Single Sign-On in the mySAP.com Workplace

MYSAP.WP_SEC

Release 2.11

Copyright

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax
	Tip

Contents

Single Sign-On in the mySAP.com Workplace

The mySAP.com Workplace provides an intranet portal that gives users access to a variety of services and information. These services and information may actually be provided by a number of different systems (SAP or others) with different user management policies.

Therefore, one of the primary usability features we offer with the Workplace is a Single Sign-On (SSO) environment. With SSO in the Workplace, users can move around within their Workplace without having to repeatedly enter their user information for authentication, even as they access different systems.

The SSO environment in the mySAP.com Workplace is available in the following variants:

- **Single Sign-On based on user ID and password**

  With this variant, users enter their mySAP.com Workplace and authenticate themselves on the mySAP.com Workplace Server using their SAP System user ID and password. Once they are successfully authenticated, they are logged onto the mySAP.com Workplace and receive their personal menus. As they access the different services and systems provided in the Workplace, they do not have to continually enter their user ID and password to authenticate themselves.

  This variant is available using either SSO cookies [Page 71] or mySAP.com logon tickets [Page 68]. mySAP.com logon tickets improve security and eliminate some of the restrictions placed on SSO cookies (for example, that a user's password needs to be the same in all systems).

- **Single Sign-On using X.509 client certificates**

  A user who enters the Workplace and presents a valid X.509 client certificate [Page 73] is authenticated on the Workplace's Web server using the Secure Sockets Layer (SSL) [Page 70] protocol. The user's client certificate is passed on to the Workplace Server and provides the information necessary to log the user on to the Workplace. As the user accesses the different services within the Workplace, his or her certificate is passed to the corresponding system and he or she is logged on to the component system. User authentication takes place in the underlying protocols and no user ID and password entries are necessary.

  The SSO environment makes it easier for users to access the different services and sources of information available in the mySAP.com Workplace. If however, you choose not to configure your Workplace system for using SSO, users are prompted for user ID and password entries as they access the various services.

See the following topics:

- Deciding Which SSO Version to Use [Page 7]
- Single Sign-On Based on User ID and Password [Page 10]
- Single Sign-On Using X.509 Client Certificates [Page 47]

Deciding Which SSO Version to Use

The optimal SSO version for you to use depends greatly on your existing system infrastructure and your security requirements. If you want to integrate component systems with earlier releases (for example, R/3 Release 3.1 systems), then you need to use Single Sign-On based on user ID and password. However, if you have higher security requirements, you can use X.509 client certificates.

The table below should help when deciding which SSO version to use.

Comparing SSO Variants

With Regard To...	SSO Cookie	mySAP.com Logon Tickets	X.509 Client Certificates
Security	- **Minimal security** Frontend components need access to the decrypting and verification routines, making the SSO cookie more susceptible to misuse.	+ **Increased security** Increased security level because the decrypting and verification processes take place in the mySAP.com kernel modules.	++ **Optimal security** Provides an even higher security level because passwords are also no longer used for authentication. User authentication takes place using the SSL protocol.
Integration with existing Infrastructure	+ **Easy to integrate** Existing systems (for example, Release 3.1 or 4.0 systems) can be integrated into the mySAP.com Workplace without modification.	+ - **Possible with kernel patches** Kernel patches are necessary before integrating systems that are older than Release 4.6C. (See SAP Note 177895.)	- **Release restrictions** Component systems must be Release 4.5B or higher.
Administration Costs	+ **Minimal administration and configuration costs**	- **Increased administration and configuration costs**	- **Increased administration and configuration costs** A public-key infrastructure (PKI) [Page 69] must be established and certificates distributed.
		+ **Automation support** The SSO administration wizard [Page 23] automates the tasks involved.	+ **Automation support** Services are also available to automate these tasks.
	- **Password synchronization is necessary** Increased administration costs due to password synchronization	+ **Password synchronization is no longer necessary**	+ **Password synchronization is no longer necessary**

With Regard To...	SSO Cookie	mySAP.com Logon Tickets	X.509 Client Certificates
Integration with non-mySAP.com Components	- **Not possible**	+ **Possible** The verification routines are available to non-mySAP.com components in a library.	+ **Possible** Possible for systems that support X.509 client certificates and the SSL protocol.

See also:

- Using SSO Variants Concurrently [Page 9]
- Single Sign-On Based on User ID and Password [Page 10]
  - Using SSO Cookies [Page 11]
  - Using mySAP.com Logon Tickets [Page 18]
  - Upgrading from SSO Cookies to mySAP.com Logon Tickets [Page 42]
- Single Sign-On Using X.509 Client Certificates [Page 47]

Using SSO Variants Concurrently

Using SSO Cookies and mySAP.com Logon Tickets Concurrently

You may concurrently use both SSO cookies and mySAP.com logon tickets for SSO. For example, you may want to use mySAP.com logon tickets for your Release 4.6C+ component systems and the SSO cookie for older systems that have not yet had the necessary kernel patches applied.

For this scenario, configure your Workplace Server to create both SSO cookies and mySAP.com logon tickets. When the Workplace user logs on to the Workplace, the system creates both an SSO cookie and a logon ticket for the user. When the user accesses a component system, both the SSO cookie and the ticket are sent to the component system and the system determines which one to use as the user authentication token. (mySAP.com logon tickets have precedence over SSO cookies.)

If you do configure your system to use both versions simultaneously, we recommend disabling the SSO cookies as soon as feasible. This eliminates the continuous transfer of two separate user authentication tokens when a user accesses component systems.

Using X.509 Client Certificates and Either SSO Cookies or mySAP.com Logon Tickets Concurrently

You may want to use both X.509 client certificates and either SSO cookies or mySAP.com logon tickets simultaneously. For example, you may want to issue certificates to a small group of users to use during a test or pilot phase. Although you can set up your installation to use the variants simultaneously, we recommend you set up a separate Workplace installation for the users that use certificates. The same component systems may be integrated into the different Workplace installations. You can thereby introduce certificates to your users in phases without mixing the authentication mechanisms.

Although you can configure your mySAP.com Workplace to support both certificates and mySAP.com logon tickets, a single user cannot use both methods simultaneously.

When a user logs on to the mySAP.com Workplace using a client certificate for authentication, then he or she must also be able to use it to log on to the component systems. He or she does not also receive an SSO cookie or a mySAP.com logon ticket. Therefore, if you have component systems that do not support the X.509 client certificate as an authentication token, then you have to rely on password-based Single Sign-On.

Single Sign-On Based on User ID and Password

Use

Single Sign-On in the Workplace based on user ID and password takes advantage of the existing SAP System user authentication mechanism. When using this variant, users enter the mySAP.com Workplace and authenticate themselves on the Workplace Server using their user ID and password. Once they are successfully authenticated, they are logged onto their individual Workplaces and receive their personal menus. As they access the different services and systems provided in the Workplace, they do not have to continually enter their user ID and password to authenticate themselves.

Integration

To establish the SSO environment, the Workplace Server provides the user's authentication information using an authentication "token", which is passed to the Workplace component systems. The user authentication token is provided in two versions:

- SSO cookies (available with all Workplace releases)
- mySAP.com logon tickets (available as of Workplace Release 2.10)

Note the following:

- The mySAP.com logon ticket or SSO cookie is only available for authentication while the user is logged on to the mySAP.com Workplace. When the user logs off of the Workplace or closes the Web browser, the user authentication information is no longer available to the Workplace services. He or she must re-authenticate themselves when they re-enter the Workplace.
- The mySAP.com logon ticket or SSO cookie expires after a designated period of time (default = 60 hours). If it expires during a session, the user has to re-authenticate him or herself on the Workplace Server.
- For security reasons and to make administration easier, we also recommend configuring all of your Workplace Web servers homogeneously for using HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer).

See:

- Using SSO Cookies [Page 11]
- Using mySAP.com Logon Tickets [Page 18]

Using SSO Cookies

Use

You have to use SSO cookies as the authentication mechanism for Single Sign-On in the mySAP.com Workplace Releases 1.00 and 2.00. As of Release 2.10, you can also use it instead of the mySAP.com logon tickets. You may wish to use SSO cookies in later releases if your administration or infrastructure deems it necessary. For example:

- You have Workplace component systems that are older than Release 4.6C and you have not yet applied the necessary patches.
- You have not yet performed the administrative tasks necessary for using mySAP.com logon tickets. (For more information, see Configuring the mySAP.com Workplace for Using Logon Tickets [Page 26].)

  If you use SSO cookies, we recommend upgrading to logon tickets as soon as it is feasible.

Prerequisites

- Users need to have the **same user ID and password** for all of the Workplace component systems they access using SSO.

  If the user accesses a system in the Workplace where his or her user ID or password is different than that on the Workplace Server, then the user is prompted for his or her user ID and password for that system.
- End users need to configure their Web browsers to accept cookies.

  In Internet Explorer 5.0, accept *session cookies* for the *local intranet zone*.
- The Web servers for the Workplace Server as well as those used for the Workplace component systems must all be located in the same DNS domain.

  The SSO cookie or mySAP.com logon ticket is only available for user authentication to services whose Web servers are defined in the same DNS domain as the Workplace Server's Web server. The SSO cookie or mySAP.com logon ticket cannot be used for authentication in systems outside of this domain, for example, the mySAP.com Marketplace. For an example, see A Sample Domain Infrastructure [Page 45].

Activities

For information about how the SSO cookie is used to authenticate users in the mySAP.com Workplace, see User Authentication when Using SSO Cookies [Page 12].

User Authentication when Using SSO Cookies

For a detailed description on the user authentication processes, see:

- User Authentication: Initial Logon (SSO Cookie) [Page 12]
- User Authentication: Access to Component Systems (SSO Cookie) [Page 13]

User Authentication: Initial Logon (SSO Cookie)

Use

To receive an SSO cookie to use for Single Sign-On in the mySAP.com Workplace, the user must initially log on to the Workplace Server using his or her user ID and password for authentication. The Workplace Server authenticates the user and sets the SSO cookie in the user's Web browser. The initial authentication process is described in more detail below.

Prerequisites

See the prerequisites for Using SSO Cookies [Page 11].

Process Flow

1. The user enters the URL for the mySAP.com Workplace in his or her Web browser.
2. The request is sent to the Workplace Server via the Workplace Server's Web server and Internet Transaction Server (ITS).
3. Because it is the user's initial logon request (that is, no SSO cookie for the user exists), the system requests the user's ID and password.
4. The user provides his or her user ID and password in the corresponding dialog.
5. The information is sent to the Workplace Server to be validated.
6. If the central Workplace server can successfully authenticate the user, then:
   a) The user is logged on to the Workplace and the Workplace Server sends the user's personalized menu back to the frontend client to be viewed in his or her Web browser.
   b) The Web server used for the Workplace Server sets the SSO cookie in the user's Web browser.

Result

The user is logged on to the mySAP.com Workplace and can use his or her SSO cookie to log on to component systems.

User Authentication: Access to Component Systems (SSO Cookie)

Purpose

The SSO cookie is used as the authentication "token" when the user accesses a component system in the Workplace. It is available to any of the following Workplace services:

- Internet applications, which include:
  - Internet Application Components (IACs)
  - Applications that use the SAP GUI for HTML
  - Applications that use WebRFC
- Applications that use the SAP GUI for Windows

The process that occurs when a user accesses a component system is described in more detail below.

Prerequisites

See the prerequisites for Using SSO Cookies [Page 11].

In addition, the user must be logged on to the mySAP.com Workplace. See User Authentication: Initial Logon (SSO Cookie) [Page 12].

Process Flow

When the user accesses a mySAP.com Workplace component system:

1. The Web browser sends the SSO cookie to the component system being accessed.
2. The component system uses the information contained in the SSO cookie to authenticate the user.

Result

If the user is successfully authenticated, then the user is logged on to the system. No further user intervention is necessary.

Otherwise, if the user cannot be authenticated based on the information contained in the SSO cookie (for example, the **user's password** in the component system is **not synchronized** with the password provided with the SSO cookie), then the system sends a dialog requesting the user's authentication information.

Removing a Workplace Component System from the Single Sign-On Environment

In this way, you can remove a particular Workplace component system from the Single Sign-On environment (for example, your HR system). In the segregated system, users can have different passwords than what is defined in the Workplace Server and you can enforce a different password policy than that for the Workplace Server. (For example, you could define a password expiration policy for the component system.)

To make sure that users can only access the particular component system from their Workplace, disable the creation of cookies in the component system by setting the ITS service file parameter `~mysapcomnosso1cookie` to the value 1 in the system's global service file `global.srvc`.

For more information about keeping passwords synchronized in the mySAP.com Workplace, see Keeping Passwords Synchronized [Page 15].

Configuring the mySAP.com Workplace for Using SSO Cookies

After installing and configuring the mySAP.com Workplace, your system should be set up to use SSO cookies for Single Sign-On. No extra configuration tasks are necessary. If you do have problems with Single Sign-On after installing or configuring the system, see Post Configuration Checks: SSO Cookies [Page 16].

HTTP communications are set up as the default protocol in the mySAP.com Workplace. If you want to require the use of HTTPS in the Workplace, then set the parameter `~ssorequiresssl` in either of the Workplace Server's ITS service files `global.srvc` or `sapwp.srvc`.

(For the mySAP.com Workplace 2.00, see SAP Note 215510.)

Keeping Passwords Synchronized

To simplify the task of keeping passwords synchronized between Workplace systems:

1. Disable the creation of cookies on the Workplace component systems by setting the ITS service file parameter `~mysapcomnosso1cookie` to the value 1 in the component systems' global service files (`global.srvc`).

   Although users can only access these systems from their Workplaces, they receive a better overview of those systems where their passwords are no longer synchronized.

2. If you have component systems that use password expiration policies, then set the password expiration time on the Workplace Server to a value smaller than that defined for any of your component systems. Users are then forced to change their passwords on the Workplace Server more frequently than on any of the component systems. The password change on the Workplace Server consequently requires a user to synchronize his or her password on all component systems before being able to access them using SSO.

   In the component system R31, you require users to change their passwords every 30 days. In the component system R32, you require a password change every 60 days. A third component system R33 does not require any password change.

   To simply the process of keeping passwords synchronized:

   a. First, disable the setting of cookies on the component systems R31, R32, and R33 (`~mysapcomnosso1cookie` = 1 in each of their global services files `global.srvc`).

   b. Then, set the password expiration time on your Workplace Server for a value less than 30 days (for example, 25 days).

   Users are then forced to change their passwords every 25 days on the Workplace Server, which makes their passwords unsynchronized throughout the Workplace. When they access a component system where they have not yet changed their password, they receive a logon screen and can immediately change their password in that system to match their password on the Workplace Server.

Post Configuration Checks: SSO Cookies

If the Single Sign-On function does not work correctly after configuring the mySAP.com Workplace, perform the checks as described in the tables below:

Workplace Server Application Server

Location	Necessary Configuration
Tables TWPURLSVR and USRURLSVR (Web server definitions)	All Web servers must belong to the same DNS domain as the Workplace Server's Web server. All Web servers must be defined using the complete DNS name and port number. Do not use abbreviated names or IP-addresses in the definitions. (For example, use `host1.mysap.company.com:1234` and not `host1:1234`.) The port you enter in the URL must match the port used for the protocol (HTTP or HTTPS).

Workplace Server ITS Instance

Location	Parameter	Value
Global service file `global.srvc`	`~cookies`	1
	`~login`	(space)
	`~password`	(space)
Workplace service file `sapwp.srvc`	`~mysapcomssonoits`	1
	`~login`	(space)
	`~password`	(space)
In either `global.srvc` or `sapwp.srvc`	`~mysapcomnosso1cookie`	0
	`~ssorequiresssl`	1 (if you want to enforce the use of SSL in the mySAP.com Workplace)

Component System ITS Instances

If you want to make the component system only accessible from the Workplace, disable the creation of cookies on the component system's ITS server by setting the parameter `~mysapcomnosso1cookie` to the value 1 in the component system's ITS global service file `global.srvc`. Otherwise, users can access the system directly (for example, by using the `webgui` service).

Web Browsers

Make sure the users' Web browsers are set to accept non-persistent cookies.

In Internet Explorer 5.0:

a. Access the security options by choosing *Tools* → *Internet Options*..., *Security* → *Custom level* option.

b. Set the option *Cookies/Allow per-session cookies (not stored)* to either *Enable* or *Prompt*.

Additional Information

For more information about troubleshooting problems with Single Sign-On in the mySAP.com Workplace, see the SAP Note 318515.

Using mySAP.com Logon Tickets

Use

mySAP.com logon tickets are available for Single Sign-On in the mySAP.com Workplace as of Release 2.10. mySAP.com logon tickets improve the security of the Single Sign-On environment in the Workplace and eliminate some of the restrictions placed on the SSO cookie (for example, the requirement that a user's password needs to be the same in all of the Workplace systems).

To assist you with the administration tasks involved when using mySAP.com logon tickets, we also provide the SSO administration wizard [Page 23]. The SSO administration wizard automates the administration tasks and provides you with the results in an easy-to-read status report.

Prerequisites

- Users need to have the same user ID in all of the Workplace systems they access using SSO. Passwords do **not** have to be same in all systems.
- In addition to the Workplace Plug-In, certain kernel patches need to be applied to Workplace component systems prior to Release 4.6C. For more information, see SAP Note 177895.
- End users need to configure their Web browsers to accept cookies.

  In Internet Explorer 5.0, accept *session cookies* for the *local intranet zone*.
- The Web servers for the Workplace Server as well as those used for the component systems must all be located in the same DNS domain.

  The SSO cookie or mySAP.com logon ticket is only available for user authentication to services whose Web servers are defined in the same DNS domain as the Workplace Server's Web server. The SSO cookie or mySAP.com logon ticket cannot be used for authentication in systems outside of this domain, for example, the mySAP.com Marketplace. For an example, see A Sample Domain Infrastructure [Page 45].
- The Workplace Server must possess a public-key pair and public-key certificate so that it can digitally sign the mySAP.com logon ticket.

  The Workplace Server automatically receives a public-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 CA. For more information, see Obtaining a Certificate Signed by the SAP CA [Page 29].
- The Workplace component systems must have access to the Workplace Server‘s public-key certificate so that they can verify the Workplace Server‘s digital signature.

  Depending on the type of certificate you use, the server's certificate is either sent with the logon ticket to the component system or the information is entered in the component system's certificate list. The SSO administration wizard automatically establishes the appropriate configuration on the component system.

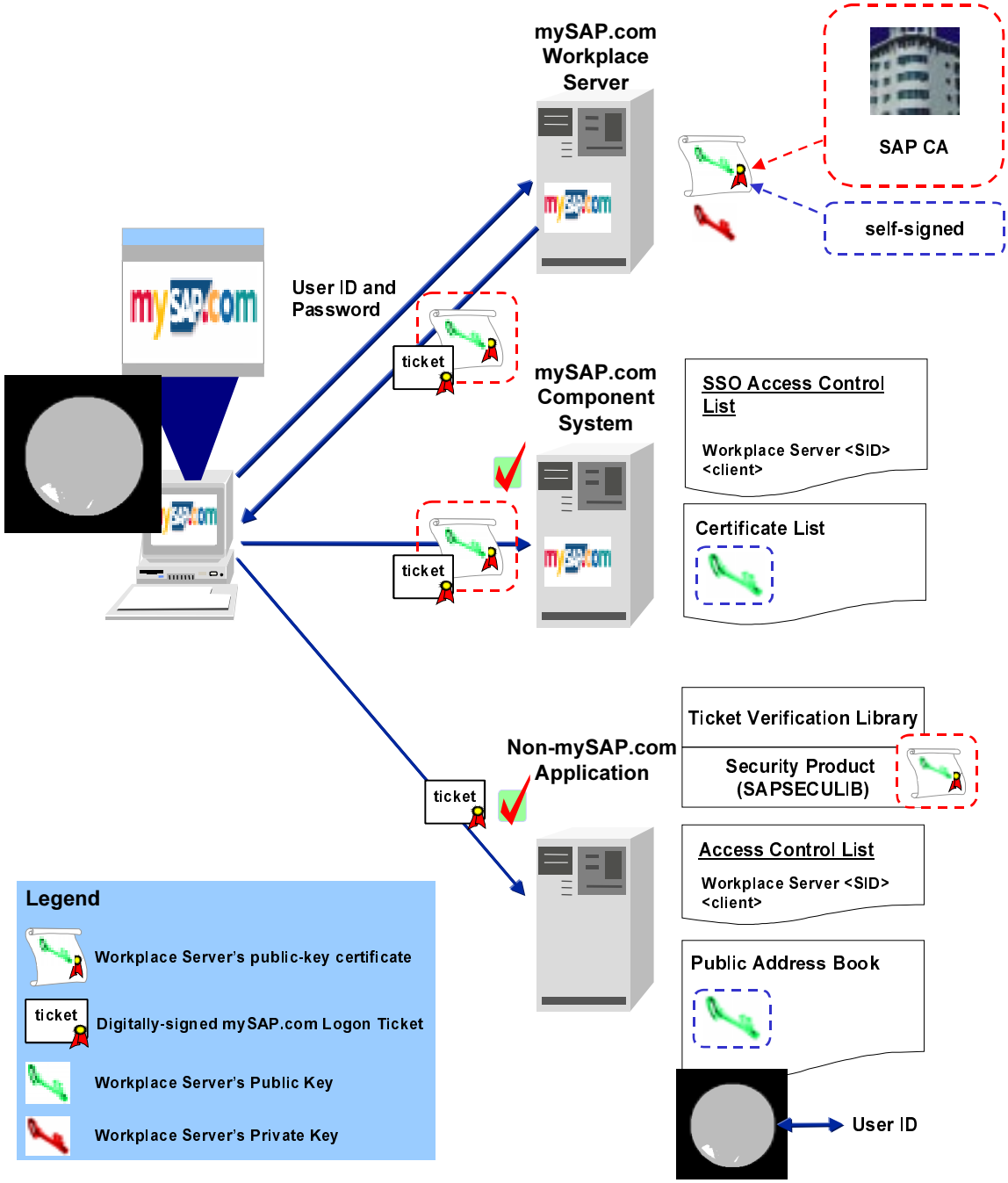
Activities

For information about how the SSO cookies and the mySAP.com logon ticket are used to authenticate users in the mySAP.com Workplace, see User Authentication when Using mySAP.com Logon Tickets [Page 21].

System Architecture When Using mySAP.com Logon Tickets

The graphic below shows an overview of the system architecture when using mySAP.com logon tickets for Single Sign-On in the mySAP.com Workplace.

System Architecture When Using mySAP.com Logon Tickets



Note the following:

- When a user logs on to the mySAP.com Workplace, the Workplace Server issues the user his or her mySAP.com logon ticket. The Workplace Server guarantees the ticket's authenticity by signing the ticket with its digital signature.
- To create its digital signature, the Workplace Server needs to possess a public-key pair and a public-key certificate. It may either use a self-signed certificate or a certificate signed by the SAP Certification Authority (CA) [Page 68].
- The component systems need to be able to verify the digital signature included with the user's mySAP.com logon ticket. Therefore, they need to have access to the Workplace Server's public-key certificate. Depending on the type of certificate you use, the certificate is either sent to the component system with the user's logon ticket or the public-key information is entered in the component system's certificate list [Page 68] (may also be referred to as a public address book).
- In addition, the component systems should only accept mySAP.com logon tickets that have been issued by the designated Workplace Server. Therefore, each component system has an SSO access control list which you use to define the system's corresponding Workplace Server.

  The SSO access control list is client-specific and builds a trust relationship between the component system's logical system (system ID and client) and the Workplace Server's logical system (system ID and client).
- Non-SAP component systems must also be able to verify the mySAP.com logon ticket. For this purpose, we provide a shared library with the verification routines. Thereby, the non-SAP component system also needs access to the Workplace Server's public-key certificate and must also maintain an access control list that contains the system's designated Workplace Server. If necessary, the system must also provide a mapping between the user ID contained in the ticket and the user's ID in the system.

  In the topics that follow, we describe the configurations for using either self-signed certificates or certificates signed by the SAP CA. If you use certificates signed by a different CA (either your own or an external CA), you may have to adjust the configurations accordingly. (For example, you have to define the location of the Workplace Server's private key on the Workplace Server and you may have to modify the component systems' certificate lists.)

User Authentication when Using mySAP.com Logon Tickets

For a detailed description on the user authentication processes, see:

- User Authentication: Initial Logon (mySAP.com Logon Ticket) [Page 21]
- User Authentication: Access to Component Systems (mySAP.com Logon Ticket) [Page 22]

User Authentication: Initial Logon (mySAP.com Logon Ticket)

Purpose

To receive a mySAP.com logon ticket to use for Single Sign-On in the mySAP.com Workplace, the user must initially log on to the Workplace Server using his or her user ID and password for authentication. The Workplace Server authenticates the user and issues the user his or her logon ticket. The initial authentication process is described in more detail below.

Prerequisites

See the prerequisites for Using mySAP.com Logon Tickets [Page 18].

Process Flow

1. The user enters the URL for the mySAP.com Workplace in his or her Web browser.
2. The request is sent to the Workplace Server via the Workplace Server‘s Web server and ITS.
3. Because it is the user‘s initial logon request (that is, no logon ticket for the user exists), the system requests the user‘s ID and password.
4. The user provides his or her user ID and password in the corresponding dialog.
5. The information is sent to the Workplace Server to be verified.
6. If the Workplace Server can successfully authenticate the user, then:
   a. The Workplace Server logs the user on to the Workplace.
   b. The Workplace Server creates and digitally signs the user's mySAP.com logon ticket.
   c. The user‘s logon ticket is sent to the user and stored in the user's Web browser.
   d. The user's personalized menu is sent back to the frontend client to be viewed in his or her Web browser.

Result

The user is logged on to the mySAP.com Workplace and can use his or her mySAP.com logon ticket to log on to component systems.

User Authentication: Access to Component Systems (mySAP.com Logon Ticket)

Purpose

The mySAP.com logon ticket is used as the authentication "token" when the user accesses a component system in the mySAP.com Workplace. It is available to any of the following Workplace services:

- Internet applications, which include:
  - Internet Application Components (IACs)
  - Applications that use the SAP GUI for HTML
  - Applications that use WebRFC
- Applications that use the SAP GUI for Windows
- Non-mySAP.com component systems that use the mySAP.com logon ticket library. (For more information, see Using mySAP.com Logon Tickets for Access to Non-mySAP.com Systems [Page 37].)

Prerequisites

See the prerequisites for Using mySAP.com Logon Tickets [Page 18].

In addition, the user must be logged on to the mySAP.com Workplace. For more information, see User Authentication: Initial Logon (mySAP.com Logon Ticket) [Page 21].

Process Flow

As the user accesses component systems within the mySAP.com Workplace:

1. The Web browser sends the user’s mySAP.com logon ticket to the system being accessed.
2. The component system verifies the user’s logon ticket. It:
   - Verifies the Workplace Server's digital signature.
   - Makes sure the ticket has been issued by the system's designated Workplace Server.
   - Checks the expiration time.

Result

If the mySAP.com logon ticket is valid, then the user is allowed access to the system. No further user intervention is necessary.

Otherwise, the user is prompted for his or her user ID and password.

SSO Administration Wizard

Use

The SSO administration wizard (transaction SSO2) assists you in configuring your mySAP.com Workplace component systems to accept and verify mySAP.com logon tickets issued and digitally signed by the mySAP.com Workplace Server.

Integration

Using a certificate signed by the SAP CA or a self-signed certificate

To ensure that a user's mySAP.com logon ticket is authentic and has been issued by the Workplace Server, the Workplace Server secures the logon ticket with its digital signature. Digital signatures are created and verified using public-key technology, and to be able to produce its digital signature, the Workplace Server needs to possess a public-key pair and a public-key certificate.

There are two types of public-key certificates that the Workplace Server can use for its digital signatures, either a public-key certificate that has been signed by the SAP CA, or a self-signed certificate. To determine which certificate you want to use, consider the following:

- When using a certificate signed by the SAP CA, the Workplace component systems can verify the Workplace Server‘s signature contained in mySAP.com logon tickets without needing any additional information.

  To obtain a certificate signed by the SAP CA, you create a certificate request on the Workplace Server. The Workplace Server generates its own public-key pair and SSO Personal Security Environment (SSO PSE) [Page 72] and sends the public-key certificate to the SAP CA to be signed. The SAP CA signs the certificate and sends it back to you to place in the Workplace Server‘s SSO PSE (See Obtaining a Certificate Signed by the SAP CA [Page 29]).

- When using self-signed certificates, the Workplace component systems need access to the public-key information contained in the Workplace Server's certificate to be able to verify the Workplace Server‘s digital signature. The SSO administration wizard enters the necessary information in the component system‘s certificate list as part of its tasks (see below).

  The Workplace Server's public-key pair and self-signed public-key certificate are provided to the Workplace Server during the installation process.

For more information, see:

- Configuring the Workplace Server for Using mySAP.com Logon Tickets [Page 26]
- Public-Key Technology (8) [Page 73]

Determining the location of the system's public-key information

When the Workplace Server uses a self-signed certificate to sign mySAP.com logon tickets, the information needed to verify the Workplace Server's digital signature is entered in the system's certificate list, which is stored in its designated SSO PSE.

The SSO administration wizard first checks whether a self-signed certificate or a SAP CA certificate is used. If a self-signed certificate is used, the wizard determines the location of the component system's SSO PSE and makes the corresponding entry in the certificate list.

For component systems prior to Release 4.6C, the SSO PSE is the file `SAPSSO2.pse` located in the directory specified by the profile parameter `DIR_PROFILE`.

As of Release 4.6C, the SSO PSE is the designated system PSE [Page 72].

In this case, you can override the use of the system PSE by entering the location of a different PSE in the SSF (Secure Store & Forward) application-specific information (table SSFARGS). Enter the location of the PSE in the public address book (*PAB*) field for the application SSO2. For more information, see the SSF User's Guide (7) [Page 73].

Assigning the system's designated Workplace Server

A component system should only accept mySAP.com logon tickets issued from its designated Workplace Server. Therefore, the SSO administration wizard also enters the Workplace Server's server ID and client in the component system's SSO access control list (table TWPSSO2ACL).

In addition, if the Workplace Server also provides services that are to be accessed using Single Sign-On (for example, MiniApps), then the Workplace Server itself needs to be entered in its own SSO ACL.

The SSO ACL is client-specific and builds a trust relationship between the component system's logical system (system ID and client) and the Workplace Server's logical system (system ID and client).

Features

- Full automation of the administration tasks necessary for accepting and verifying mySAP.com logon tickets in mySAP.com Workplace component systems.
- Easy identification of configuration errors with traffic light indicators.

Activities

When you execute the SSO administration wizard:

1. The SSO administration wizard contacts the mySAP.com Workplace Server using a Remote Function Call (RFC) and collects the information necessary for using mySAP.com logon tickets, for example:
    - Profile parameter values
    - The Workplace Server‘s system ID and client
    - The Workplace Server‘s public-key certificate
2. This information is displayed in the SSO administration report. The report also shows whether the Workplace Server‘s information has been entered in the system‘s access control list and certificate list. The traffic lights indicate whether or not the status is operational for Single Sign-On or not.

When you activate the Workplace Server using the SSO administration wizard:

1. The SSO administration wizard enters the Workplace Server‘s system ID and client in the system‘s SSO access control list.
2. If the Workplace Server‘s public-key certificate is self-signed:
   a. The SSO administration wizard enters the Workplace Server‘s public-key information in the system‘s certificate list which is contained in the system's SSO PSE.
   b. The SSO administration wizard makes the SSO PSE available to the 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 system, then you have to manually copy the SSO PSE to each application server's `DIR_PROFILE` directory.
3. The status of the SSO information is displayed in the SSO administration report.

Configuring the Workplace Server for Using mySAP.com Logon Tickets

Use

The mySAP.com Workplace Server needs to be configured to create and digitally sign mySAP.com logon tickets for users. Certain parameters need to be set on the Workplace Server's ITS and on the application server. In addition, to be able to digitally sign the tickets, the application server needs to possess a public-key pair and a public-key certificate, which are stored in the server's SSO PSE.

If the Workplace Server also provides applications that will be accessed using Single Sign-On (for example, MiniApps), then you also need to set up the Workplace Server so that it can accept and verify tickets that it issues.

Prerequisites

You need to know whether the Workplace Server is to use a self-signed public-key certificate or a certificate signed by the SAP CA.

Procedure

On the Workplace Server's ITS Instance

1. If the AGate is running, stop it.
2. In the global service file `global.srvc`:

Set the Parameter	To the Value	Comment
`~login` `~password`	(space) (space)	When these parameters are empty in both `global.srvc` and in `sapwp.srvc`, users are prompted for their user ID and password when initially logging on to the mySAP.com Workplace.
`~cookies`	1	Enables the creation of cookies on the ITS.
`~mysapcomusesso2cookie`	1	Enables the user to log on to the system using an existing mySAP.com logon ticket.
`~mysapcomnosso1cookie`	0: If you want to use SSO cookies and mySAP.com logon tickets simultaneously. 1: If you want to use mySAP.com logon tickets only.	Disables the creation of SSO cookies in the mySAP.com Workplace.

3. In the Workplace service file `sapwp.srvc`:

Set the Parameter	To the Value	Comment
`~login`	(space)	See above.
`~password`	(space)	
`~mysapcomssonoits`	1	Ensures that the SAP System client is not included in the logon ticket, allowing for Single Sign-On across multiple SAP System clients.
`~mysapcomgetsso2cookie`	1	Enables the creation of the mySAP.com logon ticket after successful logon.

4. If you want to enforce the use of HTTPS in the mySAP.com Workplace, set the parameter `~ssorequiresssl` in either `global.srvc` or `sapwp.srvc`.

5. Start the AGate.

On the Workplace Server's Application Server

1. If you want to use a certificate signed by the SAP CA, you need to obtain the signed public-key certificate for the Workplace Server and generate the server's SSO PSE. If you use a self-signed certificate, the public-key certificate already exists in the Workplace Server's SSO PSE. For more information, see:

   - Obtaining a Certificate Signed by the SAP CA [Page 29]
   - Using a Self-Signed Certificate [Page 30]

2. Set the following profile parameters on the Workplace Server's application server:

Set the Parameter	To the Value	Comment
`login/accept_sso2_ticket`	1	Allows the Workplace Server to accept an existing mySAP.com logon ticket for logon purposes.
`login/create_sso2_ticket`	1: If the Workplace Server's certificate is to be included in the logon ticket. 2: If the Workplace Server's certificate is not to be included in the logon ticket.	For best results, set this parameter to the value 1 if the Workplace Server possesses a certificate signed by the SAP CA. Set it to the value 2 if the certificate is self-signed.
`login/ticket_expiration_time`	Desired value	Default = 60 hours See SAP Note 337794 for information about how to set the expiration time in minutes.

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

3. Execute the SSO administration wizard (transaction SSO2).

   The *SSO2 Administration* screen appears.

4. Enter `NONE` as the RFC destination. (Use capital letters.)

   The following information is shown in the report:

   - Profile parameter values.
   - Contents of the Workplace Server's SSO access control list.
   - Contents of the Workplace Server's certificate list.

   Red traffic lights in any of these areas indicate configurations that are not operational for SSO.

5. Choose *Edit* → *Activate Workplace*.

   The following occurs:

   - The SSO administration wizard enters the Workplace Server's system ID and client in the SSO access control list.
   - If the Workplace 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 system's certificate list.
   - The SSO administration wizard makes the SSO PSE available to the Workplace Server's application servers:

     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 Workplace Server's system ID and client to the SSO access control list, place the cursor on the line `R/3 System <SID> Client <client>` and choose *Edit* → *Enter ACL*.

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

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

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

     You can also manually change the certificate list or export the Workplace Server's PSE to use for verification using the transaction PSEMAINT. (Choose *Edit* → *Certificate List* or *Edit* → *Verification PSE*.)

Result

The mySAP.com Workplace digitally signs mySAP.com logon tickets and issues them to users when they log on to the Workplace.

The Workplace Server can also accept and verify its own tickets.

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

Obtaining a Certificate Signed by the SAP CA

Use

To obtain a certificate signed by the SAP CA for the Workplace Server to use to digitally sign mySAP.com logon tickets, perform the procedure below.

Procedure

Sending the Certificate Request

1. Execute the PSE Management function (transaction PSEMAINT).

   The *PSE Management* screen appears.

2. Choose *PSE* → *Generate*.

   The *Generate New PSE* dialog appears.

3. Enter the corresponding information.

Field	Value	Comment
Name	`<SID>`	
Organizational Unit	Optional	Use this field, if necessary, to build a unique descriptor for the server.
Comp.	`<Company> <TEST>`	If the system is not a productive system, then include the indicator TEST in the entry.

The entries above build the Distinguished Name for the Workplace Server, which must be a unique name. Therefore, if necessary, include the department name in the company description or use the *Organizational Unit* field to supply additional information.

The entries *Name* = `WP1` and *Comp.* = `MyCompany` build the following Distinguished Name for the Workplace Server:

```
CN=WP1, OU=MyCompany, O=mySAP.com Workplace, C=DE
```

The Distinguished Name components `O=mySAP.com Workplace` and `C=DE` are automatically determined by the system.

4. To initiate the certificate request, choose *Edit* → *Certificate request* → *Certificate request*.

   The system generates the information needed for the certificate request and displays it in the *Generate Certificate Request* screen. The content of the request is generated in binary-code as shown below.

   ```
   -----BEGIN CERTIFICATE REQUEST-----

   MIIBkzCCAVICAQAwWjELMAkGA1UEBhMCREUxHDAaBgNVBAoTE215U0FQLmNvbS
   BXb3JrcGxhY2UxDzANBgNVBAsTBlNBUCBBRzEOMAwGA1UECxMFQmFzaXMxDDAK
   BgNVBAMTA0JJTzCB7jCBpgYFKw4DAhswgZwCQQCSnauC/cAfQVrmOtWznQ9I+i
   4twoPq8wCE0Fk5EAVjQnX2oMqBnyoi+ee/ZH2cLwyhp5mOOw70+exS7PHEWKiF
   AhUAw9FSY1AsFV4U9fC9w+Bg5H4ISYcCQARcC+7q3UkM0TF0A5zRaq7viO3Wj2
   MwYUNwFkc0hxzhloUQd21megZADoFiisdzkn/nF4eIxV9vq9XxcV63xTsDQwAC
   QFher18UA8YkY4/zHe4mbupBXvDSucm2nbJuQ5PgDBvVaMmtpXIisyzuAFL+qC
   zQ92mkNqUR9JLWpz09ghQdISCgADAJBgcqhkjOOAQDAzAAMC0CFA7qEluP/Kfi
   +6HF/8I7j4NfF44xAhUAqkDgAeR3tzmNegKUTQ+JzeCXawE=

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

5. Copy the certificate request's content to a customer message under the component BC-SEC.
6. The SAP CA validates your information and sends you a response, which contains the Workplace Server's signed public-key certificate.

Entering the Certificate Request Response Data

After receiving a response:

1. Execute the PSE Management function (transaction PSEMAINT).

   The *PSE Management* screen appears.

2. Choose *Edit* → *Certificate request* → *Insert response*.

   The *Insert Certificate Request Response* screen appears.

3. Copy the information from the E-mail you received from the SAP CA to the text editor (or use the import function  to import the information as a file).
4. Save the data.

   The certificate is saved in the Workplace Server's SSO PSE.

Result

The Workplace 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 mySAP.com logon tickets for SSO in the mySAP.com Workplace.

Using a Self-Signed Certificate

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

The Workplace Server receives an automatically generated public-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, see Changing the Server's Self-Signed Certificate [Page 31].

Changing the Server's Self-Signed Certificate

Use

The server's self-signed public-key certificate is automatically created using a Distinguished Name with the following syntax:

```
CN=<system ID>, OU=<organizational unit>, O=<company>,
C=<country>
```

Use the procedure below if you want to change the information contained in the certificate, for example, you want to use a different naming convention for the Distinguished Name.

Procedure

1. Execute the PSE Management function (transaction PSEMAINT).

   The *PSE Management* screen appears. The application servers belonging to the system are displayed with a traffic light indicating the status of the system PSE (which is in this case, the same as the SSO PSE).

2. If you want to change any of the information in the server's public-key certificate, you must generate a new public-key pair and public-key certificate and distribute it to the application servers in the system.

   Perform the following:

   a. Choose *PSE* → *Generate*.

      The *Generate new PSE* dialog appears.

   b. Enter the required data.

      The entered data builds the Distinguished Name that will be contained in the public-key certificate. The Distinguished Name has the following form:

      ```
      CN=<name>, OU=<organizational unit>, O=<company>,
      C=<country>
      ```

   c. Save the data.

3. Distribute the new public-key certificate by executing the SSO administration wizard in each of the component systems. (See Configuring a Component System to Accept and Verify mySAP.com Logon Tickets [Page 32].)

Result

A new public-key pair and public-key certificate are generated for the Workplace Server and made available to the Workplace Server's application servers.

Configuring a Component System to Accept and Verify mySAP.com Logon Tickets

Use

The mySAP.com Workplace Server digitally signs mySAP.com logon tickets as it issues them to the Workplace users. Component systems need to accept the tickets and verify the Workplace Server's digital signature. The following information is important for the component system to be able to accept and verify mySAP.com logon tickets:

- The component system should only accept mySAP.com logon tickets issued from their designated Workplace Server. Therefore, the identity of the Workplace Server needs to be entered in the component system's SSO access control list.
- The component system needs to be able to verify the Workplace Server's digital signature. If the Workplace Server possesses a public-key certificate that is signed by the SAP CA, the component system can verify the Workplace Server's digital signature without needing any additional information. However, if the certificate is a self-signed certificate, then the component system needs access to the Workplace Server's public-key information, which needs to be entered in the component system's certificate list.
- The component system needs to know where the information is stored that it uses to verify the Workplace 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 72] 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 Workplace Server has been configured to issue mySAP.com logon tickets (profile parameter `login/create_sso2_ticket` = 1 or 2).
- The mySAP.com Workplace Server possesses a public-key pair and a public-key certificate. This information needs to be available in the Workplace Server's SSO PSE.

See Configuring the Workplace Server for Using mySAP.com Logon Tickets [Page 26].

Procedure

On each of the component system's ITS servers

In the global service file `global.srvc`, set the following parameters:

Set the Parameter	To the Value	Comment
`~login` `~password`	(space) (space)	When these parameters are empty in both `global.srvc` and in `sapwp.srvc`, users are prompted for their user ID and password when initially logging on to the mySAP.com Workplace.
`~mysapcomusesso2cookie`	1	Enables the user to log on to the system using an existing mySAP.com logon ticket.

On all of the component system's application servers

Set the profile parameters `login/accept_sso2_ticket` = 1 and `login/create_sso2_ticket` = 0. (Use DEFAULT.PFL.)

On one of the component system's application servers

1. Execute the SSO administration wizard (transaction SSO2).

   The *SSO2 Administration* screen appears.

   As of Release 4.6C, the SSO administration wizard is executed locally on the component system. For releases prior to Release 4.6C, the SSO administration wizard is executed on the Workplace Server using an RFC connection.

2. Enter the RFC destination or the **<host name>** and **<system number>** for the Workplace Server in the appropriate fields.

   Note the following:

   – You must specify the destination host for the Workplace 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 Workplace Server and on the component system's application server.
   - The component system's SSO access control list.
   - The component system's certificate list.

   Red traffic lights in any of these areas indicate configurations that are not operational for SSO.

3. If the report indicates errors on the Workplace Server (for example, profile parameters are not set correctly), correct these errors on the Workplace Server and re-execute the SSO administration wizard on the component system.

4. To initiate the configuration steps on the component system, choose *Edit* → *Activate Workplace*. The following occurs:

   - The SSO administration wizard enters the Workplace Server's system ID and client in the component system's access control list.
   - If the Workplace 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 component system's certificate list.
   - The SSO administration wizard makes the SSO PSE available to the component 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 component 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.

5. If any of the areas indicate errors, correct these errors and re-execute the SSO administration wizard. See Post-Configuration Checks: mySAP.com Logon Tickets [Page 40] for possible sources of errors.

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 Workplace Server's system ID and client to the SSO access control list, place the cursor on the line `R/3 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 to delete 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 transaction PSEMAINT. (Choose *Edit* → *Certificate List*.)

Result

The mySAP.com component systems are able to accept mySAP.com logon tickets and verify the Workplace 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.

Upgrading a Component System to Release >= 4.6C

Use

Component systems prior to Release 4.6C use a different SSO PSE than Release >= 4.6C. Therefore, when upgrading the component system to Release 4.6C or higher, you need to inform the component system where the new SSO PSE is located.

Perform the following procedure on a **single** application server for **each** component system that you upgrade to Release >= 4.6C.

Procedure

1. Execute the SSO administration wizard (transaction SSO2) using the local system as the destination system. (Make no entries in the initial *SSO Administration* screen.)
2. Choose *Edit* → *Activate*.

   If a certificate list exists in the old SSO PSE (`SAPSS02.pse`), the SSO2 administration wizard copies it to the new SSO PSE (`SAPSYS.pse`) and deletes the old SSO PSE. It then displays the new SSO status. No further intervention is necessary.

Result

The component system stores the information it needs for SSO in the new SSO PSE.

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

Use

You may want to use the self-signed certificate when you initially install the mySAP.com Workplace Server and switch to a certificate signed by the SAP CA at a later time. Use the procedure described below to issue the new public-key pair and public-key certificate to the Workplace Server and change the necessary information on the component systems.

Procedure

Single Sign-On will **not** be available within the Workplace 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 Workplace Server and lasts until you have activated the Workplace Server on **all** of the component systems.

On the Workplace Server

1. Obtain a public-key certificate signed by the SAP CA [Page 29].
2. Set the application server profile parameter `login/create_sso2_ticket` to the value 1.

On each of the Workplace component systems

1. Execute the SSO administration wizard (transaction SSO2) using the Workplace Server as the server destination.

   The SSO administration report displays the current SSO status.
2. Delete the former public-key certificate from the component system's certificate list by choosing *Edit* → *Remove Certificate List*.
3. Activate the Workplace by choosing *Edit* → *Activate Workplace*.

   The SSO administration report displays the status of the new SSO environment.

See also Configuring a Component System to Accept and Verify mySAP.com Logon Tickets [Page 32].

Result

Instead of using its self-signed certificate, the Workplace Server uses the public-key certificate signed by the SAP CA to digitally sign mySAP.com logon tickets. The component systems can also verify the Workplace Server's new digital signature.

Using Logon Tickets for Access to Non-mySAP.com Applications

Use

The functions used to verify mySAP.com logon tickets are available to non-mySAP.com applications in a shared library. You can use the provided functions to verify a user's mySAP.com logon ticket in the mySAP.com Workplace. Available routines include:

- Initializing the library (which creates log and trace files)
- Verifying the Workplace Server's digital signature
- Parsing the issuer's certificate (if the security product used for verification is the SAPSECULIB)
- Closing the library

The parsing function is designed for use with the default security product SAPSECULIB. If you use a different security product for verification, then you must use the product's available functions for parsing.

Integration

When a user accesses a non-mySAP.com application using a logon ticket for authentication, the ticket is automatically sent to the application's Web server in a cookie. The application first needs to retrieve the ticket from the cookie. It can then use the shared library `sapssoext` to verify the Workplace Server's digital signature included with the ticket.

The library itself uses calls to an external security product to verify the Workplace Server's digital signature. The default product used is the SAPSECULIB, which is the default security library provided with SAP Systems. You may however, use any security product that conforms to the SSF interface. For more information, see the SSF User's Guide (7) [Page 73].

To be able to verify the Workplace Server's digital signature, the product must have access to the Workplace Server's public-key certificate. If the Workplace Server's public-key certificate is signed by the mySAP.com CA and you use the SAPSECULIB as the security product to verify the signature, then the Workplace Server's public key is available directly with the SAPSECULIB. Otherwise, the Workplace Server's certificate must be contained in the public address book used for SSF.

If the digital signature is valid, then the application must also maintain an access control list to make sure that the ticket was issued by its designated Workplace Server.

In addition, if the application's user IDs are not identical to those in the mySAP.com Workplace Server, then the application must also provide a user mapping between the corresponding user IDs.

The shared library is provided by the MiniApps Community (11) [Page 73] in the Development Zone (see http://www.sap.com/miniapps).

Prerequisites

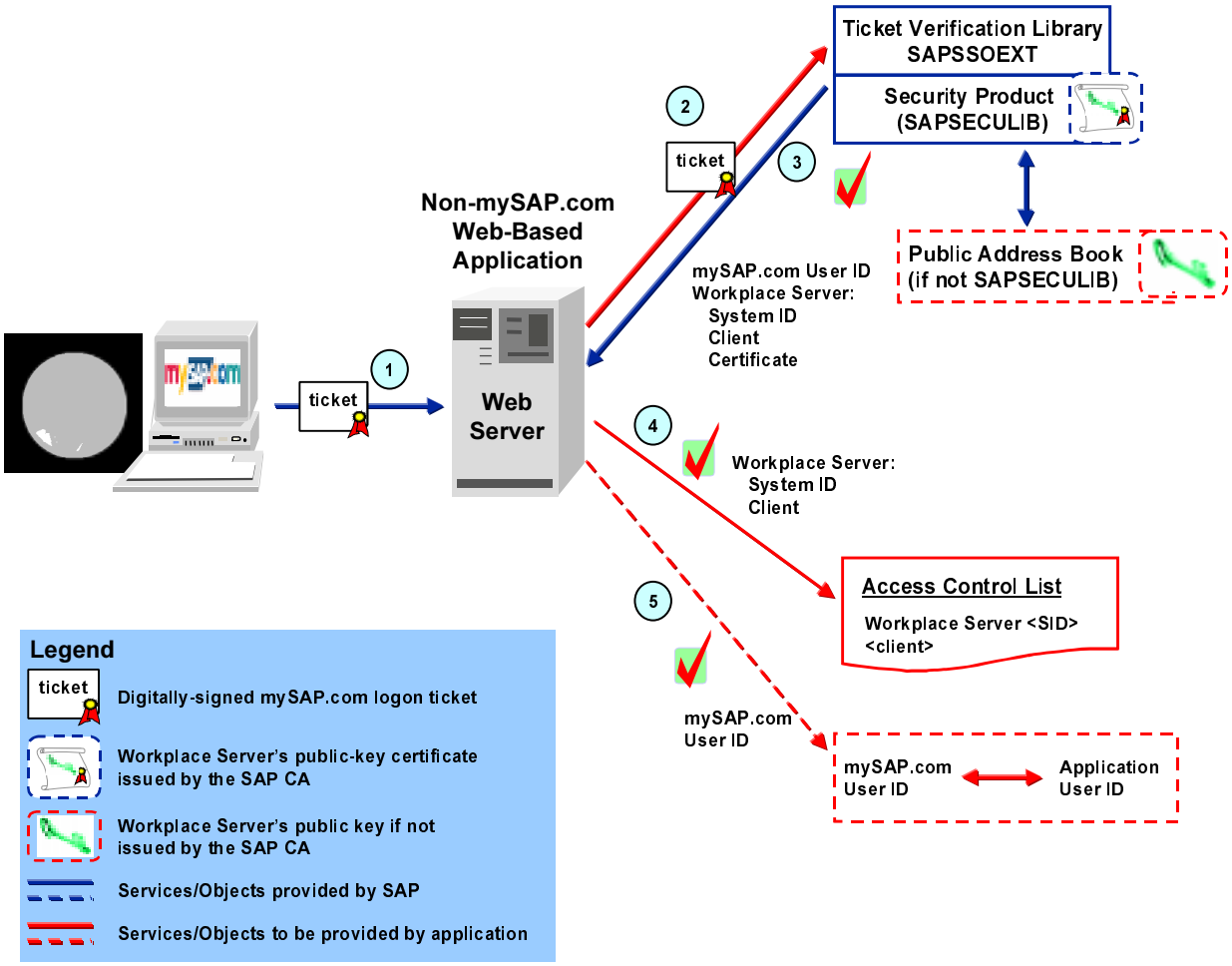
- The user has obtained a logon ticket from the mySAP.com Workplace Server.
- The application must either be Web-enabled or have access to a Web server where it can obtain the logon ticket.
- The security product (for example, the SAPSECULIB) must be available to the application.

  The SAPSECULIB is provided with the Workplace Server installation in the directory specified by the profile parameter `DIR_LIBRARY` (default) or `ssf<x>/ssfapi_lib` and `ssf<x>/ssf_name`. It is also available with the shared library package.
- The Workplace Server's public-key certificate must be available to the shared library, either by using the SAPSECULIB as the security product or making it available in a public address book.

Activities

See the graphic below:

Verifying mySAP.com Logon Tickets



1. The user accesses the application using the mySAP.com logon ticket for authentication.
2. The application retrieves the ticket from the Web server and passes it to the SSO shared library (`sapssoext`) for verification.

   The mySAP.com logon ticket is stored in the MYSAPSSO2 cookie. To extract the ticket from the cookie, use the appropriate standard Web interface (for example, ISAPI, NSAPI, or CGI-BIN).
3. The SSO shared library verifies the logon ticket by verifying the Workplace Server's digital signature.

   If the signature is valid, the verification routine returns the following information:

   - The user's ID
   - The Workplace Server's system ID
   - The Workplace Server's client
   - The Workplace Server's public-key certificate

   Other information from the Workplace Server's certificate is also available by using the parsing routine. For example, you can retrieve the Workplace Server's Distinguished Name, the certificate issuer's Distinguished Name, or the certificate's serial number.
4. The application verifies that the logon ticket was issued by its designated Workplace Server by checking the access control list.
5. If the application's user IDs are not identical to the Workplace Server's, then the application must map the user ID contained in the ticket to the corresponding user ID that it uses.

For a description of the individual routines available with the library and corresponding examples, see the documentation provided with the library.

Post-Configuration Checks: mySAP.com Logon Tickets

If the Single Sign-On function does not work correctly after configuring the mySAP.com Workplace, perform the checks as described in the tables below.

Workplace Server Application Server

Location	Necessary Configuration	Comment
Tables TWPURLSVR and USRURLSVR (Web server definitions)	All Web servers must belong to the same DNS domain as the Workplace Server's Web server. All Web servers must be defined using the complete DNS name and port number. Do not use abbreviated names or IP-addresses in the definitions. (For example, use `host1.mysap.company.com:1234` and not `host1:1234`.) The port you enter in the URL must match the port used for the protocol (HTTP or HTTPS).	
Profile parameters	`login/accept_sso2_ticket = 1` `login/create_sso2_ticket = 1 or 2`	For best results, use the value 1 if the Workplace Server possesses a certificate signed by the SAP CA and the value 2 if the certificate is self-signed.
Access control list (table TWPSSO2ACL)	An entry must exist containing the Workplace Server's server ID and client.	
PSE maintenance (transaction PSEMAINT)	Make sure no errors exist with the system PSE. (The SSO PSE is the system PSE.)	All traffic lights should be green in the PSE maintenance display. If not, then correct the system PSE. For more information, see the SSF User's Guide (7) [Page 73].

Workplace Server ITS Instance

Location	Parameter	Value
Global service file `global.srvc`	`~login`	(space)
	`~password`	(space)
	`~cookies`	1
	`~mysapcomusesso2cookie`	1
	`~mysapcomnosso1cookie`	0 or 1 Use the value 0 if you want to use both SSO cookies and mySAP.com logon tickets simultaneously. Use the value 1 if you want to use tickets only.
Workplace service file `sapwp.srvc`	`~login`	(space)
	`~password`	(space)
	`~mysapcomssonoits`	1
	`~mysapcomgetsso2cookie`	1

Component Systems' Application Servers

Location	Necessary Configuration	Comment
Profile parameters	`login/accept_sso2_ticket = 1` `login/create_sso2_ticket = 0`	
Access control list (table TWPSSO2ACL)	An entry exists for the Workplace Server's server ID and client.	
Certificate list	An entry exists for the Workplace Server's public-key certificate.	Only necessary if the parameter `login/create_sso2_ticket` on the Workplace Server contains the value 2.

Component Systems' ITS Instances

Location	Parameter	Value
Global service file `global.srvc`	`~login`	(space)
	`~password`	(space)
	`~mysapcomusesso2cookie`	1

Use the SSO administration wizard (transaction SSO2) to check the SSO status on the Workplace Server and component systems. Red traffic lights indicate configurations that are not operational for SSO.

Additional Information

For more information about troubleshooting problems with Single Sign-On in the mySAP.com Workplace, see the SAP Note 318515.

Upgrading from SSO Cookies to mySAP.com Logon Tickets

Use

If you have configured your Workplace to use SSO cookies and want to upgrade to mySAP.com logon tickets, perform the steps described below.

Prerequisites

You know whether or not the Workplace Server is to use a certificate signed by the SAP CA or a self-signed certificate.

Procedure

1. Configure the Workplace Server for using mySAP.com logon tickets [Page 26]

   Note the Workplace Server's ITS parameter `~mysapcomnosso1cookie`. Set this parameter to the value 1 to disable SSO cookies in the Workplace. Set it to the value 0 to use both SSO cookies and mySAP.com logon tickets simultaneously.

2. Configure the component systems to accept and verify mySAP.com logon tickets [Page 32]

Result

The mySAP.com Workplace uses mySAP.com logon tickets for authenticating users.

Configuring an Application to Run Under a Service User

Use

There may be applications or services (for example, MiniApps) that you want to run using a service user instead of the named user who is logged on.

Procedure

For each application or service that uses a different service user:

1. Create a service file for the application.

   For example, if the application normally uses the service file `webgui.srvc`, then copy `webgui.srvc` to a public version (for example, copy it to `webgui_public.srvc`).

2. In addition to any other necessary service file parameters, enter the service user's logon information using the parameters `~login` and `~password`.
3. Enter the name of the new service file in the URL for the application.
4. Save the data.

See An Example Service User Application [Page 43].

An Example Service User Application

To assign the MiniApp DISPLAY_NEWS to run under the service user PUBLIC whose password is PUBPASS:

1. Create a service file for the application (for example, copy the service file `webgui.srvc` to `webgui_public.srvc`).
2. Set the following parameters in the application's service file:
   - `~login` = PUBLIC
   - `~password` = PUBPASS
3. Define the URL for the MiniApp. You can make this definition when you assign the MiniApp to an appropriate role using role maintenance. (See Assigning MiniApps to a Role [SAP Library].)

   The URL needs to have the following syntax (see URL Templates [SAP Library]):

   ```
   <web_protocol>://<web_server>/<web_path_prefix>/<service_file>/!?~language=<language>&~client=<client>;LOGSYS=<logical system name>
   ```

   For example, if you use the variable assignments as shown in the table below, the URL is:

   ```
   HTTPS://host1.mysap.company.com/scripts/wgate/webgui_public.srvc/!?~language=EN&~client=000;LOGSYS=bieclnt000
   ```

URL Variables

Variable	Definition	Value to use for the above example
`<web_protocol>`	Protocol to use.	HTTPS
`<web_server>`	Host name and domain for the system where the MiniApp is located.	`host1.mysap.company.com`
`<web_path_prefix>`	Path where the ITS WGate component is located.	`scripts/wgate`
`<service_file>`	Name of the service file.	`webgui_public.srvc`
`<language>`	2-character language code	EN (English)
`<client>`	SAP System client where the MiniApp is located.	000
`<logical system name>`	Logical system name where the MiniApp is located.	`bieclnt000`

Define variables that used for all URLs, for example `<web_protocol>`, `<web_server>` and `<web_path_prefix>`, in the Customizing table SSM_VAR. For more information, see Defining Variables for URL Generation [SAP Library].

You define the `<logical system name>` when registering the local system in the Workplace. (See Registering Logical Systems [SAP Library].)

Protecting User Information

SSO cookies and mySAP.com logon tickets are used as authentication "tokens" and should therefore be protected from unauthorized use.

The measures we take for protection include:

- SSO cookies and mySAP.com logon tickets are only sent to Web servers located in the same DNS domain where the cookie was set or the ticket was issued. The user's authentication information is therefore not available to services whose Web servers exist in a domain outside of the mySAP.com Workplace domain (determined by the DNS name of the Workplace's Web server).
- SSO cookies and mySAP.com 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 Workplace services after the user closes his or her Web browser.
- SSO cookies and mySAP.com logon tickets expire after a designated period of time (default = 60 hours). You can change this value in the designated parameters.

  When using SSO cookies, use the parameter `~usertimeout` in the Workplace Server's global service file (`global.srvc`) on its Internet Transaction Server (ITS) to change this value. If you use mySAP.com logon tickets, use the profile parameter `login/ticket_expiration_time` on the Workplace Server's application server.

  (See SAP Note 337794 for information about how to set the expiration time in minutes.)
- We encrypt the contents of SSO cookies and mySAP.com logon tickets to prevent them from being read by unauthorized persons. A cryptographic checksum also makes sure that any changes made to the SSO cookies or mySAP.com logon tickets are detected.

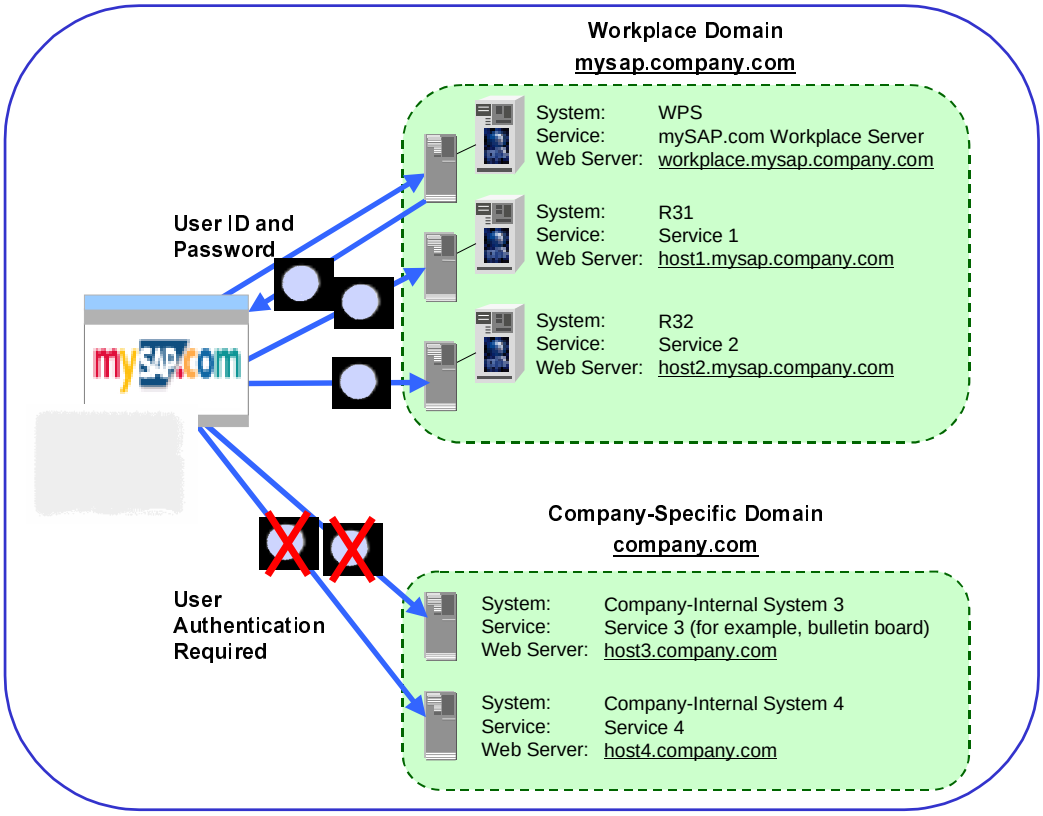
The measures you should take include:

- Use HTTPS in the Workplace.
- Define a specific DNS domain for the mySAP.com Workplace. Place your Workplace services in this domain and place other services that do not need access to the mySAP.com user authentication information in a separate domain. For more information, see A Sample Domain Infrastructure [Page 45].
- Your end users should protect access to their open Web browsers when they are logged on to the mySAP.com Workplace. In particular, they should activate password-protected screen savers on their frontend clients.

A Sample Domain Infrastructure

SSO cookies and mySAP.com logon tickets are only available to Web servers existing in the same DNS domain as the server that initially set the cookie or ticket (that is, the Web server used for the Workplace Server). If the user accesses a service where the Web server is located in a different DNS domain, he or she must be explicitly authenticated in the new domain. See the graphic below:

Sample Domain Infrastructure



Mary enters her mySAP.com Workplace by logging on to the Workplace Server, which is located at `workplace.mysap.company.com`. She uses her SAP user ID and password for authentication. After successful authentication, the Workplace Server sets Mary's SSO cookie in her Web browser.

From her Launch Pad, she accesses Service 1, which is located at `host1.mysap.company.com`. Because Service 1 is located in the same domain as the Workplace Server, the SSO cookie is sent with the request. Service 1's system can use the SSO cookie to authenticate Mary and no user intervention is necessary.

The same applies to Service 2, which is located at `host2.mysap.company.com`.

However, when Mary accesses a service located in a different domain, for example, Service 3 at `host3.company.com` or Service 4 at `host4.company.com`, she must log on to the server in the new domain and authenticate herself using the authentication method required (for example, her user ID and password for that domain).

We recommend you use this DNS domain infrastructure to separate Workplace services from other company-internal services (for example, a company-internal bulletin board). Place services that do not need access to the user's Workplace authentication information in a separate domain as shown in the above graphic.

In addition, we recommend only placing new services in the Workplace's domain once they have been checked for security by your company's designated security administrator.

If you have existing SAP Systems that already reside in an established domain and that are to be integrated into the Workplace infrastructure, then it is sufficient to place the corresponding Web servers (where the WGate components are hosted) in the Workplace's DNS domain. The AGate hosts and the SAP Systems themselves may reside in the existing domain.

Single Sign-On Using X.509 Client Certificates

Use

This Single Sign-On (SSO) variant makes use of X.509 client certificates [Page 73], which are being used more and more frequently as digital identification cards for authentication purposes across the Internet.

A user who enters the Workplace and presents a valid X.509 client certificate is authenticated on the Workplace's Web server using the Secure Sockets Layer (SSL) protocol. The information contained in the user's certificate is passed on to the Workplace Server, and the user is logged on to the Workplace based on this information. As the user accesses the different services within the Workplace, his or her user information contained in the client certificate is also passed on to the corresponding Workplace component system and he or she is logged on to the system. 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 in the mySAP.com Workplace, 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. For example, you can use the mySAP.com Trust Center to receive the mySAP.com Passport [Page 69] (which is an X.509 client certificate) issued by the SAP CA.

Using SSL for Client Authentication

When using X.509 certificates to log on to the Workplace, users are authenticated on the Workplace's Web servers using the SSL protocol. If the Web server successfully authenticates the user, it passes the information from the user's certificate on to the Workplace Server or component system. Therefore, HTTPS (Hypertext Transfer Protocol over SSL) connections are necessary for the communication between the users' Web browsers and the Web servers.

Secure Network Communications

Because user authentication takes place on the Web server and not on the Workplace Server itself or in the Workplace component systems, you need to use Secure Network Communications (SNC) [Page 70] to establish a secure channel between the Web servers and the Workplace systems. SNC protects the user's information from eavesdropping or manipulation and guarantees that the it securely arrives in the Workplace system.

In addition, SNC is necessary to establish a Single Sign-On environment for access to applications that use SAP GUI for Windows. The reason is that services that use SAP GUI for Windows are not accessed via a Web server and SSL cannot be used for authentication. In this case, the external security product used for SNC provides the authentication mechanisms and establishes the Single Sign-On environment.

Prerequisites

- Users possess valid X.509 client certificates and have imported them into their Web browsers.
- The Web servers used to access the mySAP.com Workplace services are configured to support HTTPS connections and SSL is used between the Web browser and the Web server.
- The Web servers are also configured to trust the Certification Authority (CA) that issued the user certificates.
- SNC is used to establish a secure channel between the Web servers and Workplace systems. It is also used to establish SSO for applications that use SAP GUI for Windows.
- The user's information contained in his or her certificate (namely the Distinguished Name) maps to a valid user ID in each of the Workplace systems.

Features

- Strong authentication is provided using the SSL protocol and PKI technology.
- Users can also produce digital signatures using their client certificates. Therefore, 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 the mySAP.com Marketplace, other intranet services, and Internet services.
- If you use the mySAP.com Trust Center Services, then you can save on administration costs by having certain tasks automated. With this service, your users can automatically receive their mySAP.com Passport from the SAP CA when they log on to the mySAP.com Workplace. Certain user maintenance tasks are also automatically performed by the corresponding transactions. For more information, see the mySAP.com Trust Center Services in SAPNet (http://sapnet.sap.com/tcs).

Constraints

SAP Systems support the X.509 certificate logon as of Release 4.5B. If you have component systems with earlier releases, then you need to rely on Single Sign-On based on user ID and password [Page 10].

Activities

The processes involved when using X.509 client certificates for Single Sign-On in the mySAP.com Workplace are described in detail in the following topics:

- Obtaining the mySAP.com Passport from the mySAP.com Trust Center [Page 49]
- User Authentication: Initial Logon or Accessing a Service via the ITS (X.509) [Page 50]
- User Authentication: Access a Service Using SAP GUI for Windows [Page 53]
- User Authentication: Access a Non-mySAP.com Component or a Service Outside the Workplace (X.509) [Page 52]

Obtaining the mySAP.com Passport from the mySAP.com Trust Center

Purpose

To save on administration costs, mySAP.com Workplace users can automatically receive their mySAP.com Passport from the mySAP.com Trust Center to use in the Workplace.

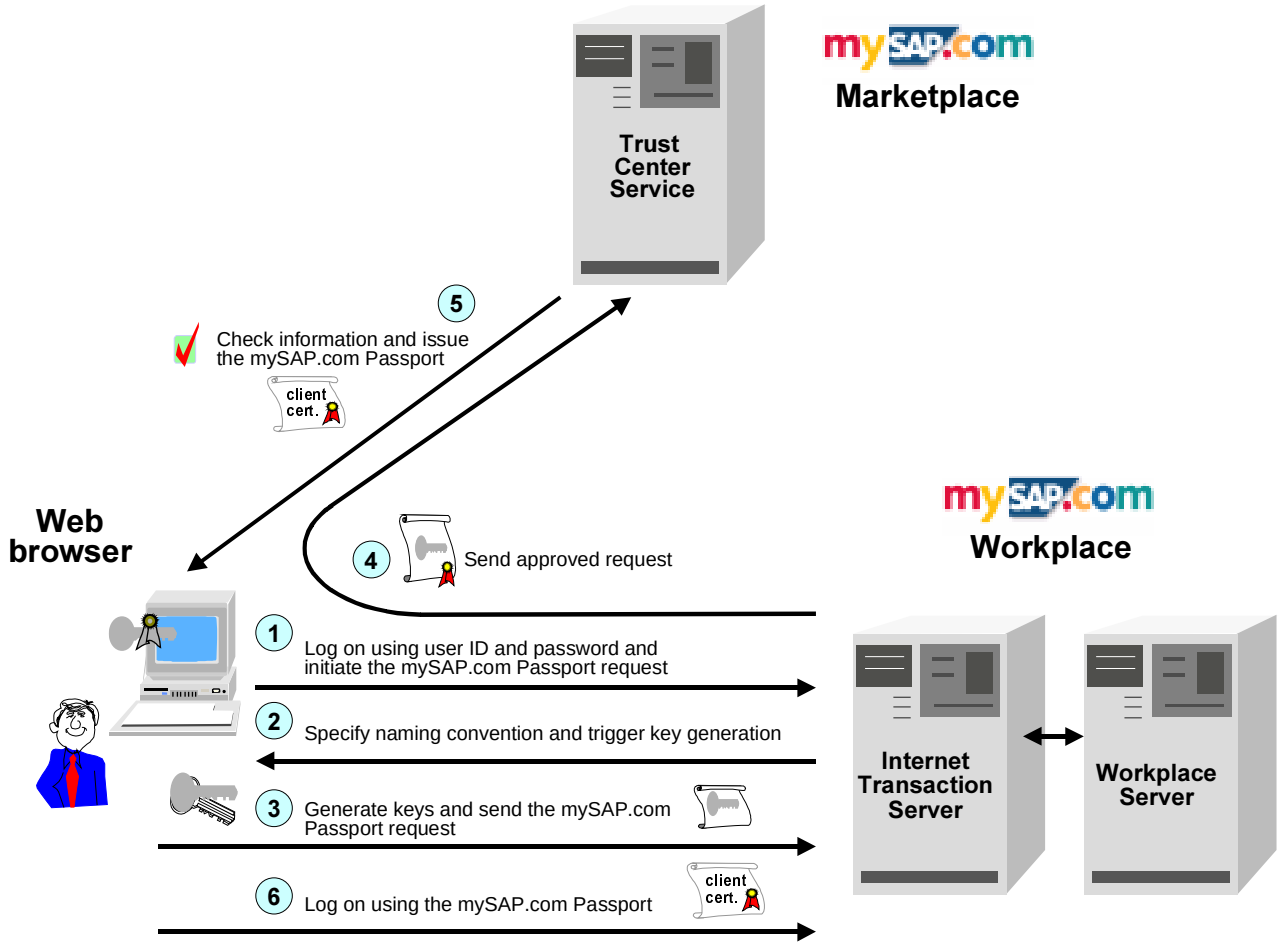
Prerequisites

- The customer must register for this service with the mySAP.com Trust Center Service. As part of the registration process, a naming convention for the user's Distinguished Name must be established. For more information, see the mySAP.com Trust Center Services (10) [Page 73] in SAPNet at http://sapnet.sap.com/tcs.
- The system infrastructure must be set up for using X.509 client certificates. For more information, see Administration Tasks [Page 55].

Process Flow

See the graphic below:

Automatic Distribution of Client Certificates



1. The user logs on to the mySAP.com Workplace using his or her user ID and password for authentication. As part of the logon process, the user confirms that he or she wishes to use the mySAP.com Passport for future logons.
2. The mySAP.com Workplace informs the user's Web browser of the naming convention to use for the certificate and triggers the generation of the user's public-key pair by the Web browser.
3. The Web browser generates the user's public-key pair and the request for the mySAP.com Passport.
4. The mySAP.com Workplace Server approves the request, which is then routed to the mySAP.com Trust Center Service.
5. The mySAP.com Trust Center Service verifies that the naming convention is correct, generates the mySAP.com Passport and issues it to the user. The mySAP.com Passport is then stored in the user's Web browser.
6. The user can then use his or her mySAP.com Passport for subsequent logons to the mySAP.com Workplace or other Internet services that accept the mySAP.com Passport as an authentication mechanism.

User Authentication: Initial Logon or Accessing a Service via the ITS (X.509)

Purpose

This topic describes how end users are authenticated when using the X.509 client certificate authentication mechanism for logging on to the mySAP.com Workplace or when accessing Workplace services via the Internet Transaction Server (ITS). The X.509 client certificate may be the mySAP.com Passport or a certificate issued by a different trusted CA.

Prerequisites

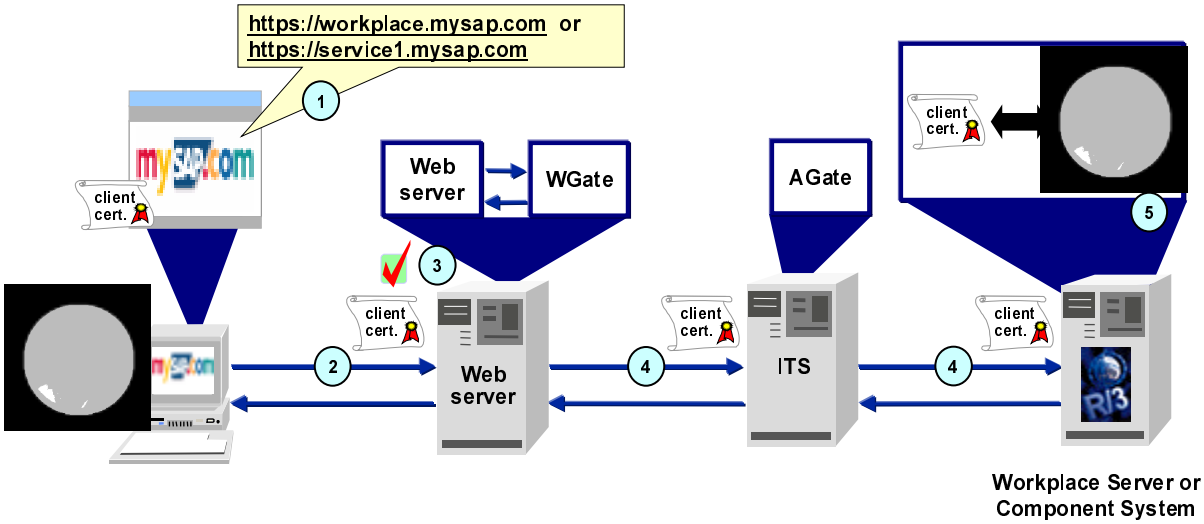
The Workplace must be configured for using client certificates. For more information, see Administration Tasks [Page 55].

In addition, see the prerequisites for Single Sign-On Using X.509 Client Certificates [Page 47].

Process Flow

See the graphic below:

Initial Logon or Accessing a Service in the Workplace via the ITS When Using X.509 Client Certificates for Authentication



1. The user logs on to the Workplace or accesses a mySAP.com service via the ITS from his or her Web browser. (The corresponding URLs must use HTTPS.)
2. The user's client certificate is sent with the request to the corresponding Web server.
3. The Web server uses the SSL protocol to authenticate the user based on the information contained in his or her client certificate.
4. If the user was successfully authenticated by the Web server, the Workplace Server's ITS retrieves the user's information from the client certificate on the Web server and sends it to the Workplace Server or component system.
5. The Workplace Server or component system searches for a SAP System user ID that corresponds to the user information contained 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.

However, if the system cannot correctly map the user to a SAP System user ID, or the SSL authentication on the Web server was not successful, then the system reverts to Single Sign-On Based on User ID and Password [Page 10]. It checks for a valid SSO cookie or mySAP.com logon ticket. If neither are found, then the user is prompted for his or her logon information (user ID and password).

User Authentication: Access a Non-mySAP.com Component or a Service Outside the Workplace (X.509)

Purpose

Users can also use their X.509 client certificates to access non-mySAP.com component systems or services available outside of the mySAP.com Workplace (for example, the mySAP.com Marketplace).

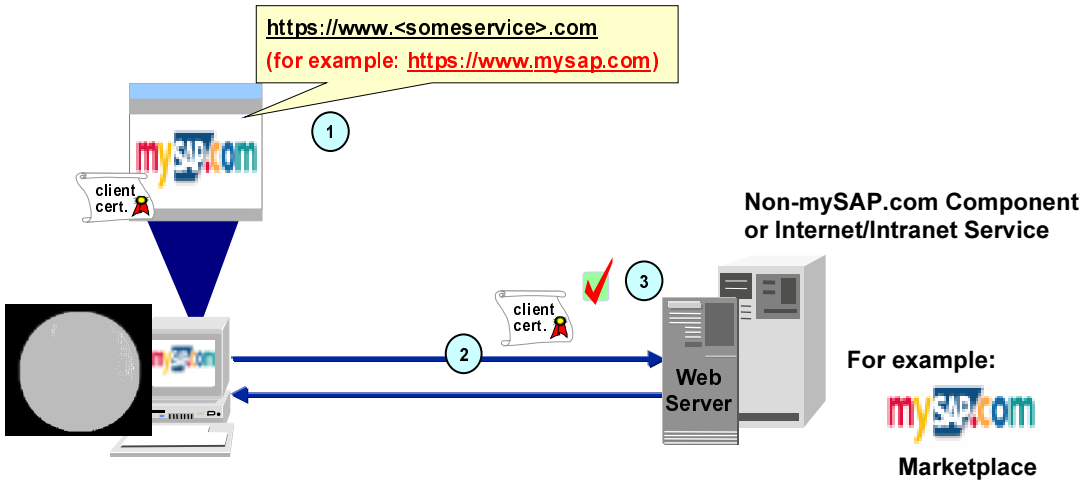
Prerequisites

- The user possesses a valid X.509 client certificate and it is available to his or her Web browser.
- The component or service being accessed supports HTTPS and uses the SSL protocol to authenticate the user.
- The service's Web server recognizes and accepts the Certification Authority (CA) who issued the user his or her certificate.
- Any service-specific configuration tasks have been completed. For example, you may have to define a mapping between the user's information contained in the certificate to a corresponding user ID.

Process Flow

See the graphic below:

Accessing a Non-mySAP.com Component or a Service Outside the Workplace Using X.509 Client Certificates for Authentication



1. The user accesses a non-mySAP.com component or an external Internet or intranet site.
2. If the corresponding Web server recognizes and accepts the CA who issued the certificate, it proceeds to authenticate the user using the SSL protocol.

Result

If the user is successfully authenticated by the Web server, he or she is allowed access to the corresponding service. Further access control and authorizations are determined by the system being accessed.

User Authentication: Access a Service Using SAP GUI for Windows

Purpose

There may be cases where the end user needs to access a service that is only available using the SAP GUI for Windows user interface. In these cases, the user's client certificate that is available to the Web browser cannot be passed along to the corresponding SAP System and therefore cannot be used for the Single Sign-On user authentication.

To establish a Single Sign-On environment in the Workplace that includes these cases, you can use the authentication mechanisms provided by Secure Network Communications (SNC) [Page 70].

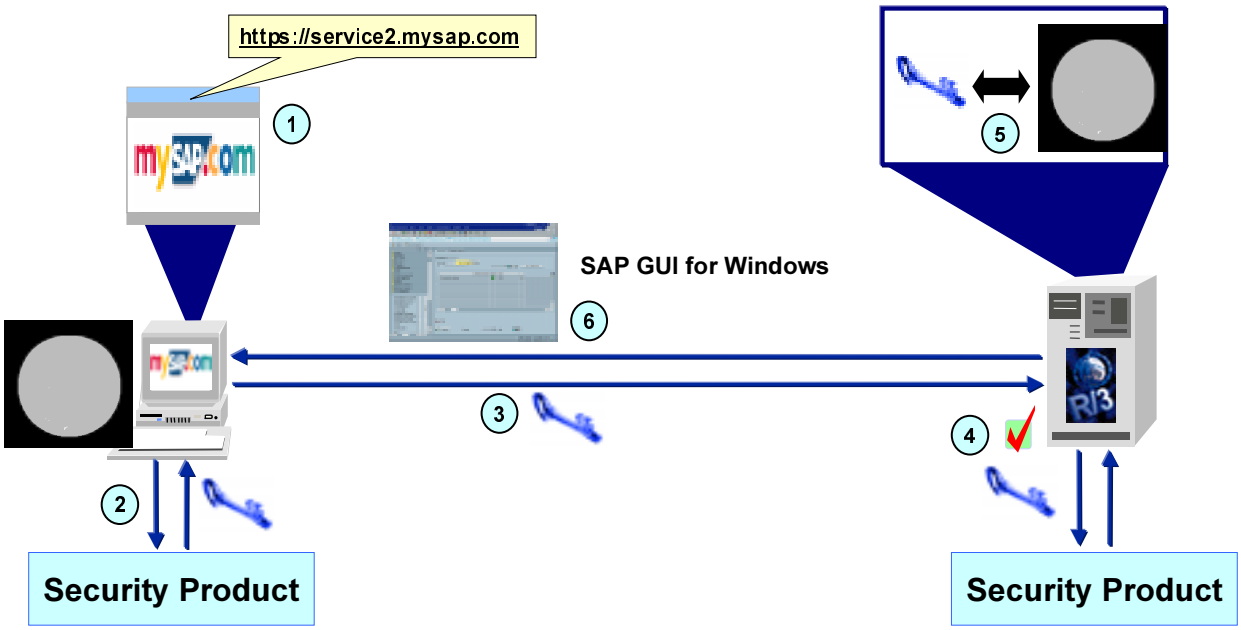
Prerequisites

- SNC requires the use of an SAP-certified external security product (see the SAP Complementary Software Program (9) [Page 73]. This product must be installed and configured on both the SAP System application server(s) and the frontend client(s). Any other product-specific tasks have been performed. For more information, see the SNC User's Guide (5) [Page 73] and the documentation provided by the security product vendor.
- The SAP System components (for example, the application server and the frontend clients) have been configured for using SNC. One of the tasks in the configuration is to establish a mapping between the user's external identification (SNC name) and the SAP System user ID. For more information, see Administration Tasks [Page 55].
- The user must be logged on to the security product before accessing the corresponding Workplace service.

Process Flow

See the graphic below:

Single Sign-On When Accessing a Service in the Workplace Using SAP GUI for Windows



1. The user accesses a service that uses the SAP GUI for Windows user interface.
2. The frontend client obtains the user's SNC authentication information from the external security product. (The user has already authenticated him or herself when logging on to the security product.)
3. The frontend client passes this information to the corresponding SAP System.
4. The SAP System uses the external security product to verify the user's authentication information.
5. The SAP System searches for a SAP System user ID that corresponds to the user's information provided by the security product.

Result

If the user is successfully authenticated and mapped to an SAP System user ID, the user is logged on to the system being accessed and the system starts the SAP GUI for Windows frontend component. No user ID and password entries are required for authentication.

Administration Tasks

The table below shows the administration tasks involved in configuring your mySAP.com Workplace system for using the X.509 client certificate authentication mechanism.

X.509 Certificate Logon Administration Tasks

Component and Tasks	See
Workplace Server and Component System Application Servers • Configure SNC • Configure the use of client certificates • Map users' external IDs to SAP System user IDs	Configuring the Workplace Server and Component System Application Servers [Page 56]
ITS Components • Configure SNC • Configure the use of client certificates • Map users' external IDs to SAP System user IDs	Configuring the ITS Components [Page 59]
Web Servers • Enable HTTPS • Configure the server to use SSL for providing client and server authentication • Specify the Certification Authorities (CAs) the Web server should accept.	Web server documentation
Front End Clients, Workplace Server, and Component System Application Servers • Configure SNC for users that access services using SAP GUI for Windows.	Configuring SNC for Users [Page 63]

In the following topics we describe the configuration for using X.509 client certificates and SNC for Single Sign-On in the mySAP.com Workplace. However, this is only a brief description of the parameters used in this scenario. For more information about these topics, see the SNC User's Guide (5) [Page 73] and the document X.509 Certificate Logon via the ITS (6) [Page 73].

Configuring the Workplace Server and Component System Application Servers

Use

To be able to accept client certificates in the mySAP.com Workplace, you need to configure the Workplace Server and all of the component system application servers for using client certificates and SNC. You also need to maintain the users' external ID (Distinguished Name) defined in their certificates so that the system can determine the correct mySAP.com user ID to use when the user logs on.

The configuration steps are described below.

Prerequisites

- You have installed the security product on the Workplace Server and on each of the component system's application servers.
- You know the AGate's SNC name.

  To find complete information about activating and configuring SNC, see the SNC User's Guide [5] [Page 73]. In this topic, we only include the information relevant when using client certificates for authentication in the mySAP.com Workplace.
- You know the Distinguished Names of the users who will use client certificates to log on to the mySAP.com Workplace.

  The Distinguished Name is **not** the same as the SNC name. It is the name as it is declared in the user's X.509 client certificate. (It does **not** contain a prefix such as `p:` or `s:`.) In addition, when you enter this name in the table USREXTID, note that the entry is case-sensitive and blanks can neither be omitted nor their number increased.

Procedure

On the Workplace Server and on each of the component system's application servers:

1. Activate SNC by setting the following profile parameters:

Parameter	Value	Comment
`snc/enable`	1	Activate SNC on the application server
`snc/gssapi_lib`	Path and file name of the security library	Determined when installing the security product
`snc/identity/as`	SNC name of the application server	Determined when installing the security product
`snc/data_protection/max`	Maximum level of protection to use	Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection
`snc/data_protection/min`	Minimum required data protection level	Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection

Parameter	Value	Comment
`snc/data_protection/use`	Default level of data protection to use	Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection 9: use the value from `snc/data_protection/max`

2. Configure the servers to accept client certificates by setting the following parameters:

Parameter	Value
`snc/extid_login_diag`	1
`snc/extid_login_rfc`	1

3. Specify the AGate's SNC information in the system access control list for SNC (table SNCSYSACL, view VSNCSYSACL, TYPE=E).
   a. Enter the SNC name for the AGate in the *SNC name* field. The *System-ID* field is optional.
   b. Activate the options:
      - *Entry for RFC activated*
      - *Entry for diag activated*
      - *Entry for certificate activated*
   c. Save the data.
4. Create a generic entry for the AGate in the extended user access control list (table USRACLEXT):
   a. Enter an asterisk (*) in the *User* field.
   b. Enter a sequence number in the *Seq.number* field. If this is the only entry in the table for the AGate, then use the sequence number 000. (Sequence numbers are necessary if you create several entries for a single SNC name.)
   c. Enter the AGate's SNC name in the *SNC name* field.
   d. Save the data.

   You receive an entry due to the wildcard entry in the *User* field.

5. Maintain the users' Distinguished Names in the table USREXTID.

   a. Enter the following information in the corresponding fields:

Field	Value	Comment
Type of external ID	DN	Enter in the *Determine Work Area: Entry* dialog box.
Extern.ID	Distinguished Name as found in the user's certificate	
Serial no.	Serial number of the certificate; 000 is the default value	Optional and not currently checked in the system
User	User ID in the mySAP.com Workplace	
Min. date	Earliest date on which the certificate is valid for logging on to the system.	Optional and not currently checked in the system

   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 their use at a later time.

   c. Save the data.

Repeat the procedure on each of the application servers in the mySAP.com Workplace.

Result

The Workplace Servers and component systems can accept X.509 client certificates and can also use SNC protection. The user's identification defined in his or her certificate is mapped to his or her user ID in the mySAP.com Workplace.

Configuring the ITS Components

Use

The ITS components must also be configured to accept X.509 client certificates and to use SNC protection for communicating with the corresponding application server.

The configuration steps are described below.

Prerequisites

- The security product for using SNC has been installed on the AGate and WGate servers. See the product's documentation for more information.

  To find complete information about activating and configuring SNC, see the SNC User's Guide (5) [Page 73]. In this topic, we only include the information relevant when using client certificates for authentication in the mySAP.com Workplace.

- You need to know the SNC names for the AGate and the WGate and the locations of the security libraries on each of their hosts. You also need to know the SNC name of the Workplace Server and component systems' application servers.
- Any other product-specific tasks have been completed. For example, you may have to create security environments and distribute certificates for each component. For more information, see the security product's documentation.

Procedure

Proceed as described below.

The changes made in the following procedure only take effect after you restart the ITS WGate and AGate components.

AGate Hosts (Workplace Server and all Component Systems)

1. Define the following parameters:

Parameter	Value
`Type`	2: Use NISNC based connection (SAP protocol NI plus SNC)
`SncNameAGate`	SNC name of the AGate and ITS Manager
`SncNameWGate`	SNC name of the WGate

   If you use the ITS Administration Tool, make the entries under *Security* → *Network Security*.

   Otherwise, you can make the entries directly in the registry key:

   ```
   KEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual
   ITS>\Connects
   ```

   The AGate and the ITS Manager share the same security environment and SNC name.

2. Make sure the environment variable `SNC_LIB` contains the path and file name of the security product's library.

3. Establish the security environment for each of the components and perform any other product-specific tasks. For example, the component may have to log on to the security product under its own security environment. For more information, see the product's documentation.

   The security product you use for SNC may require you to set certain SNC options in environment variables or Windows NT Registry keys. If you have installed the WGate and AGate on a single host, then you cannot use global environment variables or registry keys for such settings.

   In this case, use the following process-specific registry keys to specify different variable values for each component:

   ```
   HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual
   ITS>\Programs\[AGate|MManager|WGate]\environment\<variable>
   ```

4. In the global service file `global.srvc` (or in the local service files for the services that should accept certificates for logon), set the following parameters:

Parameter	Value	Comment
`~clientcert`	0: Client certificates are not accepted 1: Client certificates are accepted but not required 2: Client certificates are required	This parameter specifies whether you want to deny, accept, or require client certificates.
`~sncNameR3`	SNC name of the application server	This entry activates SNC for the AGate ←→ application server connection and should therefore be the last step you perform in the configuration process.
`~sncNameAGate`	SNC name of the AGate	Optional. This parameter is only necessary in the service file if the AGate is to use a different SNC name for the AGate ←→ application server connection than it uses for the AGate ←→ WGate connection.
`~sncQoPR3`	Quality of protection level to use for the communication	Possible values: 1: authentication only 2: data integrity protection 3: data privacy protection 9: use the value from the application server's profile parameter `snc/data_protection/max` If omitted, the default level of protection is used (as defined in the application server's profile parameter `snc/data_protection/use`)

5. If your WGate resides on the same host, then configure the WGate. Otherwise, restart the Web server and the ITS Manager.

WGate Hosts (Workplace Server and all Component Systems)

1. Define the following parameters:

Parameter	Value
`Type`	2: Use NISNC based connection (SAP protocol NI plus SNC)
`SncNameAGate`	SNC name of the AGate and ITS Manager
`SncNameWGate`	SNC name of the WGate

You can make the entries as follows:

- You can use the ITS Administration Tool. Make the entries under *Security* → *Network Security*.
- For ITS WGate releases up to and including Release 4.6C, you can make the entries directly in the registry key:

  `KEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual ITS>\Connects`

- As of the ITS Release 4.6D, you can make the entries for the WGate in the configuration file `wgate.conf`. Make the entries in the `<instance xxx>` block. (See the example provided later.)

  Although you can configure several WGate instances in a single WGate configuration file, in the current version, the WGates all need to have the same SNC name.

2. Make sure the environment variable `SNC_LIB` contains the path and file name of the security product's library.
3. Establish the security environment for each of the components and perform any other product-specific tasks. For example, the component may have to log on to the security product under its own security environment. For more information, see the product's documentation.

   The security product you use for SNC may require you to set certain SNC options in environment variables or Windows NT Registry keys. If you have installed the WGate and AGate on a single host, then you cannot use global environment variables or registry keys for such settings.

   In this case, use the following process-specific registry keys (prior to Release 4.6D) to specify different variable values for each component:

   `HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual ITS>\Programs\[AGate|MManager|WGate]\environment\<variable>`

   As of Release 4.6D, use the WGate configuration file to set the environment variables.

4. If you use a CGI-BIN WGate, then set the parameter `clientCertAlias` to the name of the CGI variable used by the Web server for client certificates. For example, the Apache Web server uses the variable HTTP_CLIENT_CERT.

   The following shows the corresponding entries in the WGate configuration file for the component system R31:

```
.
.
.
<instance R31>
  available  yes
  tracefile  /var/log/wgate-r31.trc
  tracelevel 1
  <agate>
     Host              host1.mysap.company.com
     PortAGate         sapavw00_r31
     PortMManager      sapavwmm_r31
     Secure            1
     Type              2
     SncNameAGate      “p:CN=R31_AGate, O=SAP-AG, C=DE”
     SncNameWGate      “p:CN=R31_WGate, O=SAP-AG, C=DE”
     available         yes
     multiprocess      yes
  </agate>
</instance>   # R31

<global>
   clientCertAlias HTTP_CLIENT_CERT
   setenv          ENVIRONMENT_VARIABLE_1    value-1
   setenv          SNC_LIB    <path and file name
library>
</global>
.
.
.
```

   For more information, see the ITS Administration Guide (4) [Page 73] in the topic → *WGate Configuration* → *WGate Configuration File.*

5. Restart the Web server, and if the AGate resides on the same host, and you have not already done so, then also restart the ITS Manager.

Web Servers (Workplace Server and all Component Systems)

1. Configure the Web server to accept (or require) client certificates.
2. Make sure the CA that issues the users’ certificates is entered as a trusted root CA on your Web server.

Result

The ITS components can now accept X.509 client certificates for logon and they can communicate with each other and with the Workplace Server and component systems using SNC protection.

Configuring SNC for Users

Use

To be able to use Single Sign-On for access to services that use the SAP GUI for Windows when using the X.509 client certificate scenario, you need to use SNC. The configuration procedure is briefly described below; however, for a complete description, see the SNC User's Guide [5] [Page 73].

You only need to configure SNC for users if they are to use Single Sign-On to access services that use the SAP GUI for Windows.

If you choose not to configure SNC for users, they will be prompted for their user ID and password when they access a service that uses SAP GUI for Windows.

Prerequisites

- The security product used for SNC must be installed on the frontend client.
- SNC has been activated on the application server (see step 1 in Configuring the Workplace Server and Component System Application Servers [Page 56]).

Procedure

On the Workplace Server and the Component Systems' Application Servers: User Maintenance

Enter the users' IDs and SNC names in the SNC user access control list (table USRACL). You can either enter the information in user maintenance (transaction SU01) or you can use table maintenance (for example, transaction SM30) to directly enter the SNC names in the table.

The SNC name is **not** the same as the X.509 Distinguished Name. It may contain the same information, but contains a prefix (such as `p:` or `s:`).

Note also, that when you enter this name in the table USRACL, the entry is case-sensitive and blanks can neither be omitted nor their number increased.

The *Insecure communication permitted* indicator is only effective if the profile parameter `snc/accept_insecure_gui` = U (available as of Release 4.0) and allows the user to log on to the system either with SNC or without. (To set up the system to allow all users access either with or without SNC, set `snc/accept_insecure_gui` to the value 1.)

On the Frontend Clients: Configuring SAP Logon

When a user accesses a service that uses SAP GUI for Windows from the mySAP.com Workplace, the information needed to establish the connection to the component system is obtained from the SAP Logon configuration. Therefore, you have to configure the SAP Logon entries for the Workplace Server and the component systems accordingly. Perform the following on the frontend clients:

1. Make sure the environment variable `SNC_LIB` contains the path and file name of the security library provided by the external product.
2. Enter the SNC options in the *Advanced Options* for the Workplace Server and each of the component system (or group) entries in the SAP Logon list.
   a. Activate SNC by selecting the *Enable Secure Network Communication* indicator.
   b. Select a level of protection (*Authentication*, *Integrity*, *Encryption*, *Max. available*).

      The default is *Max. available*. We recommend you use this value.
   c. Enter the SNC name of the application server. Note the following:
      - If you created the entry using *Server Selection* and SNC is already active on the application server, then the server's SNC name is automatically provided in the field.
      - If you created the entry using *Group Selection*, then you can only enter the SNC options if SNC has been activated for the group. In addition, a temporary SNC name is entered in the field, but you cannot change it. The actual SNC name of the application server is retrieved by the message server when the connection is established.

Result

The user can access the corresponding system from the mySAP.com Workplace without having to re-authenticate him or herself using user ID and password. Note that the user does have to log on once to the external security product before being able to access the component system using SSO.

Post-Configuration Checks: X.509 Client Certificates

If the Single Sign-On function does not function correctly after configuring the mySAP.com Workplace, perform the checks as described in the tables below.

Workplace Server

Location	Necessary Configuration
Tables TWPURLSVR and USRURLSVR (Web server definitions)	HTTPS must be defined as the protocol to use for the component systems' Web servers where certificates are used. The HTTPS port for each of these servers must be correctly entered in the URL.

Workplace Server and Component System Application Servers

Location	Necessary Configuration
Profile parameters and tables used for SNC	The application server must be configured and enabled for using SNC. For more information, see the SNC User's Guide (5) [Page 73].
Profile parameters	The application server must be configured for accepting client certificates: • `snc/extid_login_diag` = 1 • `snc/extid_login_rfc` = 1
Table SNCSYSACL (view VSNCSYSACL, type = E)	An entry must exist for the application server's ITS AGate component.
Table USRACLEXT	A generic entry must exist for the application server's ITS AGate component. (This entry should contain a wildcard (*) in the *User* field, a sequence number in the *Seq.number* field, and the AGate's SNC name in the *SNC name* field.)
Table USREXTID (view VUSREXTID, type = DN)	The Distinguished Names for all users who log on to the system using X.509 client certificates must be entered correctly.
Table USRACL	The SNC names for users who access the system using SAP GUI for Windows must be entered correctly.

ITS AGate Hosts

Location	Parameter	Value
Registry key `KEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual ITS>\Connects`	`Type`	2 (SNC connections are used)
	`SncNameAGate`	AGate's SNC name
	`SncNameWGate`	WGate's SNC name
Environment Variable	`SNC_LIB`	Path and file name of the security product's library used for SNC
Service file `global.srvc` (or in all service files where the X.509 client certificate logon should be accepted)	`~clientCert`	Possible values: 0: Client certificates are not accepted 1: Client certificates are accepted but not required 2: Client certificates are required
	`~sncNameR3`  Because this parameter activates SNC for the AGate ←→ application server connection, setting this parameter should be the last step in the SSO configuration process.	Corresponding application server's SNC name

ITS WGate Hosts

Location	Parameter	Value
Registry key `KEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<virtual ITS>\Connects` or, as of Release 4.6D, in `wgate.conf`	`Type`	2 (SNC connections are used)
	`SncNameAGate`	AGate's SNC name
	`SncNameWGate`	WGate's SNC name
	`clientCertAlias`	For CGI-BIN only: Name of the environment variable the Web server uses for certificates.
Environment Variable	`SNC_LIB`	Path and file name of the security product's library used for SNC

In addition, make sure any product-specific tasks have been correctly completed. For example, you may need to create credentials for the AGate or WGate or specify values in other environment variables or registry keys.

Web Servers

Make sure:

- The Web servers in the Workplace are configured to accept or require client certificates.
- The CA that issued the users their client certificates has been specified as a trusted CA.
- If necessary, access control lists have been maintained.

Web Browsers

Make sure:

- Users have imported their certificates into their Web browsers.
- The issuing CA for the Web servers' certificates is specified as a trusted CA in the user's Web browser.
- If users access services using SAP GUI for Windows, then make sure that:
  - The SNC information in SAP Logon has been correctly maintained.
  - The environment variable `SNC_LIB` on the front end contains the location of the security product's library.
  - Any other product-specific tasks have been completed.
  - The user logs on to the security product before accessing the service.

Additional Information

For more information about troubleshooting problems with Single Sign-On in the mySAP.com Workplace, see the SAP Note 318515.

For additional documentation, see also:

- SNC User's Guide (5) [Page 73]
- X.509 Certificate Logon via the ITS (6) [Page 73]
- Web server documentation
- Security product documentation

Appendix 1: Terminology and Abbreviations

Certificate List

Definition

A list that contains the information from other users' or system components' public-key certificates (namely the public key).

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 the mySAP.com logon ticket for Single Sign-On in the mySAP.com 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 either sends 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.

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.

mySAP.com Logon Ticket

Definition

The mySAP.com logon ticket is a piece of information used to provide Single Sign-On in the mySAP.com Workplace.

Use

The mySAP.com logon ticket is issued to a user when he or she logs on to the mySAP.com Workplace. It is then sent to the component systems when the user accesses the various Workplace services. The component systems verify the validity of the logon ticket before allowing the user access to the system‘s services.

Before the Workplace server issues the mySAP.com logon ticket to 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 mySAP.com logon ticket contains the following information:

- Version
- Expiration time

  The mySAP.com 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
- Workplace Server identifier
- Workplace Server's public-key certificate (optional)
- Workplace Server's digital signature

  The Workplace server's digital signature is verified by the component system when the user accesses the corresponding service. The digital signature guarantees that the Workplace server issued the mySAP.com logon ticket for the user and that the contents have not been changed.

mySAP.com Passport

Definition

X.509 client certificate [Page 73] issued by the mySAP.com Trust Center.

Use

The mySAP.com Passport is used for user authentication with mySAP.com.

mySAP.com Trust Center

Service available with mySAP.com that issues the mySAP.com Passport to mySAP.com Workplace users.

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 (8) [Page 73].

Secure Network Communications (SNC)

SNC is a software layer in SAP Systems that provides an interface to an external security product.

The security product provides for secure communications between system components by using strong authentication mechanisms and encryption for integrity and privacy protection.

The security product used must be certified for use by the SAP Complementary Software Program (CSP). For more information, see the CSP Program in SAPNet: BC-SNC interface (9) [Page 73].

As an alternative, you can use the Microsoft Windows NT LAN Manager Security Support Provider (NTLMSSP) as the security provider. Note however, the Microsoft Windows NTLMSSP provides for authentication only and does not offer the full range of SNC protection.

For more information, see the SNC User's Guide (5) [Page 73].

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 70] 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:

- http://www.netscape.com/security/techbriefs/ssl.html
- http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

SSO Cookie

Definition

A piece of information stored in the user's Web browser used for authentication in the mySAP.com Workplace.

Use

When using SSO cookies, the Workplace Server's Web server sets a user's SSO cookie in his or her Web browser when he or she initially logs on to the mySAP.com Workplace. When the user accesses any of the various systems available in the mySAP.com Workplace, the SSO cookie is passed to the corresponding system. The cookie provides the system with the information necessary to authenticate the user.

SSO Personal Security Environment (SSO PSE)

Definition

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

Use

The mySAP.com Workplace Server uses its SSO PSE to digitally sign users' mySAP.com logon tickets issued for Single Sign-On in the Workplace.

The mySAP.com component systems use their SSO PSEs to verify the Workplace Server's digital signature when users present their mySAP.com logon tickets for access to the systems.

Structure

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

On the Workplace Server, this information includes:

- The Workplace Server's public-key certificate
- The Workplace Server's private key

On the component systems, this information includes:

- The Workplace Server's public-key certificate
- The component system's certificate list

Integration

Each application server in the mySAP.com Workplace 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

System or Server	Release	Name	Location	Comment
Component system application servers	< 4.6C	`SAPSSO2.pse`	Directory specified in the profile parameter `DIR_PROFILE`	
Component system application servers and Workplace Server	>= 4.6C	`SAPSYS.pse`	`<instance directory>/sec`	In this case, the SSO PSE is the system PSE [Page 72].

System PSE

Personal Security Environment (PSE) for the mySAP.com Workplace Server and component systems.

The system PSE is created during the system's installation process and contains the system's security information (for example, the public-key pair). In Release 4.5A component systems, each application server receives its own system PSE. For the Workplace Server and component systems as of Release 4.5B, the system creates a single system PSE and distributes it to all of the system application servers.

X.509 Client Certificate

Definition

A digital document that acts as a user's digital identification card on the Internet.

The 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

X.509 client 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) [Page 68] guarantees the certificate owner's identity and approves or issues the certificate to the user.

Specifically, you use client certificates as follows:

- You use your own certificate to identify yourself to others.
- You use someone else's certificate to verify their digital signatures.

For more information, see Public-Key Technology (8) [Page 73].

Appendix 2: Sources of Additional Information

Sources of additional information you are likely to need when configuring your system for using Single Sign-On in the mySAP.com Workplace include:

Ref.	Source	Location
1	*mySAP.com Workplace Installation Guide*	SAPNet: http://service.sap.com/instguides → *mySAP.com Workplace*
2	*mySAP.com Workplace: Configuration and Administration Overview*	SAPNet: http://service.sap.com/workplace SAP Library: *mySAP.com Workplace* → mySAP.com Workplace: Configuration and Administration Overview [SAP Library]
3	*SAP@Web Installation Guide*	SAPNet: http://service.sap.com/instguides → *R/3 Standard* → *<Release>*
4	*ITS Administration Guide*	SAP Library: *Basis Components* → *Frontend Services (BC-FES)* → *ITS / SAP@Web Studio* → ITS Administration Guide [SAP Library]
5	*SNC User's Guide*	SAPNet: http://service.sap.com/security → *Secure Network Communications*
6	*X.509 Certificate Logon via the ITS*	SAPNet: http://service.sap.com/security → *Secure Network Communications* or → *Internet Applications Security*
7	*SSF User's Guide*	SAP Library: *Basis Components* → *Security (BC-SEC)* → Secure Store & Forward / Digital Signatures (BC-SEC-SSF) [SAP Library]
8	*Public-Key Technology*	SAP Library: *Basis Components* → *Security (BC-SEC)* → *Secure Store & Forward / Digital Signatures (BC-SEC-SSF)* → Public-Key Technology [SAP Library]
9	SAP Complementary Software Program	http://www.sap.com/csp (for SNC, see: http://www.sap.com/products/compsoft/scenarios/bc/bcsnc.htm
10	mySAP.com Trust Center Service	http://service.sap.com/tcs
11	MiniApps Community	http://www.sap.com/miniapps
12	SAP Note 318515: Collective Note: SSO Problems in the mySAP.com Workplace	
13	SAP Note 304450: mySAP.com logon tickets in external programs	
14	SAP Note 177895: Refitting the mySAP.com Single Sign-On capability	
15	SAP Note 337794: Validity of mySAP.com Logon Tickets	

In addition, you need the documentation for your Web server and, if you use SNC, you also need the documentation for the security product that you use.