TrustBroker | Authentication for GDPR compliance

GDPR General Data Protection Regulation

Protecting access to personal data with Multi-Factor Authentication (MFA) and Secure Single Sign-On (SSO)

Overview

Which data needs to be protected?

For GDPR compliance, you are required to protect access to personal data belonging to individuals in the EU. This includes individuals who are not an EU citizen or resident. The personal data is most likely being held in your SAP® systems, so you need to protect it.

How do you protect access to the personal data?

Ensure that SAP users have been assigned the correct roles, so that personal data access is restricted only to those that need access to it. You can use the SAP GRC products or products from Security Weaver to assist you with this.

You also need to consider your use of static passwords...

Using static passwords under GDPR is not good enough...

Somebody may be able to determine a password (see Verizon DBIR) belonging to a user who is allowed access to personal data. The GDPR discourages the use of a weak protection method for sensitive/personal data, and requires that you carry out a risk assessment. Have you completed your GDPR risk assessment yet? It is very unlikely that your risk assessment determines that just using static passwords is acceptable.

Using multi-factor authentication (MFA) instead of passwords

Using MFA will significantly reduce the risk of stolen passwords (see Verizon DBIR) giving unauthorised access to personal data, causing GDPR non-compliance and significant fines.

These fines can be up to 4% of the global annual turnover of your company, or €20 million, whichever is greater. Fines of this size could lead to business insolvency.

How can the TrustBroker products help?

When using the CyberSafe TrustBroker products, a user can be required to use MFA, but **only when needed**; otherwise it becomes an inconvenience, causes frustration and reduces user productivity.

The user can be given the ability to use Single Sign-On (SSO) when they logon to an SAP business application that doesn't give them access to personal data. This flexibility allows strong authentication to be used for protecting access to personal data, as well as giving the convenience of SSO when MFA is not required.

Verizon DBIR

The most common cause of a data breach

The Verizon 2017 Data Breach Investigation Report (DBIR) confirms that **81%** of actual data breaches were caused by an attacker using one or more of the following methods:

- Guessing an end user's weak password.
- Recognizing that the user has not changed their password, and is using a default password.
- Using phishing or social engineering, to steal a user's password. This method accounted for **43%** of data breaches...

The attackers are getting more effective !

In the 2016 edition of the Verizon DBIR the data breaches figure was **63%**, so gaining access to end-users' passwords is clearly becoming easier and more common.

The risk of an attack is far greater than ever before. Attackers are clearly getting more effective at gaining access to your data, including personal data that you need to protect for GDPR compliance.

Multi-Factor Authentication (MFA)

What is it?

A method of confirming a user's identity only after they successfully present 2 or more pieces of evidence (or factors).

Sometimes two-factor authentication (2FA) is sufficient which is just using 2 factors.

Factors can be:

- **Knowledge** - something the user and only the user knows, such as a password.
- **Possession** - something the user and only the user has, such as a token device or mobile phone.
- **Physical characteristic** - something that confirms who the user is, such as a fingerprint or an iris scan.

Multi-Level Authentication (MLA)

What is it?

The TrustBroker products provide multi-level authentication (MLA) for SAP application users.

TrustBroker first authenticates the user during their logon to an SAP system (this is referred to as level 1 authentication), e.g. using Single Sign-On (SSO), or just asking the user to enter their Active Directory credentials.

After level 1 authentication, the TrustBroker product on the SAP application server can use an authentication policy. This policy might be configured to check the SAP roles assigned to the authenticated user to determine if stronger authentication is required (this is referred to as level 2 authentication) before the logon is allowed to complete.

For GDPR

The level 2 authentication policy can be configured to check whether the user is assigned a SAP role which is only used for access to personal data. This means that MFA will only be used when required. This policy can also check the user's network address so the authentication method used can change depending on which network the user logs on from.

For Administrators

The level 2 authentication policy can also be configured to force MFA for an administrator logon by checking whether the user is assigned an SAP administrator role.

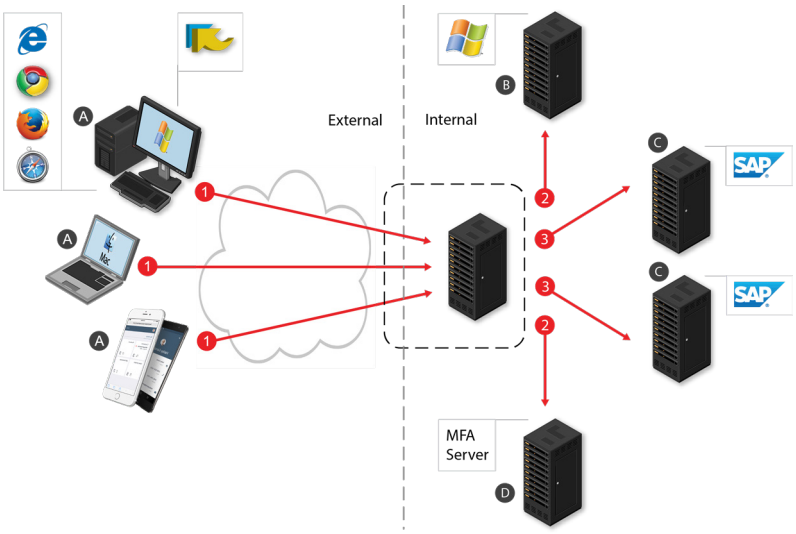
Taking authentication to another level...

After the user has logged into the application, an optional level 3 authentication policy can be used to determine if they need to authenticate again based on what data they access, transaction they enter (when using SAP GUI), or SAP Fiori® tile they click on.

Perimeter and end-point authentication

Using a Virtual Private Network (VPN) at the network perimeter to remotely access SAP systems

When users need to login to the SAP systems on the Internal network (as shown by 1 and 3 in the diagram below), they first need to authenticate to the VPN.



The VPN can be configured to authenticate users with their Active Directory credentials or using an MFA Server (see 2 in the above diagram).

The user's identity can only be fully trusted if MFA is used, as per best practice. This is recommended, as far as it goes, but MFA should be used for all access methods, not just for VPN user authentication.

Accessing SAP systems using other access methods

In modern networks, **the perimeter is becoming harder to define**, and is no longer the only access method which needs to be protected using MFA. Users need to access SAP systems on the Internal network from the Internet as well as from workstations on the Internal network.

Data Breach Examples

The 2017 breach at Deloitte was caused by the attacker being able to gain administrative access. They subsequently implemented MFA to enhance security and help avoid a similar attack in the future. *

* (Source: https://bit.ly/2yrRU92)

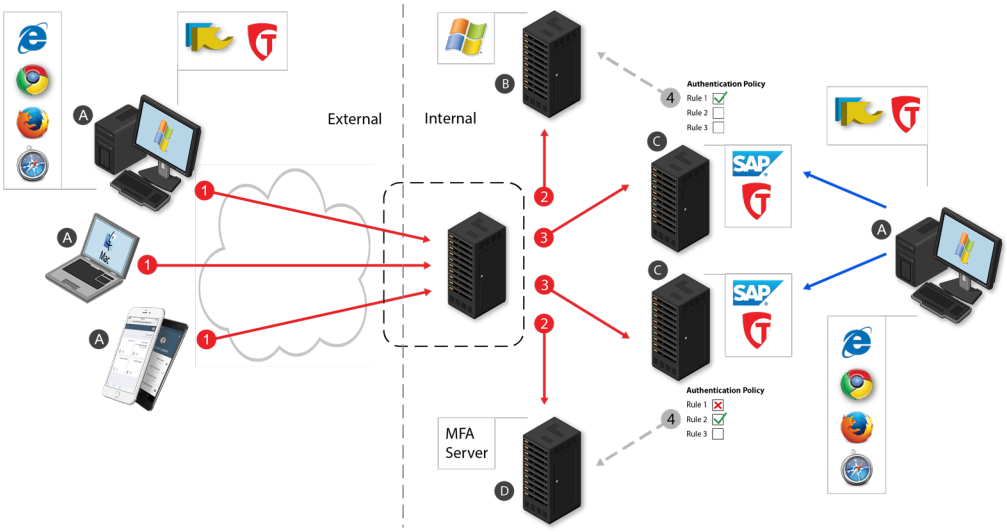
In 2014 a data breach occurred at a well-known American entertainment company. The attackers were able to find SAP users' passwords in text files, as well as IT security assessment reports allowing them to discover and exploit weak spots found during a recent audit. To reduce the risk of another breach, they have recently implemented MFA for users who logon to the company's SAP systems.

The Greek Ministry of Finance was hacked in 2012, involving a "sweet 0day SAP exploit", and files containing SAP users' passwords were accessed. It was also discovered that a large volume of user passwords were 123456. *

* (Source: https://bit.ly/2Ic5z8X)

Using TrustBroker products to authenticate the user at the end-point

The TrustBroker products can use multi-level authentication (MLA) to enforce MFA at the end-point (e.g. the SAP system application server, shown by C in the diagram below) so it doesn't matter which access method is used to access the SAP systems.



From the Internal network (the internal access method)

The TrustBroker products will protect access to personal data by authenticating the user at the end-point C. The level 2 authentication policy (see Multi-Level Authentication) will enforce MFA only if they have been assigned an SAP role that gives them access to personal data.

Making the authentication method decision at the end-point C ensures that MFA is used for both external access and for access whilst on the internal network, and only when required.

From the Internet (the external access method)

If the VPN is configured to use MFA and the TrustBroker products are protecting access to personal data at the end-point C, then you might expect the user to be required to use MFA twice. However, TrustBroker can be configured to accept the VPN authentication so the user only needs to use MFA once when they access the SAP systems over the Internet.

Using SAP Fiori Client on mobile devices

Many companies are implementing SAP Fiori applications for end users, and these end users might not access the SAP Fiori Launchpad via a VPN. Instead, an Internet-facing gateway such as a reverse proxy might be used, but this doesn't always affect how the user is authenticated. The end user is able to reach the SAP Fiori Launchpad Sign-On screen without being forced to use MFA, but the TrustBroker products can solve this by authenticating the user with MFA at the end-point.

Summary

These other access methods can become **a weak link** - so, you need MFA for access to SAP business applications regardless of whether the application is accessed remotely or via the Internal network. If you use the TrustBroker products, the end-point (e.g. SAP NetWeaver AS for ABAP, SAP Fiori Launchpad, C in the above diagram) can enforce MFA only for users who have access to personal data - just using a static password cannot be trusted for GDPR compliance.

Key

- A — A mobile phone with a Web browser or SAP Fiori Client, or a Windows workstation or Mac with a Web browser, SAP GUI and TrustBroker.
- B — Microsoft Active Directory domain controller.
- C — Server running SAP NetWeaver AS for ABAP and TrustBroker.
- D — An MFA Server.

Step-by-Step

1. The user attempts to logon to an SAP system.
2. The VPN / Gateway uses Active Directory domain controllers and/or the MFA Server to authenticate users who logon from the External network.
3. After the user has been authenticated by the VPN / Gateway, their session is forwarded to the SAP system application server.
4. When TrustBroker is used to authenticate the user at the SAP system end-point, the authentication policy is checked - if the user has access to personal data (determined by checking the users SAP role assignment) they are authenticated using Active Directory credentials and/or MFA.

Data Privacy / Confidentiality

Why do you need it?

If personal data is being transmitted over a network after users logon to your SAP systems, this data can potentially be captured and could get into the wrong hands, causing a significant GDPR fine.

How do you make data private?

You should use Secure Network Communications (SNC) for thick client security (e.g. when users logon with SAP GUI) and HTTPS for Web based applications. You will then ensure that all data transmitted over the network is encrypted after users logon to your SAP business applications.

How can the TrustBroker products help?

The TrustBroker products include an SAP certified SNC library that can be used to encrypt application data as it passes over the network after a user has logged on. The same SNC library also offers MLA features to help you protect access to personal data for GDPR. It is only possible to use one SNC library at a time on SAP NetWeaver AS for ABAP, so make sure you choose an SNC library that does everything you need.

CyberSafe can help you implement the TrustBroker products, and realise the many benefits. It might only take a few days/weeks. You should not implement an SNC library without first talking to CyberSafe and checking the costs and implementation effort involved.

Key Features & Benefits

1 One Active Directory unique identity and credential for each user

Increased user productivity

Reduced costs

Quick ROI ✓

Protects personal data for GDPR

- ✓ Quick and easy product installation.
- ✓ No additional infrastructure is required.
- ✓ Can be used for Single Sign-On as well as MFA.
- ✓ A level 2 authentication policy can be configured to enforce MFA, only when required.
- ✓ SAP passwords are not required, transmitted or used.
- ✓ You can use your existing MFA Server.
- ✓ Easy troubleshooting to minimise downtime.
- ✓ Improves user satisfaction and productivity.
- ✓ Very affordable and flexible.

Top Tips / GDPR Checklist

Follow this checklist to ensure success

- ✓ Arrange your GDPR risk assessment as soon as possible, and make sure that all user authentication methods are considered.
- ✓ Make sure you consider access to SAP systems from the Internet as well as from your Internal network.
- ✓ Implement MFA for both your external access requirements and access from your Internal network.
- ✓ Contact CyberSafe to discuss your requirements, and to learn more about the TrustBroker products...

Tel: +44 203 510 6333
Tel: +1 929 333 4499
Email: Info@CyberSafe.com
Web: https://CyberSafe.com/SAP

CyberSafe

Version 1.3 - 26/03/2018