SAP Web Application Server
Security

Release 6.20
Document Version 2.1
10/26/02

SAP
Copyright

© Copyright 2002 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft®, WINDOWS®, NT®, EXCEL®, Word®, PowerPoint® and SQL Server® are registered trademarks of Microsoft Corporation.

IBM®, DB2®, DB2 Universal Database, OS/2®, Parallel Sysplex®, MVS/ESA, AIX®, S/390®, AS/400®, OS/390®, OS/400®, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere®, Netfinity®, Tivoli®, Informix and Informix® Dynamic ServerTM are trademarks of IBM Corporation in USA and/or other countries.

ORACLE® is a registered trademark of ORACLE Corporation.

UNIX®, X/Open®, OSF/1®, and Motif® are registered trademarks of the Open Group.

Citrix®, the Citrix logo, ICA®, Program Neighborhood®, MetaFrame®, WinFrame®, VideoFrame®, MultiWin® and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc.

HTML, DHTML, XML, XHTML are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

JAVA® is a registered trademark of Sun Microsystems, Inc.

JAVASCRIPT® is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, SAP Logo, R/2, R/3, R/3, SAP ArchiveLink, SAP Business Workflow, WebFlow, SAP EarlyWatch, BAPI, SAPPHIRE, Management Cockpit, mySAP, mySAP.com, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. MarketSet and Enterprise Buyer are jointly owned trademarks of SAP Markets and Commerce One. All other product and service names mentioned are the trademarks of their respective owners.
Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Caution Icon]</td>
<td>Caution</td>
</tr>
<tr>
<td>![Example Icon]</td>
<td>Example</td>
</tr>
<tr>
<td>![Note Icon]</td>
<td>Note</td>
</tr>
<tr>
<td>![Recommendation Icon]</td>
<td>Recommendation</td>
</tr>
<tr>
<td>![Syntax Icon]</td>
<td>Syntax</td>
</tr>
</tbody>
</table>

Typographic Conventions

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example text</em></td>
<td>Words or characters that appear on the screen. These include field names, screen titles, pushbuttons as well as menu names, paths and options.</td>
</tr>
<tr>
<td><em>Example text</em></td>
<td>Cross-references to other documentation.</td>
</tr>
<tr>
<td><strong>Example TEXT</strong></td>
<td>Emphasized words or phrases in body text, titles of graphics and tables.</td>
</tr>
<tr>
<td><strong>EXAMPLE TEXT</strong></td>
<td>Names of elements in the system. These include report names, program names, transaction codes, table names, and individual key words of a programming language, when surrounded by body text, for example, SELECT and INCLUDE.</td>
</tr>
<tr>
<td><em>Example text</em></td>
<td>Screen output. This includes file and directory names and their paths, messages, source code, names of variables and parameters as well as names of installation, upgrade and database tools.</td>
</tr>
<tr>
<td><strong>EXAMPLE TEXT</strong></td>
<td>Keys on the keyboard, for example, function keys (such as F2) or the ENTER key.</td>
</tr>
<tr>
<td><em>Example text</em></td>
<td>Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.</td>
</tr>
<tr>
<td><code>&lt;Example text&gt;</code></td>
<td>Variable user entry. Pointed brackets indicate that you replace these words and characters with appropriate entries.</td>
</tr>
</tbody>
</table>
Contents

SAP Web Application Server Security ................................................................. 6
Using the Secure Sockets Layer Protocol ......................................................... 6
 The Application Server's Personal Security Environments .............................. 8
 SSL Server PSE ....................................................................................... 8
 SSL Client PSEs ................................................................................... 9
The SAP Cryptographic Library Installation Package .................................... 10
Configuring the SAP Web AS for Supporting SSL .......................................... 10
 Installing the SAP Cryptographic Library on the SAP Web AS ....................... 11
 Setting the Profile Parameters for Using SSL ............................................... 12
 Creating the SSL Server PSE .................................................................... 13
 Generating Certificate Requests for the SSL Server PSEs ......................... 15
 Sending the Certificate Requests to a CA .................................................... 16
 Importing the Certificate Request Response ................................................. 17
 Maintaining the SSL Server PSE's Certificate List ........................................ 18
 Creating the Standard SSL Client PSE ......................................................... 20
 Creating the Anonymous SSL Client PSE ..................................................... 20
 Creating Individual SSL Client PSEs ............................................................ 21
 Specifying that a Connection Should Use SSL .............................................. 22
 Testing the SSL Configuration ...................................................................... 23
 Making Sure the SSL Port is Set up Correctly .......
User Authentication ...................................................................................................................... 39
Using Logon Tickets.................................................................................................................. 39
 Configuring the System for Issuing Logon Tickets............................................................ 40
   Obtaining a Certificate Signed by the SAP CA............................................................... 41
   Using a Self-Signed Certificate...................................................................................... 42
   Changing from a Self-Signed Certificate to a Certificate Signed by the SAP CA.......... 42
 Configuring the System for Accepting Logon Tickets...................................................... 43
 Protecting User Information............................................................................................... 46
 Using X.509 Client Certificates .......................................................................................... 46
   Configuring the System for Using X.509 Client Certificates.......................................... 47
Terminology and Abbreviations............................................................................................ 49
SAP Web Application Server Security

The SAP Web Application Server supports various security features that you can take advantage of when running your applications. In particular:

?? Support of the Secure Sockets Layer (SSL) protocol
?? User authentication using either:
   ?? Logon tickets
   ?? X.509 client certificates

For information about establishing the network infrastructure, see the SAP Web Application Server: Technical Infrastructure guide available on the SAP Service Marketplace at http://service.sap.com/network under the Network Integration Guides.

Using the Secure Sockets Layer Protocol

Use

You can use the Secure Sockets Layer (SSL) protocol to secure HTTP connections to and from the SAP Web Application Server. When SSL is used, the data being transferred between the two parties (client and server) is encrypted and the two partners can be authenticated. For example, if a user must transfer his or her account information, then you can use SSL to authenticate the user and encrypt the information during transfer.

Users that access a service that is protected with SSL use the prefix https: in the URL instead of http:.

Prerequisites

?? The server possesses a public and private key pair and public-key certificate.

The SSL protocol uses public-key technology to provide its protection. Therefore, the server must possess a public and private key pair and a corresponding public-key certificate. It must possess one key pair and certificate to identify itself as the server component and another key pair and certificate if it is to identify itself as a client component. These key pairs and certificates are stored in the server’s own Personal Security Environments (PSEs), the SSL server PSE and the SSL client PSE, respectively. (For more information, see Public-Key Technology [SAP Library].)

?? You are authorized to receive the SAP Cryptographic Library.

The distribution of the SAP Cryptographic Library is subject to and controlled by German export regulations and is not available to all customers. In addition, the library may be subject to local regulations of your own country that may further restrict the import, use and (re-)export of cryptographic software. If you have any further questions on this issue, contact your local SAP subsidiary.
Features

By supporting SSL, the SAP Web Application Server can provide the following:

?? Server-side authentication
   With server-side authentication, the server identifies itself to the client when the connection is established, which reduces the risk of using "fake" servers to gain information from clients.

?? Client-side authentication
   With client-side authentication, the client identifies itself when the connection is established. You can use SSL client-side authentication, for example, to authenticate users instead of using user IDs and passwords.

?? Mutual authentication
   In this case, both the server and the client are authenticated.

?? Data encryption
   In addition to authenticating the communication partners, the data being transferred between the client and server is encrypted, which provides for integrity and privacy protection. An eavesdropper cannot access or manipulate the data.

Integration

Use the following functions to maintain the server’s SSL information:

?? Profile parameter maintenance (transaction RZ10)

?? Trust manager (transaction STRUST)
   For more information, see Using the Trust Manager [SAP Library].

?? RFC destination maintenance (transaction SM59)

?? ICM Monitor (transaction SMICM)
   For more information, see Monitoring the ICM with the ICM Monitor [SAP Library].

?? Configuration tool sapgenpse (for configuring a stand-alone SAP Web Dispatcher)

See also:

For more information about public-key technology and SSL, see:

?? Public-Key Technology [SAP Library]

?? Terminology and Abbreviations [Page 48]

?? SSL information provided by Netscape:
The Application Server’s Personal Security Environments

The information that the application server needs to communicate using SSL is stored in the server's Personal Security Environment (PSE). Because the information needed is different depending on whether the application server is the server or the client component for the communication, the server possesses multiple PSEs as follows:

?? The SSL Server PSE

The SAP Web Application Server uses this PSE when the application server is the server component for the communication, for example, when a user accesses the SAP Web Application Server using a Web browser.

?? SSL Client PSEs

The SAP Web Application Server uses one of the SSL client PSEs when the application server is the client component for the communication. The server can also use multiple SSL client PSEs, for example, it can use an anonymous PSE to access Web services that do not require client authentication and a different PSE to access services that do.

These PSEs are described in more detail in the topics that follow.

SSL Server PSE

Definition

The application server’s PSE for securing HTTP communications using the SSL protocol (HTTPS connections) when the application server is the server component for the communication.

If the SAP Web Application Server also communicates as a client component, then it uses one of the SSL client PSEs when establishing the HTTPS connection.

Structure

This PSE contains the application server's security information including its key pair and its corresponding certificate list. The certificate list contains the list of Certification Authorities (CAs) that the server trusts. The SSL server PSE's certificate list should be quite restrictive and contain only those public-key certificates from the CAs that the server accepts.

Integration

When you create the SSL server PSE, the system generates a default PSE for the system. Alternatively you can create individual SSL server PSEs for specific servers. The system then distributes the PSEs to the application servers accordingly. The application servers that are not assigned an individual SSL server PSE receive the default SSL server PSE. The system stores the PSE in the file $(DIR_INSTANCE)/sec/SAPSSLS.pse on each application server.
SSL Client PSEs

Definition
The application server's PSEs to use for securing communications with the SSL protocol when the application server is the client component for the communication.

Use
There are three different types of SSL client PSEs that the server can use:

?? Anonymous SSL Client PSE
   The application server uses the anonymous SSL client PSE to connect to other Web servers where only server-side authentication is used. It does not use it for its own authentication.

?? Standard SSL Client PSE
   The SAP Web AS uses the standard SSL client PSE to authenticate itself on other Web servers when SSL client authentication is used and where no individual SSL client PSE is specified to use for the connection.

?? Individual SSL Client PSEs
   The SAP Web AS can also use additional individual SSL client PSEs for authenticating itself on other Web servers. By using these PSEs, you can specify different "identities" for the application server to use for different services.

   If the SAP Web AS communicates as the server component for the SSL connection, then it uses the SSL server PSE to establish the HTTPS connection.

Structure
The SSL client PSEs contain the application server's security information, which includes the public and private key pair to use for the particular identity and the corresponding certificate list.

Integration
When you create an SSL client PSE, the system creates a single PSE for the system that is distributed to all of the application servers. The system stores the PSEs in the directory 
$(DIR_INSTANCE)/sec. The file names for the PSEs are:

?? Anonymous: SAPSSLA.pse
?? Standard: SAPSSLC.pse
?? Individual: SAPSSL<name>.pse
The SAP Cryptographic Library Installation Package

Definition
The installation package available for using the SAP Cryptographic Library.

Structure
The SAP Cryptographic Library installation package sapcrypto.car contains the following files:

?? The SAP Cryptographic Library (sapcrypto.dll for Windows NT or libsapcrypto.<ext> for UNIX)
?? A corresponding license ticket (ticket)
?? The configuration tool sapgenpse.exe

Configuring the SAP Web AS for Supporting SSL

Procedure
1. Install the SAP Cryptographic Library [Page 11] on the application server.
2. Set the profile parameters [Page 12].

Creating the SSL Server PSEs
Perform the following to create and maintain the SSL server PSE:
3. Create the SSL server PSEs [Page 13].
4. Generate a certificate request for each SSL server PSE [Page 15].
5. Send the certificate requests to a CA to be signed [Page 16].
6. Import the certificate request responses into the server’s SSL server PSEs [Page 17].
7. Maintain the SSL server PSE’s certificate list [Page 17].

Creating the SSL Client PSEs
Perform the following to create and maintain the SSL client PSEs:
8. Repeat the procedure for the standard SSL client PSE. [Page 20]
9. If you want the application server to be able to use the anonymous identity to communicate with other Web servers, then repeat the procedure for the anonymous SSL client PSE [Page 20].
10. If you want the application server to be able to use individual identities to communicate with other Web servers using SSL, then create individual SSL client PSEs [Page 21].

Defining Which SSL Client PSE to Use
11. In transaction SM59, you define the HTTP destinations for the SAP Web Application Server. In these destinations, you can specify whether SSL should be used for the connection and which SSL client PSE the server should use. See Specifying that a Connection Should Use SSL [Page 22].
12. Restart the ICManager to make sure that any changes take effect.
13. Test the connections. [Page 23]
Installing the SAP Cryptographic Library on the SAP Web AS

Use

Use the following procedure to install the SAP Cryptographic Library on the SAP Web AS.

Prerequisites

You have obtained the SAP Cryptographic Library installation package [Page 9].

Procedure

As user <sid>adm:

1. Extract the contents of the SAP Cryptographic Library installation package.

2. Copy the library file and the configuration tool sapgenpse.exe to the directory specified by the application server's profile parameter DIR_EXECUTABLE. In the following, we represent this directory with the notation $(DIR_EXECUTABLE).

   Examples
   
   UNIX:
   ?? DIR_EXECUTABLE: /usr.sap/<SID>/SYS/exe/run/
   ?? Location of SAP Cryptographic Library: 
      /usr.sap/<SID>/SYS/exe/run/libsapcrypto.so
   
   Windows NT:
   ?? DIR_EXECUTABLE: \\usr\sap\<SID>\SYS\exe\run\ 
   ?? Location of SAP Cryptographic Library: 
      <DRIVE>:\usr\sap\<SID>\SYS\exe\run\sapcrypto.dll

3. Check the file permissions for the SAP Cryptographic Library. If, for example, you copied the library to its location using ftp on UNIX, then the file permissions may not be set correctly. Make sure that <sid>adm (or SAPService<SID> under Windows NT) is able to execute the library's functions.

4. Copy the ticket file to the sub-directory sec in the instance directory $(DIR_INSTANCE):

   Examples
   
   UNIX:
   ?? DIR_INSTANCE: /usr.sap/<SID>/<instance>
   ?? Location of the ticket: /usr.sap/<SID>/<instance>/sec/ticket
   
   Windows NT:
   ?? DIR_INSTANCE: \usr\sap\<SID>\<instance>
   ?? Location of the ticket: \usr\sap\<SID>\<instance>\sec\ticket

5. Set the environment variable SECUDIR to the sec sub-directory. The application server uses this variable to locate the ticket and its credentials at run-time.

   If you set the environment variable using the command line, then the value may not be applied to the server's processes. Therefore, we recommend setting SECUDIR in the startup profile for the server's user or in the registry (Windows NT).
Result
The SAP Cryptographic Library is installed on the application server and the environment is set up correctly so that the server can locate the library at run-time.

Setting the Profile Parameters for Using SSL

1. Set the profile parameters SAP Web AS’s instance profile as shown in the tables below. If you used the recommended directory DIR_EXECUTABLE, then use the following values for the location of the SAP Cryptographic Library:

   ?? On Unix:  $(DIR_EXECUTABLE)/libsapcrypto.<ext>

   ?? On Windows NT:  $(DIR_EXECUTABLE)\sapcrypto.dll

Trust Manager Parameters

<table>
<thead>
<tr>
<th>Profile Parameter</th>
<th>Value</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssl/ssl_lib</td>
<td>Path and file name of the SAP Cryptographic Library</td>
<td>UNIX: /usr/sap/&lt;SID&gt;/SYS/exe/run/libsapcrypto.so</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows NT: &lt;DRIVE&gt;:\usr\sap&lt;SID&gt;\SYS\exe\run\sapcrypto.dll</td>
</tr>
<tr>
<td>sec/libsapsecu</td>
<td>Path and file name of the SAP Cryptographic Library</td>
<td>UNIX: /usr/sap/&lt;SID&gt;/SYS/exe/run/libsapcrypto.so</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows NT: &lt;DRIVE&gt;:\usr\sap&lt;SID&gt;\SYS\exe\run\sapcrypto.dll</td>
</tr>
<tr>
<td>ssf/ssfapi_lib</td>
<td>Path and file name of the SAP Cryptographic Library</td>
<td>UNIX: /usr/sap/&lt;SID&gt;/SYS/exe/run/libsapcrypto.so</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows NT: &lt;DRIVE&gt;:\usr\sap&lt;SID&gt;\SYS\exe\run\sapcrypto.dll</td>
</tr>
<tr>
<td>ssf/name</td>
<td>SAPSECULIB</td>
<td>SAPSECULIB</td>
</tr>
</tbody>
</table>

Ignore the warnings that the parameters are not known to the system.
ICManager Parameters

<table>
<thead>
<tr>
<th>Profile Parameter</th>
<th>Value</th>
<th>Examples</th>
</tr>
</thead>
</table>
| icm/plugin_<xx>   | PROT=HTTPS, PLG=<path_and_filename_of_httpplugin> | UNIX: PROT=HTTPS, PLG=${DIR_EXECUTABLE}/httpplugin.<ext>  
Windows NT: PROT=HTTPS, PLG=${DIR_EXECUTABLE}\httpplugin.dll |
| icm/server_port_<xx> | PROT=HTTPS, PORT=<port>, TIMEOUT=<timeout_in_seconds> | PROT=HTTPS, PORT=1443, TIMEOUT=900 |
| icm/HTTPS/verify_client | 0: Do not use certificates  
1: Allow certificates (default)  
2: Require certificates | 1 |

If icm/HTTPS/verify_client = 1, then any users who use Microsoft's Internet Explorer as their Web browser and who do not possess a client certificate will receive an empty certificate selection dialog box when they access the SAP Web Application Server. Therefore, if your users are not going to use client certificates for authentication, then set this parameter to the value 0.

2. Restart the application server or the ICManager.

If you only make changes to the ICManager parameters, then it suffices to only restart the ICManager.

Creating the SSL Server PSE

Use

The SSL Server PSE contains the application server's security information that it needs to communicate using SSL. If you have a system with multiple application servers, then the following options are available:

?? Use a single system-wide SSL server PSE for all servers.

?? Use server-specific SSL server PSEs for individual application servers.

?? Use a combination of both types. (Some application servers use a system-wide SSL server PSE, and other application servers use server-specific SSL server PSEs.)

Use a system-wide PSE for those application servers that are accessed via a Network Address Translator (NAT). Use the NAT's fully-qualified host name as the Common Name (CN) part of the Distinguished Name.
Prerequisites

?? The SAP Cryptographic Library is installed in the $(DIR_EXECUTABLE) directory on the application server.

If the SAP Cryptographic Library is not installed, then the SSL Server PSE and SSL Client PSE nodes are not included in the trust manager's PSE status section.

?? You know the naming convention to use for the server's Distinguished Name. The syntax of the Distinguished Name depends on the Certification Authority (CA) you use.

For example, if you use the SAP CA, the naming convention is CN=<host_name>, OU=I<installation_number>-<company_name>, OU=SAP Web AS, O=SAP Trust Community, C=DE.

For more information about the SAP CA naming conventions, see the SAP Trust Center Service at http://service.sap.com/tcs.

Procedure

From the Trust Manager screen:

1. Select the SSL Server PSE node.
2. Using the context menu, choose Create (if no PSE exists) or Replace.

The <Create/Replace> PSE dialog appears.

3. Enter the Distinguished Name parts for a default SSL server PSE in the corresponding fields. For the default SSL server PSE, use a wildcard character (*) as the host name in the Name field. For example:

?? Name = *.mycompany.com
?? Org. (opt.) = Test
?? Comp./Org. = MyCompany
?? Country = US

If you want to use a reference to a CA name space, then elements contained in the CA's name space are automatically used for the server's Distinguished Name. In addition, you cannot modify the Country field. Use the toggle function () to activate or deactivate the reference to a CA name space.

The system uses these components to build a default Distinguished Name to use for a system-wide PSE, as well as for building the server-specific names for individual PSEs.

The SSL Server screen then appears. In this screen, you can decide whether the individual application servers should use the default Distinguished Name and system-wide SSL server PSE or individual PSEs. The default Distinguished Name appears in the Default PSE DN field. The server-specific Distinguished Names appear in the table in the Distinguished Name column.
4. If necessary, modify or delete any of the individual application server's Distinguished Names to meet your own needs.

For example:

- Delete the Distinguished Name entry for any servers that should receive the default Distinguished Name.
- Assign the same Distinguished Name to all servers that are to be accessed via a NAT.
- Modify the Distinguished Name to adhere to your CA's naming convention (for example, adding an attribute such as L=<Locality>).

If the system could not determine a Distinguished Name for the server, then an error has occurred (for example, the ICManager has not been installed on the server).

5. Choose Enter.

You return to the Trust Manager screen.

Result

The system creates the SSL server PSEs and distributes them to the individual application servers.

Generating Certificate Requests for the SSL Server PSEs

Use

You must generate an individual certificate request for each application server that uses a server-specific PSE. If you use a system-wide SSL server PSE, then you only need to generate a single certificate request.

To determine each unique SSL server PSE, expand the SSL server PSE node in the trust manager and select each application server with a double-click. The server's Distinguished Name appears in the Own certif. field. For each application server with a unique Distinguished Name, you must generate a certificate request.

Procedure

From the Trust Manager screen:

1. Expand the SSL server PSE node.

2. For each unique SSL server PSE (each server-specific PSE or a single system-wide PSE):
   a. Select the application server.

      The application server's certificate appears in the PSE maintenance section in the Own certif. field.

   b. In the PSE maintenance section, choose Create Certificate Request.

      A dialog appears showing the certificate request.

   c. Select the content of the request and copy it to your clipboard (Copy) or save the certificate request to a file (<file_name>.P10) using Save as local file.
Sending the Certificate Requests to a CA

Use

After you have generated a key pair and certificate request, you must send the certificate request to a CA to be signed. The response from the CA is a signed public-key certificate for the server.

Prerequisites

You can send the certificate request to the SAP CA or another CA of your choice. Note however, the trust manager requires that the certificate request response adheres to the **PKCS#7 certificate chain** format. This means that the response contains both the requestor’s signed public-key certificate as well as the CA’s root certificate. As an alternative, the CA may issue a stand-alone certificate in **PEM format**. Note the following:

?? PKCS#7 certificate chain format

In this case, the issuing CA provides the certificate request response in the necessary format. For example, the SAP CA provides the response in this format, or you can request this format from your CA.

?? PEM format

As an alternative, you may receive a certificate request response from your CA in PEM format, which contains only the signed public-key certificate.

In this case, the CA's root certificate must also exist in the database. The trust manager then automatically modifies the certificate request response so that it exists in the necessary format before importing it into the server's PSE.

Procedure

For each certificate request that you generated:

1. If you saved the contents of the request to a file, then make sure the contents have not been corrupted during download. For example, if you generate the certificate request on a UNIX system and save it to a Windows frontend client, the line feeds and carriage returns may be replaced with special characters.

   To check the contents, open the certificate request with a text editor and repair any corrupt line feeds or carriage returns. Because many editors use hidden characters for formatting, use a text editor that does not support formatting features, for example, Notepad.

   The example below shows a correct certificate request.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBkzCCAVICAQAwWJELMAkGA1UEBhMCREUxHDAaBgNVBAoTE215U0FQLmNvbS
BXb3JrcGxhY2UxQzANBgNVBAgTJEJPCmxpbmcxUTEwHhcNMDIwMjA5MTc4NDQ1
sha256
-----END CERTIFICATE REQUEST-----
```

2. Send the contents of the certificate request to the CA of your choice.

The exact procedure to use depends on the CA that you use. For the SAP CA, follow the instructions provided by the SAP Trust Center Service at [http://service.sap.com/tcs](http://service.sap.com/tcs).

Result

The CA will validate the information contained in the certificate request (according to its own policy) and return a response that contains the signed public-key certificate.
**Importing the Certificate Request Response**

**Use**
The CA will send you a certificate request response that contains the signed public-key certificate for the application server. Once you have received this response, import it into the corresponding PSE.

For a PSE that is used by multiple application servers, you only have to import the response into one of the PSEs. The PSE is then redistributed to all of the application servers.

For example, for those application servers that use a system-wide SSL server PSE, you only need to import the certificate request response into the SSL server PSE on one of the servers.

**Prerequisites**
- The certificate request response contains either the signed public-key certificate in PEM format and the issuing CA's root certificate exists in the server's certificate store, or the response adheres to the PKCS#7 certificate chain format.
- You have access to the certificate request response. For example, it exists as a file in the file system.

**Procedure**
From the Trust Manager screen:

1. Expand the SSL server PSE node.
2. For each application server that is to receive a signed certificate:
   a. Select the application server with a double-click.
      The application server's SSL server PSE is displayed in the PSE maintenance section.
   b. In the PSE maintenance section, choose **Import Cert. Response**.
      The dialog for the certificate request response appears.
   c. Insert the contents of the certificate request response into the dialog's text box (using **Paste**) or select the response from the file system by using **Load local file**.
      The signed public-key certificate is imported into the server's SSL server PSE, which is displayed in the PSE maintenance section. You can view the certificate by selecting it with a double-click. The certificate information is then shown in the certificate maintenance section.
3. Save the data.
Maintaining the SSL Server PSE’s Certificate List

Use

If users are to be authenticated on the SAP Web Application Server using client certificates, then you must maintain the server’s certificate list, which is contained in the server’s SSL server PSE. The application server uses this list to determine which CAs the server trusts. Only users who present client certificates issued by these CAs can be authenticated based on their certificates.

You must also perform additional maintenance tasks to be able to use client certificates for authentication. For more information, see Configuring the System for Using X.509 Client Certificates [Page 47].

You only need to maintain the certificate list for a single application server's SSL server PSE. The certificate list is distributed to all servers, even if you use server-specific SSL server PSEs.

The certificate list is only stored in the selected PSE and distributed to the other application servers after saving the data in the trust manager.

Prerequisites

You have access to the CA’s root certificate. For example, the SAP CA’s certificate is available in the SAP System. If you use a different CA, then you must obtain its public-key certificate and store it in one of the available storage locations (for example, in the certificate database). If you have already imported the CA’s certificate to a different PSE on the application server, then you can also use the trust manager to copy it from the PSE into the SSL server PSE.

Procedure

Importing the CA’s Root Certificate From the Certificate Database

If the CA’s public-key certificate is located in the certificate database:

1. In the certificate section, choose Import certificate.
   The Import Certificate dialog appears.
2. Select the Database tabstrip.
3. Select the certificate from the certificate database and choose Enter.
   The certificate appears in the certificate section.
   The certificate is added to the certificate list for the PSE displayed in the PSE maintenance section.
5. Save the data.
Importing the CA’s Root Certificate From the File System

If the CA’s public-key certificate is located in the file system:
1. In the certificate section, choose Import certificate.
   The Import Certificate dialog appears.
2. Enter the corresponding file name from the file system.
3. Select the certificate’s file format.
   If you are not sure which format to select, open the certificate in a text browser that does not use formatting, for example, Notepad. If the contents are readable (although encoded), then the format is Base 64. Otherwise the format is binary.
4. Choose Enter.
   The certificate appears in the certificate maintenance section.
5. Choose Add to Certificate List.
   The certificate is added to the certificate list for the PSE displayed in the PSE maintenance section.
6. Save the data.

Importing the CA’s Root Certificate From a Different PSE

If the CA’s public-key certificate is located in a different PSE in the SAP System:
1. Expand the node for the PSE that contains the certificate and select one of the application servers with a double-click.
   The PSE and its certificate list appear in the PSE maintenance section.
2. Select the certificate with a double-click.
   The certificate appears in the certificate maintenance section.
3. Select one of the application servers under the SSL server PSE node with a double-click.
   The certificate is added to the certificate list for the PSE displayed in the PSE maintenance section.
5. Save the data.

Importing the SAP CA’s Root Certificate

To import the SAP CA’s root certificate:
   The SAP CA’s certificate appears in the certificate maintenance section.
2. Choose Add to Certificate List.
   The certificate is added to the certificate list for the PSE displayed in the PSE maintenance section.
3. Save the data.
Repeat the procedure for all CA root certificates that the server should trust.

Result
The certificate list in the application server’s SSL server PSE contains the public-key certificates belonging to the CAs that the server trusts.
Creating the Standard SSL Client PSE

Use
To be able to communicate using SSL, the SAP Web Application Server must also possess the standard SSL client PSE. Therefore, repeat the procedure for the standard SSL client PSE.

Procedure
The procedure is similar to that for generating and maintaining SSL server PSEs. Exceptions are indicated as necessary.

Using the trust manager:
1. **Create the standard SSL client PSE [Page 13].**
   In this case, you specify the CN part of the Distinguished Name (default = system ID). You only create one PSE, which is then distributed to the rest of the application servers.
2. **Generate a certificate request for the standard SSL client PSE [Page 15].**
   Because the SSL client PSE is system-specific and not server-specific, you only need to create a single certificate request and import it once.
3. **Send the certificate request to a CA to be signed [Page 16].**
4. **Import the certificate request response into the server's standard SSL client PSE [Page 17].**
5. **Maintain the standard SSL client PSE's certificate list [Page 17].**
   The SSL client PSE's certificate list is typically less restrictive than the list contained in the SSL server PSE.

Result
The SAP Web Application Server can use HTTPS connections to communicate with other Web servers.

Creating the Anonymous SSL Client PSE

Use
The SAP Web Application Server uses the anonymous SSL client PSE when accessing other Web servers using the SSL protocol. Note that the server does not use the information contained in this PSE for its own authentication; it only uses the PSE's information to authenticate the Web server that it is accessing. Therefore, you do not have to have the corresponding public-key certificate signed by a CA and the steps for generating and importing a certificate request are not necessary.

Procedure
1. **Create the anonymous SSL client PSE [Page 13].**
   In this case, the system automatically defines the server's Distinguished Name (CN=anonymous). You cannot modify this name.
2. **Maintain the PSE's certificate list [Page 17].**
   Import the root certificates from the CAs that have issued the public-key certificates to the Web servers that the SAP Web Application Server accesses using the anonymous SSL client PSE.
For example, if the SAP Web Application Server accesses a Web server that possesses a public-key certificate issued by myCA, then the certificate list in the application server's SSL client PSE must contain myCA's root certificate so that the application server can authenticate the Web server accordingly.

**Result**
The SAP Web Application Server can authenticate the Web servers that it accesses using the SSL protocol.

### Creating Individual SSL Client PSEs

**Use**
The SAP Web Application Server can also possess additional individual "identities" that it can use to access other Web servers using SSL. These individual identities are defined in the individual SSL client PSEs.

**Procedure**
1. First, you must create an entry for each individual SSL client PSE in the table STRUSTSSL.
2. Then create and maintain the individual SSL client PSEs.

See the procedures below.

#### Creating an Entry for the Individual SSL Client PSE

From the *Trust Manager* screen:
   
   The *Change View: SSL Client Identities* maintenance screen appears. Default entries include the anonymous SSL client PSE (ANONYM) and the standard SSL client PSE (DEFAULT).
2. Choose `New Entries`.
   
   The *New Entries: Overview of New Entries* maintenance screen appears.
3. Enter the PSE's information (`SSL ID` and `Description`) in the appropriate columns and activate the PSE by selecting the `Active` indicator.
4. Save the data.
5. Go `Back`.

You return to the *Trust Manager* screen. An entry for each individual PSE appears in the PSE status section.

#### Creating the Individual SSL Client PSE

The procedure is similar to that for creating the other PSEs. Exceptions are indicated as necessary.

From the *Trust Manager* screen:
1. **Create the individual SSL client PSE** [Page 13].
   
   In this case, you specify the CN part of the Distinguished Name (default = system ID). You only need to generate one PSE, which is then distributed to the rest of the application servers.
2. **Generate a certificate request for the individual SSL client PSE** [Page 15].
   
   Because the individual SSL client PSE is system-specific and not server-specific, you only need to create a single certificate request and import it once.
3. Send the certificate request to a CA to be signed [Page 16].
4. Import the certificate request response into the individual SSL client PSE [Page 17].
5. Maintain the individual SSL client PSE's certificate list [Page 17].

Result
The SAP Web Application Server can authenticate itself using the individual SSL client PSE when using HTTPS connections to communicate with other Web servers.

Specifying that a Connection Should Use SSL

Use
Use the following procedure to specify the connections that should use SSL when the SAP Web AS is the client component in the connection.

Prerequisites
The HTTP destination for the connection is defined in transaction SM59.

Procedure
Using the maintenance transaction for RFC destinations (SM59):
1. From the RFC destination tree, select the HTTP destination to modify.
   Details about the RFC destination appear.
2. Select the Logon/Security tabstrip.
3. If the target system is an SAP System, then select the logon method to use.
   When you activate SSL with client authentication (see step 4), then the logon method that you specify here is only used if the server that you are connecting to is not configured to accept client authentication. The following options are available:
   - Basic Authentication
   - SAP Standard (logon tickets)
   - SAP Trusted System (RFC trusted systems)
4. Under SSL, select Active and enter the name of the SSL client PSE to use in the field provided, for example, DFAULT (standard), ANONYM (anonymous), or the name of one of your individual SSL client PSEs.

If you select the standard or an individual SSL client PSE, then the system will attempt to use SSL with mutual authentication. However, if the server you are connecting to is only configured for SSL with server authentication, then the system reverts to the logon method that you specified above (in step 3).

If you select the anonymous SSL client PSE, then the SSL connection is set up for SSL with server authentication only and the system will use the logon method that you specified above.
5. If you want to protect the use of the connection with an authorization, enter the value of the activity allowed in the Authorization field. The system then checks for the authorization when the destination is used. The authorization object used is S_ICF.

For example, if you enter the value CHECK, then the system checks for this value in the user's authorizations when he or she uses this HTTP destination. In this case, the user must have the following authorization: S_ICF-ICF_FIELD = 'DEST' and S_ICF-ICF_VALUE = 'CHECK' to be able to use the HTTP destination.

Result

The system will use HTTPS connections for this destination using the client identity contained in the SSL client PSE that you specify.

Testing the SSL Configuration

To test the SSL configuration:
1. Make sure the SSL port is set up correctly. [Page 23]
2. Test the SSL connection for server authentication. [Page 24]
3. Test the SSL connection for client authentication. [Page 24]

Making Sure the SSL Port is Set up Correctly

Use

Use this procedure to make sure the profile parameters are set correctly and that the ICManager is listening to the correct HTTPS port.

Prerequisites

The SAP Cryptographic Library is installed and the following profile parameters are set correctly:

?? icm/plugin_<xx>
?? icm/server_port_<xx>

These parameters should be set correctly during the SAP Web AS's installation procedure.

Procedure

1. Start the ICM Monitor (transaction SMICM).
2. From the ICM Monitor screen, choose Goto ? Services.
   
   The ICM Monitor - Service Display screen appears, which shows the protocols and ports that are set up on the SAP Web AS.
3. If there is no port entry for HTTPS, then make sure the profile parameters are set correctly and restart the ICManager.
Testing the Connection for SSL Server Authentication

Use

Use this procedure to make sure that SSL support is set up correctly for connections where the SAP Web AS is the server component in the connection.

Prerequisites

?? The SSL server PSE exists.

?? You know the port number that the SAP Web AS is using for HTTPS connections. (See Making Sure the SSL Port is Set up Correctly [Page 23].)

Procedure

1. Start a Business Server Page (BSP) using an HTTPS connection and the SSL port.

   For example, start the standard BSP test application IT00 with the URL https://host123.mycompany.com:443/sap/bc/bsp/sap/it00/default.htm.

   If your Web browser cannot completely verify the SAP Web AS's server certificate, then you will receive a dialog that states the reason why. For example, if your Web browser does not possess the issuing CA's root certificate as a trusted root certificate, then you are informed and have the opportunity to trust the server at this time.

2. If you trust the server's certificate (either automatically or manually), then the next step is to authenticate yourself. If you have also set up the SAP Web Application Server for using client certificates (see Using X.509 Client Certificates [Page 46]), then you can also use a public-key certificate for authentication. Otherwise, you are prompted for user ID and password.

   After you have authenticated yourself, the BSP appears.

Result

You are connected to the SAP Web AS using SSL, which is indicated in your Web browser. For example, Microsoft Internet Explorer displays a lock in the lower right corner of the Web browser.

Testing the Connection for SSL Client Authentication

Use

Use this procedure to make sure that SSL support is set up correctly for connections where the SAP Web AS is the client component in the connection.

Prerequisites

?? The SSL client PSE exists.

?? The HTTP destination is set up to use SSL.

Procedure

1. Start the maintenance transaction for RFC destinations (SM59).

2. From the RFC destination tree, select the HTTP destination to test.

   Details about the RFC destination appear.

3. Choose Test connection.
**Result**

If the connection was successful, then the SAP Web AS has connected to the target server using SSL. The identity it uses for the connection is the identity specified in the SSL client PSE that is entered in the destination.

If the connection failed, then deactivate SSL and test the connection again. If the connection still fails, then there is a problem with the network connection. Otherwise, check the SSL client PSE in the trust manager and if necessary, replace or redistribute the SSL client PSE.

---

**Configuring the SAP Web Dispatcher to Support SSL**

**Use**

If you are using a stand-alone SAP Web Dispatcher in front of the SAP Web AS, then use the procedures below to configure the SAP Web Dispatcher to support SSL. The SAP Web Dispatcher can either pass the SSL connection to the server in the backend, or it can terminate the SSL connection. See the graphics below.

**Passing the SSL Connection**

![Diagram showing the SAP Web Dispatcher passing the SSL connection](image)
Terminating the SSL Connection

Procedure

Configuring the SAP Web Dispatcher to Pass the SSL Connection to the Backend Server

If the SAP Web Dispatcher is to pass the SSL connection to the server in the backend, then, in addition to the standard parameters, set the following profile parameter in the SAP Web Dispatcher’s profile:

\[
\text{icm/server_port_<xx> = PROT=ROUTER, PORT=<port>, TIMEOUT=<timeout_in_seconds>}
\]

For more information about the SAP Web Dispatcher’s profile, see The SAP Web Dispatcher Profile Parameter [SAP Library].

Configuring the SAP Web Dispatcher to Terminate the SSL Connection

If the SAP Web Dispatcher is to terminate the SSL connection, then it must possess a security environment. To set up this security environment, perform the following:

1. Install the SAP Cryptographic Library on the SAP Web Dispatcher [Page 26].
2. Set the profile parameters [Page 27].
3. Create the SAP Web Dispatcher’s PSE and certificate request [Page 29].
4. Send the certificate request to a CA to be signed [Page 32].
5. Import the certificate request response into the PSE [Page 34].
6. Create credentials for the SAP Web Dispatcher [Page 35].
7. Restart the SAP Web Dispatcher.
8. Test the connection [Page 37].
Installing the SAP Cryptographic Library on the SAP Web Dispatcher

Use

The SAP Cryptographic Library contains the security functions necessary for using the SSL protocol. Therefore, if the SAP Web Dispatcher is to terminate the SSL connection, then use the following procedure to install the library on the SAP Web Dispatcher.

If the SAP Web Dispatcher passes the SSL connection to the application server in the backend, then it does not need to possess its own security environment and you can skip these steps.

Prerequisites

You have obtained the SAP Cryptographic Library installation package [Page 9].

Procedure

1. Extract the contents of the SAP Cryptographic Library installation package.
2. Copy the library file and the configuration tool sapgenpse.exe to a local directory, for example, the directory where the SAP Web Dispatcher is located. For this documentation, we will use the directory C:\Program Files\SAP\SAPWebDisp.
3. Check the file permissions for the SAP Cryptographic Library. If, for example, you copied the library to its location using ftp on UNIX, then the file permissions may not be set correctly. Make sure that the user that runs the SAP Web Dispatcher is able to execute the library's functions.
4. Create a sub-directory called sec and copy the ticket file to this directory. This is also the directory where the SAP Web Dispatcher's PSEs and credentials are to be located.

Location of the SAP Cryptographic Library

C:\Program Files\SAP\SAPWebDisp\sapcrypto.dll

Location of the Configuration Tool sapgenpse

C:\Program Files\SAP\SAPWebDisp\sapgenpse.exe

Location of the License Ticket

C:\Program Files\SAP\SAPWebDisp\sec\ticket

Result

The SAP Cryptographic Library is installed on the SAP Web Dispatcher.
Setting the SSL Profile Parameters for the SAP Web Dispatcher

In addition to the standard parameters, set the SSL-relevant parameters in the SAP Web Dispatcher’s profile as shown in the tables below.

Profile Parameters

<table>
<thead>
<tr>
<th>Profile Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIR_INSTANCE</td>
<td>Directory where the sec sub-directory is located.</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\SAP\SAPWebDisp</td>
</tr>
<tr>
<td>icm/server_port_&lt;xx&gt;</td>
<td>PROT=HTTPS, PORT=&lt;port&gt;, TIMEOUT=&lt;timeout_in_seconds&gt;</td>
</tr>
<tr>
<td></td>
<td>If the SAP Web Dispatcher is to pass the SSL connection to the server in the backend, then set this parameter to PROT=ROUTER, PORT=&lt;port&gt;, TIMEOUT=&lt;timeout_in_seconds&gt;. In this case, the rest of the parameters in this table are not necessary.</td>
</tr>
<tr>
<td>icm/HTTPS/verify_client</td>
<td>0: Do not use certificates</td>
</tr>
<tr>
<td></td>
<td>If the SAP Web Dispatcher is to terminate the SSL connection, then you cannot use client certificates for authentication. In this case, set the parameter icm/HTTPS/verify_client to the value 0.</td>
</tr>
<tr>
<td>ssl/ssl_lib</td>
<td>Path and file name of the SAP Cryptographic Library</td>
</tr>
<tr>
<td>ssl/server_pse</td>
<td>Path and file name of the SSL server PSE.</td>
</tr>
<tr>
<td></td>
<td>Default: SAPSSLS.pse in the sec sub-directory for DIR_INSTANCE.</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\SAP\SAPWebDisp\sec\SAPSSLS.pse</td>
</tr>
</tbody>
</table>

For more information about the SAP Web Dispatcher’s profile, see The SAP Web Dispatcher Profile Parameter [SAP Library].

For an example, see Sample Profile for the SAP Web Dispatcher When Using SSL [Page 28].
Sample Profile for the SAP Web Dispatcher When Terminating SSL

# SAPSYSTEMNAME must be set so that the default profile is
# read. If not, a warning is displayed on the console.
SAPSYSTEMNAME = ABC

# SAPSYSTEM must be set so that the shared memory areas
# can be created.
# The number must be different from the other SAP instances
# on the host.
SAPSYSTEM = 26

# Set DIR_INSTANCE so that the SAP Cryptographic Library can
# find the sec sub-directory.
DIR_INSTANCE = C:\Program Files\SAP\SAPWebDisp

# Message Server Description
rdisp/mshost = abcmain
ms/http_port = 8081

# Description of the Access Points
icm/server_port_0 = PROT=HTTP, PORT=1081, TIMEOUT=900
icm/server_port_1 = PROT=HTTPS, PORT=1443, TIMEOUT=900
icm/HTTPS/verify_client = 0

# Parameters for the SAP Cryptographic Library
ssl/ssl_lib = C:\Program Files\SAP\SAPWebDisp\sapcrypto.dll
ssl/server_pse = C:\Program Files\SAP\SAPWebDisp\sec\SAPSSLS.pse
Creating the SSL Server PSE and Certificate Request

Use

If the SAP Web Dispatcher is to terminate the SSL connection, then it needs to possess a key pair and public-key certificate to use for the SSL connection. This information is stored in the SAP Web Dispatcher's SSL server PSE.

You can either use the trust manager to create the PSEs or you can use the configuration tool sapgenpse. See the procedures below.

If the SAP Web Dispatcher is to pass the SSL connection to the SAP Web Application Server, then you do not need to perform these steps.

Prerequisites

?? If you are using the trust manager to create the PSE, then the SAP Cryptographic Library is installed on the application server. (See also Installing the SAP Cryptographic Library on the SAP Web AS on Page 11.)

If you are using sapgenpse, then the SAP Cryptographic Library is installed on the SAP Web Dispatcher. (See also Installing the SAP Cryptographic Library on the SAP Web Dispatcher on Page 28.)

?? The environment variable SECUDIR is set to the directory where the license ticket is located.

?? You know the naming convention to use for the SAP Web Dispatcher's Distinguished Name. The syntax of the Distinguished Name depends on the CA that you use.

For example, if you use the SAP CA, the naming convention is CN=<host_name>, OU=I<installation_number>-<company_name>, OU=SAP Web AS, O=SAP Trust Community, C=DE.

Procedure

Creating the SAP Web Dispatcher’s SSL Server PSE Using the Trust Manager

From the Trust Manager screen:

1. Using the context menu for the File node, choose Create (RSA).

For SSL, you must create a PSE that contains an RSA key pair. If you choose Create, then a DSA key pair is created, which cannot be used for SSL.

The Create PSE dialog appears.

2. Enter the Distinguished Name parts in the corresponding fields according to your CA's naming convention.

The Common Name part of the Distinguished Name must correspond to the fully-qualified host name used to access the Web Dispatcher.

For more information about how the trust manager builds the Distinguished Name from the field entries, see Creating or Replacing a PSE in the documentation for the Trust Manager (SAP Library).

3. Save the PSE to local file (for example, the Web Dispatcher's SECUDIR directory). Use the file name that you specified in the profile parameter ssl/server_pse.
Creating the Certificate Request Using the Trust Manager

Once you have created the PSE, you must create a corresponding certificate request. For this procedure you can also use the trust manager. Perform the following:

1. Select the File node with a double-click.
   
The Open dialog appears.

2. Select the PSE that you saved in the previous procedure.
   
The corresponding certificate appears in the PSE maintenance section in the Own certif. field.

3. In the PSE maintenance section, choose Create Certificate Request.
   
A dialog appears showing the certificate request.

4. Select the content of the request and copy it to your clipboard (Copy) or save the certificate request to a file (<file_name>.P10) using Save as local file.

Continue with Sending the Certificate Request to a CA [Page 32].

Creating the SAP Web Dispatcher's SSL Server PSE and Certificate Request Using SAPGENPSE

As an alternative, you can use the configuration tool sapgenpse to create the SAP Web Dispatcher’s SSL server PSE.

Before you can use sapgenpse to create the SSL server PSE, the environment variable SECUDIR must be set to the directory where the license ticket is located. If the environment variable is not yet set, then set it using the command line as shown below.

```
set SECUDIR=<SECUDIR_directory>
```

Use the tool’s command get_pse as shown below to create the SAP Web Dispatcher’s PSE.

```
sapgenpse get_pse <additional_options> -p <PSE_Name> -r <cert_req_file_name> -x <PIN> <Distinguished_Name>
```

Where:

**Standard Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Parameter</th>
<th>Description</th>
<th>Allowed Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>&lt;PSE_Name&gt;</td>
<td>Path and file name for the PSE.</td>
<td>The file name must correspond to the file name specified in the profile parameter ssl/server_pse (for example, SAPSSL.S.pse).</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the complete path is not included, then the PSE file is created in the SECUDIR directory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-r</td>
<td>&lt;file_name&gt;</td>
<td>File name for the certificate request</td>
<td>Path description (in quotation marks, if spaces exist)</td>
<td>stdout</td>
</tr>
<tr>
<td>-x</td>
<td>&lt;PIN&gt;</td>
<td>PIN that protects the PSE</td>
<td>Character string</td>
<td>None</td>
</tr>
<tr>
<td>None</td>
<td>&lt;Distinguished_Name&gt;</td>
<td>The Distinguished Name for the SAP Web Dispatcher</td>
<td>Character string (in quotation marks, if spaces exist)</td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Parameter</td>
<td>Description</td>
<td>Allowed Values</td>
<td>Default</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>---------</td>
</tr>
<tr>
<td>-s</td>
<td>&lt;key_len&gt;</td>
<td>Key length</td>
<td>512, 1024, 2048</td>
<td>1024</td>
</tr>
<tr>
<td>-a</td>
<td>&lt;algorithm&gt;</td>
<td>Algorithm used</td>
<td>RSA, DSA</td>
<td>RSA</td>
</tr>
<tr>
<td>-noreq</td>
<td>None</td>
<td>Only generate a key pair and PSE. Do not create a certificate request.</td>
<td>Not applicable</td>
<td>Not set</td>
</tr>
<tr>
<td>-only req</td>
<td>None</td>
<td>Generate a certificate request for the public key stored in the PSE specified by the –p parameter.</td>
<td>Not applicable</td>
<td>Not set</td>
</tr>
</tbody>
</table>

The command line below creates the SAP Web Dispatcher’s SSL server PSE and certificate request using the following information:

- The environment variable SECUDIR is set to C:\Program Files\SAP\SAPWebDisp\sec.
- The PSE is to be located at C:\Program Files\SAP\SAPWebDisp\sec\SAPSSLS.pse.
- The PIN used to protect the PSE is abcpin.
- The name of the certificate request file is abc.req.
- The SAP Web Dispatcher is accessed using the fully-qualified hostname host123.mycompany.com.
- The CA used is the SAP CA.

Therefore, the server’s Distinguished Name is CN=host123.mycompany.com, OU=I1234567890-MyCompany, OU=SAP Web AS, O=SAP Trust Community, C=DE.

```
sapgenpse get_pse -p SAPSSLS.pse -x abcpin -r abc.req
"CN=host123.mycompany.com, OU=I1234567890-MyCompany, OU=SAP Web AS, O=SAP Trust Community, C=DE"
```
Sending the Certificate Request to a CA

Use

After you have generated a key pair and certificate request, send the certificate request to a CA to be signed. The response from the CA is a signed public-key certificate for the server.

Prerequisites

You can send the certificate request to the CA of your choice, for example, the SAP CA. Note however, the corresponding certificate request response from the CA must be available in one of the following formats:

- **PKCS#7 certificate chain format**
  
  In this case, the issuing CA provides the certificate request response in the necessary format. For example, either the SAP CA provides the response in this format, or you can request this format from your CA.

- **PEM format**
  
  In this case, the certificate request response from your CA contains only the signed public-key certificate. Therefore, you must also have access to the CA's root certificate. If you are using the trust manager, then this root certificate must exist in the database. If you are using `sapgenpse`, then it must exist as a file in the file system.

Procedure

For each certificate request that you created, send the contents of the certificate request to your CA.

The exact procedure to use depends on the CA that you use. For the SAP CA, follow the instructions provided by the SAP Trust Center Service at [http://service.sap.com/tcs](http://service.sap.com/tcs).

To view the contents of the certificate, open the certificate request with a text editor. Because many editors use hidden characters for formatting, use a text editor that does not support formatting features, for example, Notepad. If carriage returns or line feeds have been corrupted, for example, during download, then correct these errors.

The example below shows a correct certificate request.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBkzCCAVICAQAwWjELMAkGA1UEBhMCREUxHDAdBgNVBAoTE215U0FQLmNvbS
BXb3JrcGxhY2UxuDzANBgNVBAElOZXNzdW5JZGVkMREwGzAUMAwGA1UECxMC
FmFzazMxMDAKBgNVBAMTAm15QTAxGzEvMjUxGzEvMjUxGzEvMjUx
-----END CERTIFICATE REQUEST-----
```

Result

The CA will validate the information contained in the certificate request (according to its own policy) and return a response that contains the signed public-key certificate.
Importing the Certificate Request Response

Use
The CA will send you a certificate request response that contains the signed public-key certificate for the SAP Web Dispatcher. Once you have received this response, import it into the SAP Web Dispatcher’s SSL server PSE. You can either use the trust manager or you can use the configuration tool sapgenpse. See the procedures below.

Prerequisites
?? If you are using sapgenpse, then the certificate request response exists as a file in the file system. Otherwise, if you are using the trust manager, then the response can either exist as a file or you can use Copy&Paste to insert it into the PSE.

?? If the certificate request response does not contain the CA’s root certificate, then you also have access to this certificate. If you are using the trust manager, then it must exist in the trust manager’s database. If you are using sapgenpse, then it exists as a file in the file system.

Procedure

Importing the Certificate Request Response Using the Trust Manager
If you used the trust manager to create the SAP Web Dispatcher’s PSE, then you can easily use it again to import the certificate request response. Perform the following:

1. If the certificate request dialog is still open, then close it.
2. If the SAP Web Dispatcher’s PSE is not loaded in the PSE maintenance section, then load it by selecting the File node with a double-click and selecting the SSL server PSE from the file system.

3. In the PSE maintenance section, choose Import Cert. Response.

   The dialog for the certificate response appears.

4. Insert the contents of the certificate request response into the dialog’s text box either using Copy&Paste or by loading the file from the file system.

   The signed public-key certificate is imported into the SAP Web Dispatcher’s PSE, which is displayed in the PSE maintenance section. You can view the certificate by selecting it with a double-click. The certificate information is then shown in the certificate maintenance section.

5. Create a PIN for the PSE.

   Although a PIN for the PSE is optional, we recommend using a PIN to protect the PSE, especially if the SAP Web Dispatcher is located in your demilitarized zone.

6. Save the data in the trust manager.

   You are prompted for the location to which to save the PSE. Replace the PSE that you created earlier.

7. If you saved the PSE to a local file on the application server, then copy it to the SECUDIR directory on the SAP Web Dispatcher.
Importing the Certificate Request Response Using SAPGENPSE

As an alternative, you can use the configuration tool sapgenpse to import the certificate request response into the SAP Web Dispatcher’s SSL server PSE. Use the tool’s command `import_own_cert` as shown below.

\[\text{sapgenpse import\_own\_cert <Additional\_options> \text{ -p } <\text{PSE\_file}> \text{ -c } <\text{Cert\_file}> [\text{ -r } <\text{RootCA\_cert\_file}>] \text{ -x } <\text{PIN}>\]

Where:

**Standard Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Parameter</th>
<th>Description</th>
<th>Allowed Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>&lt;PSE_Name&gt;</td>
<td>Path and file name for the PSE. If the complete path is not included, then the PSE file used is the corresponding PSE located in the SECUDIR directory.</td>
<td>Path description (in quotation marks, if spaces exist)</td>
<td>None</td>
</tr>
<tr>
<td>-c</td>
<td>&lt;Cert_file&gt;</td>
<td>Path and file name of the certificate request response</td>
<td>Path description (in quotation marks, if spaces exist)</td>
<td>None</td>
</tr>
<tr>
<td>-r</td>
<td>&lt;RootCA_cert_file&gt;</td>
<td>File containing the CA’s root certificate (optional)</td>
<td>Path description (in quotation marks, if spaces exist)</td>
<td>Not set</td>
</tr>
<tr>
<td>-x</td>
<td>&lt;PIN&gt;</td>
<td>PIN that protects the PSE</td>
<td>Character string</td>
<td>None</td>
</tr>
</tbody>
</table>

**Result**

The certificate request response is imported into the PSE.

The following command line imports the certificate request response (`ABC.cer`) into the SAP Web Dispatcher’s SSL server PSE that is stored at `C:\Program Files\SAP\SAPWebDisp\sec\SAPSSL.pse`. (SECUDIR is set to `C:\Program Files\SAP\SAPWebDisp\sec`). The PIN that protects the PSE is `abcpin`.

\[\text{sapgenpse import\_own\_cert \text{ -c } ABC.cer \text{ -p SAPSSL.pse \text{ -x } abcpin} \]
Creating Credentials for the SAP Web Dispatcher

Use

The SAP Web Dispatcher must have active credentials at run-time to be able to access its PSEs. Therefore, to produce active credentials, use the configuration tool’s command `seclogin` to “open” each PSE.

⚠️ The credentials are located in the file `cred_v2` in the directory specified by the environment variable `SECUDIR`. Make sure that only the user under which the SAP Web Dispatcher runs has access to this file (including read access).

💡 If the SAP Web Dispatcher is to pass the SSL connection to the SAP Web Application Server, then you do not need to perform these steps.

Prerequisites

?? The SAP Cryptographic Library is installed and the environment variable `SECUDIR` is set to the directory where the license ticket and SSL server PSE is located.

?? You know the user that runs the SAP Web Dispatcher.

Procedure

Use the following command line to open the PSE and create credentials.

```
sapgenpse seclogin <additional options> -p <PSE_Name> -x <PIN> -O [<Windows_Domain>\]<user_ID>
```

Where:

### Standard Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Parameter</th>
<th>Description</th>
<th>Allowed Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td><code>&lt;PSE_Name&gt;</code></td>
<td>Path and file name for the PSE. If the complete path is not included, then the PSE file used is the corresponding PSE located in the <code>SECUDIR</code> directory.</td>
<td>Path description (in quotation marks, if spaces exist)</td>
<td>None</td>
</tr>
<tr>
<td>-x</td>
<td><code>&lt;PIN&gt;</code></td>
<td>PIN that protects the PSE</td>
<td>Character string</td>
<td>None</td>
</tr>
<tr>
<td>-O</td>
<td>[ <code>&lt;Windows_Domain&gt;\</code> ] <code>&lt;user_ID&gt;</code></td>
<td>User for which the credentials are created. (The user that runs the SAP Web Dispatcher process.) If the user that runs the SAP Web Dispatcher is the current user, then do not include this parameter in the command line.</td>
<td>Valid operating system user</td>
<td>The current user</td>
</tr>
</tbody>
</table>
Additional Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Parameter</th>
<th>Description</th>
<th>Allowed Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l</td>
<td>None</td>
<td>List all available credentials for the current user.</td>
<td>Not applicable</td>
<td>Not set</td>
</tr>
<tr>
<td>-d</td>
<td>None</td>
<td>Delete credentials</td>
<td>Not applicable</td>
<td>Not set</td>
</tr>
<tr>
<td>-chpin</td>
<td>None</td>
<td>Specifies that you want to change the PIN</td>
<td>Not applicable</td>
<td>Not set</td>
</tr>
</tbody>
</table>

After creating the credentials, restart the SAP Web Dispatcher.

Result

The credentials file (cred_v2) for the user provided with the –O option is created in the SECUDIR directory.

The following command line opens the SAP Web Dispatcher's SSL server PSE that is located at C:\Program Files\SAP\SAPWebDisp\sec\SAPSSLS.pse and creates credentials for the user ABCadm. (SECUDIR is set to C:\Program Files\SAP\SAPWebDisp\sec). The PIN that protects the PSE is abcpin.

```
sapgenpse seclogin -p SAPSSLS.pse -x abcpin –O ABCadm
```

Testing the SSL Connection to the SAP Web Dispatcher

Use

Use this procedure to make sure that SSL support is set up correctly on the SAP Web Dispatcher.

Prerequisites

?? The SAP Web Dispatcher’s SSL server PSE and credentials exist.
?? The SAP Web Dispatcher has been restarted.
?? You know the port number that the SAP Web Dispatcher is using for HTTPS connections.

The port number is specified in the profile parameter icm/server_port_<xx> in the SAP Web Dispatcher’s profile.

Procedure

1. Start a Business Server Page (BSP) using an HTTPS connection to your SAP Web Dispatcher and the corresponding SSL port.

   For example, start the standard BSP test application IT00 with the URL https://mywebdisp.mycompany.com:443/sap/bc/bsp/sap/it00/default.htm.

   If your Web browser cannot completely verify the SAP Web Dispatcher's public-key certificate, then you will receive a dialog that states the reason why. For example, if your Web browser does not possess the issuing CA's root certificate as a trusted root certificate, then you are informed and can choose to trust the server at this time.

2. If you trust the server's certificate (either automatically or manually), then the next step is to authenticate yourself.

   If your authentication was successful, the BSP appears.
**Result**

You are connected to the SAP Web AS via the SAP Web Dispatcher. SSL is used for the connection between your Web browser and the SAP Web Dispatcher, which is indicated in your Web browser. For example, Microsoft Internet Explorer displays a lock in the lower right corner of the Web browser.

![Lock Icon]

If the SAP Web Dispatcher terminates the SSL connection, then it establishes a new HTTP connection to the SAP Web AS in the backend. SSL is currently not supported for this connection.
User Authentication

Using Logon Tickets

Use

For authentication on the SAP Web AS that allows for Single Sign-On (SSO) to other systems as well, you can have the system issue logon tickets to the users. The user can then access other systems using the logon ticket as the authentication token instead of having to repeatedly enter his or her user ID and password.

Prerequisites

?? Users need to have the same user ID in all of the systems they access using the logon ticket. Passwords do not have to be the same in all systems.

?? End users need to configure their Web browsers to accept cookies.

?? In Internet Explorer 5.0, accept session cookies for the local intranet zone.

?? Any Web servers or SAP Web AS servers that are to accept the logon ticket as the authentication mechanism must be placed in the same DNS domain as the issuing server. The logon ticket cannot be used for authentication to servers outside of this domain.

?? The issuing server must possess a public and private key pair and public-key certificate so that it can digitally sign the logon ticket.

SAP System application servers (to include the SAP Web AS) receive a key pair and a self-signed public-key certificate during the installation process. As an alternative, you can obtain a certificate signed by the SAP Certification Authority (SAP CA).

?? Systems that accept logon tickets must have access to the issuing server's public-key certificate so that they can verify the digital signature provided with the ticket.

Depending on the type of certificate you use, the server's certificate is either sent with the logon ticket to the accepting system or the information is entered in the accepting system's certificate list. We provide a configuration tool, the SSO administration wizard (transaction SSO2), that automatically establishes the appropriate configuration for the accepting system.

Activities

In the following, we describe the processes when the issuing or accepting server is an SAP Web AS. Note however, depending on the scenario you use, other server components may act as the issuer or acceptor.

Receiving a Logon Ticket from the SAP Web AS

1. The user authenticates him or herself on the SAP Web AS (for example, using user ID and password).

2. The SAP Web AS verifies the user's information. If the authentication was successful, then the user is logged on to the server and a ticket is issued to him or her. The ticket is stored in the user's Web browser and used for authentication on successive systems.
Using the Logon Ticket to Access the SAP Web AS as an Accepting System

When the user accesses the SAP Web AS as an accepting system:
1. The Web browser sends the user's logon ticket with the access request.
2. The SAP Web AS verifies the information contained in the ticket. This includes:
   - Verifying the issuing server's digital signature.
   - Making sure the ticket has been issued by a trusted server (either itself or a server listed in the corresponding access control list).
   - Checking the expiration time.
     If the ticket is valid and has been issued by a trusted server, then the user is granted access to system.

Configuring the System for Issuing Logon Tickets

Prerequisites

You must know whether the server should use a self-signed public-key certificate or a certificate signed by the SAP CA.

Procedure

1. If you use a certificate signed by the SAP CA, you need to obtain the certificate and import it into the server's Personal Security Environment (PSE) to use for Single Sign-On (the SSO PSE [Page 54]). For the SAP Web Application Server, the SSO PSE is the system PSE [Page 55].
   - If you use a self-signed certificate, then the public-key certificate already exists.
   - For more information, see:
     - Obtaining a Certificate Signed by the SAP CA [Page 41]
     - Using a Self-Signed Certificate [Page 42]
2. Set the following profile parameters on the SAP Web Application Server:

   Profile Parameters Used for Logon Tickets

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/accept_sso2_ticket</td>
<td>1</td>
<td>Allows the server to accept an existing logon ticket.</td>
</tr>
<tr>
<td>login/create_sso2_ticket</td>
<td>1: If the server's certificate is to be included in the logon ticket. 2: If the server's certificate is not to be included.</td>
<td>For best results, set this parameter to the value 1 if the server possesses a certificate signed by the SAP CA. Set it to the value 2 if the certificate is self-signed.</td>
</tr>
<tr>
<td>login/ticket_expiration_time</td>
<td>Desired value</td>
<td>Default = 60 hours</td>
</tr>
</tbody>
</table>

For more information, see the documentation provided for the profile parameters in transaction RZ11.

You can use the SSO administration wizard to view the current server's SSO configuration. (Execute the tool without specifying an RFC destination.)
Obtaining a Certificate Signed by the SAP CA

Use

To obtain a certificate signed by the SAP CA for the SAP Web Application Server to use for digitally signing logon tickets, you must generate a key pair and PSE for the application server. You also generate the corresponding certificate request, which you send to the SAP CA. You then import the certificate request response into the server's PSE as described in the procedures below.

A certificate request and corresponding response belong to a specific key pair and PSE. You can therefore only import the response into the PSE for which the request was generated.

If, for example, you generate a new PSE after you have already sent a certificate request to the SAP CA, then the response you receive is invalid and cannot be imported into the server's PSE.

Procedure

Sending the Certificate Request

1. Execute the trust manager (transaction STRUST).

   The Trust Manager screen appears.

2. Expand the System PSE node.

3. Create a new system PSE. (See Creating or Replacing a PSE in the documentation for the Trust Manager [SAP Library].)

   The information for the system PSE appears in the PSE maintenance section.

4. Choose PSE ? Generate certificate request and save it to a file.

   The content of the request is generated in binary-code as shown below.

   -----BEGIN CERTIFICATE REQUEST-----
   MIIBkzCCAVICAQAwjELMAkGA1UEBhMCREUxHDAaBgNVBAoTE215U0FQLmNvbSBEb3JrcGxhY2UxOzANBgNVBAsTBlNBUCBBRzEOMAwGA1UECxMFQmFzaXmxDDAKBgNVBAMTA0JJTzCB7jCBpgYFKw4DAhswg2wCQQCSnauC/cAfQVrmOtaWznQ9I+i4twoFbpc5EAV5jQx2oMqBnyoi+e/ZH2cLwyhp5mO0w70+exS7PHEWKIfAhUw9FSY1AsFV4U9fC9w+Bg5H4ISYccQARcc+7q3ukM0UF0A5zRaq7viO3Wj2MwYUNwFkc0hxhloUQd21megZADOflisdzkn/nF4eIvV9vg9XxcV63xTsDQwACQFher18UA8Yky4/zHe4mbupBXvDScum2nbJUQ5PqDBVaMntpXIisyzuAFL+qCzQ92mNqUR9JLMwpz09ghQdICgBALbqckhj0OAQDzAAAMCC0CFA7qe1uP/Kfi+6HF/817j4NfF44xAhUAqkgDgAeR3tmNegKUTQ+JzeCXawE=

   -----END CERTIFICATE REQUEST-----

5. Copy the certificate request's content to a customer message under the component BC-SEC.

   The SAP CA validates your information and sends you a response, which contains the server's signed public-key certificate.
**Entering the Certificate Request Response Data**

After receiving a response:

1. Save the contents of the response to a file.
2. Execute the trust manager (transaction STRUST).
   
   The Trust Manager screen appears.
3. Expand the System PSE node and select an application server.
5. Select the file containing the response and choose OK.
6. Save the data.

**Result**

The server possesses a public-key certificate signed by the SAP CA. It can use the corresponding public-key information (that is, the private key) to digitally sign logon tickets issued by the SAP Web Application Server.

---

**Using a Self-Signed Certificate**

If you prefer, you can let the server use its self-signed certificate for digitally signing logon tickets instead of a certificate signed by the SAP CA.

The application server receives an automatically generated public and private key pair and a self-signed public-key certificate during the installation process. This information is stored in the server's SSO PSE and automatically distributed to the application server(s). You do not need to perform any additional tasks for configuring the system to use its self-signed certificate.

If you do want to change the information contained in the self-signed certificate (for example, to change the Distinguished Name), generate a new PSE and distribute it to the system's application servers. In addition, you must republish the public-key certificate to accepting systems by executing the SSO administration wizard (transaction SSO2) in the accepting system.

---

**Changing from a Self-Signed Certificate to a Certificate Signed by the SAP CA**

**Use**

Initially, you may want to use the self-signed certificate and change to a certificate signed by the SAP CA at a later date.

- User authentication using logon tickets will **not** be available to accepting systems while you are switching from a self-signed certificate to a certificate signed by the SAP CA.

- The time frame where SSO is not available starts when you save the new certificate on the issuing server and lasts until you have activated the server on **all** accepting systems.
Procedure

On the Issuing Server
1. Obtain a public-key certificate signed by the SAP CA [Page 41].
2. Make sure the profile parameter `login/create_sso2_ticket` is set to the value 1.

On Accepting Systems
1. Execute the SSO administration wizard (transaction SSO2) using the issuing server as the RFC destination.
   The SSO administration report displays the current SSO status.
2. Delete the former public-key certificate from the accepting system’s certificate list by choosing `Edit ? Remove Certificate List`.
3. Activate the issuing server by choosing `Edit ? Activate Workplace`.
   The SSO administration report displays the status for the new SSO environment.

See also Configuring the System for Accepting Logon Tickets [Page 43].

Result
The system now uses the key pair and public-key certificate signed by the SAP CA for digitally signing logon tickets. The accepting systems can also accept the logon tickets and verify the new digital signature.

Configuring the System for Accepting Logon Tickets

Use
Accepting systems need to be able to verify the logon tickets and the issuing server’s digital signature. The following information is necessary for the verification:

?? The system should only accept logon tickets issued from a trusted server. Therefore, the identity of the trusted server needs to be entered in the accepting system’s SSO access control list.

?? The system must be able to verify the issuing server’s digital signature. If the issuing server possesses a public-key certificate that is signed by the SAP CA, the accepting system can verify the issuing server’s digital signature without needing any additional information. However, if the certificate is a self-signed certificate, then the accepting system needs access to the issuing server’s public-key information, which needs to be entered in the system’s certificate list.

?? The system needs to know where the information is stored that it uses to verify the issuing server’s digital signature. The file name and location where this information is stored (the server’s designated SSO PSE) is release-dependent. See SSO Personal Security Environment (SSO PSE) [Page 54] for the file name and location of the SSO PSE according to release.

The SSO administration wizard accomplishes these configuration tasks automatically. The rest of the configuration tasks and the steps you need to take to use the SSO administration wizard are described below.
Prerequisites

?? The issuing server must possess a public and private key pair and a public-key certificate. This information needs to be available in the issuing server’s SSO PSE.

?? If the accepting system is an SAP Systems <= Release 4.6D, then the system must have the Workplace PlugIn installed and must meet the following release requirements:

?? Release 4.6x: 4.6D kernel as of Support Package level 74
?? Release 4.5x: 4.5B kernel as of Support Package level 459
?? Release 4.0x: 4.0B kernel as of Support Package level 758

?? The SAP Security Library (or the SAP Cryptographic Library) must be installed on all of the accepting system’s application servers.

You can obtain the most recent version of the SAP Security Library from the sapser<x> under /general/misc/security/SAPSECU/<platform>.

The SAP Cryptographic Library is available on the SAP Service Marketplace at http://service.sap.com/swcenter. Note however, the delivery of this library underlies German export regulations and is not available to all customers. For more information, see Using the Secure Sockets Layer Protocol [Page 6].

Procedure

On all of the accepting system’s application servers

1. Set the profile parameter login/accept_sso2_ticket = 1. Set
   login/create_sso2_ticket = 0 unless the server should also be able to issue tickets. (Use DEFAULT.PFL.)
2. For Releases 4.0 and 4.5, also set the profile parameter SAPSECULIB to the location (path and file name) of the SAP Security Library (or SAP Cryptographic Library).

On one of the accepting system’s application servers

1. Execute the SSO administration wizard (transaction SSO2).
   The SSO2 Administration screen appears.
2. Enter the RFC destination or the <host name> and <system number> for the issuing server in the appropriate fields.
   Note the following:

   ?? You must specify the destination host for the issuing server’s logical system, namely, the system ID and client.
   ?? If you do not enter a destination host in the SSO2 Administration screen, then the status for the local system is displayed.
   ?? If you enter the <host name> and <system number>, the system automatically creates a corresponding RFC destination to use for the connection.

The SSO administration report for the designated server is displayed.

The following information is shown in the report:

?? Profile parameter values on both the issuing server and on the accepting system’s application server.

?? The accepting system’s SSO access control list.

?? The accepting system’s certificate list.

Red traffic lights in any of these areas indicate configurations that are not operational for using logon tickets.
3. If the report indicates errors on the issuing server (for example, profile parameters are not set correctly), correct these errors on the issuing server and re-execute the SSO administration wizard on the accepting system.

4. To initiate the configuration steps on the accepting system, choose *Edit ? Activate Workplace* (↑).

   The following occurs:

   ?? The SSO administration wizard enters the issuing server’s system ID and client in the accepting system’s access control list.

   ?? If the issuing server’s public-key certificate is a self-signed certificate, then the SSO administration wizard enters the public-key information contained in the certificate in the accepting system’s certificate list.

   ?? The SSO administration wizard makes the SSO PSE available to the accepting system’s application servers:

   ?? In Releases >= 4.6C, the SSO administration wizard distributes the SSO PSE to all of the system’s application servers.

   ?? In Releases < 4.6C, it stores the SSO PSE in the directory specified by the profile parameter `DIR_PROFILE`.

   ![](Diagram)

   If the `DIR_PROFILE` directory is not globally accessible to all of the application servers in the accepting system, then you have to manually copy the SSO PSE to each application server’s `DIR_PROFILE` directory.

   All changes take place immediately and you do not have to explicitly save any data.

If any of the areas indicate errors, correct these errors and re-execute the SSO administration wizard.

You can also add or delete entries from the access control list or certificate list by placing the cursor on the appropriate line and choosing *Edit ? <function>.*

For example:

?? To add the issuing server’s system ID and client to the SSO access control list, place the cursor on the line `SAP System <Workplace_Server_SID> Client <client>` and choose *Edit ? Enter ACL*.

?? To delete an entry from the certificate list, place the cursor on the system ID and choose *Edit ? Delete from certificate list*.

?? To add the SAP CA certificate to the certificate list, choose *Edit ? Add SAP CA*.

You can also manually change the access control list (table TWPSSO2ACL) using the table maintenance transactions (for example, SM30).

You can also manually change the certificate list using the PSE maintenance transaction (PSEMAINT) or the trust manager (transaction STRUST).

The PSE maintenance transaction PSEMAINT is available for SAP Systems <= Release 4.6D and the trust manager (transaction STRUST) is available with the SAP Web Application Server.
Result

The accepting systems are able to accept logon tickets and verify the issuing server’s digital signature when they receive a logon ticket from a user.

You may execute the SSO administration wizard at any time and as often as you wish.

Protecting User Information

Logon tickets are used as authentication "tokens" and should therefore be protected from unauthorized use.

The measures we take for protection include:

?? Logon tickets are only sent to Web servers or SAP Web Application Servers that are located in the same DNS domain as the Web server that issued the ticket.

?? Logon tickets are stored in the Web browser’s main memory and are not written to disk. A user’s authentication information is therefore no longer available to services after the user closes his or her Web browser.

?? Logon tickets expire after a designated period of time as specified in the profile parameter login/ticket_expiration_time (default = 60 hours).

?? We encrypt the contents of the logon ticket to prevent it from being read by unauthorized persons. A cryptographic checksum also makes sure that any changes made to the ticket are detected.

The measures you should use include:

?? Use HTTPS to protect the communication paths.

?? Define a specific DNS domain where the ticket is to be used.

?? Your end users should protect access to their open Web browsers. In particular, they should activate password-protected screen savers.

Using X.509 Client Certificates

Use

An X.509 client certificate is a digital "identification card" for use in the Internet, also known as a public-key certificate.

A user who accesses the SAP Web Application Server and presents a valid certificate is authenticated on the server using the SSL protocol. The information contained in the certificate is passed to the server and the user is logged on to the server based on this information. User authentication takes place in the underlying protocols and no user ID and password entries are necessary.

Integration

Public-Key Infrastructure / Trust Center Services

Users need to receive their X.509 client certificates as part of a public-key infrastructure (PKI). The role of the PKI is to verify the identity of certificate owners and to issue, validate, renew, and revoke certificates. If you use X.509 client certificates for authentication, then you need access to a PKI. You can either establish your own PKI or you can rely on a Trust Center for these tasks.
Using SSL for Client Authentication

When using X.509 client certificates, users are authenticated on the SAP Web Application Server using the SSL protocol. Therefore, HTTPS connections are necessary for the communication between the users' Web browsers and the SAP Web Application Server.

Prerequisites

- Users possess valid X.509 client certificates and have imported them into their Web browsers.
- The SAP Web Application Server is configured to support HTTPS connections and SSL. (For more information, see Using the Secure Sockets Layer Protocol [Page 6].)
- The user's identification, the Distinguished Name, that is specified in his or her certificate must map to a valid user ID on the SAP Web Application Server.

Features

- Strong authentication is provided using the SSL protocol and PKI technology.
- Users can also produce digital signatures using the client certificates. There, higher levels of trust and non-repudiation for business transactions are also possible.
- Passwords are no longer used for authentication purposes.
- Users can also use their certificates for access to other intranet or Internet services.

Activities

1. The user accesses a service on the SAP Web Application Server.

   The corresponding URL must use HTTPS.

2. The SAP Web Application Server uses the SSL protocol to authenticate the user based on the information contained in the certificate.

3. If the authentication was successful, the server searches for a valid SAP System ID that corresponds to the user's Distinguished Name in the certificate.

Result

If the SSL authentication was successful and the user can be mapped to a SAP System user ID, then the user is logged on to the system. No user ID or password entries are necessary.

If however, the system cannot correctly map the user ID, or the SSL authentication failed, then the system checks for a logon ticket. If no ticket exists, then the system prompts the user for user ID and password using the HTTP basic authentication prompt.

Configuring the System for Using X.509 Client Certificates

Procedure

1. Configuring the SAP Web AS for Supporting SSL [Page 10].

2. Set the profile parameters snc/extid_login_diag = 1, snc/extid_login_rfc = 1

   icm/HTTPS/verify_client = 1 (accept certificates) or 2 (require certificates).

3. Restart the ICMan (using transaction SMICM).
4. Maintain the user mapping in table USREXTID.
   a. Enter the following information in the corresponding fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of external ID</td>
<td>DN</td>
<td>Enter in the Determine Work Area: Entry dialog.</td>
</tr>
<tr>
<td>Extern.ID</td>
<td>Distinguished Name as found in the user's certificate.</td>
<td></td>
</tr>
<tr>
<td>Serial no.</td>
<td>Serial number of the certificate: 000 is the default value.</td>
<td>Optional and not currently checked in the system.</td>
</tr>
<tr>
<td>User</td>
<td>SAP System user ID</td>
<td></td>
</tr>
<tr>
<td>Min. date</td>
<td>Earliest date on which the certificate is valid for logging on to the system. Optional and not currently checked in the system.</td>
<td></td>
</tr>
</tbody>
</table>

   b. Set the Activated indicator to activate the client certificate logon for the user.

   ![Tip]
   You may want to enter users' data in preparation for using certificates and activate them at a later time.

   c. Save the data.

**Result**

The SAP Web Application Server can accept X.509 client certificates as the authentication mechanism.
Terminology and Abbreviations

Certificate List [Page 49]
Certification Authority (CA) [Page 49]
Credentials [Page 49]
Logon Ticket [Page 50]
Personal Security Environment (PSE) [Page 50]
Private Key [Page 50]
Public Key [Page 51]
Public-Key Certificate [Page 51]
Public-Key Infrastructure (PKI) [Page 52]
Public-Key Technology [Page 52]
SAP Cryptographic Library (SAPCRYPTOLIB) [Page 52]
SAP Security Library (SAPSECULIB) [Page 53]
Secure Sockets Layer (SSL) Protocol [Page 53]
Secure Store & Forward (SSF) [Page 54]
SSO Personal Security Environment (SSO PSE) [Page 54]
System PSE [Page 55]
Verification PSE [Page 55]

Certificate List

Definition
A list that contains other users' or system components' public-key certificates.

Use
The certificate list is stored in the user's or system component's own Personal Security Environment (PSE) and is used to verify other user's or component's digital signatures.

Certification Authority (CA)

A third-party instance that issues public-key certificates. The role of the CA is to guarantee the identity of the certificate owner.

Credentials

User or component-specific information that allows the user or component to access his or her security information.

The credentials may be located, for example, in a protected file in the file system. They often have a limited life span. For example, the credential file for a user may be created when the user logs on to a security product and deleted when he or she logs off.
Logon Ticket

Definition
The logon ticket is a piece of information used as an authentication token for access to SAP (or non-SAP) systems.

Use
The logon ticket is issued to a user when he or she logs on to the issuing server in the system landscape. It is then sent to the accepting systems when the user accesses the various services. The accepting systems verify the validity of the logon ticket before allowing the user access to the system’s services.

Before the issuing server creates a logon ticket for a user, the user must provide his or her authentication information (that is, user ID and password). Afterwards, the logon ticket is used to allow the access to the various systems and no further user ID and password entries are necessary.

Structure
The logon ticket contains the following information:

?? Version
?? Expiration time
  The logon ticket is only available for a designated length of time (default = 60 hours). You can define the expiration period for the ticket in the parameter login/ticket_expiration_time.
  (See SAP Note 337794 for information about how to set the expiration time in minutes.)

?? User ID
?? Identifier for the issuing server
?? Issuing server's public-key certificate (optional)
?? Issuing server's digital signature
  The issuing server's digital signature is verified by the accepting system when the user accesses the corresponding service. The digital signature guarantees that the issuing server issued the logon ticket to the user and that the contents have not been changed.

Personal Security Environment (PSE)
Secure location where a user or component's public-key information is stored. The PSE for a user or component is typically located in a protected directory in the file system or on a smart card. It contains both the public information (public-key certificate and certificate list) as well as the private information (private key) for its owner. Therefore, only the owner of the information should be able to access his or her PSE.
**Private Key**

**Definition**
Private part of the key pair used for encryption or for digital signatures.

**Use**
The other part of the key pair is the public key. A piece of information encrypted with the private key can only be decrypted with the corresponding public key (and vice versa). A digital signature is created using the private key, and can therefore only be verified by using the signer's public key.

**Public Key**

**Definition**
Public part of the key pair used for encryption or for digital signatures.

**Use**
The other part of the public-key pair is the private key. A piece of information encrypted with the public key can only be decrypted with the corresponding private key (and vice versa). A digital signature is created using the private key, and can therefore only be verified by using the signer's public key.

**Public-Key Certificate**

**Definition**
A digital document that acts as a user's digital identification card.

The public-key certificate (also known as an X.509 client certificate) is based on the X.509 format, which is an Internet standard developed by the International Telecommunication Union (ITU). For more information, see the ITU at [http://www.itu.int](http://www.itu.int).

**Use**
Public-key certificates contain the public part of a user's public-key information and are used for authentication purposes and for verifying digital signatures. A Certification Authority (CA) guarantees the certificate owner's identity and approves or issues the certificate to the user.

Specifically, you use public-key certificates as follows:

?? You use your own certificate to identify yourself to others.

?? You use someone else's certificate to verify his or her digital signatures.

?? You can use a certificate to encrypt a message meant for the certificate's owner.

For more information, see [Public-Key Technology [SAP Library]](http://www.itu.int).
**Public-Key Infrastructure (PKI)**

**Definition**
A system that manages the trust relationships involved with using public-key technology.

**Use**
The role of the PKI is to make sure that public-key certificates and Certification Authorities (CAs) can be validated and trusted. The collection of services and components involved with establishing and maintaining these trust relationships is known as the PKI.

**Public-Key Technology**
Technology used for securing digital documents.

Public-key technology uses key pairs to provide its protection. Each participant receives an individual key pair consisting of a public key and a private key. These keys have the following characteristics:

- The keys are pairs; they belong together.
- You cannot obtain the private key from the public key.
- As the name suggests, the public key is to be made public. The owner of the keys distributes the public key as necessary. For example, a recipient of a digitally signed document needs to have knowledge of the signer’s public key in order to verify the digital signature. In addition, to send an encrypted document, the sender needs to know the recipient’s public key.
- The private key is to be kept secret. The owner of the keys uses the private key to generate his or her digital signature and to decrypt messages encrypted with his or her public-key. Therefore, the owner of the keys needs to make sure that no unauthorized person has access to his or her private key.

For more information, see [Public-Key Technology [SAP Library]](https://saplibrary).

**SAP Cryptographic Library (SAPCRYPTOLIB)**

**Definition**
Default security product provided by SAP to use for encryption with SAP Systems.

**Use**
The SAP Cryptographic Library not only supports the use of digital signatures in SAP Systems, but also provides encryption functions. You can use it for example, as the security provider for Secure Network Communications (SNC) or for SSL support with the SAP Web Application Server.

**Integration**
The SAP Cryptographic Library is available for download on the SAP Service Marketplace. However, because the library includes encryption functions, its delivery underlies German export regulations. If you are not authorized to receive the library, then you are not offered it from the download site.

In addition, you must adhere to any import regulations that apply.
**SAP Security Library (SAPSECULIB)**

**Definition**
Default security provider provided with SAP Systems.

**Use**
The SAP Security Library is a dynamic link library that is located on each application server. The library provides the functions for using digital signatures in SAP Systems, but does not support functions for using encryption.

**Secure Sockets Layer (SSL) Protocol**
The Secure Sockets Layer (SSL) protocol is an Internet standard developed by Netscape that is used to secure communications across the Internet.

The SSL protocol layer exists between the network-layer protocol (for example, TCP/IP) and the application layer protocol (for example, HTTP). The protocol uses public-key technology [Page 52] to secure the communication between a client and server.

The SSL protocol provides for the following:

?? **Encrypted connections**
SSL is used to encrypt connections between the client and server. The SSL encryption protects the data from potential eavesdroppers, providing a higher degree of privacy for the communications. The data is also protected from manipulation – any changes made to the data during transfer are detected.

?? **SSL server authentication**
SSL server authentication is used to verify a server's identity. A user may want to verify the identity of a server to which he or she is sending personal information, for example, credit card information.

?? **SSL client authentication**
SSL client authentication allows a server to verify a user's identity. A company may want to verify the identity of the client-side communication partner for access control purposes.

?? **SSL mutual authentication**
SSL mutual authentication is used to verify both the client and server's identity. Both communication partners may want to have identities verified, for example, when high-value contracts are being closed.

To access Internet addresses that use SSL connections, you use URLs starting with https: instead of http:

**See also:**

Secure Store & Forward (SSF)

Interface for secure data storage and transmission that allows the SAP System to communicate with an external security product. In this way, digital signatures and encryption can be used by the SAP System to protect data and documents as independent units when they are saved or transmitted over communication paths.

SSO Personal Security Environment (SSO PSE)

Definition

The Personal Security Environment (PSE) used for Single Sign-On when using logon tickets for user authentication.

Use

The issuing server uses the information contained in its SSO PSE to digitally sign users’ logon tickets.

The accepting systems use the information contained in their SSO PSEs to verify the issuing server’s digital signature when users present their logon tickets for access to the systems.

Structure

The SSO PSE contains the security information needed to create or verify the issuing server's digital signature.

On the issuing server, this information includes:

?? The server’s public-key certificate
?? The server’s private key

On the accepting systems, this information includes:

?? The issuing server’s public-key certificate
?? The accepting system’s certificate list

Integration

Each application server in a system that issues or accepts logon tickets needs access to the SSO PSE. Depending the system’s release, the location of the SSO PSE is determined as shown in the table below.

Location of SSO PSEs

<table>
<thead>
<tr>
<th>Server</th>
<th>Release</th>
<th>Name</th>
<th>Location</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accepting servers</td>
<td>&lt; 4.6C</td>
<td>SAPSSO2.pse</td>
<td>Directory specified in the profile parameter DIR_PROFILE</td>
<td>In this case, the SSO PSE is the system PSE [Page 55].</td>
</tr>
<tr>
<td>Issuing or accepting servers</td>
<td>&gt;= 4.6C</td>
<td>SAPSYS.pse</td>
<td>&lt;instance directory&gt;/sec</td>
<td></td>
</tr>
</tbody>
</table>

In this case, the SSO PSE is the system PSE [Page 55].
**System PSE**

An SAP System’s Personal Security Environment (PSE) that contains the system’s security information (for example, the public and private key pair).

The system PSE is automatically created during the system’s installation process. In Release 4.5A systems, each application server receives its own system PSE. For systems as of Release 4.5B, the system creates a single system PSE and distributes it to all of the system’s application servers.

---

**Verification PSE**

**Definition**

PSE (Personal Security Environment) used to verify a signer's digital signature.

**Use**

The verification PSE can only be used to verify a signer's digital signature. It cannot be used to create a digital signature. It contains the public-key certificates of the signer's key pair, but not the private key.