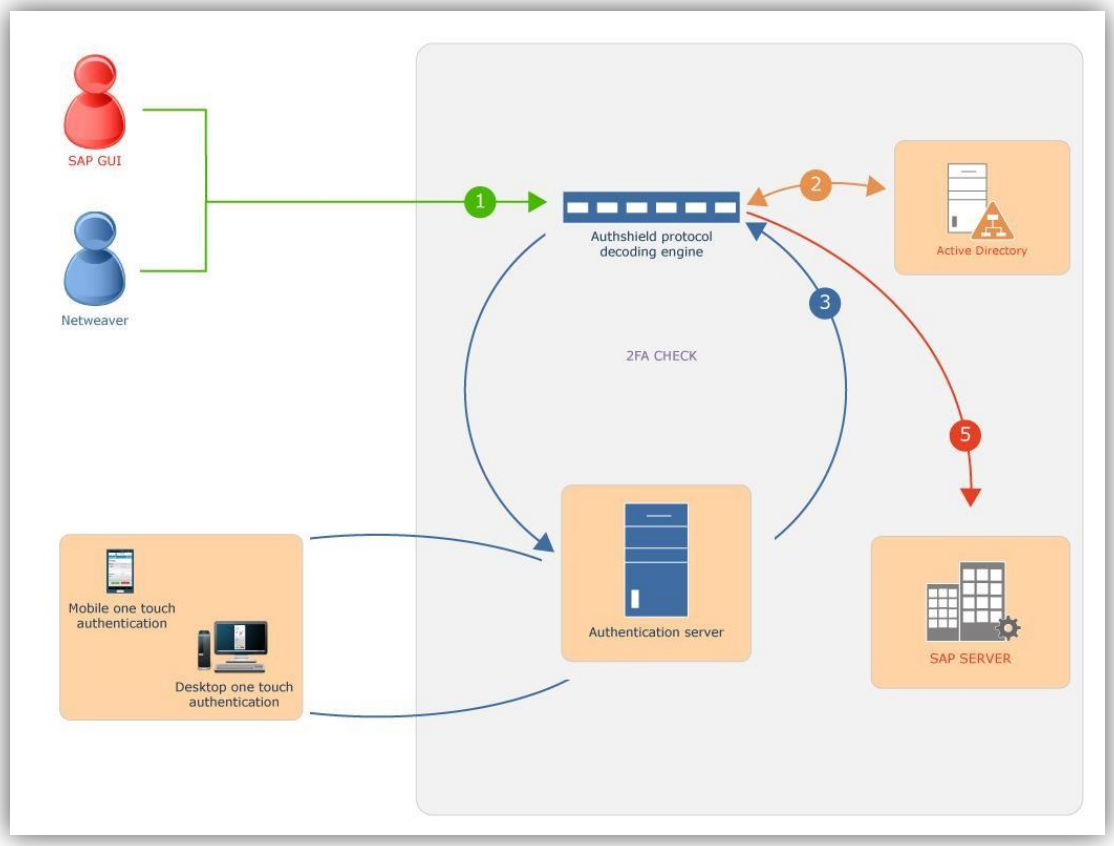


Desktop One Touch Authentication

Desktop One Touch authentication mechanism bypasses the entire concept of One Time Passwords by converting the user's registered desktop / laptop into a secondary form factor using a challenge Response mechanism. Any time the user wishes to log in, a 'push' notification is sent to the registered desktop of the user with the login details including IP address, Time stamp, location (based on IP) etc.

4. Two-Factor Authentication for SAP systems

Technical Architecture



Process

- The client enters his user name and password in SAP GUI or on Netweaver
- The authentication request is forwarded to the protocol decoding engine which identifies Authentication packets and then validates from Authentication Server whether the user has to be validated for Second factor of authentication or not
- Authentication Server generates an One Touch Authentication Request and sends it to the registered device of the user
- In case the client approves the request, the original request is forwarded to the SAP Server else the original request is rejected.

5. Features

- OS Independent Authentication Mechanism
- Seamless Integration with the current business and security architecture
- Increases the log on security for Mails
- 99% security from Phishing attacks and identity thefts
- Unbreakable encryption on the lines of those used by US Government
- Logs are maintained to fix responsibility in case of an unlawful event.

6. Advantages of using AuthShield

For Users

Using AuthShield Multi-factor authentication can help in preventing-

- Online credit card fraud Phishing
- Card cloning
- Unauthorized access to data by employees.

For the organization

- OS Independent Authentication Mechanism
- Seamless Integration with the current business and security architecture
- Increases the log on security for critical applications.

7. About Us

The world today revolves around information. Information today is the energy that plays a critical role in our personal lives and drives our businesses. As we move further into this digital age, it has become imperative to not just protect our information from outsiders but to also draw intelligence from the vast amount information available to us.

Internet is the new playground for unwanted elements of society intent on committing terrorist or espionage activities, financial frauds or identity thefts. Keeping this in mind, it has become imperative to not only prevent these acts but also be in a position to intercept, monitor and block Internet communication to draw intelligence out of them.

AuthShield is an Authentication Security solution with a patented technology on implementing Multifactor Authentication at a protocol level. This makes it an application independent technology and needs no changes at the application. As an advantage of working at protocol rather than application level, an organization can use AuthShield to implement Multifactor Authentication in any and every technology such as **Downloading mails on phones / desktops,** SAP, Database queries, Internet of Things, or any other enterprise or cloud technology in a matter of minutes.

For more information visit - www.auth-shield.com