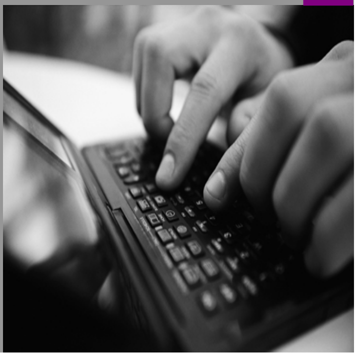
How-to Guide

SAP xRPM 4.0



How To … Configure SSO in an SAP NetWeaver 2004s Dual Stack

Version 1.00 – December 2005

Applicable Releases:

SAP xRPM 4.0

THE BEST-RUN BUSINESSES RUN SAP

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

These materials are provided “as is” without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

SAP NetWeaver “How-to” Guides are intended to simplify the product implementation. While specific product features and procedures typically are explained in a practical business context, it is not implied that those features and procedures are the only approach in solving a specific business problem using SAP NetWeaver. Should you wish to receive additional information, clarification or support, please refer to SAP Consulting.

Any software coding and/or code lines / strings (“Code”) included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

1 (Business) Scenario

As of SAP xApp Resource and Portfolio Management (SAP xRPM) 4.0, you can install SAP xRPM in a dual stack environment (ABAP and Java stack of SAP NetWeaver 2004s in one system). If you also want to implement SAP xApp Product Definition (SAP xPD) 2.0, it makes sense to keep both products in one system.

This guide explains how to configure Single Sign-On (SSO) for such a dual stack environment.

2 Introduction

The SSO configuration for a dual stack installation is different to the configuration required for distributed installations. The identity of the certificate issuer is determined by the distinguished name (DN), and the combination of system ID (SID) and client. Both the DN and SID/client pair must be unique in the whole system.

Since the ABAP stack and the Java stack use the same DN and client number (000) by default, you must change the DN and client number in the Java stack.

The sections below describe how to change this data.

This guide is written for xRPM 4.0 and SAP NetWeaver 2004s SP4. Since the guide will not be updated in the future, we strongly recommend that you check that the procedure described here is still up-to-date. Particularly when using a different basis release, such as SAP NetWeaver 2004s SR1.

For details and updates, see SAP Note 701205.

3 The Step-By-Step Solution

The following section provides an example of how to configure Single Sign-On (SSO) in a dual-stack system.

This process consists of the following steps:

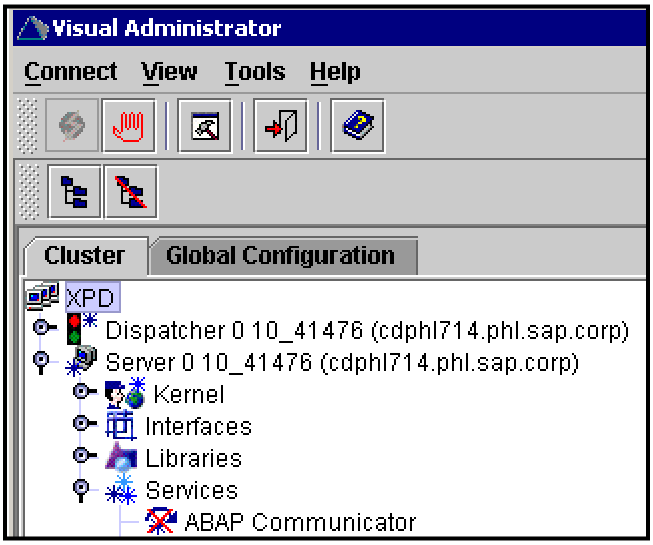
1. Create a new SAPLogonTicketkeypair for the Java stack.
   This is necessary to have a different distinguished name (DN) to the system ID (SID) in the ABAP system.
2. Change the client of the Java stack.
   Since the ABAP system already uses the default client 000, you must change the client.
3. Set the ABAP profile variables so the system accepts SSO tickets.
4. Import the Java stack certificate into the ABAP stack.

3.1 Creating a New SAP LogonTicketKeypair

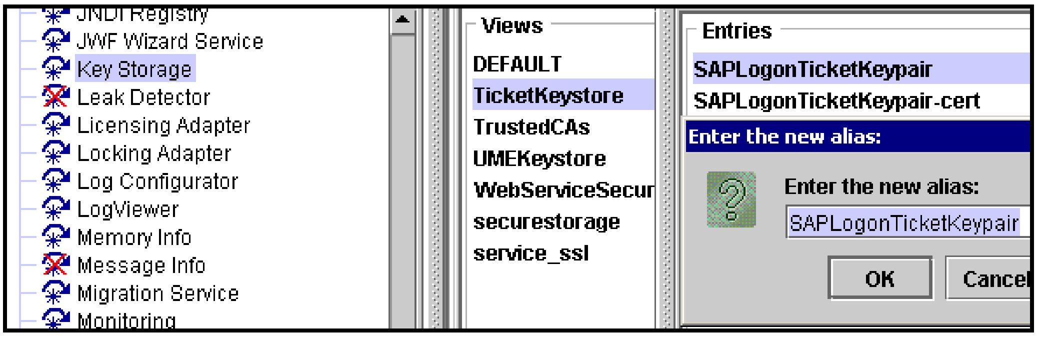
The distinguished name (DN) is embedded in the certificate that the Java stack issues when you log on to SAP Enterprise Portal. Since the DN of the Java stack must be different to the DN of the ABAP stack, you must rename the default SAPLogonTicketKeypair and create a new SAPLogonTicketKeypair with a different DN.

For more information, see SAP Note 701205.

1. Log on to the Visual Administrator of the Java stack as an administrator and choose *cluster-data à Instance_... à server_... à services à Key Storage*.



2. Navigate to *TicketKeystore* and rename your existing `SAPLogonTicketKeypair`.

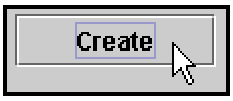


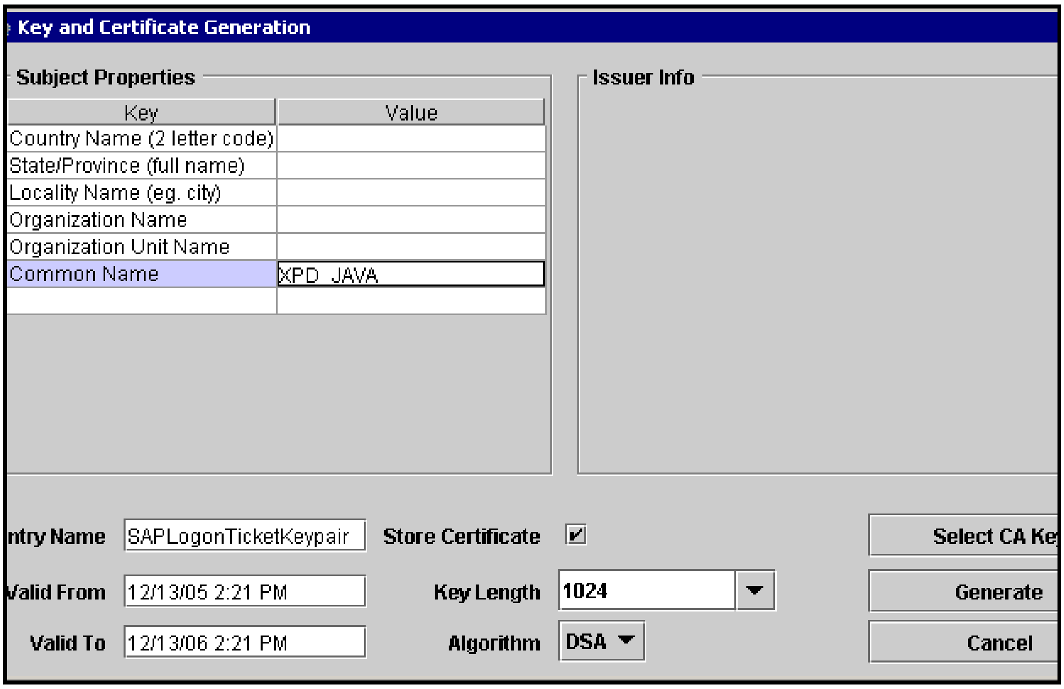
Enter the new alias:

Enter the new alias: SAPLogonTicketKeypair

Repeat this step for `SAPLogonTicketKeypair-cert`.

3. Create a new SAPLogonTicketKeypair as follows:




Key and Certificate Generation

Subject Properties

Key	Value
Country Name (2 letter code)	
State/Province (full name)	
Locality Name (eg. city)	
Organization Name	
Organization Unit Name	
Common Name	XPD_JAVA

ntry Name: SAPLogonTicketKeypair

Store Certificate: ☑

Valid From: 12/13/05 2:21 PM

Key Length: 1024

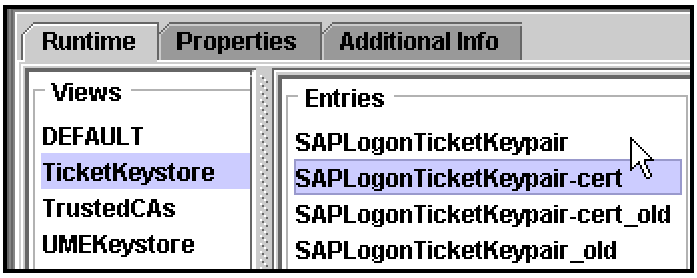
Valid To: 12/13/06 2:21 PM

Algorithm: DSA

Enter a common name; make sure that you use a different common name to your SID.

Select the algorithm `DSA`, and select *Store Certificate*.

4. Choose *Generate*.
An old pair and a new pair of SAPLogonTickets appear:



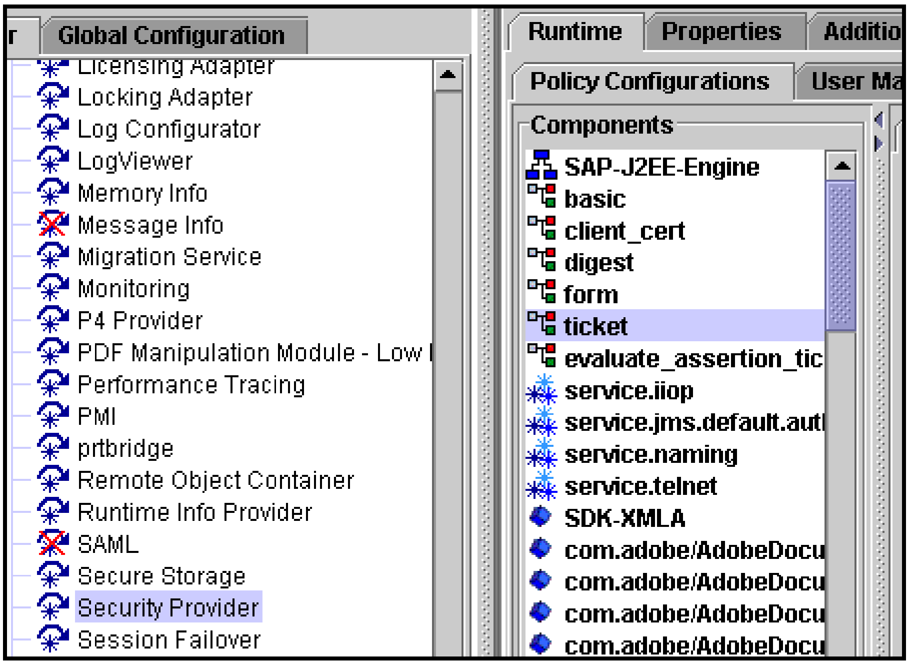
3.2 Changing the Java Stack Client

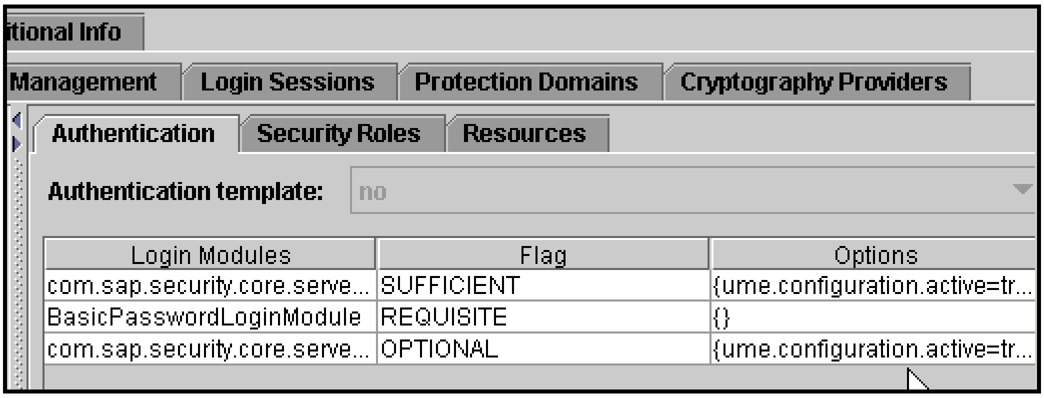
When the ABAP stack reads a certificate issued by the Java stack, it uses the combination of system ID (SID) and client number to identify the issuer. This combination must be unique. However, since the default client in the Java stack is 000 and this combination is already in use by the ABAP stack, in a dual stack installation, you must change the client number of the Java stack.

There are two locations where you can maintain the client number. Depending on whether `ume.configuration.active` is set to *true* or *false*, it gets the information from *UME property sheet* or *options for the login module*.

Since `ume.configuration.active` is set to *true* by default, the following steps only describe this scenario. For more information, see SAP Note 701205.

1. Check that the parameter `ume.configuration.active` is set to *true.*

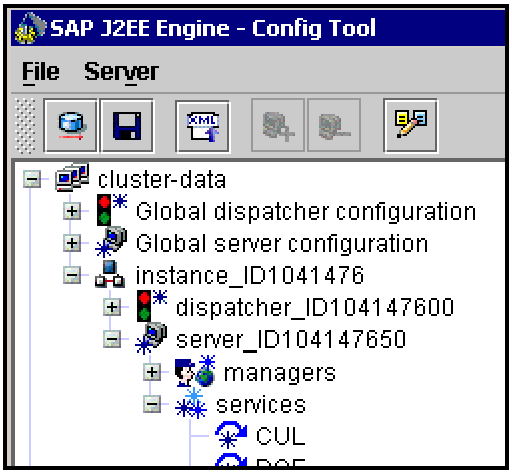


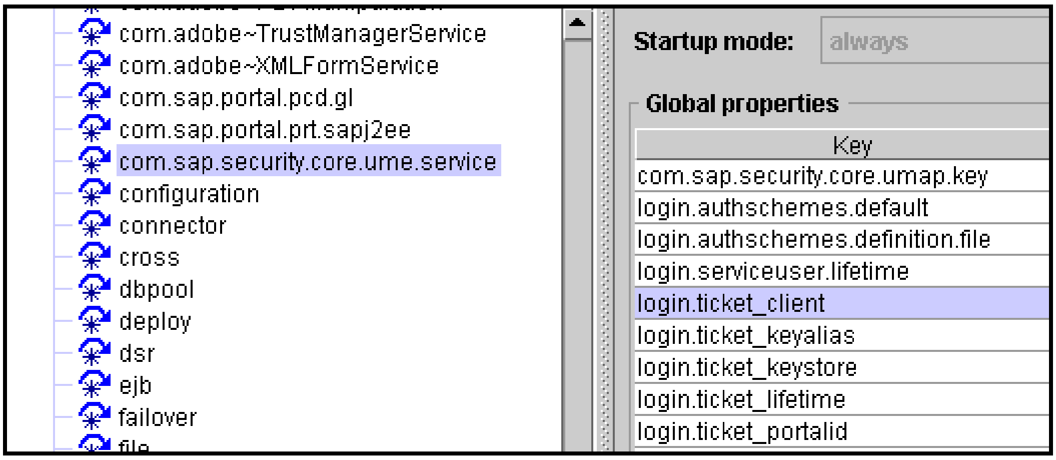


Authentication template: no

Login Modules	Flag	Options
com.sap.security.core.serve...	SUFFICIENT	{ume.configuration.active=tr...
BasicPasswordLoginModule	REQUISITE	{}
com.sap.security.core.serve...	OPTIONAL	{ume.configuration.active=tr...

2. Open the Config Tool and choose *cluster-data* à *Instance_...* à *server_...* à *services* à *com.sap.security.core.ume.service* à *login.ticket_client*



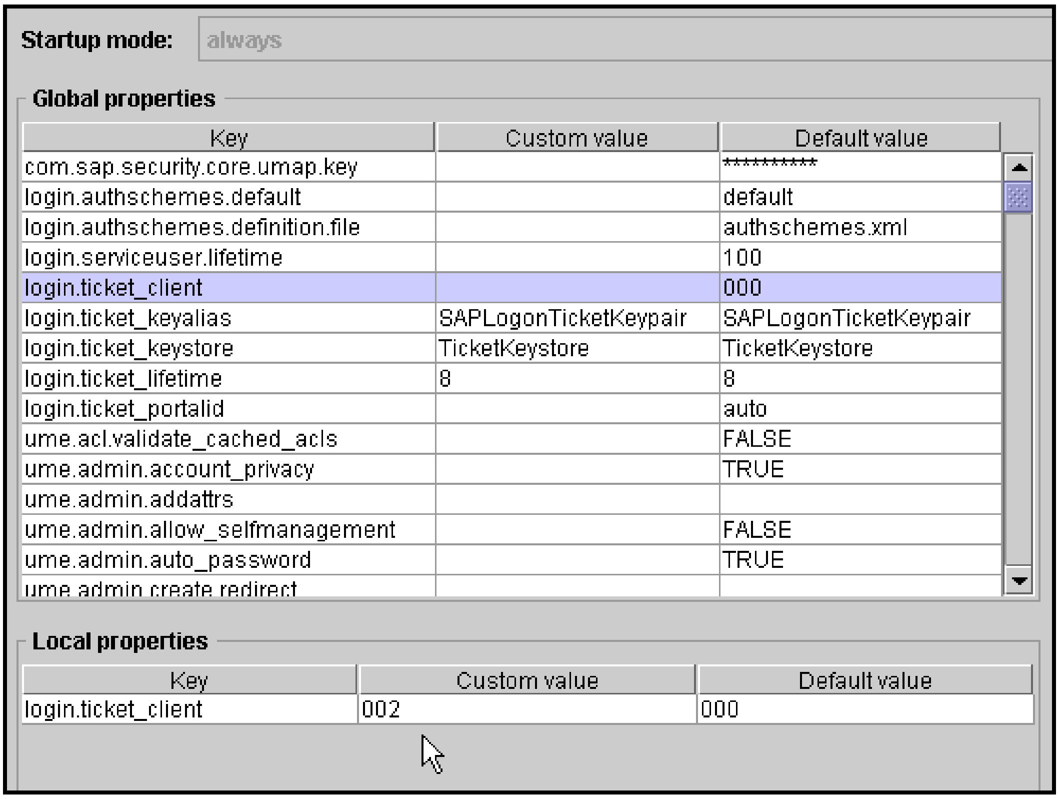


Startup mode: always

Global properties

Key
com.sap.security.core.umap.key
login.authschemes.default
login.authschemes.definition.file
login.serviceuser.lifetime
login.ticket_client
login.ticket_keyalias
login.ticket_keystore
login.ticket_lifetime
login.ticket_portalid

3. Enter a client number for `login.ticket_client`.
Make sure that the client number entered here is not already in use in the ABAP stack.



Startup mode: always

Global properties

Key	Custom value	Default value
com.sap.security.core.umap.key		**********
login.authschemes.default		default
login.authschemes.definition.file		authschemes.xml
login.serviceuser.lifetime		100
login.ticket_client		000
login.ticket_keyalias	SAPLogonTicketKeypair	SAPLogonTicketKeypair
login.ticket_keystore	TicketKeystore	TicketKeystore
login.ticket_lifetime	8	8
login.ticket_portalid		auto
ume.acl.validate_cached_acls		FALSE
ume.admin.account_privacy		TRUE
ume.admin.addattrs		
ume.admin.allow_selfmanagement		FALSE
ume.admin.auto_password		TRUE
ume.admin.create_redirect		

Local properties

Key	Custom value	Default value
login.ticket_client	002	000

4. To activate the changes to the UME settings, restart the Java stack.

3.3 Setting ABAP Profile Parameters

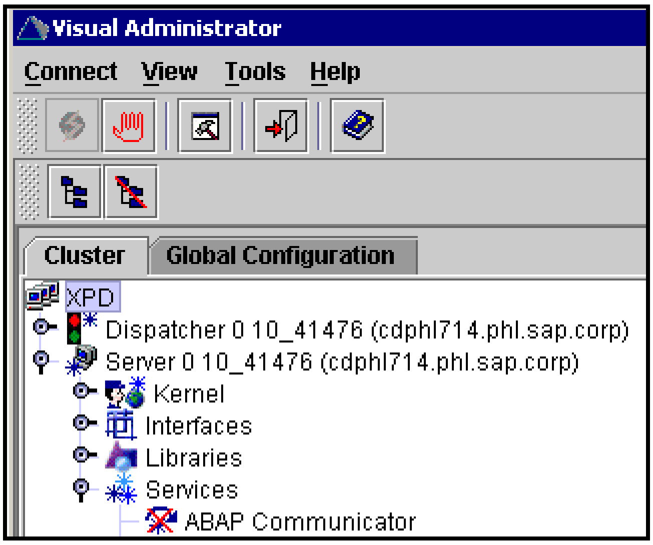
You must set up the ABAP stack to accept logon tickets.

Since this step is usually well-known, it is not described in this guide.
See the *Configuring the System for Issuing Logon Tickets* section in SAP Help Portal at **`help.sap.com/nw2004s`** à *English* à *SAP NetWeaver Library* à *SAP NetWeaver by Key Capability* à *Security* à *User Authentication and Single Sign-On* à *Authentication on the SAP Web Application Server ABAP* à *Using Logon Tickets* à *Configuring the System for Issuing Logon Tickets*.

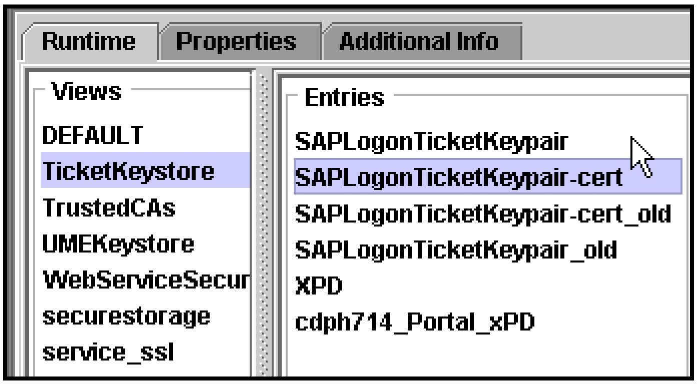
3.4 Importing the Java Stack Certificate into the ABAP Stack

The last step is to export SAPLogonTicketKeypair and import it into the ABAP stack.

1. Log on to the Visual Administrator of the Java stack as an administrator and choose *<SID>* à *Server...* à *services* à *Key Storage*



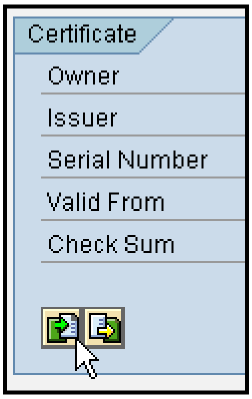
2. Select *SAPLogonTicketKeypair-cert* and click *Export*.
Save the object in a folder that you can access from the PC on which the SAP GUI is running.



3. Start your SAP GUI and log on to the ABAP stack as an administrator.
Start transaction STRUSTSSO2.

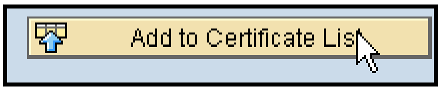
4. Import the certificate into the ABAP stack.

Note: The certificate file is uploaded through the SAP GUI. This means that you do not need to browse through the server's file system, but your PC's file system.



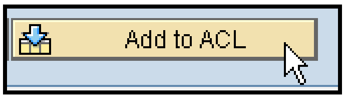
Once the certificate is successfully uploaded, the certificate information appears.

5. Add the certificate to the certificate list.

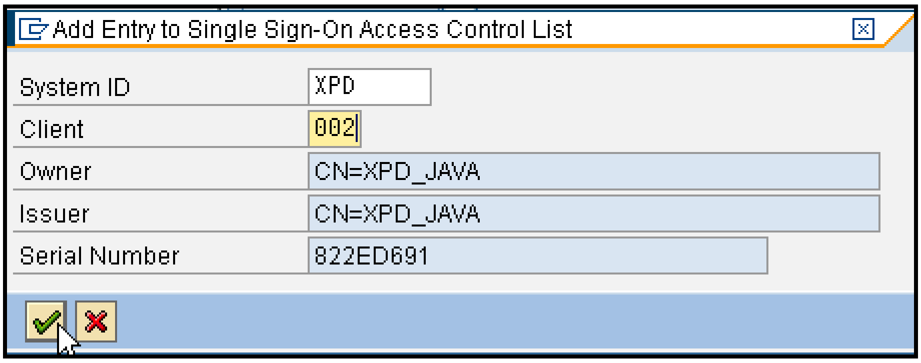


The certificate appears in the top part of the screen.

6. Add the certificate to the access control list (ACL).



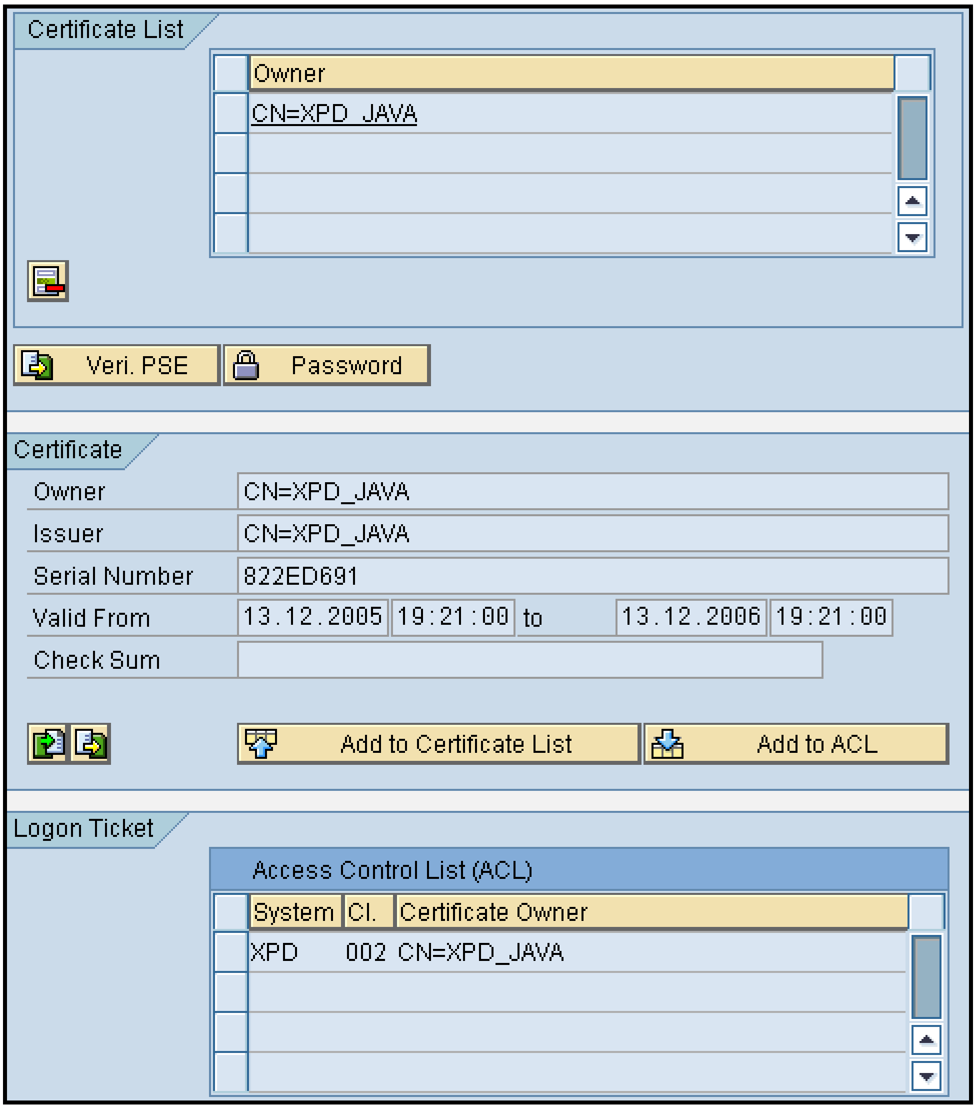
Note: Make sure that you enter the new client number.


Add Entry to Single Sign-On Access Control List

System ID	XPD
Client	002
Owner	CN=XPD_JAVA
Issuer	CN=XPD_JAVA
Serial Number	822ED691

7. Save your entries.

The figure below is an example of how the final screen looks:



Certificate List

Owner
CN=XPD_JAVA

Certificate

Owner	CN=XPD_JAVA
Issuer	CN=XPD_JAVA
Serial Number	822ED691
Valid From	13.12.2005 19:21:00 to 13.12.2006 19:21:00
Check Sum	

Logon Ticket

Access Control List (ACL)

System	Cl.	Certificate Owner
XPD	002	CN=XPD_JAVA