Copyright

© Copyright 2001 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®, OS/2®, DB2/6000®, Parallel Sysplex®, MVS/ESA®, RS/6000®, AIX®, S/390®, AS/400®, OS/390®, and OS/400® are registered trademarks of IBM Corporation.

ORACLE® is a registered trademark of ORACLE Corporation.

INFORMIX®-OnLine for SAP and Informix® Dynamic Server™ are registered trademarks of Informix Software Incorporated.

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

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, ABAP, SAP ArchiveLink, SAP Business Workflow, WebFlow, SAP EarlyWatch, BAPI, SAPPHIRE, Management Cockpit, mySAP.com Logo and mySAP.com are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other products mentioned are trademarks or registered trademarks of their respective companies.
## Icons

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

### SAP Web Application Server Security

- Using the Secure Sockets Layer Protocol ......................................................... 6
- The Application Server's Personal Security Environments .................................. 7
  - The SSL Server PSE .......................................................................................... 8
  - The SSL Client PSE .......................................................................................... 8
- Installing the SAP Cryptographic Library (SAP Web Application Server) ............. 9
- Configuring the SAP Web Application Server for Supporting SSL .................... 11
  - Generating SSL Server PSEs ........................................................................... 12
  - Generating Certificate Requests for the SSL Server PSEs ................................. 13
  - Sending the Certificate Requests to a CA ......................................................... 14
  - Importing the Certificate Request Response ..................................................... 15
  - Maintaining the SSL Server PSE's Certificate List ............................................. 15
  - Generating and Maintaining SSL Client PSEs .................................................. 17
- User Authentication .............................................................................................. 18
  - Configuring the System for Issuing Logon Tickets ........................................... 19
  - Obtaining a Certificate Signed by the SAP CA ................................................. 20
  - Using a Self-Signed Certificate ........................................................................ 21
  - Changing from a Self-Signed Certificate to a Certificate Signed by the SAP CA 21
  - Configuring the System for Accepting Logon Tickets ...................................... 22
  - Protecting User Information ............................................................................ 25
- Configuring the System for Using X.509 Client Certificates ................................ 27
- Terminology and Abbreviations .......................................................................... 28
  - Certificate List .................................................................................................. 28
  - Certificate Store ................................................................................................ 28
  - Certification Authority (CA) ............................................................................. 29
  - Credentials ......................................................................................................... 29
  - Logon Ticket ...................................................................................................... 29
  - Personal Security Environment (PSE) ............................................................... 30
  - Private Key ......................................................................................................... 30
  - Public Key .......................................................................................................... 30
  - Public-Key Certificate ....................................................................................... 30
  - Public-Key Infrastructure (PKI) ....................................................................... 31
  - Public-Key Technology ..................................................................................... 31
  - SAP Cryptographic Library (SAPCRYPTOLIB) ............................................... 31
  - SAP Security Library (SAPSECULIB) ................................................................. 32
  - Secure Sockets Layer (SSL) Protocol ............................................................... 32
Secure Store & Forward (SSF) ...................................................................................................... 33
SSO Personal Security Environment (SSO PSE)............................................................................ 33
System PSE ................................................................................................................................... 34
Verification PSE ............................................................................................................................. 34
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](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 SAP Cryptographic Library performs the SSL cryptographic functions and is therefore subject to and controlled by German export regulations. It is not available to all customers. If you are authorized to receive the library, then you will be offered the SAP Cryptographic Library node at the download site. (See Installing the SAP Cryptographic Library [Page 9].)
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.

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

- Public-Key Technology [SAP Library]
- Terminology and Abbreviations [Page 27]
- 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 the application server’s role in the communication, the server possesses two separate SSL PSEs:

- **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, a user accesses the SAP Web Application Server using a Web browser.

- **The SSL Client PSE**
  The SAP Web Application Server uses this PSE when the application server is the client component for the communication. For example, the application server itself accesses a different Web server.

These PSEs are described in more detail in the topics that follow.
The SSL Server PSE

Definition
The application server's PSE for securing communications using the SSL protocol when the application server is the server component for the communication.

Use
The SAP Web Application Server uses the SSL server PSE for establishing secure HTTP connections using the SSL protocol (HTTPS connections) when the application server is the server component for the connection.

If the SAP Web Application Server also communicates as a client component, then it uses the SSL client PSE to establish the HTTPS connection.

Structure
This PSE contains the application server's security information including its key pair and its 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
To install the SSL server PSE, you must initiate the PSE generation. The system then creates a default, system-wide PSE, which it distributes to all remaining application servers. Alternatively, you may use individual PSE's for single application servers.

The path and file name for the SSL server PSE is <instance_directory>/sec/SAPSSLS.pse, where the <instance_directory> is the directory specified by the profile parameter DIR_INSTANCE.

The SSL Client PSE

Definition
The application server's PSE for securing communications using the SSL protocol when the application server is the client component for the communication.

Use
The SAP Web Application Server uses the SSL client PSE for authenticating the system as the client component when secure HTTP connections using the SSL protocol (HTTPS connections) are used.

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

Structure
This PSE contains the application server's security information including its key pair and certificate list. The SSL client PSE's certificate list can be less restrictive than that is the SSL server PSE and may contain a larger number of CA certificates.

Integration
To install the SSL client PSE, you must initiate the PSE generation. The system then creates a single PSE for the system that is distributed to all of the application servers. The path and file name for the SSL client PSE is <instance_directory>/sec/SAPSSLc.pse, where the <instance_directory> is the directory specified by the profile parameter DIR_INSTANCE.
Installing the SAP Cryptographic Library (SAP Web Application Server)

Use

The cryptographic functions needed to use the SSL protocol are performed by the SAP Cryptographic Library, which is available for download at http://service.sap.com/swcenter. The library's 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.

The configuration tool is not necessary for the configuration of SSL on the SAP Web Application Server. You only need it to generate key pairs and PSEs to use for Secure Network Communications (SNC).

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.

Procedure

As user <sid>adm:

1. Copy the library file 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).

   **Example values for DIR_EXECUTABLE**

   - UNIX: /usr.sap/<SID>/SYS/exe/run
   - Windows NT: <DRIVE>:\usr\sap<SID>\SYS\exe\run

2. Copy the configuration tool sapgenpse.exe to any local directory, for example, also $(DIR_EXECUTABLE).

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 application server's instance directory $(DIR_INSTANCE):

   **Examples**

   - UNIX: /usr/sap/<SID>/<instance>/sec/ticket
   - Windows NT: <DRIVE>:\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 application server's processes. Therefore, we recommend setting SECUDIR in the login profile for the application server's user.

6. Set the profile parameters in the application server's instance profile as shown in the table below. If you used the recommended directory DIR_EXECUTABLE (see above), 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

<table>
<thead>
<tr>
<th>Profile Parameters</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.

7. Restart the application server.

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.
Configuring the SAP Web Application Server for Supporting SSL

Prerequisites

- The SAP Cryptographic Library must be installed in the $(DIR_EXECUTABLE) directory. (See Installing the SAP Cryptographic Library [Page 9].)

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.

- The following profile parameters must be defined in the application server's instance profile. These parameters are normally set during the installation, however, you may want to adjust their default values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>icm/plugin_&lt;xx&gt;</code></td>
<td>PROT=HTTPS, PLG=$(DIR_EXECUTABLE)/httpplugin.so</td>
</tr>
<tr>
<td><code>icm/server_port_&lt;xx&gt;</code></td>
<td>HTTPS port</td>
</tr>
<tr>
<td><code>icm/HTTPS/verify_client</code></td>
<td>0: Do not use certificates</td>
</tr>
<tr>
<td></td>
<td>1: Allow certificates (default)</td>
</tr>
<tr>
<td></td>
<td>2: Require certificates</td>
</tr>
</tbody>
</table>

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.

If you make changes to any of the `icm` profile parameters, then restart the ICManager.

**Example Parameters:**

- `icm/plugin_2` PROT=HTTPS, PLG=$(DIR_EXECUTABLE)/httpplugin.so
- `icm/server_port_2` PROT=HTTPS, PORT=443, TIMEOUT=15
- `icm/HTTPS/verify_client` 1

Procedure

Using the trust manager (transaction STRUST):

1. Generate SSL server PSEs [Page 12].
2. Generate a certificate request for each SSL server PSE [Page 13].
3. Send the certificate requests to a CA to be signed [Page 13].
4. Import the certificate request responses into the server's SSL server PSEs [Page 14].
5. Maintain the SSL server PSE's certificate list [Page 15].
6. Generate and maintain SSL client PSEs. [Page 17]
Generating SSL Server PSEs

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 CN part of the Distinguished Name.

Prerequisites
You know the naming convention to use for the server's Distinguished Name. The syntax of the Distinguished Name depends on the Certification Authority you use. If you use the SAP CA, the naming convention is CN=<host_name>, OU=I<installation_number>-<company_name>, OU=SAP Web Application Server, O=SAP Trust Community, C=DE. These components are needed for the Distinguished Name entries below.

Procedure
From the Trust Manager screen:
1. Select the SSL Server PSE node.
2. Using the context menu, choose Generate (if no PSE exists) or Replace.
   The <Generate/Change> PSE dialog appears.
3. Enter the Distinguished Name components in the corresponding fields. For example:
   - Name = <host_name>
   - Org. (opt.) = Test
   - Company = MyCompany
   - Country = US

   If you use the SAP CA, see the SAP Web AS certificate request area on the SAP Service Marketplace at http://service.sap.com/ssltest for information about how to determine the server's Distinguished Name.

   If a reference to a CA is active, then elements contained in the CA reference 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 Certification Authority (CA).

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

4. Select those servers that should receive an individual PSE by activating the checkbox in the Create column. These servers receive the Distinguished Name as shown in the Distinguished Name column. You can modify these Distinguished Names.

The other application servers receive the Distinguished Name as shown in the Default PSE DN field.

Initially, those application servers whose host names could be determined are automatically selected. If a server has not been automatically selected, then an error has occurred (for example, the ICMan has not been installed on the server). Select any of these servers manually, as necessary.

5. Choose Enter.

You return to the Trust Manager screen.

6. Restart the ICMan (using transaction SMICM)

Result

The SSL server PSEs are generated and distributed to the individual application servers.

Generating Certificate Requests for the SSL Server PSEs

Use

You must create 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 certificate field. For each application server with a unique Distinguished Name, you must generate a certificate request.

Procedure

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.
   b. Choose Edit → Generate certificate request.
      The Save dialog appears.
   c. Save the certificate request to a file (<file_name>.P10).

Result

Each certificate request is stored as a file in the file system.
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.

You may send the request to the SAP CA or you can use a different CA. However, note that the CA must provide a signed certificate that adheres to the PKCS#7 certificate chain format. For example, you can request an SSL Chained CA Cert or PKCS#7 cert chain format from the Thawte CA at www.thawte.com.

The SAP CA is not automatically recognized as a trusted CA in the standard Web browsers. Therefore, if you use the SAP CA as the issuing CA, then your users will receive a dialog when they first access the SAP Web Application Server. The dialog asks them whether or not they want to trust the SAP CA. To avoid this dialog for future accesses, they must install the SAP CA's root certificate in their Web browser.

Procedure

1. Make sure the contents of the certificate request 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 (for example, Notepad) and repair any line feeds or carriage returns as necessary.

   The example below shows a correct certificate request.

   Example certificate request:

   -----BEGIN CERTIFICATE REQUEST-----
   MIIBkzCCAVICAQAwWjELMAkGA1UEBhMCREUxHDAaBgNVBAoTE215U0FQLmNvbSAwXzA7BgNVBAsTBlNBUCBBRzEOwGA1UECxMFQmFzaXMxDDAKBgNVBAMTA0JJTzCB7jCBpgYFKw4DAhswgZwCQQCSnauC/cAfQVrmOtWznQ9I+i4twOp8wCE0Fk5EAVjQnX2oMgBnvci+ee/ZH2cLwyhp5mOOW70+exS7PHEWK1F
   AhUAw9FSY1AsFV4U9fc9w+Bg5H4ISYcCQARcC+7q3UkM0TF0A5rzRaq7viO3Wj2
   MwYUNwFkc0xmlboUQd2lmegZADoFiiisdzkn/nF4eIxV9vq9XxcV63xTsDQwAC
   QFher18UA8YkY4/zHe4mbupExVDScum2nbJuQ5PgDBvVaMntpxIissyzuAFL+qC
   zQ92mNqUR9JLWpz09ghQdIScGdAJSBcgkhjO0AQDAzAAMC0FCA7qEluP/Kf1
   +6HF/8I7j4NfF44xAhUAqkDgAeR3tznNegKUTQ+JzeCXawE=
   -----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/ssltest.

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 server’s SSL server PSE.

For each application server that uses a server-specific SSL server PSE, you must import the corresponding certificate request response into the server's SSL server PSEs. For those servers that use a system-wide SSL server PSE, you only need to import the certificate request response into one of the SSL server PSEs.

Procedure
1. Save the certificate request response to a file in the file system.
2. Start the trust manager (transaction STRUST).
3. Expand the SSL server PSE node.
4. 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. Choose Edit → Import certificate request response.
   c. Select the certificate request response from the file system and choose Open.
      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 in the trust manager.
5. 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 and 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 26].

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 saved to the PSE and distributed to the other application servers after saving the data.
Prerequisites
You must have access to the CA's public-key certificate (also known as 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 a file in the file system). 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 a CA’s Public-Key Certificate that is Located in the File System
   The Import Certificate dialog appears.
2. Enter the corresponding file name from the file system.
3. Select the DER option.
4. Choose Enter.
   The certificate appears in the certificate maintenance section (lower right).
5. Choose Edit → Add certificate to certificate store.
   The certificate is added to the certificate list in the PSE maintenance section (upper right).
6. Save the data.

Importing a CA’s Public-Key Certificate that 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.
4. Choose Edit → Add certificate to certificate store.
   The certificate is added to the certificate list in the PSE maintenance section.
5. Save the data.

Importing the SAP CA’s Root Certificate
   The SAP CA's certificate appears in the certificate maintenance section.
2. Choose Edit → Add certificate to certificate store.
   The certificate is added to the certificate list 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 certificate belonging to the CAs that the server trusts.
Generating and Maintaining SSL Client PSEs

Use
Repeat the procedure for the SSL client PSEs if the SAP Web Application Server is to communicate as a client component for HTTPS connections.

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

Using the trust manager (transaction STRUST):
1. **Generate an SSL client PSE [Page 12].**
   
   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 SSL client PSE [Page 13].**
   
   Because the SSL client PSE is system-specific and not server-specific, you only need to create a single certificate request and import it on one application server.

3. **Send the certificate request to a CA to be signed [Page 13].**
4. **Import the certificate request response into the server's SSL client PSE [Page 14].**
5. **Maintain the SSL client PSE’s certificate list [Page 15].**

   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 where the SAP Web Application Server is the client component in the communication.
User Authentication

Using Logon Tickets

Use
For authentication on the SAP Web Application Server 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 Application 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 Application Server) 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 Application Server. Note however, depending on the scenario you use, other server components may act as the issuer or acceptor, for example, a Workplace Server used in a mySAP Workplace solution.

Receiving a Logon Ticket from the SAP Web Application Server
1. The user authenticates him or herself on the SAP Web Application Server (for example, using user ID and password).
2. The SAP Web Application Server verifies the user's information. If the authentication was successful, then a ticket is issued to the user that is stored in the user's Web browser and the user is logged on to the server.
Using the Logon Ticket to Access an Accepting System

When the user accesses an accepting system:

1. The Web browser sends the user's logon ticket with the access request.
2. The SAP Web Application Server 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 33]). For the SAP Web Application Server, the SSO PSE is the system PSE [Page 34].

   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 20]
   - Using a Self-Signed Certificate [Page 21]

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></td>
<td>1: If the server's certificate is to be included in the logon ticket.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2: If the server's certificate is not to be included.</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. Generate a new system PSE (see Generating a PSE [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-----
MIIBkzCCAVICAQAwjELMAkGA1UEBhMCREUxHDAaBgNVBAoTE215U0FQLmNvbSBXb3JrcGxhY2UxDzANBgNVBAsTBlNBUCBBRhzEMAwGAEwIMAwGA1UECxMFQmFzaXMxDDAKBgNVBAMTA0JJTzCB7jCBpgYFKw4DAhswgZwCQQCSnauC/cAfQVzmOtWznQ9I+i4towoP9we0Fk5EAvJqNzGmQnBoyi+ee/ZH2cLwyhp5mOw70+exS7FHEWKhIFAhUaW9SY1AsEV4U9fc9w+Bg5H4ISyCQARCC+C7q3UKM0TF0A5zRaq7viONJj2MwYUNwFkscOhxzhloUQd21megZADcFlisdzn/nF4eIvx9vq9XsV65xTsDQwACQFher18U8a8YvY4/zHe4mbufEXxDSucm2nbJuQ5PfgDBvVamMtpXIiszyuAFLqCz92mkmNcURJLMP09ghQuDSgADAJbqchkJCOAQDAsZAMC0CFA7qEiup/Kfi+6HF/8I7j4NF44xAhUAqkDgeEr3tzmNegKUTQ+JzeCXawE=
----END CERTIFICATE REQUEST-----
4. 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 20].
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 22].
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 33] for the file name and location of the SSO PSE according to release.

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 sapserv<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 export regulations and may not be available to all customers. For more information, see Installing the SAP Cryptographic Library [Page 9].

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 SAPSEULIB 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`.

   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 an 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](#).
- 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. Configure the SAP Web Application Server for using SSL [Page 11]. In this case, the server must possess an SSL server PSE, but not necessarily an SSL client PSE.

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.</td>
<td>Optional and not currently checked in the system.</td>
</tr>
</tbody>
</table>

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

   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 28]
Certificate Store [Page 28]
Certification Authority (CA) [Page 29]
Credentials [Page 29]
Logon Ticket [Page 29]
Personal Security Environment (PSE) [Page 30]
Private Key [Page 30]
Public Key [Page 30]
Public-Key Certificate [Page 30]
Public-Key Infrastructure (PKI) [Page 31]
Public-Key Technology [Page 31]
SAP Cryptographic Library (SAPCRYPTOLIB) [Page 31]
SAP Security Library (SAPSECULIB) [Page 32]
Secure Sockets Layer (SSL) Protocol [Page 32]
Secure Store & Forward (SSF) [Page 33]
SSO Personal Security Environment (SSO PSE) [Page 33]
System PSE [Page 34]
Verification PSE [Page 34]

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.

Example
When using logon tickets for Single Sign-On in the mySAP Workplace, the Workplace Server issues each user his or her logon ticket and secures it with its digital signature. To be able to verify the Workplace Server's digital signature to allow user access to a component system, the component system needs access to the Workplace Server's public-key. The Workplace Server can either send its public-key certificate with the user's logon ticket or the public-key information needs to be saved in the component server's certificate list.

Certificate Store

Definition
Location in the database where you can store certificates belonging to Certification Authorities (CAs).

Use
You can then import the certificates from the system's certificate store into the Personal Security Environments (PSEs) to be used as trusted CAs.
**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.

**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].
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][1] [SAP Library].

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 31] 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 on 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 34].</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>
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.

Example
When using logon tickets for SSO in the mySAP Workplace, the Workplace Server digitally signs the user's logon ticket when the user logs on to the Workplace. The Workplace component systems then use the Workplace server's verification PSE to verify the Workplace server's digital signature contained in the user's logon ticket to allow the user access to the system.