

TrustBroker Security Solutions
for SAP Business Applications

Solutions Overview


Version 1.0
29th August 2011

Security and authentication solutions that adapt to your needs

The TrustBroker Security Solutions are a comprehensive range of solutions, implemented using various CyberSafe TrustBroker products, and designed to provide strong user and application authentication and improve security for SAP business applications. If you are looking for secure SSO or have more complex requirements, the TrustBroker products can be used to implement a solution to meet your needs.

The details in this document, which describe our comprehensive range of security solutions for SAP business applications, can be found on the [CyberSafe SAP Solutions website](#). We suggest you check the website to ensure you are referring to the latest information.

What is TrustBroker?

 A family of security products from CyberSafe, which provide strong user and application authentication and take full advantage of an existing Microsoft Active Directory infrastructure, enforcing security policy when authenticating users and ensuring that application data is secured when in transit. You can read more about the product family [on the CyberSafe website](#), and discover the many features and benefits.

Used for SSO

TrustBroker products can be justified on the basis of their secure single sign-on (SSSO) capabilities alone, for example:

- Reduced chance of forgetting passwords, therefore fewer calls to the help desk;
- Increased productivity, since productivity is effected when users forget their passwords;
- Passwords are not stored or transmitted, so security is improved;
- Protection of data in transit, so business data cannot be intercepted.

Beyond SSO

Many organizations find that they want more than SSO, so they take advantage of the products' numerous capabilities to gain additional benefits. Indeed, an increasing number of CyberSafe customers use TrustBroker products **without using their SSO capabilities** at all. This is because TrustBroker products provide a lot more than SSO, especially when used with SAP business applications. The security solutions described below, demonstrate that TrustBroker products are scalable and flexible enough to meet virtually any company's SAP application user authentication and security needs, whether they are SSO or non-SSO related.

TrustBroker Security Solutions for SAP Business Applications

Environment

The requirements and solutions described on the following pages can be applied to these environmental conditions.

Workstation Platforms

Windows, Linux or Mac OSX

Application Server Platforms

Unix, Linux, or Windows Server

Workstation Applications

Any of the following:

- SAP GUI (Windows or Java)
- Other SAP Front End software
- SAP Business Explorer Analyzer
- Any RFC or JCO enabled application
- SAP Crystal Reports
- A product from an SAP partner that uses SAP protocols to logon to SAP applications (examples include Cideon AutoCAD Utilities, Korasoft Excel and many more...)

For Web based SAP business applications:

- A Web browser (IE, Firefox, Safari, Chrome)

Server Applications

For applications which include a workstation component:

- SAP NetWeaver AS for ABAP

For Web based SAP business applications:

- SAP NetWeaver AS for ABAP or Java

CyberSafe Products

For applications which include a workstation component:

- TrustBroker Secure Client for Workstations - installed on each user's workstation.
- TrustBroker Secure Client for Servers - installed on the servers running SAP NetWeaver AS for ABAP, or on a middle tier server (e.g. BusinessObjects Enterprise, or .NET Application Server).

For Web based SAP business applications:

- TrustBroker Adapter - deployed into the SAP NetWeaver AS for Java.

Requirements and Solutions

Various requirements are described below, along with an explanation of the security solution and a list of benefits. Each solution involves implementing various TrustBroker products.

1. Secure SSO using Active Directory for authentication and key management

Requirement

A user logs onto their workstation using an Active Directory domain account. The credentials issued during this logon are then used to authenticate the user to SAP business applications, and the application data in transit is secured.

Solution

When a user logs onto their workstation using an Active Directory account, they are issued with Kerberos credentials. These credentials are used by TrustBroker to authenticate the user when they subsequently logon to the SAP business applications, so they don't have to re-authenticate. Also, the application data in transit is encrypted between the application on the user's workstation and the SAP applications on the servers.

We have prepared a series of 5 short videos, which demonstrate the TrustBroker products being installed and configured to implement SAP GUI Secure SSO.

[Watch the demonstration videos](#)

Benefits

- Many security benefits due to the Windows domain logon being linked to the SAP application logon. For example, you can be sure that the user who logs into the SAP application, is the same user who logged onto the Workstation.
- No passwords are passed over the network in clear text, so security and compliance are improved.
- Improving user productivity and reducing frequency and costs of help desk calls.
- For SAP GUI Secure SSO, this solution can be installed and users can benefit from it, in less than ten minutes.

2. Secure SSO using Active Directory for authentication and key management, where SAP NetWeaver is installed on a server in 'the cloud'

Requirement

The same as solution 1, but the user is logging onto SAP applications hosted in the cloud, e.g. using cloud hosting company services such as those provided by [Cirrus SAP Cloud Computing](#) or [Secure-24](#).

Solution

As with solution 1, secure SSO can be easily and quickly achieved, but the SAP NetWeaver software is installed on application servers in the cloud. For this to be achievable, the TrustBroker product installed on the SAP application servers needs to be configured so that it does not require Active Directory domain controllers to be available in the cloud, and the server doesn't need to communicate with the Active Directory domain controllers when authenticating users. Instead, the domain controllers are on your intranet, where the workstations are.

Benefits

- The same as with solution 1.
- The deployment and management of SAP systems in the cloud delivers many cost savings, especially related to infrastructure costs.
- Users can benefit from the same secure SSO experience they get when logging onto SAP applications which are not in the cloud.

3. Secure SSO with ability to turn off SSO for ad-hoc logon requirements

Requirement

When using secure SSO as described in solutions 1 and 2, occasionally a user wants to logon to an SAP application using a different Active Directory account from the one they used to log onto their workstation.

Solution

When using TrustBroker, it is possible to turn off SSO for these ad-hoc logon requirements. For example, Sally is logged on and enjoying the benefits of SSO, and she encounters a problem in the SAP application she is using, so she calls Andrew from the application support team. Andrew visits Sally and logs onto the SAP application as himself using Sally's workstation, so that he can make application changes to fix the issue. When Andrew has made the changes, he can logoff and Sally can then logon to the application as herself, using the credentials issued during her initial workstation logon.

Benefits

- Both users can use the same workstation and do not need to logon using a SAP user and password.
- The Active Directory infrastructure can be used for all authentication requirements, rather than just when SSO is used.
- The application data in transit is encrypted, improving security at all times.
- Sally can enjoy and benefit of SSO, and doesn't have to close all of her open applications, then log off her workstation and allow Andrew to logon to her workstation in order to logon to the SAP applications as himself, which would be typically be required to meet this requirement, if it was not possible to turn off SSO.
- The disruption to Sally's work is minimized, whilst Andrew uses Sally's workstation to assist her.

4. Active Directory authentication from shared workstations and kiosk computers

Requirement

In many companies, each user has their own workstation and can enjoy the benefits of secure SSO and strong authentication, yet there are still a number of "shared" workstations. For example, in a restaurant or coffee area, kiosk computers might be provided for all to use, or a manufacturing company might have workers in the factory or warehouse who need to logon to SAP applications.

If the SAP applications are configured to securely authenticate users in Active Directory, providing them with SSO (for example, when they open their browser they are logged onto a portal, or when they use SAP GUI they are authenticated using their existing domain credentials), these cases are not suited to shared workstations. The user would find it frustrating and time-consuming to log off Windows and logon again using their own Active Directory account and then open their browser or SAP GUI.

Solution

TrustBroker can come to the rescue, because the user can now logon to SAP applications on a shared workstation, via a web browser or via workstation applications such as SAP GUI, and they will be asked to authenticate to Active Directory during the SAP application logon. When they have finished they can log off and the next user can use the same workstation logon session and get the same secure logon experience.

Benefits

- No need to use less secure authentication methods on shared workstations. Many SSO products used for SAP applications do not address this requirement, so less secure authentication methods have to be used on shared workstations. With other products, if a user has a need to logon from a shared workstation and also from their desk where they want SSO, they would need two passwords.
- TrustBroker products allow the user to logon to both shared workstations and workstations on the intranet where SSO is demanded, using the same Active Directory account.

5. Active Directory authentication without SSO

Requirement

Some companies don't want SSO, perhaps due to a security policy decision, but they do want to use Active Directory for authentication when logging onto SAP business applications, so that the user doesn't have multiple passwords to remember.

Solution

The user logs on to their workstation, then, when they logon to the SAP application, they will be asked by TrustBroker to authenticate to Active Directory, and they can enter their account and password (or use a certificate on a smart card if desired - see solution 7). Once this process is successful, they will be authenticated to the SAP application. This is sometimes referred to as common authentication, since the user is taking advantage of Active Directory as a common authentication infrastructure, but it is not SSO since the user has to sign-on each time they logon to their applications.

[Watch a demonstration](#)

Benefits

- With common authentication, many of the benefits mentioned in solution 1 and 2 are achieved
- Users have fewer passwords to remember.
- The logon to SAP applications is secured, with no passwords transmitted over the network.
- The corporate security policy, which specifies that SSO is not allowed, can be adhered to, since TrustBroker products allow this level of flexibility.
- Active Directory can be used as a central infrastructure to manage access to the network and to business applications; For example, a user can be locked out of the company network and also prevented from logging onto SAP by just deactivating their domain account in Active Directory.
- There is no need to change anything in the many SAP applications related to user access, since SAP will always be using Active Directory authentication when users logon.

6. Partner company/extranet logon

Requirement

Many organisations have strategic business relationships with partner companies that offer added value services, for example managing their SAP systems. This kind of relationship often involves connecting the companies' networks to form an extranet. The use of Active Directory in an extranet would normally require Active Directory domain or forest level trust to be established, but often the organizations don't want to setup this kind of global company trust.

Solution

With TrustBroker, users in the partner organization can logon to the SAP applications via Active Directory authentication, but using the Active Directory domain of the company, and no domain or forest trust is required. The user in the partner organisation would logon to their workstation using their own domain, but when they logon to the SAP applications, TrustBroker will shown a sign-on screen where they are able to authenticate to the company's domain. Once authenticated to the domain, they will be logged onto the SAP application, and the application data in transit will be secured.

Benefits

- The benefits of managing SAP application logon using Active Directory can be achieved even when users are logged onto a different domain. This is a good example of where SSO is not desirable, but still Active Directory can be used to authenticate users logging on from the partner company network.
- Using Active Directory to manage authentication for all user logons to the SAP applications, regardless of which company they represent, has many advantages, including the fact that password policy and user authentication requirements can be maintained in one central infrastructure.

7. Smart card and certificate logon

Requirement

A company has invested in a smart card infrastructure and is using the certificates for secure e-mail and/or workstation Active Directory domain logon. When a user who has a certificate needs to logon to their workstation, they select their certificate and enter their PIN code. If SSO is not desirable for logon to SAP applications, and strong two-factor authentication is required for some or all users, it makes sense (in terms of optimizing the existing infrastructure, protocols and procedures) to use the same smart card and certificate already used by the users, and not invest in a new infrastructure or use proprietary protocols for smart card authentication to SAP applications.

Solution

The logon to SAP application using the same smart card and certificate used when logging onto the Windows domain is possible using TrustBroker products. The user logs onto Windows, and when they logon to the SAP application using SAP GUI, TrustBroker Secure Client shows a sign-on screen where they can select their certificate, enter their PIN and the certificate will then be used to authenticate them to Active Directory. If authentication is successful, the Active Directory Kerberos credentials issued using their certificate will be used to log them onto the SAP application.

[Watch a smart card logon demonstration](#)

Benefits

- Existing standard protocols and infrastructure can be used for certificate logon to SAP applications.
- There are no special requirements or changes on the SAP NetWeaver AS for ABAP, to support certificate logon.
- The decision on whether the user needs to logon using two-factor authentication with a smart card or logon using SSO is made in Active Directory policy configuration, or using standard software distribution tools to configure the users' workstations.

8. Active Directory domain policy configuration

Requirement

An organization might have a mix of user authentication requirements: some users might need SSO, some common authentication, others might need to logon with user account and password, while others might need to logon using smart cards. Maybe extranet logon to SAP application will require two-factor smart card authentication, but logon to SAP applications from the intranet can be performed using Active Directory based SSO.

Solution

All of these options and security policy requirements can be configured using Active Directory domain security policy tools, and TrustBroker products will ensure that the policy is adhered to when users need to logon to SAP applications.

Benefits

- No proprietary tools required for configuration of security and user authentication policy – instead, Active Directory standard features allow TrustBroker to determine how to authenticate the user when they logon to the SAP applications.

9. Active Directory authentication using web form as fallback if Integrated Windows Authentication (IWA) logon is not possible

Requirement

If Active Directory Integrated Windows Authentication (IWA) is used to logon to SAP applications via a web browser, the user gets an SSO experience, since the domain credentials issued during their logon to the workstation are used to authenticate them to the SAP applications. With this method of logon to SAP applications, the user will be authenticated via the HTTP Negotiate protocol (SAP refers to this as SPNEGO authentication). However, users who logon from workstations not joined to or logged onto a domain will get a browser dialog box, asking them to logon to the domain, which in many cases is not possible, or not user friendly.

Solution

For users who are not logged onto a domain, or who are logged onto an untrusted domain, TrustBroker Adapter can stop the attempt to authenticate the user to the domain and, instead, a fallback authentication method can be used where the user is shown a login form in their browser. Entering an Active Directory account and password into this form allows them to logon to the SAP application without their workstation being logged onto a domain. If during this form-based login the user's Active Directory password has expired, they can change it using a "change

password" screen, and the Kerberos change password protocol is used by TrustBroker Adapter to change their domain password.

Benefits

- This solution is very useful when contractors or other temporary staff need to logon to the SAP applications and are given an Active Directory account, but they are allowed to use their own laptop to logon to SAP applications. Since their own laptop typically won't be joined to the company domain, they would not be able to benefit from IWA. With TrustBroker Adapter, they can logon using the browser login form instead, and still use an Active Directory account to authenticate. This can also be used to logon to a SAP portal via the Internet: in this case, the user will not be asked for a domain logon.
- This logon method is more secure than using LDAP, and the UME user store configuration can be local to the Java stack or using the ABAP user store – there is no need to configure UME to use Active Directory.
- When using LDAP to authenticate, the user's password is sent to the LDAP server, but TrustBroker Adapter uses the more secure Kerberos protocol instead of LDAP, so no passwords are stored or transmitted.
- It is possible to deny access and manage identities, from a single point (e.g. in Active Directory) instead of in each SAP system.

10. BOBJ end to end authentication, and improved security

Requirement

SAP BusinessObjects™ Enterprise (BOBJ) allows users to logon via a web browser with IWA, so they get authenticated to BOBJ without needing to enter any credentials (the credentials issued during initial workstation logon are used). If they then request information which results in BOBJ needing to access SAP BW/BI, they would normally be asked to enter user and password to logon to BW/BI. Users don't like being asked to enter their credentials, and would prefer to be authenticated to SAP BW/BI using their already authenticated credentials.

Solution

TrustBroker Secure Client can be installed on the BOBJ server and the SAP BW/BI server, and a trusted server side connection can be established. Then, the user's SAP identity can be used to authenticate them to SAP BW/BI, with a secure connection between BOBJ and BW/BI and without the user having to re-authenticate. The SAP BW/BI application server will know who the user is at the workstation, and BOBJ will be able to get the information that the user requested.

Benefits

- The user experience is greatly improved and Active Directory authentication is fully utilized.
- The security of data retrieval from the SAP BW/BI system is enhanced, since this connection is encrypted using TrustBroker Secure Client.

11. RADIUS logon via browser

Requirement

Users need to logon to SAP business applications using a Web browser, and using two-factor authentication devices, such as RSA SecurID tokens.

Solution

One of the login modules included with TrustBroker Adapter includes support for the RADIUS authentication protocol. This can be used to logon to SAP web based applications using RADIUS. Two-factor authentication products such as RSA SecurID can use this protocol, so an RSA SecurID token can be used, or any other token from a vendor that supports RADIUS.

Benefits

- A user can logon to SAP applications with a web browser and, depending on security policy configuration, they will be able to use two-factor authentication, or any RADIUS authentication server which requires a username and password.
- RADIUS is commonly used for internet authentication and VPN products, so TrustBroker Adapter allows the user to logon using the same username and password adopted for remote access to the company network.

12. Secure email approval and SAP shortcuts

Requirement

Sending shortcuts to users in emails can often be difficult without compromising security by putting the user's ID and password in the shortcut, or expecting the user to enter their user ID and password when they open the shortcut. What is needed is a way to ensure that the user who receives the e-mail containing the shortcut is the same user who is authenticating to SAP when they open the shortcut.

Solution

Using TrustBroker, when the shortcut is sent to users in emails, the shortcut does not include a user's password. Instead, the user can double click on the shortcut and they are logged into the SAP ABAP transaction as themselves, without any security compromise. The identity of the user who is authenticated to SAP will always be the same as the identity of the user who received the email.

A web hyperlink (similar to a SAP shortcut, but for Web based applications) can be sent in e-mails which the user clicks on when they need to approve changes/workflow. They don't have to enter a password since TrustBroker Adapter will authenticate them using their Active Directory domain credentials – the same credentials used to receive the e-mail.

Benefits

- Users can login to SAP with less effort, and more securely than before. Now, the user doesn't have the inconvenience of having to enter a user and password to login each time.
- The recipient of the e-mail (especially if Microsoft Exchange is used) will be tightly linked to an Active Directory account, and this same account will be used to logon to the SAP system when the user opens the shortcut or clicks on the hyperlink.

13. A secure connection for managing SAP identities

Requirement

Some identity management (IdM) products are able to manage identities in SAP NetWeaver. To do this, they need a secure connection; otherwise they cannot perform SAP password changes or make other changes to SAP users without security being compromised.

Solution

When using TrustBroker Secure Client, a secured session can be established to make the identity management solution more secure. Also, having the TrustBroker Secure Client installed on the SAP application server means that users can take advantage of Secure SSO when logging on using SAP GUI or other supported applications (see solutions 1 and 2).

Benefits:

- Improved security of user related data in transit when managing identities in SAP applications.

14. Mobile device support – logon using Kerberos/Active Directory authentication

Requirement

Sometimes Active Directory domain user authentication is needed when users logon to SAP applications from mobile devices.

Solution

If TrustBroker Adapter is deployed into SAP NetWeaver to provide IWA, and a user logs on from a workstation that is not joined to the Active Directory domain, they are presented with a forms based sign-on screen (as in solution 9). This same feature can be used for mobile device authentication, e.g. from an iPad, Windows Mobile Phone, iPhone, or Android phone. These devices won't be joined to an Active Directory domain so a form will be shown in browser and the user can still logon using their Active Directory account and password, just like they do when they logon to their workstation on the intranet. If their domain account password has expired, TrustBroker Adapter will prompt them to change it and then, next time they logon from their workstation on the intranet, they will be able to use the new password.

Benefits

- Users can logon to SAP applications from any mobile device and still benefit from using Active Directory as a common authentication infrastructure. In this case, SSO is not used, since common authentication is more suited to this kind of environment.

15. High performance Kerberos-based web authentication – not using SAP SPNEGO

Requirement

When users logon to SAP business applications using a web browser (e.g. SAP portal or BSP applications) in a large environment, performance is critical.

Solution

TrustBroker Adapter uses the Active Directory Kerberos protocol, and is designed to be high performance and scalable. Only a very limited amount of native Java code is used, and the cryptographic operation required for Kerberos authentication is written in C and runs outside of the NetWeaver AS for Java environment.

Benefits

- Having high performance authentication reduces use of system resources, so hardware upgrades are minimized, costs reduced and users are kept satisfied, since they don't have to wait when they logon to a busy system.

Security Solutions for everybody...

Whether you are looking for secure SSO or have more complex requirements, we will be happy to discuss your organization's needs and propose a solution for you to consider.

CyberSafe North America, LLC. Atlanta, GA, United States +1 (678) 824-4411

CyberSafe Limited. Abbey House, 450 Bath Road, Longford, Middlesex, UB7 0EB, United Kingdom +44 208 757 8910

E-mail: Info@CyberSafe.com Web: <http://CyberSafe.com>

Copyright © 2011 CyberSafe Limited. All rights reserved.