SSO, Configuration Steps

What is SSO?

Single sign-on (SSO) is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again (enter ID and password).

Definition:

“Single sign-on (SSO) is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.”

Single Sign-On (SSO) is a key feature of the Enterprise Portal that eases user interaction with the many component systems available to the user in a portal environment. Once the user is authenticated to the enterprise portal, he/she can use the portal to access external applications. With SSO in the Enterprise Portal, the user can access different systems and applications without having to repeatedly enter his or her user information for authentication.

Why should we use SSO?

- A Typical net user needs at least nine passwords
- 30% never change passwords, 29% less than once a year
- 70% have forgotten a password at least once
- 35% of people use the same password for multiple applications
- 60% of people cycle two passwords across all applications

How to use it in SAP Net Weaver?

There are several user authentication and Single Sign-On (SSO) mechanisms available with SAP Net Weaver. The Enterprise Portal SSO mechanism is available in two variants depending on security requirements and the supported external applications:

1. SSO with ID and password
2. SSO with SAP logon tickets

Both variants eliminate the need for repeated logons to individual applications after the initial authentication at the enterprise portal. SSO with user ID and password forwards the user's logon data (user ID and password) to the systems that a user wants to call, whereas SSO with SAP logon tickets is based on a secure ticketing mechanism.

1) Single Sign-On with User ID and Password

The Single Sign-On (SSO) mechanism with user name and password provides an alternative for applications that cannot accept and verify SAP logon tickets. With this SSO mechanism the Portal Server uses user mapping information provided by users or administrators to give the portal user access to external systems. The portal components connect to the external system with the user's credentials. Either the end user or the administrator must map each user's user ID and password to the user ID and passwords used in the component systems, if these are different to the portal user data. As the user's user ID and password are sent across the network, you should use a secure protocol such as Secure Sockets Layer (SSL) for sending data.

2) Single Sign-On with SAP Logon Tickets

SAP logon tickets represent the user credentials. The Portal Server issues a logon ticket to a user after successful initial authentication. The logon ticket itself is stored as a cookie on the client and is sent with each request of that client. It can then be used by external applications such as SAP systems to authenticate the portal user to those external applications without any further user logons being required. SAP logon tickets contain information about the authenticated user. They do not contain any passwords. Specifically, logon tickets contain the following items:

- Portal user ID and one mapped user ID for external applications
- Validity period
- Information identifying the issuing system
- Digital signature

Thus SSO is a very powerful technique to get access to all the resources with just one password. You don't have to remember passwords for accessing each resource once SSO is implemented. But we must be very careful while using SSO as that one password is the only key which can unlock all the other locks; hence it should be in safe hands.

Configuring Single Sign-On (SSO) Between SAP EP 6.0 and the SAP Net Weaver 7.0 Portal

Use

The logon method SAPLOGONTICKET ensures that no logon prompt appears when an SAP Net Weaver 7.0 iView is called in an SAP NetWeaver 2004 portal (SAP EP 6.0). The administrator or the actual user are not required to maintain users and passwords for each user manually.

If you selected SAPLOGONTICKET as the logon method, proceed as follows:

**Procedure**

You configure Single Sign-On (SSO) in two steps:

1. Export the portal certificate from the J2EE Engine of the SAP NetWeaver 7.0 portal.
2. Import the portal certificate to the SAP NetWeaver 2004 portal (SAP EP 6.0) and add it to the Access Control List (ACL).

Exporting the Portal Certificate from the SAP Net Weaver 7.0 Portal

1. Start the SAP J2EE Engine Administrator with %INSTALLATION_ROOT%\admin\go.bat.
2. Connect to the portal server.
3. Choose <SID> ® Server<#> ® Services ® Key ® Storage.
4. IViews: Select the view TicketKeystore.
5. Entries: Select SAPLogonTicketKeypair-cert.

If SAPLogonTicketKeypair-cert does not exist, you need to create a portal certificate manually.

**Procedure**

1. Entry: Choose Create. Enter the following values in Key and Certificate Generation:

   **Subject Properties:** Every key must have a value under Value. The value **CN=Common Name** is the first value that is displayed. This is the certificate name. The recommendation of <SID> from the portal server also applies.

Entry Name: SAPLogonTicketKeypair (the system generates the entry SAPLogonTicketKeypair-cert).

Store Certificate: X

Algorithm: DSA

   ii. To generate the certificate, choose Generate.
   iii. Entries: Select SAPLogonTicketKeypair-cert.

6. Entry: Choose Export.
7. Export the portal certificate as <PORTAL_SID>certificate.crt in the file format _X.509 Certificate (*.crt).

Importing the Portal Certificate to the SAP NetWeaver 2004 Portal (SAP EP 6.0)

---

1. Start the SAP J2EE Engine Administrator with %INSTALLATION_ROOT%/admin/go.bat.
2. Connect to the portal server.
3. Choose <SID> ® Server<#> ® Services ® Key ® Storage.
4. Views: Select the view TicketKeystore.
5. Entry: Choose Load.
6. Open the file <PORTAL_SID>_certificate.crt.

In the Service Security Provider, under Ticket, perform the following steps to ensure that the SAP J2EE Engine accepts SAP logon tickets from the SAP NetWeaver 7.0 portal as an external system.

7. Start the SAP J2EE Engine Administrator with %INSTALLATION_ROOT%/admin/go.
8. Connect to the portal server.
10. Components: Choose Ticket.
11. Choose the Authentication tab page.
12. Add the following values for com.sap.security.core.server.jaas.EvaluateTicketLoginModule:

   - trustedsys<Number>="<PORTAL_SID>, <PORTAL_CLIENT>" (for example, J2E, 000)
   - trustediss<Number>="<ISSUER_DISTINGUISHED_NAME>" (for example, CN=J2E)
   - trusteddn<Number>="<SUBJECT_DISTINGUISHED_NAME>" (for example, CN=J2E)

   <Number> is an individual number for all three entries, but must be incremented by one for each external system. <PORTAL_SID> and <PORTAL_CLIENT> are the system ID and client of the SAP NetWeaver 7.0 portal. The client is the value of the parameter loginticket.client. The default value is 000. <ISSUER_DISTINGUISHED_NAME> and <SUBJECT_DISTINGUISHED_NAME> are the values of [issuerDN] and [DN] of certificate SAPLogon TicketKeypair-cert (see above).

You also have to add these values under evaluate_assertion_ticket:

13. Start the SAP J2EE Engine Administrator with %INSTALLATION_ROOT%/admin/go.
14. Connect to the portal server.
15. Choose <SID> ® Server<#> ® Services ® Security ® Provider.
17. Choose the Authentication tab page.
18. Add the following values for com.sap.security.core.server.jaas.EvaluateAssertionTicketLoginModule:

   - trustedsys<Number>="<PORTAL_SID>, <PORTAL_CLIENT>" (for example, J2E, 000)
   - trustediss<Number>="<ISSUER_DISTINGUISHED_NAME>" (for example, CN=J2E)
   - trusteddn<Number>="<SUBJECT_DISTINGUISHED_NAME>" (for example, CN=J2E)

The values are the same as the above values under Ticket.

Thanks and Regards
Srinivasarao.Kambala
WNSGlobalServices Pvt Ltd