Test Plan
Secure Network Communications
BC-SNC

SAP R/3 4.0

Version 1.13

Copyright

1 Test plan SNC (Secure Network Communications)

Secure Network Communications (SNC) is a layer in the SAP R/3 software to integrate and interface to third party security software that conforms to the *Generic Security Service API Version 2* (GSS-API v2) specification. This standard is being developed in the Internet Engineering Task Force (IETF), an international standardizations body. Through SNC, strong authentication, integrity protection and confidentiality services of external security products can be used by the distributed components of the SAP R/3 Software to protect their network communication.

To guarantee the interoperability of external security products with the SAP Software the external product has to be certified for the BC-SNC interface by SAP's Integration & Certification Center (ICC). This document describes the certification tests that have to be passed by a security product to receive the BC-SNC certificate.

For general information about SNC functionality please check the Service Marketplace under http://service.sap.com/security (→ Security in Detail → Secure System Management).

For more information about the BC-SNC certification go to the Web page http://sdn.sap.com/sdn/icc.sdn?page=network_security.htm.

1.1 Test objective

The BC-SNC certification tests cover installation and configuration of the security product together with SAP Software client and server components. After installation and configuration, the test analyses the runtime behavior of the third party security software, simulating the behavior of SAP Software components that use the SNC layer. Additionally, the standalone GSSTEST test tool collects statistical data on the runtime performance of individual GSS-API function calls, on the characteristics and attributes of names, credentials and security contexts.

The return values of all API calls are checked for conformance to the GSS-API v2 Standard. Furthermore, the conformance to certain SAP-specific constraints on parameter values, token sizes and runtime behavior is verified. Besides the functional test, GSSTEST simulates common configuration and usage errors caused by misspelled names for credential owners and for security context targets and logs the observed behavior into the output protocol.

To further validate the interoperability with the SAP Software components secure connections and sessions have to be set up and used for the SAPgui (SAP Graphical User Interface), RFC (Remote Function Call) and remote printing with the SAPlpd.

1.2 Test environment

The BC-SNC certification procedure requires the following preconfigured hardware and software.

Provided by SAP:

- A current Microsoft Windows Server
  running an SAP R/3 system of release 4.0B or above or a Web Application Server (below always Web Application Server).
- Two PCs with different Microsoft Windows operating systems with a local SAP front end installation.

- The GSS-API test tool "GSSTEST" for BC-SNC certification, precompiled for the hardware platforms from above.

It is necessary that the hostnames of all these machines can be correctly resolved via DNS. When DHCP is used, this will require the use of DNS-Servers that will be dynamically updated from the DHCP server. If dynamic update of DNS with the DHCP information is not available or not configured, static IP addresses and static DNS entries will have to be used.

Provided by vendor:

- The third party security software to be examined for interoperability with SAP Software components through the BC-SNC interface supporting the hardware platforms from above.
- Any installation and configuration tools required as part of the security product's infrastructure.
- Preinstalled SAP R/3 application server of release 4.0B or above or a Web Application Server, as well as front end installation and security product installations on additional hardware other than the above (either bring to SAP certification site or on-site certification at vendor or customer site).

1.3 Test scenario overview

The interoperability of the third party security software and SAP Software components over the BC-SNC-Interface are tested by the following steps and scenarios:

- Installation and configuration of the third party security software on the SAP Web Application Server.
- Installation and configuration of the third party security software on the SAP front end computers.
- Examination of shared library supplied by the third party security software with the standalone test tool GSSTEST on application server and front end machines.
- Configuring/enabling the third party security software for the Web Application Server (R/3 and security product settings).
- Configuring/enabling the third party security software for the SAP front end components (SAPlogon, SAPgui, SAPlpd, rfcinfo, rfcexec).
- Testing SNC-Name retrieval via SAPlogon for starting SAPguis directly and with load balancing.
- Testing secure R/3 access with SAPgui.
- Testing secure printing with SAPlpd.
- Testing secure RFC connections in different scenarios using sapinfo and rfcexec.

2 The test procedure

This chapter describes details of the test procedure; required steps and actions.

2.1 Preparing the environment

Before the certifications tests can be performed the test environment has to be set up as follows:

2.1.1 Application server

Installation and configuration of an SAP Web Application Server with SNC disabled.

Dialog Workprocesses:	>= 2
Spool Process:	1

2.1.2 Front end

Installation and configuration of a current SAP front end running on two different Windows machines with the components SAPlogon, SAPgui, SAPlpd and the RFC SDK.

‘Add or remove one or more SAP Front-End component(s)’ using the SAP Front-End Configuration Wizard:

Select from the component list at least:

- SAP GUI
  - ➢ SAP GUI with SAP Logon
  - ➢ Shortcut to SAPlpd
- Development Tools
  - ➢ RFC SDK Libraries

2.1.3 SAP system administration

Use transaction **SU01** *User Maintenance* to create two SAP User Accounts:

SNCTEST1	Logon data --> User type:	Dialog
SNCTEST2	Logon data --> User type:	Dialog

Use transaction **SMLG** *CCMS: Maintain Logon Groups* to define two logon groups:

PUBLIC	containing Web Application Servers that permit insecure logon
SNC logon	containing the Web Application Server that will be configured for SNC-

In the case of a standalone Web Application Server, both groups will point to the same server.

2.1.4 Functional test of the conventional (insecure) environment

Start the R/3 application server. Watch the console output and trace files (if required) to verify the successful establishment of the connection to the database and the correct status of the work and spool processes.

Start SAPlogon and configure an entry to logon to the R/3 test system. Launch a SAPgui and logon to the R/3 test system with the SNCTEST1 and SNCTEST2 users using the conventional password-based mechanism.

2.2 Installing the security product on the application server

Complete any steps required to install the security product on the application server.

A Web Application Server requires initiating and accepting credentials both referring to the same identity/name for its operation. If either of both types of these credentials are short-lived (several hours or a few days), the procedure for automatic credentials refresh must be documented in the test report.

2.3 Installing the security product on the front end machines

Complete any steps required to install the security product on the front end machines.

Most components of the SAP front end require only the default initiating credentials for operation and for connecting to SAP-Systems. SAPlpd requires the availability of accepting credentials, and gsstest requires availability of both, initiating and accepting credentials, however, these are *not* required to refer to the same identity/name.

2.4 GSSTEST on the Web Application Server

Start the GSSTEST tool on the application server and provide the path to the security product library which contains the GSS API v2 functions and SNC adapter.

```
gsstest    –l <drive>:\path\to\your\snclib.dll
           -a <target_name>
           -p appserv-nt.log
```

The parameter –a is optional. You only need it if the default credential cannot be used as an accepting credential. In this case, the target name is the name for the accepting credential.

If the security product offers special configuration or usage options that will affect the operation of GSSTEST at the GSS-API level, these must be documented in the test report. Examples of such options are: use of software- or hardware-based authentication, possibility to configure different cryptographic algorithms for confidentiality and integrity for GSS_C_DEFAULT_QOP.

Save/Archive the output protocol **"appserv-nt.log"** created by the GSSTEST tool and interpret its contents according to Section 3. „Reading the Output Protocol of GSSTEST“.

2.5 GSSTEST on the front end machines

Start the GSSTEST tool on the front end machine and provide the path to the security product library which contains the GSS API v2 functions and SNC adapter.

```
gsstest    –l <drive>:\path\to\your\snclib.dll
           -a <target_name>
           -p frontend-xx.log
```

If the security product offers special configuration or usage options that will affect the operation of GSSTEST at the GSS-API level, these must be documented in the test report. Examples of such options are: use of software- or hardware-based authentication, possibility to configure different cryptographic algorithms for confidentiality and integrity for

GSS_C_DEFAULT_QOP.

Run GSSTEST additionally on both frontend platforms once without valid credentials. Although this will cause GSSTEST to abort prematurely, we need the resulting log file with the error messages that indicate the absence of valid credentials.

Save/Archive the output protocol **"frontend-*xx*.log"** created by the GSSTEST tool and interpret its contents according to Section 3. „Reading the Output Protocol of GSSTEST“.

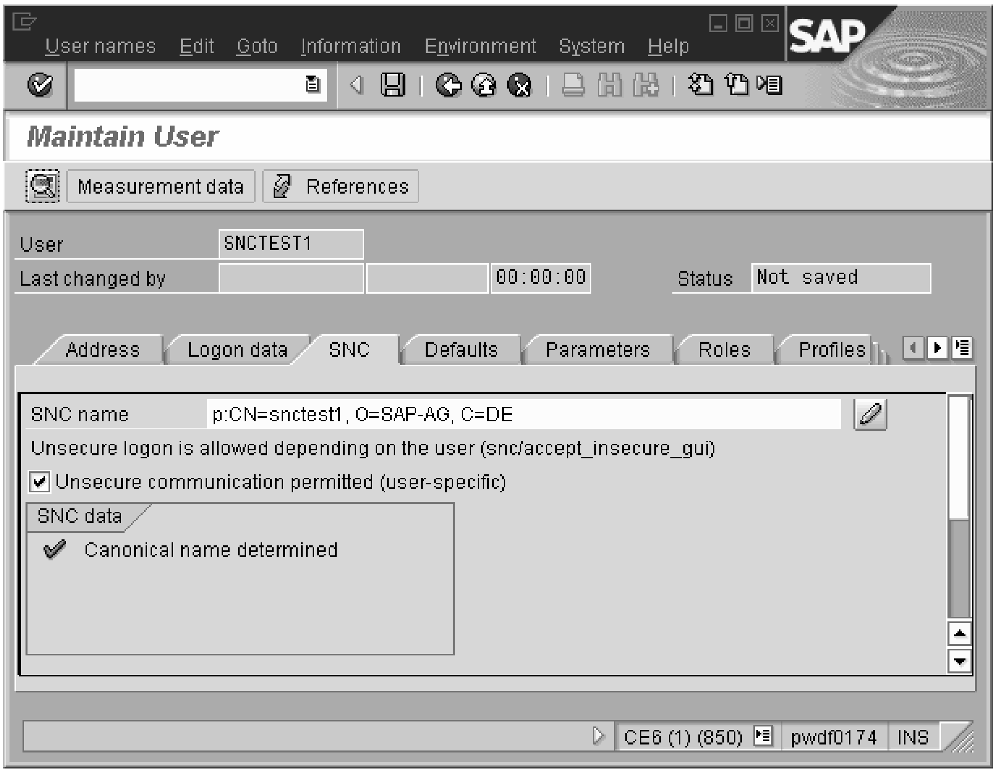
2.6 Enabling SNC on the Web Application Server

Shut down the Web Application Server. Add the following SNC-specific parameters to the instance profile of the application server:

```
snc/enable                  = 1
snc/gssapi_lib              = <drive>:\path\to\your\snclib.dll
snc/identity/as             = <SNC-Name_of_R/3_AppServer>
snc/data_protection/max     = 3
snc/data_prodection/min     = 1
snc/data_protection/use     = 9
snc/accept_insecure_gui     = 1
snc/accept_insecure_rfc     = 1
snc/accept_insecure_cpic    = 1
snc/r3int_rfc_secure        = 0
snc/r3int_rfc_qop           = 9
snc/permit_insecure_start   = 1
```

Start up the R/3 application server. If there are problems with the startup of SNC, they will be logged in the file **dev_w0**, which is located in the **work** directory of the Web Application Server (e.g. under Windows: `<DRIVE>:\usr\sap\<SID>\<instance>\work`)

Logon to the R/3 test system, user-account SNCTEST1 using the conventional password-based mechanism. Use SAP transaction **SU01** now to enter the SNC-name of the users SNCTEST1 and SNCTEST2, matching the names of the client credentials that are used on the front ends. Verify the new settings after saving them; especially if the canonical names were actually created (they are stored in the table USRACL).



Maintain User

User SNCTEST1
Last changed by 00:00:00
Status Not saved

SNC name p:CN=snctest1, O=SAP-AG, C=DE

Unsecure logon is allowed depending on the user (snc/accept_insecure_gui)

☑ Unsecure communication permitted (user-specific)

SNC data
✓ Canonical name determined

2.7 Enabling SNC on the front end machines

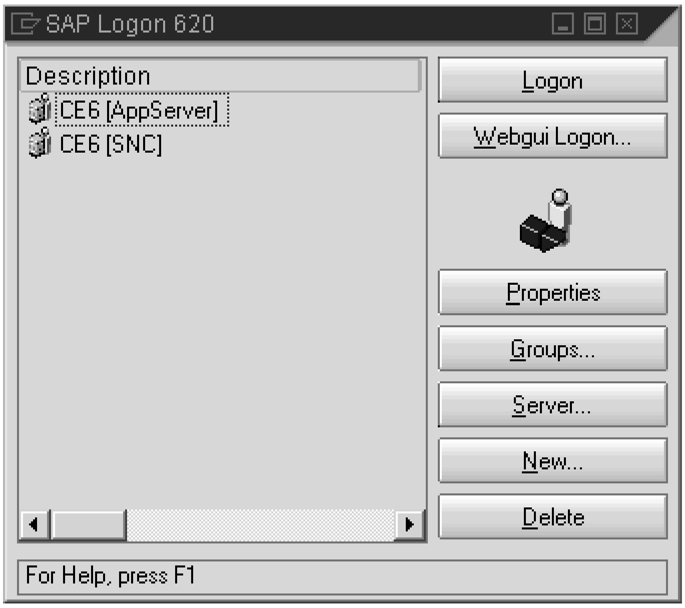
Set the environment variable SNC_LIB to contain the path to the security product library:

```
SNC_LIB = <drive>:\path\to\your\snclib.dll
```

Windows NT:	Control Panel → System → Environment
Windows 2000:	Control Panel → System → Advanced → Environment variables
Windows XP:	Control Panel → System → Advanced → Environment variables

2.8 SNC-Name retrieval via SAPlogon

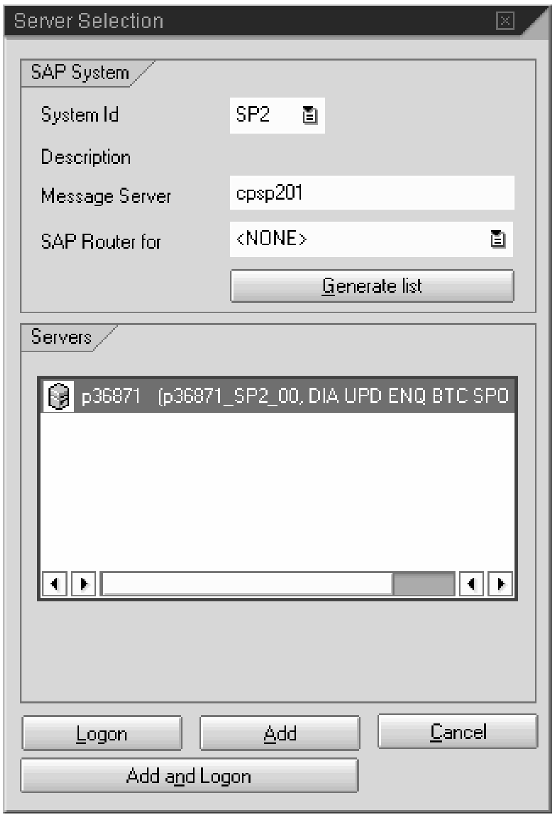
Start SAPlogon.



Create two new entries as described in the next sections.

2.8.1 Server selection

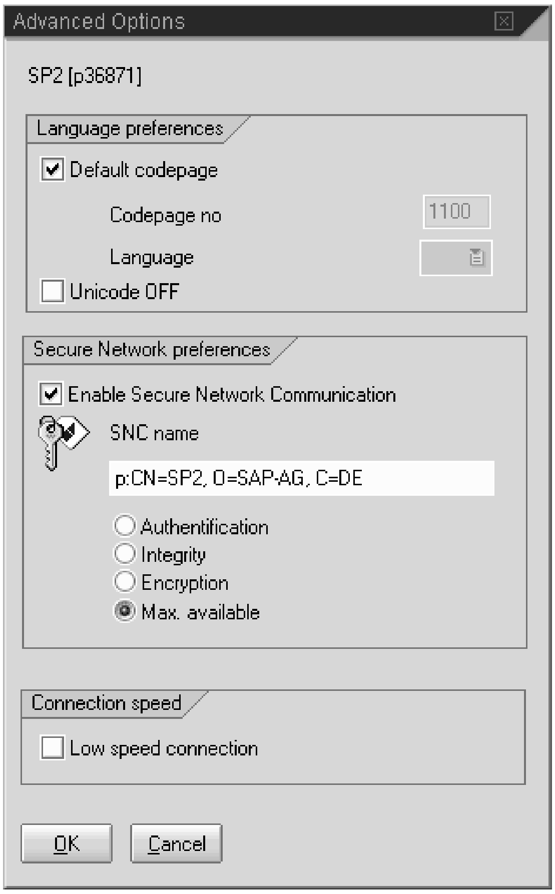
Add a new entry for the test system using "Server Selection".



System Id: SP2
Description:
Message Server: cpsp201
SAP Router for: <NONE>

p36871 (p36871_SP2_00, DIA UPD ENQ BTC SPO

Select ‘Add' and in the ‘New Entry’ dialog, open the 'Advanced Options' and configure the SNC parameters.



Advanced Options

SP2 [p36871]

Language preferences

☑ Default codepage

Codepage no 1100

Language

□ Unicode OFF

Secure Network preferences

☑ Enable Secure Network Communication

SNC name

p:CN=SP2, O=SAP-AG, C=DE

○ Authentification
○ Integrity
○ Encryption
● Max. available

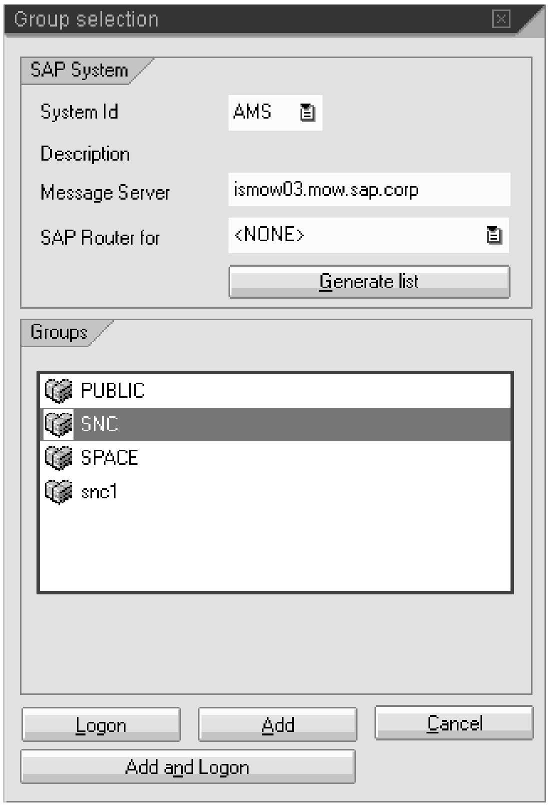
Connection speed

□ Low speed connection

Since the SNC-Name of the application server is distributed by the message server, it should already appear in its field. Activate the checkbox to enable SNC and select 'Max. available' for the message protection (it is the default).

2.8.2 Group Selection / "Load Balancing"

Add a new entry for the SAP test system using "Group Selection".



Groups

System Id: AMS

Description:

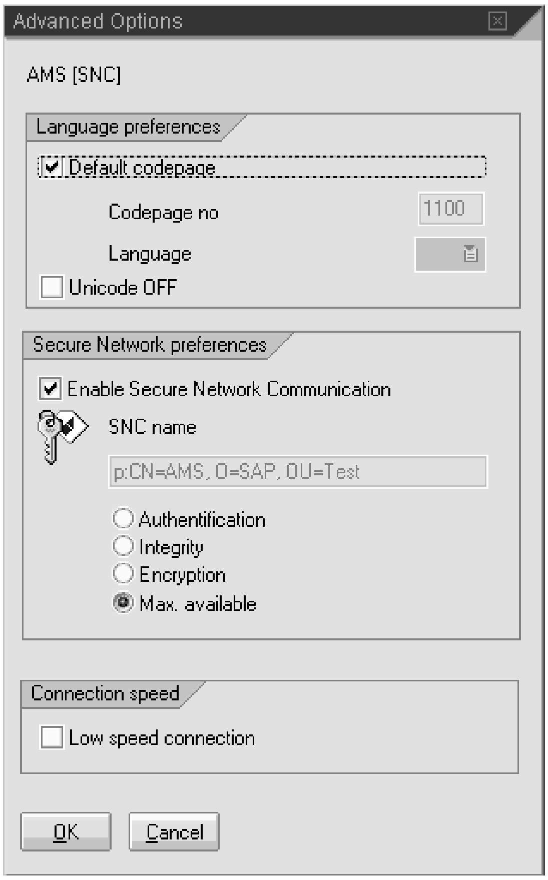
Message Server: ismow03.mow.sap.corp

SAP Router for: <NONE>

Groups:

- PUBLIC
- SNC
- SPACE
- snc1

Select ‘Add’ and in the 'New Entry' dialog, open the 'Advanced Options' and configure the SNC parameters.



AMS [SNC]

Language preferences

☑ Default codepage

Codepage no: 1100

Language:

□ Unicode OFF

Secure Network preferences

☑ Enable Secure Network Communication

SNC name: p:CN=AMS, O=SAP, OU=Test

○ Authentification
○ Integrity
○ Encryption
● Max. available

Connection speed

□ Low speed connection

When using Logon Groups instead of Server Selection, the actual application server is dynamically selected by the message server at the time of login. Since in general the SNC names for the different application server in the same logon group will differ, the SNC name of the selected application server has to be provided by the message server at the time of login as well. For this reason, you cannot define the SNC name in the dialog above and the field for it is grayed out. Activate the checkbox to enable SNC and select 'Max. available' for the message protection (it is the default).

2.9 Secure system access with SAPgui

First, verify that you have valid client credentials available for one of the accounts SNCTEST1 and SNCTEST2 that you have created in step *2.1.3 SAP system administration* and assigned to externally authenticated SNC-Names in step *2.6 Enabling SNC on the Web Application Server* .

If the user was externally authenticated, the system will try to map your externally authenticated name to an account in the Web Application Server. If there is no user account matching your externally authenticated name, then your logon request will be denied with an error message in the status bar at the bottom of the SAPgui window. If there is exactly one account matching this name, no logon screen is displayed and you are logged on automatically.

Log on to the Web Application Server via the SAPLogon entry created by server selection and open some extra windows using the menu path "*System → Create Session*".

Open the Status window on every new window using the menu path "*System → Status...*". This opens a new window displaying the system status. Under *Usage data* you can see the user account name as well as the SNC name.

Close the first two windows identified by (1) and (2) in the window status bar, leftmost field, just behind the name of the SAP-System.

Open two more windows using the menu path "*System->Create Session*" and request the status window using menu path "*System->Status...*" again.

Log on again – this time using the SAPLogon entry created by group selection – while the old session is still running and select "Continue with this logon and end any other logons in system". The open windows from the previous session should all disappear. The old SAPgui will terminate and a new one will be started with the initial SAP Easy Access screen.

2.10 Secure printing with SAPlpd

2.10.1 Configuring SAPlpd at the frontend PCs

Besides the procedure in Section 2.7: "Enabling SNC on the front end machines", secure printing via SAPlpd requires additional configuration. SAPlpd operates as a standalone server and a security context acceptor at the GSS-API level, so it requires its own accepting credentials independent of the credentials of the user that may be working at the PC.

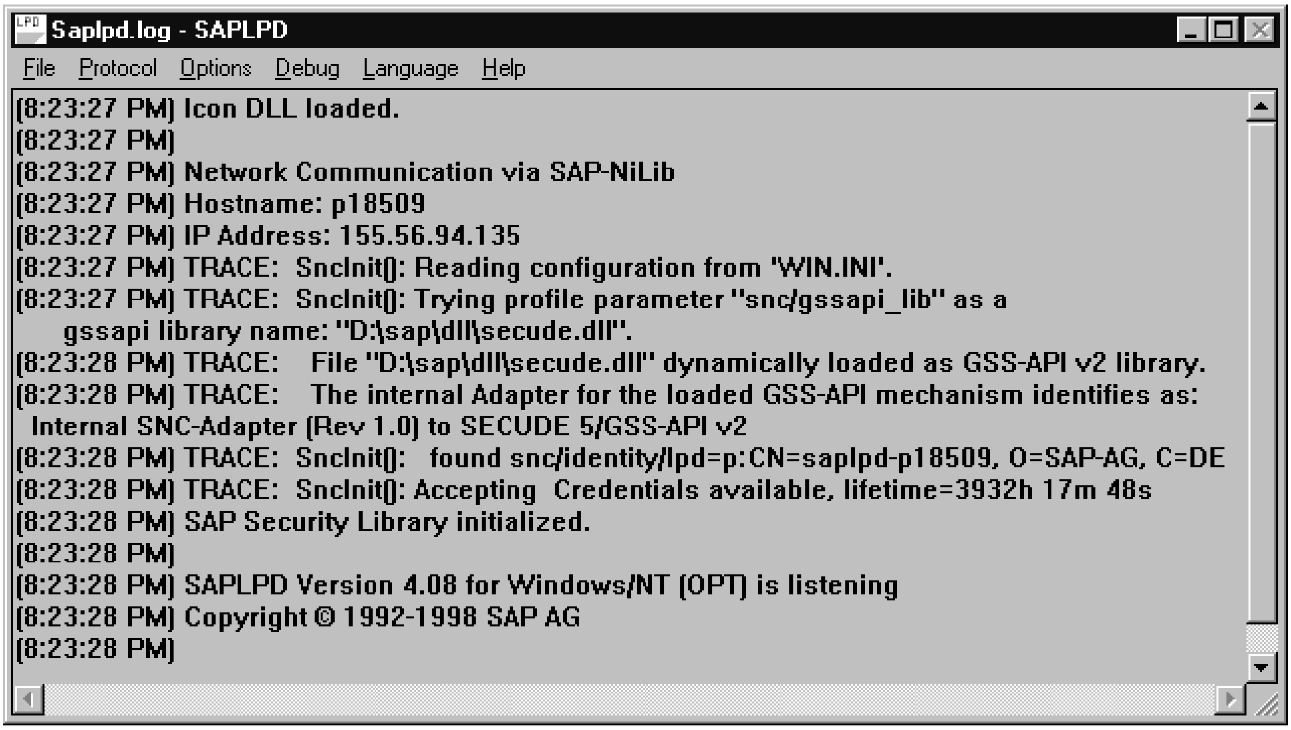
SAPlpd reads SNC-specific from the *.ini-File "SAPLPD.INI" that will be searched in the Windows directory. If this file does not exist or does not contain a section [snc] with the entry "enable=1", SAPlpd will also search "WIN.INI" (also to be found in the Windows directory) for SNC-specific information.

Sample SAPlpd configuration in SAPLPD.INI (or WIN.INI):

```
[snc]
enable=1
identity/lpd=<SNC-Name_of_saplpd>
gssapi_lib=<drive>:\path\to\your\snclib.dll
```

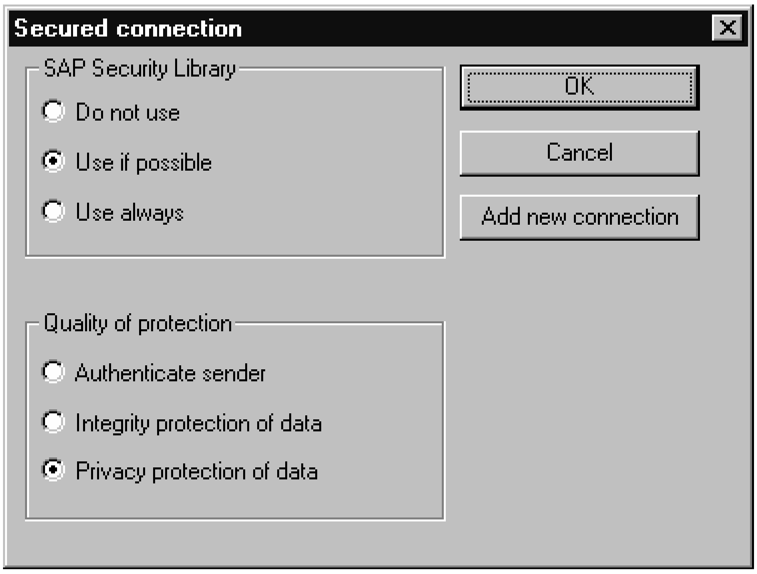
The line with "gssapi_lib=" can be omitted when the environment variable SNC_LIB is configured to be globally visible to all processes.

SAPlpd will always try to acquire its accepting credentials by specifying the explicit name from the configuration parameter "identity/lpd". The third-party security product may require additional configuration and setup changes to provide separate accepting credentials to SAPlpd that will not interfere with credentials of interactive users, who may be independently using secure SAPgui with this PC.



```
(8:23:27 PM) Icon DLL loaded.
(8:23:27 PM)
(8:23:27 PM) Network Communication via SAP-NiLib
(8:23:27 PM) Hostname: p18509
(8:23:27 PM) IP Address: 155.56.94.135
(8:23:27 PM) TRACE:  SncInit(): Reading configuration from 'WIN.INI'.
(8:23:27 PM) TRACE:  SncInit(): Trying profile parameter "snc/gssapi_lib" as a
     gssapi library name: "D:\sap\dll\secude.dll".
(8:23:28 PM) TRACE:    File "D:\sap\dll\secude.dll" dynamically loaded as GSS-API v2 library.
(8:23:28 PM) TRACE:    The internal Adapter for the loaded GSS-API mechanism identifies as:
  Internal SNC-Adapter (Rev 1.0) to SECUDE 5/GSS-API v2
(8:23:28 PM) TRACE:  SncInit():   found snc/identity/lpd=p:CN=saplpd-p18509, O=SAP-AG, C=DE
(8:23:28 PM) TRACE:  SncInit(): Accepting  Credentials available, lifetime=3932h 17m 48s
(8:23:28 PM) SAP Security Library initialized.
(8:23:28 PM)
(8:23:28 PM) SAPLPD Version 4.08 for Windows/NT (OPT) is listening
(8:23:28 PM) Copyright © 1992-1998 SAP AG
(8:23:28 PM)
```

Start SAPlpd, select "Options->Secured Connection" from the menu and the following dialog box will open:



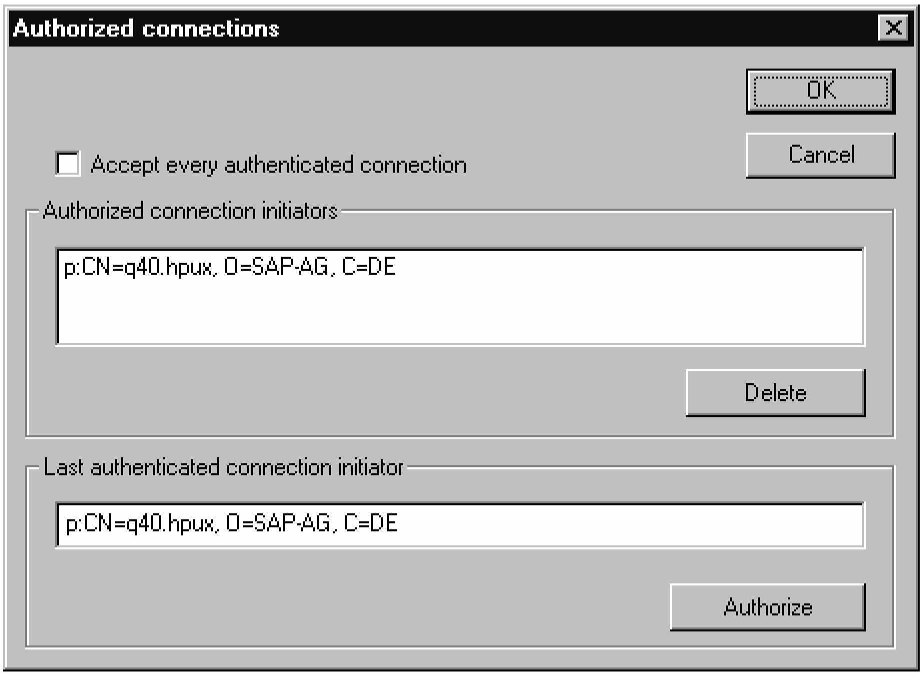
Secured connection

SAP Security Library
- ○ Do not use
- ● Use if possible
- ○ Use always

Quality of protection
- ○ Authenticate sender
- ○ Integrity protection of data
- ● Privacy protection of data

Select **Use if possible** from the list for the SAP Security Library,

select **Privacy protection of data** from the list for Quality of protection,



Authorized connections

□ Accept every authenticated connection

Authorized connection initiators

p:CN=q40.hpux, O=SAP-AG, C=DE

Last authenticated connection initiator

p:CN=q40.hpux, O=SAP-AG, C=DE

and press the button **Add new connection** to go ahead to the maintenance of the Access Control List (ACL) of SAPlpd.

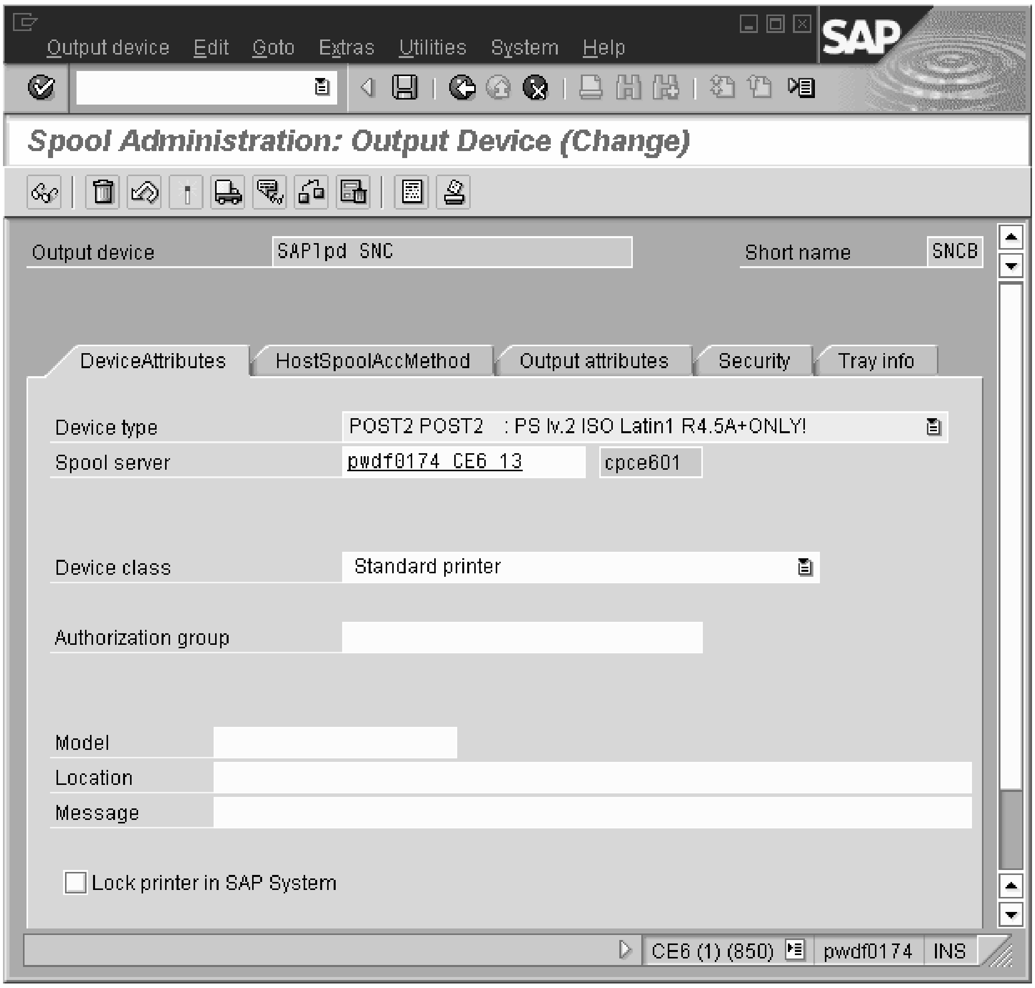
Enter the SNC-name of the application server(s) that will be transferring print jobs securely to this SAPlpd into the field **Last authenticated connection initiator** and hit the button **Authorize** to add this name into the list of authorized connection initiators.

Close the dialog boxes again by hitting their OK buttons, but keep SAPlpd running.

2.10.2 Configuring the secure printer output device within R/3

Create a new Printer with the transaction **SPAD** ("Spool Administration"). Press the Button for "Output Devices", click on the ‘pencil’ icon in order to switch to the change mode and click on the ‘paper’ icon to create a new output device (Printer):

You start on tab strip ‘*DeviceAttributes*’:



Spool Administration: Output Device (Change)

Output device: SAPlpd SNC
Short name: SNCB

Device type: POST2 POST2 : PS lv.2 ISO Latin1 R4.5A+ONLY!
Spool server: pwdf0174_CE6_13 cpce601

Device class: Standard printer

Authorization group:

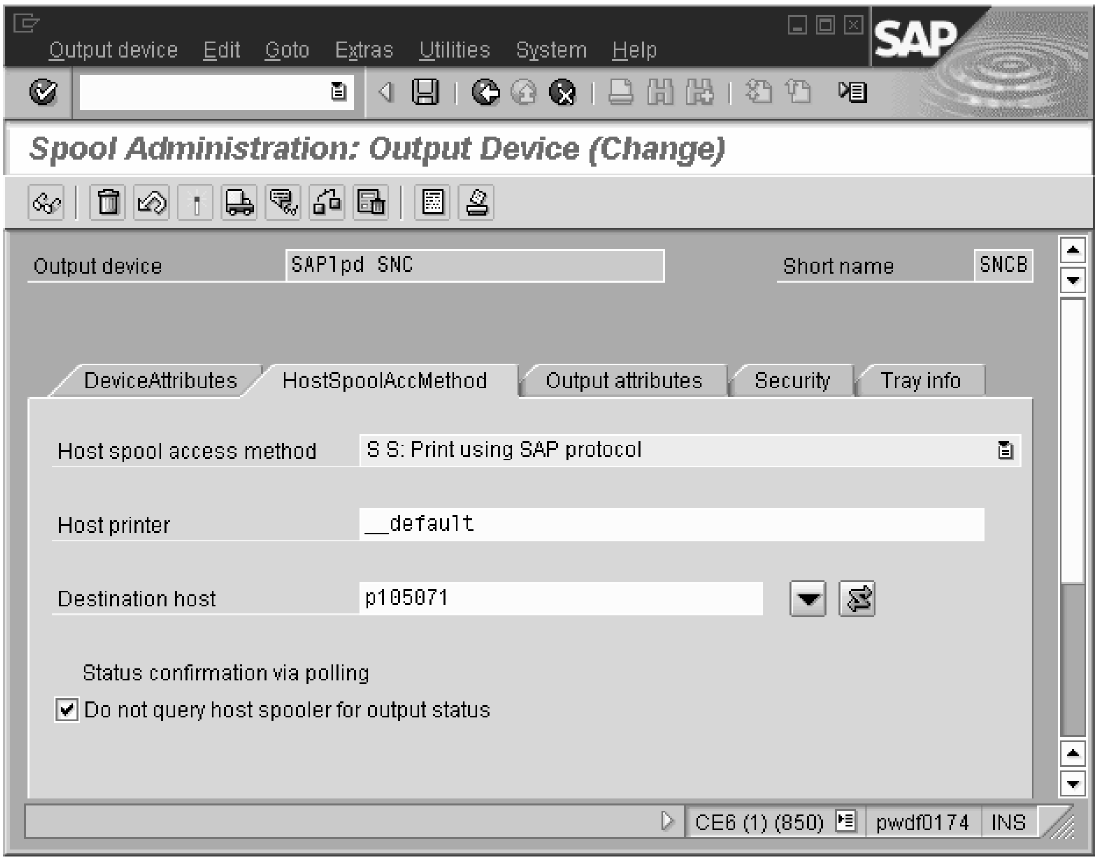
Model:
Location:
Message:

□ Lock printer in SAP System

CE6 (1) (850) pwdf0174 INS

Fill in the fields **Output device**, **Short name**, **Device type**, and **Spool Server**. If the SAP system consists of several application servers, the F4-help for **Spool Server** will show you all application servers with a color-coded background; only the ones with a running spool process will be displayed with a green background.

Go ahead to the next tab strip ‘*HostSpoolAccMethod*’.



Spool Administration: Output Device (Change)

Output device SAPlpd SNC

Short name SNCB

Host spool access method S S: Print using SAP protocol

Host printer __default

Destination host p105071

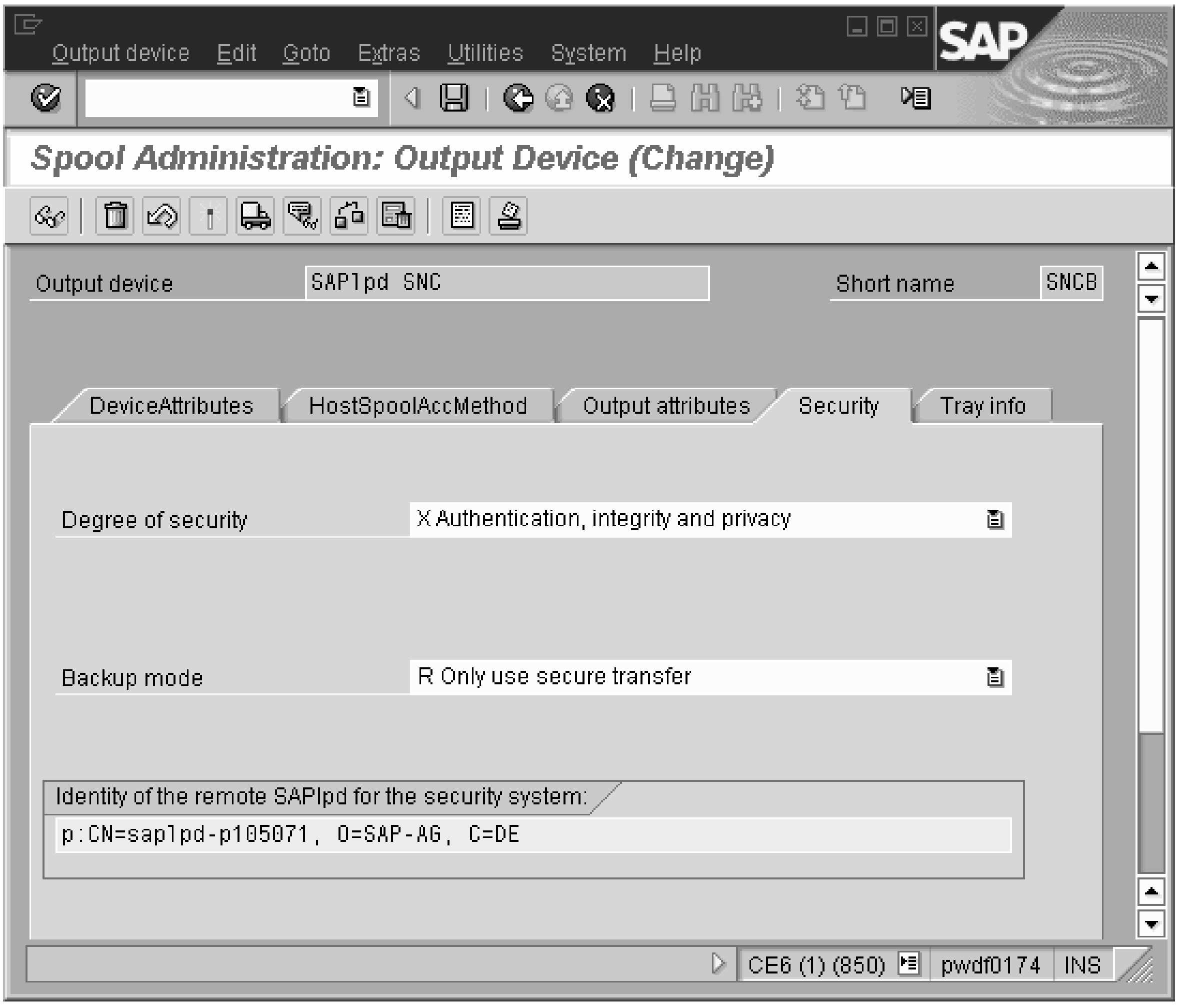
Status confirmation via polling

☑ Do not query host spooler for output status

Select "S: Print using SAP Protocol" in the field **Host spool Access method** and enter the name of the **Host printer** as well as the host name of the front end PC as the **Destination host**.

Checkmark the option ‘**Do not query host spooler for output status**’.

You can skip the tab strip ‘*Output attributes*’. The next important one is ‘*Security*’:



Spool Administration: Output Device (Change)

Output device SAPlpd SNC

Short name SNCB

Degree of security X Authentication, integrity and privacy

Backup mode R Only use secure transfer

Identity of the remote SAPlpd for the security system:

p:CN=saplpd-p105071, O=SAP-AG, C=DE

CE6 (1) (850) pwdf0174 INS

Select **Authentication, integrity and privacy** from the list of security degrees for the SAPlpd connection, additional entry fields will appear.

Select **Only use secure transfer** for the field **Backup mode**.

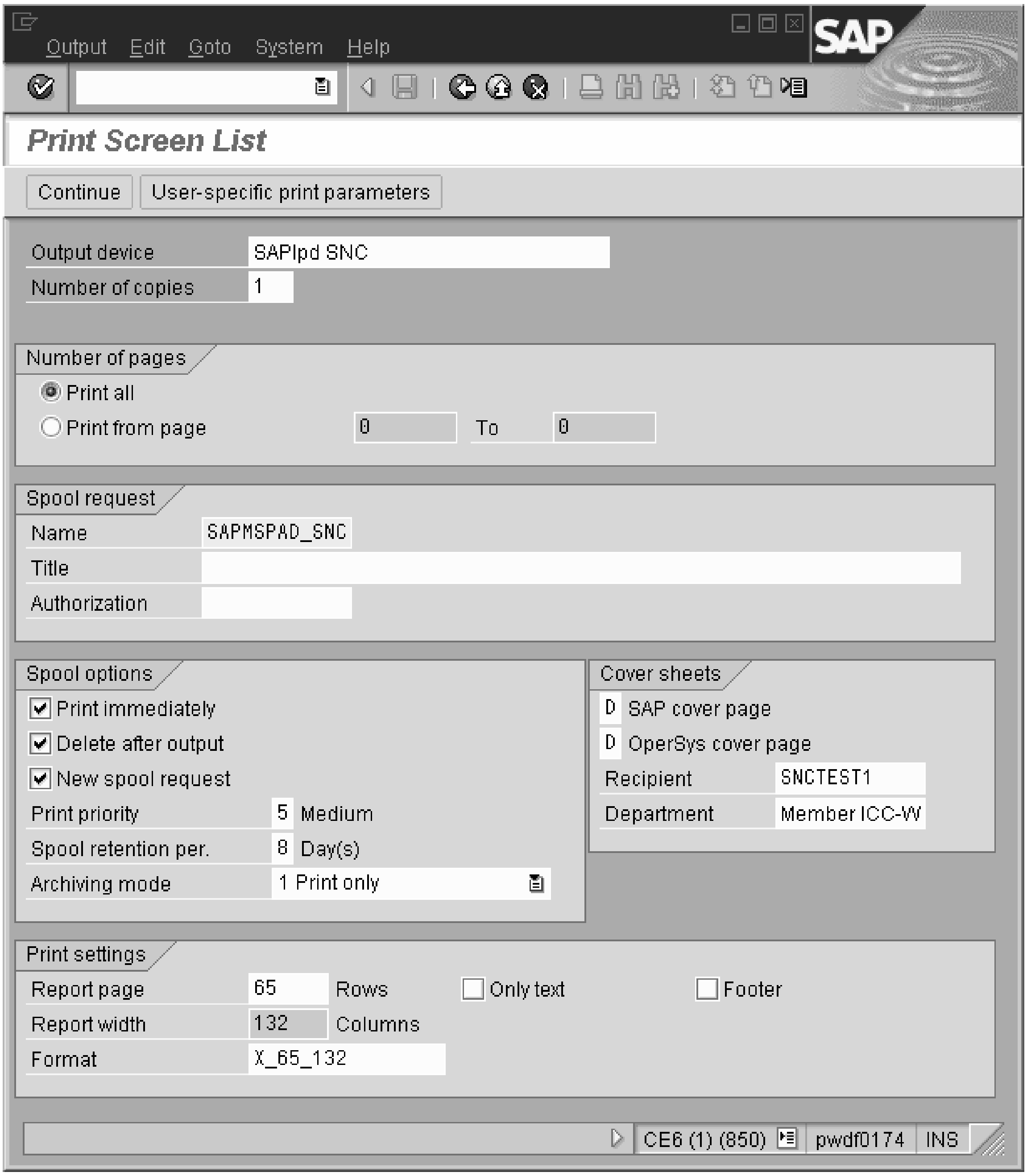
Enter the SNC-Name of the credentials that SAPlpd on the frontend machine will be using for accepting the connections.

Save the printer definition.

Return to the list of output devices with the 'back' arrow.

2.10.3 Starting a print job

Make sure that saplpd is still running and create a print job by printing the list of output devices using the ‘printer’ icon or the menu path
"*System* → *List* → *Print*".



Print Screen List

Output device	SAPlpd SNC
Number of copies	1

Number of pages

● Print all

○ Print from page 0 To 0

Spool request

Name	SAPMSPAD_SNC
Title	
Authorization	

Spool options

☑ Print immediately

☑ Delete after output

☑ New spool request

Print priority	5	Medium
Spool retention per.	8	Day(s)
Archiving mode	1 Print only	

Cover sheets

D SAP cover page

D OperSys cover page

Recipient	SNCTEST1
Department	Member ICC-W

Print settings

Report page	65	Rows	□ Only text	□ Footer
Report width	132	Columns		
Format	X_65_132			

CE6 (1) (850) pwdf0174 INS

Select the **Output Device** that you just created with the F4-selection or just enter its name or its short name.

Checkmark the spool control option **Print immediately**. On newer Web Application Servers, you first have to click on **Properties** in order to be able to activate this option (*General attributes* → *Time of printing: Print out immediately*)

Submit the print request with pressing **Continue**.

You can track status and progress of the print request with transaction **SP01**. If an error occurs on SAPlpd for any reason, processing of output requests for this the output device will be suspended for several minutes. To reactivate the processing of this output device immediately, use transaction SPAD, select the output device from the list and open the definition for change. You can now reactivate the output device with <Ctrl-F2> or via the menu "*Edit* → *Reactivate*".

2.11 Testing Secure RFC-connections, front end to SAP (SAPINFO)

Create an RFC configuration file SAPRFC.INI. This file should either be located in the same directory as the program executable, or the environment variable RFC_INI must be used to specify the full path and filename to this file.

The following test procedure is using SAPINFO.EXE, which is contained in the *RFC SDK* of the front end software. It can be found in the directory

<drive>:*\path\of\frontend*`\SAPGUI\RFCSDK\BIN\`

To run this test, it may be preferable to copy the programs SAPINFO.EXE and RFCINFO.EXE, the file LIBRFC32.DLL into a separate/new directory and create the SAPRFC.INI file there.

2.11.1 RFC with specific application servers (RFC Type A)

An RFC-destination (Type A) in SAPRFC.INI is built with the following pattern:

DEST=*<choose_your_name>*
TYPE=A
ASHOST=*<hostname_of_SAP_AppServer>*
SYSNR=*<system-nr_of_SAP_system>*

When using SNC, one must specify additional parameters:

SNC_MODE=1
SNC_PARTNERNAME=*<SNC-Name_of_SAP_AppServer>*
SNC_LIB=*<drive>*:*\path\to\your\snclib.dll*

Here is a sample SAPRFC.INI with 3 destinations:

```
/*=========================================================*/
/*  Type A:  R/3 system - specific application server      */
/*=========================================================*/

/* Conventional access */
DEST=Q40_hs0017
TYPE=A
ASHOST=hs0017
SYSNR=01

/* Access using SNC-protected communication */
DEST=snc_Q40_hs0017
TYPE=A
ASHOST=hs0017
SYSNR=01
SNC_MODE=1
SNC_PARTNERNAME=p:CN=Q40.hpux, O=SAP-AG, C=DE
SNC_LIB=D:\sap\dll\secude.dll

/* Tickle an SNC-error by specifying a wrong target name */
DEST=error_Q40_hs0017
TYPE=A
ASHOST=hs0017
SYSNR=01
SNC_MODE=1
SNC_PARTNERNAME=p:CN=error, O=SAP-AG, C=DE
SNC_LIB=D:\sap\dll\secude.dll
```

Use this sample to create a SAPRFC.INI matching the R/3 test environment.

Now run the SAPINFO program with each of the 3 destinations:

1. `SAPINFO dest=Q40_hs0017`
2. `SAPINFO dest=snc_Q40_hs0017`
3. `SAPINFO dest=error_Q40_hs0017`

The first two destinations should succeed, the third destination should fail with an SNC-Error (provided that the security product provides mutual authentication at the GSS-API level). The third test/destination is primarily to check whether SNC is actually being used and working.

2.11.2 RFC with load-balancing (RFC Type B)

Load-balancing or "group-logon" dynamically retrieves the target SNC-Name from the message server. Logon groups can be defined within R/3 using transaction **SMLG**.

An RFC-destination (Type B) in SAPRFC.INI is built with the following pattern:

DEST=*<choose_your_name>*
TYPE=B
R3NAME=*<sid>*
MSHOST=*<hostname_of_SAP_MessageServer>*
GROUP=*<name_of_SAP_logon_group>*

When using SNC, one must specify additional parameters:

SNC_MODE=1
SNC_PARTNERNAME=p:unused
SNC_LIB=*<drive>***:***\path\to\your\snclib.dll*
where an SNC partner name has to be present even if it is not validated.

Here is a sample SAPRFC.INI with 2 destinations:

```
/*=========================================================*/
/*  Type B:  R/3 system - load balancing feature          */
/*=========================================================*/

/* Conventional access */
DEST=Q40_PUBLIC
TYPE=B
R3NAME=Q40
MSHOST=hs0017
GROUP=public

/* Access using SNC-protected communication */
DEST=Q40_SNC
TYPE=B
R3NAME=Q40
MSHOST=hs0017
GROUP=SNC
SNC_MODE=1
SNC_PARTNERNAME=p:unused
SNC_LIB=D:\sap\dll\secude.dll
```

Use this sample to create a SAPRFC.INI matching the R/3 test environment.

Now run the SAPINFO program with each of the 2 destinations:

1. `SAPINFO dest=Q40_PUBLIC`
2. `SAPINFO dest=Q40_SNC`

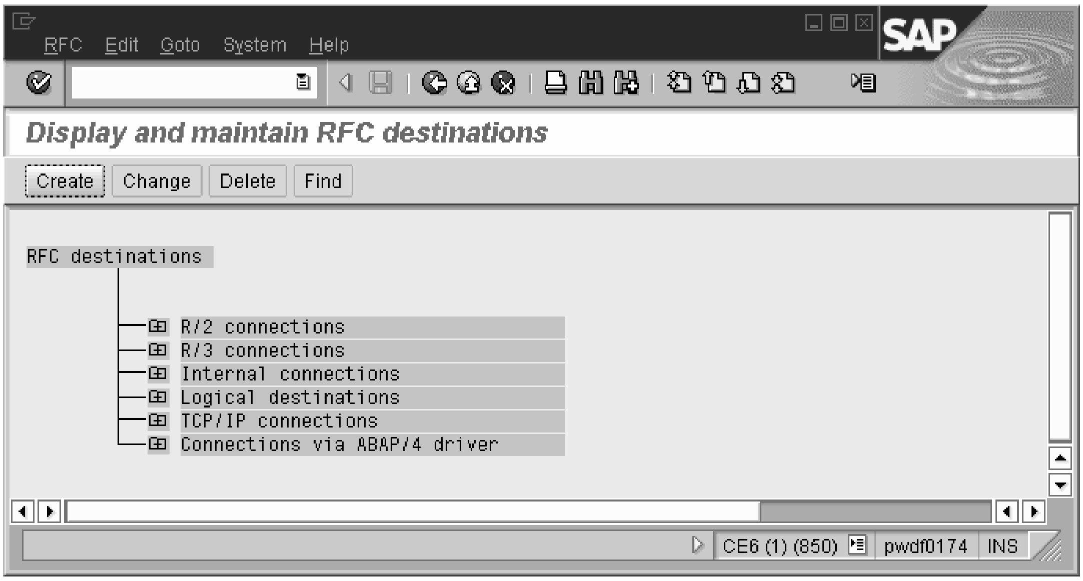
Traces of SNC-related activities can be enabled by setting the environment variable CPIC_TRACE=2. A trace file starting with the letters "CPIC" will be written into the current directory for every new process/program that is started.

2.12 Secure RFC-connections SAP to RFC-Server programs (RFCEXEC)

2.12.1 Start at front end

Log on to the R/3-System using a secure front end.

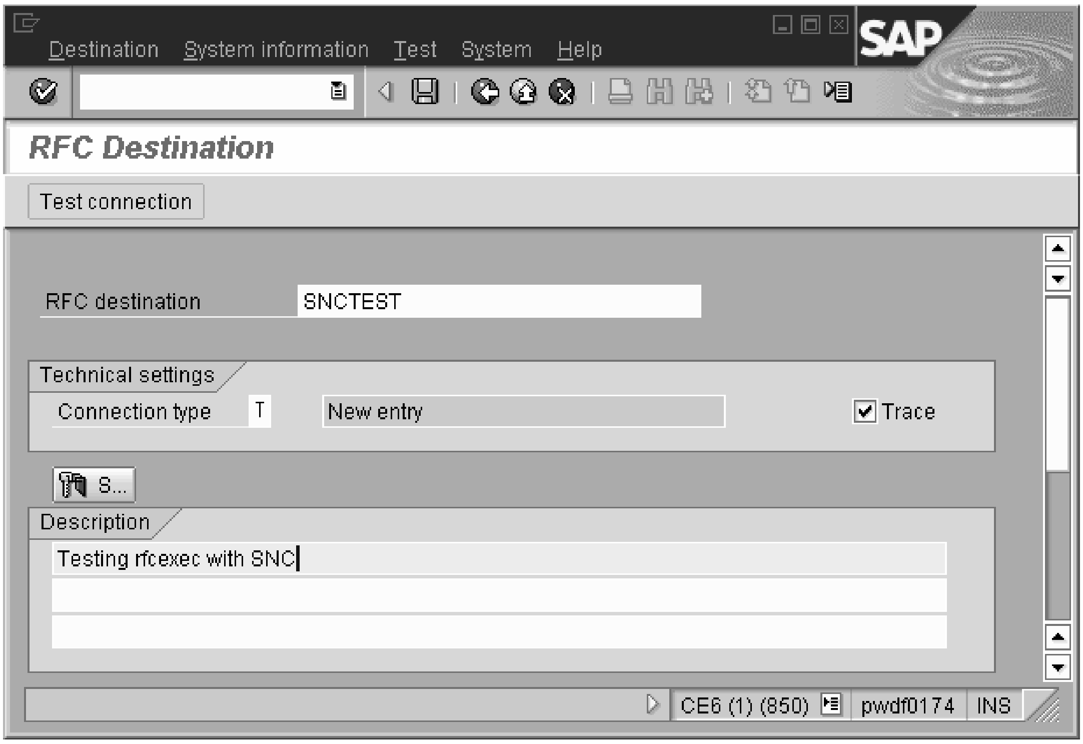
Start transaction **SM59** to create a new RFC destination:



Display and maintain RFC destinations

RFC destinations
- R/2 connections
- R/3 connections
- Internal connections
- Logical destinations
- TCP/IP connections
- Connections via ABAP/4 driver

Hit the **Create** button.



RFC Destination

RFC destination: SNCTEST

Technical settings
Connection type: T — New entry
☑ Trace

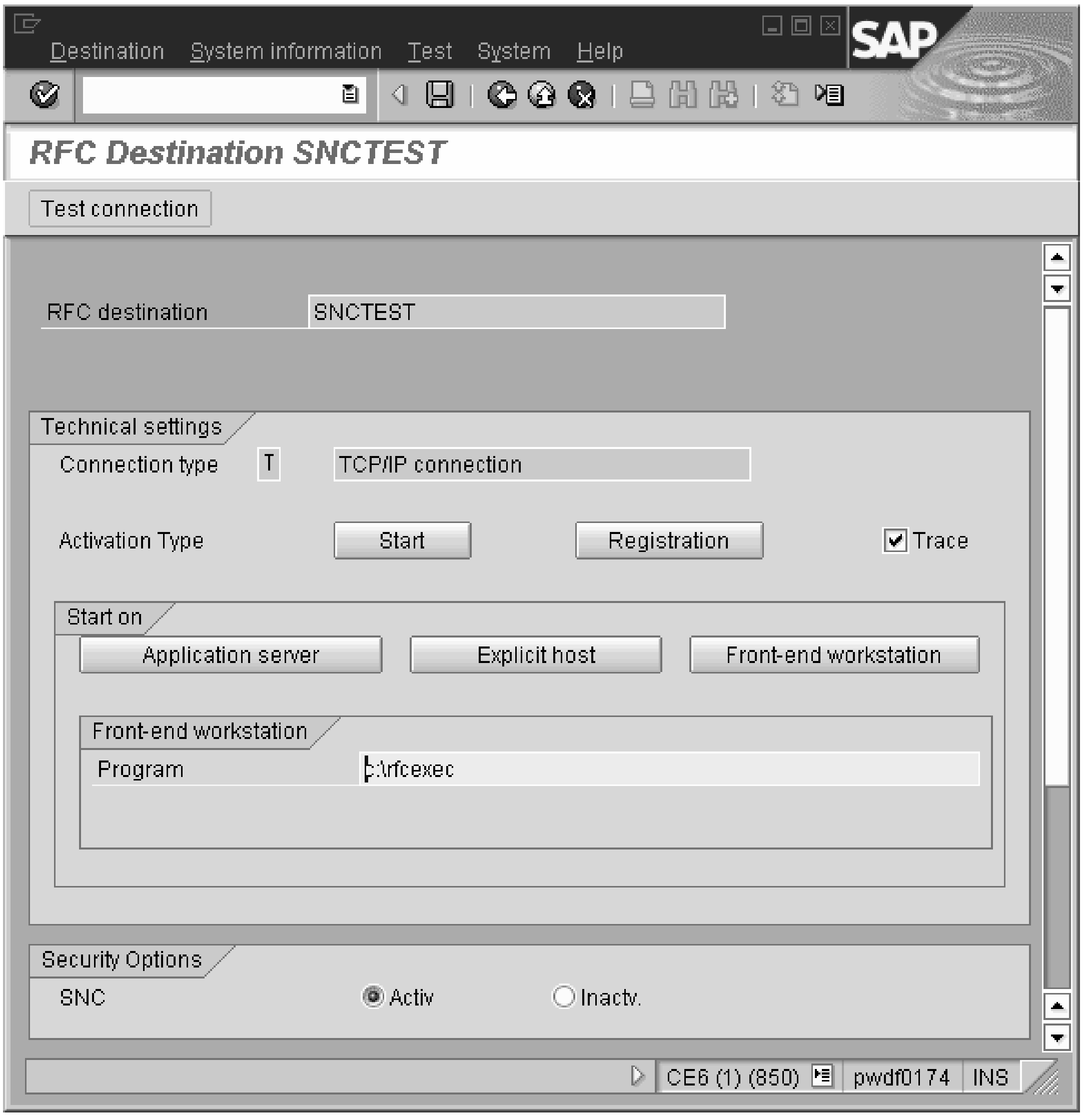
Description
Testing rfcexec with SNC

Enter the name of the RFC destination "SNCTEST".

Enter the connection type "T" for "TCP/IP connection".

Checkmark the **Trace** option.

Enter a description into the description field.
Hit <Enter> on the keyboard.



RFC Destination SNCTEST

RFC destination: SNCTEST

Technical settings

Connection type: T TCP/IP connection

Activation Type: Start | Registration | ☑ Trace

Start on: Application server | Explicit host | Front-end workstation

Front-end workstation

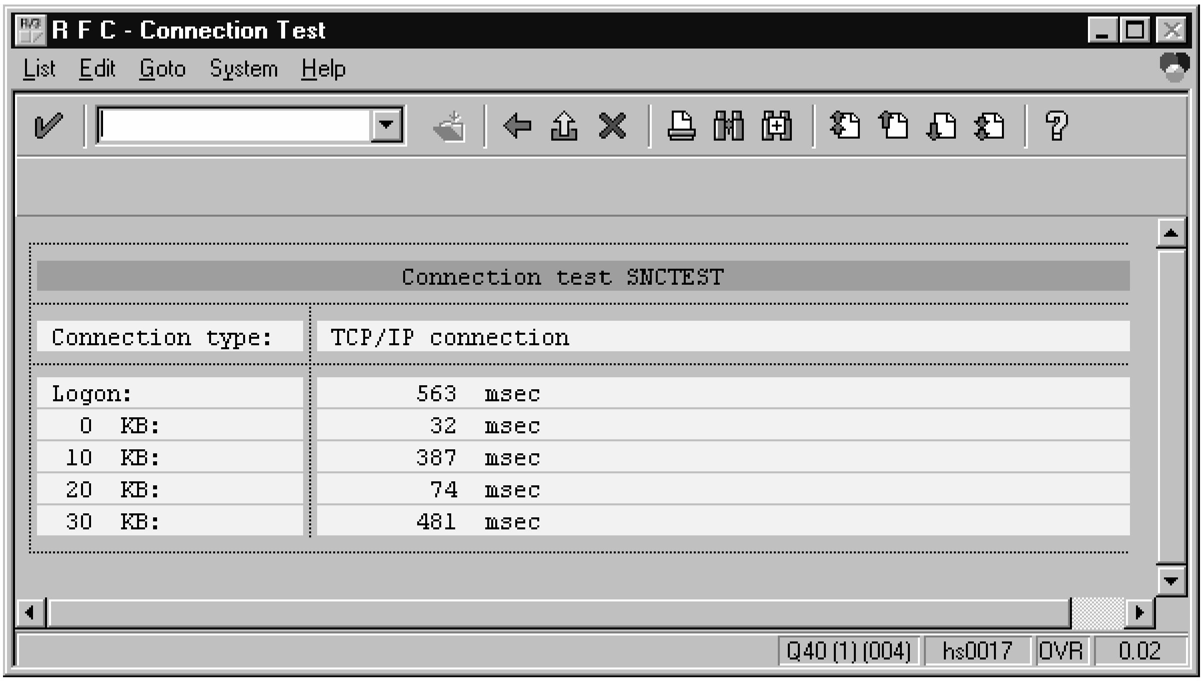
Program: c:\rfcexec

Security Options

SNC: ● Activ ○ Inactv.

CE6 (1) (850) pwdf0174 INS

Select the *Activation type* button **Start**.
Select the *Start on* button **Front-end workstation**.
Enter **rfcexec** including the path where it is located as the name of the Program.
Go to the SNC Options under *Destination* → *SNC-Options* and save them. Select the radio button **Active** for *Security Options* SNC.
Save the RFC destination using the save icon in the toolbar.
Hit the button **Test connection**.



Connection test SNCTEST

Connection type:	TCP/IP connection
Logon:	563 msec
0 KB:	32 msec
10 KB:	387 msec
20 KB:	74 msec
30 KB:	481 msec

3 Reading the output protocol of GSSTEST

When the test of the security product completes, GSSTEST compiles an output summary on the test results. At the end of that summary, a final rating is printed whether the security product met the technical interoperability requirements for the SNC Interface in SAP R/3 during the test. It will look similar to this one:

```
==================

Passing all API result tests.
Passing all SAP constraints.

--- Passed ---   SAP GSS-API v2 Test (builtin SNC-Adapter)

  Mechanism  = {1 3 6 1 4 1 694 2 1 2}        MECH= SAPntlm SSO (NT4/Win95)
  Nametype   = {1 3 6 1 4 1 694 2 1 2 1}        NT= GSS_SAP_NT_DOMAIN_USER

  Max. data protection level =   1 (Authentication only)

  Hardware Platform          =   Microsoft Windows NT 4.0 (Build 1381)

==================
```

Besides the functionality of the security product according to the GSS-API specification, GSSTEST also verifies certain interoperability requirements with SNC / SAP R/3, indicated as *SAP constraints*.

For the BC-SNC certification, all API and SAP constraints tests must be passed.