SAP AG
Neurottstr. 16
D-69190 Walldorf

Security

X.509 Certificate Logon via the ITS

Security

Version 1.3: English

September 17, 1999

Copyright

Copyright

Contents

Contents

Style Conventions

The following table explains the meanings of the various formats, symbols, and standard notations used in this document.

This text format	helps you identify
Screen Text	words or characters you see on the screen (this includes system messages, field names, screen titles, menu names, and menu items).
`User Entry`	exact user input. These are words and characters you type on the keyboard exactly as they are in the documentation.
`<Variable User Entry>`	variable user input. Pointed brackets indicate that you replace these variables with appropriate keyboard entries.
ALL CAPITALS	report names, program names, transaction codes, table names, ABAP language elements, file names, and directories.
Book Title	cross-references to other books or references.
KEY name	keys on your keyboard. Most often, function keys (for example, F2 and the ENTER key) are represented this way.
`Technical Object Name`	names of technical objects outside of the SAP System (for example, UNIX or Windows NT filenames or environment variables).

Icons in Text

Icon	Meaning
	an Example. Examples help clarify complicated concepts or activities.
	a Note. Notes can contain important information like special considerations or exceptions.
	a Caution. Cautions help you avoid errors such as those that could lead to data loss.

Introduction

In Release 3.0D, we introduced the SAP Internet Application Components (IACs) to enable you to offer certain business scenarios to Internet (or Intranet) users. By implementing IACs, users can access your SAP Systems from the Internet or Intranet to perform business to business, customer to business, or company-internal processes. For example, you can publish an online company product catalog or create an employment opportunities site.

Internet Transaction Server

To integrate SAP Systems with the Internet, we have implemented the SAP Internet Transaction Server (ITS). The ITS allows you to perform your tasks in the SAP Systems using a Web browser as the user interface. It controls the communications and makes the necessary data format conversions between the Web server and the SAP System.

User Context

To establish the context under which the IAC should run, each Internet application has its own service file. The service file contains information such as the host name of the application server, the client in the SAP System, or the language. You can also use a global service file to specify default information for all of your IACs. Entries in an application-specific service file override those in the global service file.

The IAC also establishes the user context depending on entries in the service file. There are two main scenarios:

- Service User Scenario

  The IAC establishes a service user if there is a user and password entry in either its own local service file or in the global service file. The service user must have a user master record and authorizations in the corresponding SAP System. Internet users who call the IAC log on to the SAP System under the service user ID and work in the SAP System using its authorizations.

- Named User Scenario

  If no user and password entries exist in either of the service files, then the IAC requests the logon information from the user in an HTML logon screen. The user logs on to the SAP System by providing his or her user ID and password (or client certificate). The user session runs under his or her user account in the SAP System and he or she must have the appropriate authorizations to be able to process the IAC.

  

  The application decides which scenario it uses. An application designed for service users cannot also use named users.

Client Certificate Authentication for Named Users

It is becoming increasingly more popular for Internet users to authenticate themselves on Web servers using client certificates, and as of Release 4.5B, we further integrate SAP Systems into the Internet world by supporting the use of this common practice. When accessing SAP Internet applications that require named users, Internet users who have authenticated themselves on the Web server using their client certificates can also log on to the corresponding SAP System over the ITS without having to provide further authentication. As with the standard named-user scenario, the user session runs under the user ID of the certificate owner and not under a service user.

Prerequisites for Using this Document

This document describes how you can set up your SAP System and the ITS to accept X.509 client certificates for user authentication. It describes the logon process and the administration measures that are necessary to support it. To effectively use this document, you should be familiar with the SAP System's user and system administration, as well as the ITS architecture and administration.

Terminology and Abbreviations

You should be familiar with the following terms and abbreviations:

- **HyperText Transfer Protocol (HTTP)**

  Application-level protocol used in Internet communications. The HyperText Transfer Protocol controls the communication between the Web browser (HTTP client) and the Web server (HTTP server).

- **Secure Sockets Layer (SSL) protocol**

  Protocol that uses strong authentication mechanisms and encryption to secure data being transferred over the Internet.

- **HTTPS**

  HTTP over SSL. Data packets transferred across a HTTPS connection are encrypted using SSL. When using HTTPS, you also have the option of requiring strong authentication for both the client and the server sides of a HTTP connection.

- **Client certificates / X.509 client certificate**

  A digital document that contains the information necessary to prove a user's identity as well as for encrypting and decrypting messages. The most widely used format for client certificates is the X.509 standard.

- **Certification Authority (CA)**

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

- **Internet Application Component (IAC)**

  Complete business solution for linking SAP Systems to the Internet. Internet Application Components allow you to run your company's business processes from the Internet (or within your Intranet). Internet users execute their tasks in the SAP System using a Web browser as their user interface.

- **Internet Transaction Server (ITS)**

  Interface between SAP Systems and the Internet. When an Internet user starts an Internet Application Component (IAC) from a Web browser, the request is passed to the HTTP server. The HTTP server transmits the request to the Internet Transaction Server (ITS), which sets up a connection to the SAP System. Once a connection has been established, the ITS controls the communication and the data exchange between the SAP System and the HTTP server. The ITS consists of several components including the WGate, the AGate, and the ITS Manager.

- **WGate**

  ITS component located on the Web server. The WGate controls the communication between the Web server and the AGate component of the ITS. Because the Web server ←→ WGate communication uses the HTTP(S) protocol, and the WGate ←→ AGate communication uses SAP-defined protocols, the WGate is needed to make the protocol conversions necessary for successful communication.

- **AGate**

  ITS component located on the main ITS server. The AGate controls the communication to and from the SAP System application server. It receives the data from the WGate and converts it to the SAP DIAG protocol or RFC, and vice versa. It also handles the logon process to the SAP System application server.

- **ITS Manager**

  A unit similar to the message server in an SAP System. It manages the AGates and their current workload for load balancing. For example, it starts new AGates if the load requirements demand it, or it restarts an AGate that terminated unexpectedly.

- **Secure Network Communications (SNC)**

  Software layer in SAP Systems that enables the SAP Systems to communicate with an external security product. The external product can protect the communication links between the components of the SAP System. In addition, you can use features provided by the security product to complement and enhance the standard functions already provided by the SAP System. For example, you can apply encryption to the data communications between the SAP System components and the ITS components.

Reference Material

You should also have the following documentation available for further reference:

- *SNC User's Guide*, Version 1.2

  The *SNC User's Guide* is available in SAPNet. Use the alias *systemmanagement* and then choose *Security* → *Secure Network Communications* (for example, see http://sapnet.sap.com/systemmanagement).

- *R/3 Security Guide VOLUME II: R/3 Security Services in Detail, Chapter 2-3: Network Infrastructure* and *Chapter 2-10: Special Topics*

  The *R/3 Security Guide* is available in SAPNet. See the alias *securityguide.*

- *SAP@Web Installation Guide,* Releases 3.0D to 4.5B, Material Number: 51006024

  The *SAP@Web Installation Guide* is also available in SAPNet. See the alias *instguides* and then choose the appropriate release.

- SAP library: *Internet Transaction Server*
  - Release 4.5B: *CA – Cross-Application Components* → *Business Framework Architecture* → *Web Basis*

    (The path in other releases may vary.)

- Documentation on your Web server
- Documentation for the security product that you use for SNC

Logon to the SAP System using Client Certificates

Using client certificates to log on to SAP Systems via the ITS is a new usability and security feature for the SAP Internet Application Components (IACs). Internet users who posses valid client certificates and authenticate themselves on the Web server (using SSL) can access SAP IACs via the ITS without having to provide further authentication. This feature is available for those IACs that use named users in the SAP System instead of the service user scenario.

Prerequisites

There are several administration tasks that you need to perform before being able to use client certificate logons over the ITS. Figure 1 shows the elements and components that are involved in each of these tasks. A description of each task follows.

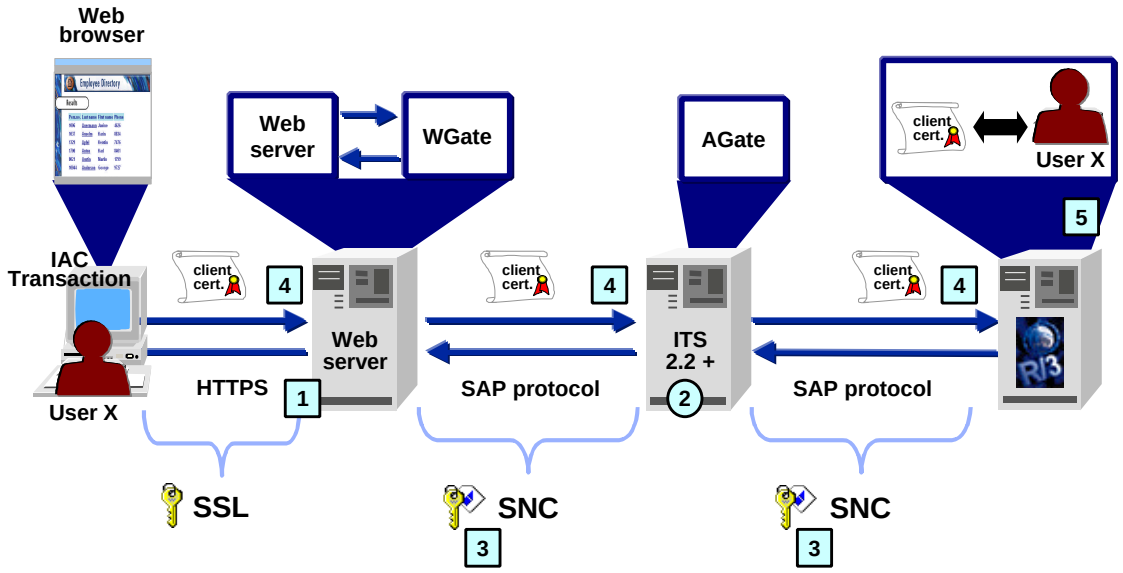

Figure 1: Prerequisites for using Client Certificates for Logon via the ITS

1. You need to enable HTTPS connections on the Web server and configure it to authenticate users' client certificates. For more information, see the section titled *Configuring the Web Server* and your Web server documentation.

   When using client certificates for logon to the SAP System, **the user authentication process occurs on the Web server.** The Internet user's authentication in the SAP System is based on a trust relationship. The SAP System itself does not additionally verify the client certificate; it **trusts** that the Web server has authenticated the user. Therefore, it is very important to configure your Web server correctly.

2. You need to install the ITS version 2.2 or higher.

   We do not describe the ITS installation process in this document. Refer to the *SAP@Web Installation Guide* for more information.

   

   We also highly recommend that you protect the ITS network by using firewalls and SAProuters. For information on how to configure the firewalls and SAProuters, see the *R/3 Security Guide VOLUME II: R/3 Security Services in Detail, Chapter 3: Network Infrastructure* and *Chapter 10: Special Topics → Protecting R/3 Internet Application Components*.

3. You need to use Secure Network Communications (SNC) to guarantee secure communications (to include authentication) between the WGate and the SAP System.

   SNC requires the use of an external security product to provide its protection. There are three levels of protection that are available with SNC: authentication, integrity, and privacy protection. To receive integrity and privacy protection, you need to use a security product that has been certified by the SAP Complementary Software Program (CSP™). For authentication only, you can use the Microsoft NT LAN Manager Security Support Provider (NTLMSSP).

   

   The Microsoft NTLMSSP offers authentication only. If you use it as the security provider, then you do not have any integrity or privacy protection for the communication between the WGate and the SAP System. Because user authentication in the SAP System in this scenario is based on a trust relationship, we also recommend protecting the communications from manipulation, which requires the complete SNC solution. A certified security product can guarantee not only the user's authentication; it can also guarantee the integrity of the client certificate once it has reached the SAP System.

   You can find information on both scenarios, as well as a complete description on activating and configuring SNC, in the *SNC User's Guide*. For configuration information specific to the client certificate logon scenario, see the sections in this document titled *Configuring the ITS Components* and *Configuring the SAP System's Application Server*.

4. You need to configure the SAP System and the ITS for using client certificates. For details on the configuration, see the sections *Configuring the ITS Components* and *Configuring the SAP System's Application Server*.

5. You need to enter the external identifications for the users who use client certificates in the SAP System. See the section titled *Maintaining the User's External Identification in the SAP System* for details.

Process Flow

Figure 2 shows an overview of the logon process using client certificates over the ITS.

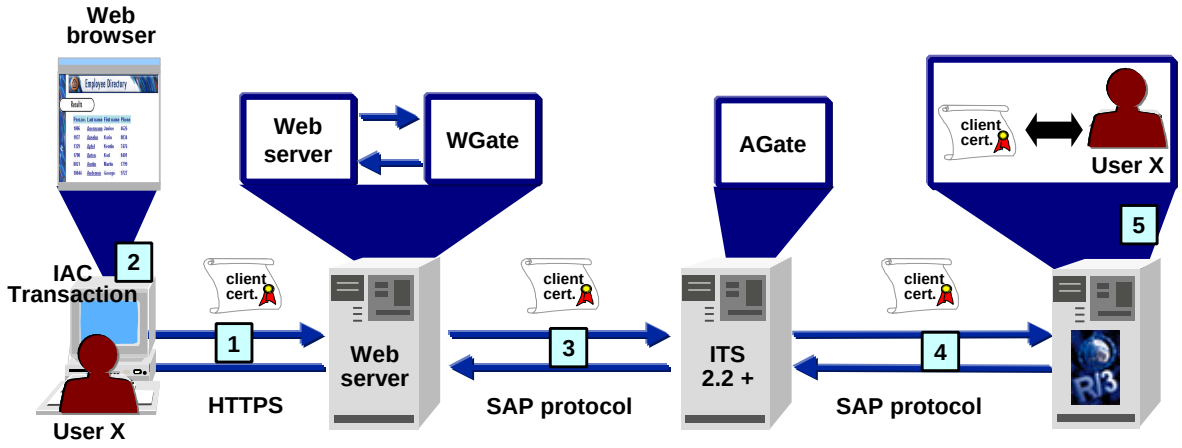

Figure 2: Logon via the ITS Using Client Certificates

1. The Internet user authenticates him or herself on the Web server using his or her client certificate (using SSL).

2. He or she then accesses an IAC transaction.

3. If the user's authentication on the Web server was successful, the ITS WGate passes the user's client certificate from the Web server to the AGate.

4. The AGate establishes the connection to the SAP System's application server and passes the client certificate on to the SAP System.

5. If the system can uniquely identify the owner of the client certificate as a user in the SAP System, then it logs the user on under the SAP System user ID and continues processing the IAC. If not, then:

   - If the logon is a dialog connection, and certain information cannot be resolved (for example, if the SAP System client is not available, or if the certificate belongs to more than one user in the SAP System), then the user is prompted for the information.
   - If the logon occurs using RFC, and the client or user cannot be determined, then the connection terminates with an error.

Result

The Internet user is logged on to the SAP System under his or her user ID, without having to provide further authentication.

Administration Tasks

You need to perform the following administration tasks to enable SNC and the use of X.509 client certificates for logging on to the SAP System via the ITS:

- **Configure the Web Server**
- **Configure the ITS Components**
- **Configure the SAP System's Application server**
- **Maintain the User's External Identification in the SAP System**

We describe these tasks in the following sections.

Configuring the Web Server

1. Enable HTTPS on the Web server and configure it to accept certificates that you trust.

   The exact procedure for this step depends on your Web server and the operating system that you use. Refer to the documentation provided by your vendor for more information.

   

   This step is very important! When Internet users use client certificates for logging on to the SAP System over the ITS, they are not further authenticated in the SAP System. The SAP System makes sure that the user has an account, but it trusts that the Web server has authenticated the user and accepts the client certificate without performing any further verification.

   In addition, the SAP System does not verify the issuer of the certificate. If a user possesses more than one certificate issued from different Certification Authorities (CAs), but they contain the same identification, the SAP System does not detect a difference between the certificates.

   Therefore, we recommend that you take special care when configuring your Web server. For example, you could establish your own CA and configure your Web server to only accept certificates that you have issued.

2. Configure your Web server to pass the certificate on to the WGate.

   This step also depends on the Web server and the operating system that you use. Again, refer to your Web server documentation for more information.

Configuring the ITS Components

Prerequisites

- The ITS components have been installed. See the *SAP@Web Installation Guide*.
- The security product for using SNC has been installed on the AGate and WGate servers. See the product's documentation for more information.
- 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 SAP System's application server.
- Any other product-specific tasks have been completed. For example, you may have to create security environments and distribute certificates for each component. Again, refer to the product's documentation for more details.

Procedure

1. Enter the following values in each of the component's configuration:

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

   Depending on your environment, you can make the entries with the following methods:

   - If you are using the ITS Administration Tool, then make the entries under *Security* → *Network Security*.
   - Otherwise, make the entries 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 that the path and filename of the security product's library are specified in the environment variable `SNC_LIB` on both the AGate and WGate hosts.

3. Establish the security environment for each of the components.

   This step is product-specific and you need to refer to the security product's documentation. For example, you may have to create and establish security environments for each of the components. The component may then need to logon to the security product under the secure environment.

   

   The security product you use for SNC may require you to set certain SNC options in environment variables or Windows NT Registry keys. Note that 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. For each of the IAC transactions that support client certificate logons, enter the following parameters in the corresponding service file on the AGate server:

Parameter	Value	Comment
`~clientCert`	1	Allow X.509 client certificates for the IAC.
`~sncNameAGate`	SNC name of the AGate	Optional. However, you must specify the SNC name of the AGate in one of the following ways: • Registry entry Use the same SNC name for the AGate as with the WGate ←→ AGate connection. • Entry in the global service file Specify a default SNC name for the AGate for all services that may differ from that in the WGate ←→ AGate connection. • Entry in the local service file Specify a service-specific SNC name for the AGate.
`~sncNameR3`	SNC name of the application server	The entry is mandatory either in the local service file or in the global service file `global.srvc`. An entry in `global.srvc` specifies a default application server SNC name for all services. An entry in a local service file overrides that in `global.srvc`.
`~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`

5. Restart the Web server and the ITS Manager.

The SNC installation process also produces trace files for evaluation purposes. The ITS trace files are `WGate.trc`, `AGate.trc`, and `Mmanager.trc`. After installing SNC on the ITS, you should check these files for errors. If the SNC installation was successfully completed, then each of the files should contain an entry similar to the following example. (Note that some of the information is product-specific, and your entries may contain different information depending on the product that you use.)

Trace File Entries after Successful SNC Installation

```
Fri Aug 08 13:36:17 1997
SncInit(): Trying environment variable SNC_LIB as a
gssapi library name: "c:\program files\secude\secude.dll"
File "c:\program files\secude\secude.dll" dynamically loaded as GSS-
API v2 library.
The internal Adapter for the loaded GSS-API mechanism identifies as:
Internal SNC-Adapter (Rev 1.0) to SECUDE 5/GSS-API v2
```

Result

The ITS components can now communicate with each other and with the SAP System using SNC (provided that SNC is also activated on the SAP System's application server). The ITS is also capable of passing X.509 client certificates to the SAP System.

Configuring the SAP System's Application Server

Prerequisites

- You have installed the security product on the application server.
- You know the AGate's SNC name.

To find complete information on activating and configuring SNC in your SAP System, refer to the *SNC User's Guide*. In this section, we include only the information relevant to the ITS communications.

Procedure

1. Activate SNC on the application server 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
`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 SAP System to accept X.509 client certificates by setting the following profile parameters:

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

3. Specify the AGate's SNC information in the SNC access control list table (table SNCSYSACL, view VSNCSYSACL, TYPE=E). You can access the table using transaction SM30 or in Customizing for *System Administration* under *Management of External Security Systems → Secure Network Communication → Access control lists → Systems → Maintain access control list for R/3 Systems*.

   a) Enter the *System-ID* and the *SNC name* for the AGate.

      The *System-ID* field is optional. The SAP System does not need it to identify the AGate; it uses the SNC name. However, you can assign a system ID to the AGate to improve transparency.

   b) Activate the following options:

      - *Entry for RFC activated*
      - *Entry for diag activated*
      - *Entry for certificate activated*

   c) Save the data.

4. If you use WebRFC, then you also have to create a generic entry in the extended user access control list (table USRACLEXT). This entry allows WebRFC users access to the SAP System using the AGate's SNC-protected connection.

   You can access the table using transaction SM30 or in Customizing for *System Administration* under *Management of External Security Systems → Secure Network Communication → Access control lists → Systems → Maintain extended access control list of user*.

   The specifics for this scenario are as follows:

   a) Enter an asterisk (*) in the *User* field.

   b) If you create several entries for the same SNC name, then enter the appropriate sequence number in the *Seq.number* field.

   c) Enter the AGate's SNC name in the *SNC name* field.

   d) Save the data.

      

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

Result

The SAP System and the AGate can now communicate using SNC protection. The SAP System is also capable of accepting X.509 client certificates.

Maintaining the User's External Identification in the SAP System

The SAP System must be able to identify the owner of the certificate. Therefore, you need to enter an external identification for each user who uses a client certificate to log on to the SAP System. The information is stored in the table USREXTID. When the SAP System receives a client certificate, it searches the table for a corresponding user ID.

Prerequisites

You need to know the X.509 Distinguished Names of the users who will use client certificates to log on to the SAP System via the ITS.

The X.509 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

1. Maintain the user's external identification in the table USREXTID.

   You can access the table using transaction SM30 or in Customizing for *System Administration* under *Management of External Security Systems* → *External identification* → *Maintain external identification for the user (All types)*.

   The *Determine Work Area: Entry* dialog box appears.

2. Enter **`DN`** in the *Type of external ID* field.

   The *Change View "Assign external ID to users": Overview* screen appears with a list of existing entries. If only one entry exists, then the *Overview* screen is skipped and the *Details* screen appears for the single entry.

3. To create an entry, choose *Edit* → *New entries*. (To modify an existing entry, select the entry and choose *Goto* → *Detail*. Note that not all fields are modifiable.)

4. Enter the following information in the appropriate fields:

The fields *Serial no.* and *Min. date* are optional and are not currently checked in the SAP System.

Field	Value
Extern.ID	Distinguished Name as found in the user's certificate
Serial no.	Serial number of the certificate; 000 is the default value
User	User ID in the SAP System
Min. date	Earliest date on which the certificate is valid for logging on to the SAP System

5. Set the *Activated* indicator.

6. Save the data.