

# Secure Network Communications for ERP-Link Configuration Guide

Software Version 5.4.0 March 2019 Title: Secure Network Communications for ERP-Link Configuration Guide

© 2019 Gimmal LLC

Gimmal<sup>®</sup> is a registered trademark of Gimmal Group.

Microsoft<sup>®</sup> and SharePoint<sup>®</sup> are registered trademarks of Microsoft.

ArchiveLink<sup>®</sup> is a registered trademark of SAP.

All other trademarks are the property of their respective owners.

Gimmal LLC believes the information in this publication is accurate as of its publication date. The information in this publication is provided as is and is subject to change without notice. Gimmal LLC makes no representations or warranties of any kind with respect to the information contained in this publication, and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any Gimmal software described in this publication requires an applicable software license. For the most up-to-date listing of Gimmal product names and information, visit <u>www.gimmal.com</u>. All other trademarks used herein are the property of their respective owners.

If you have questions or comments about this publication, you can email <u>TechnicalPublica-</u><u>tions@Gimmal.com</u>. Be sure to identify the guide, version number, section, and page number to which you are referring. Your comments are welcomed and appreciated.

# Contents

Chapter 1. Configuring Secure Network Communications ERP-Link	for 1
1.1 Prerequisites	1
1.2 Downloading SAP Cryptography Software	2
1.3 Installing the SAP Cryptography Software	5
1.4 Creating the PSE for the Server	8
1.5 Setting SNC Additional Parameters	10
1.6 Creating PSE for RFC Client i-e for ERP-link iNet Connection Service	e 13
1.6.1 Installing SAP Cryptography on the Gimmal Connection Service Machine	13
1.6.2 Creating Client PSE	14
1.6.3 Importing and Exporting Client Certificates between Client PSE and SAP Applic Server	cation 
1.6.4 Creating the cred_v2 File	19
1.7 Configuring SAP for Secure Network Communications	20
1.7.1 Allowing SNC Connection with RFC	20
1.7.2 Mapping X.509 Certificate to User	22
1.8 Configuring Connection Service for SNC	24
1.8.1 Configuring SNC for iNet Connection Service	24
1.8.2 Testing SNC Using the Gimmal Connection Service	26

# **1 Configuring Secure Network Communications for ERP-Link**

This document provides information on how to install and configure secure network communications (SNC).

# **1.1 Prerequisites**

You must have the following present in your system:

- SAP Cryptography Software download
- SAP Application server installed and configured
- ERP-Link software installed and configured

For a complete list of ERP-Link prerequisites, see the *ERP-Link V5.2.0 Installation and Administration Guide* for details on installing and configuring this product, available on the <u>Gimmal product</u> <u>download site.</u>

# **1.2 Downloading SAP Cryptography Software**

To download SAP cryptography software, follow these steps.

1. Download the SAP cryptography software from the SAP marketplace and navigate to **Installation and Upgrade**.

俞	<	SAP Software D	ownloads
			SAP oProject Suite
			SAP CPS FOR SAP NETWEAVER SAP Central Process Scheduling by Redwood
			SAP CR. CHANNEL ORDER MGMT SAP Cross-Channel Order Management for Retail
			SAP CRM SAP Customer Relationship Management
			SAP CRM DESKTOP PE Desktop Connection for SAP CRM
			SAP CRM SERVICE MANAGER SAP CRM Service Manager
			SAP CRM VANSTOCK add-on for vehicle stock management with SAP CRM
			SAP CRYPTOGRAPHIC SOFTWARE
			SAP CRYSTAL SERVER SAP Crystal Server
			SAP CUSTOMER CHECKOUT SAP Customer Checkout
			SAP CYT MANAGEMENT SAP Capital Yield Tax Management
			SAP CYT MGMT FOR BANKING SAP Capital Yield Tax Management for Banking

Figure 1-1 Selecting SAP CRYPTOGRAPHIC SOFTWARE to Download

2. Click **SAP CRYPTOGRAPHIC SOFTWARE.** The **SAP CRYPTOGRAPHIC SOFTWARE DOWNLOADS** options display.

俞	<	SAP Software I	Downloads
			SAP CRYPTOGRAPHIC SOFTWARE
			DOWNLOADS INFO ECCN INFO
			SAPCRYPTOLIB
			SAP JVM JCE POLICY FILES 1.0
			SAP MOBILE ENGINE SSL
			SNC CLIENT ENCRYPTION 1.0
			XCEEDZIP 6.5.9417.0

Figure 1-2 SAP CRYPTOGRAPHIC SOFTWARE Download Options

3. Click SAPCRYPTOLIB. The SAPCRYPTOLIB DOWNLOADS options display.

俞	<	SAP Software	Downloads
			SAP CRYPTOGRAPHIC SOFTWARE / SAPCRYPTOLIB
			DOWNLOADS INFO ECON INFO
			COMMONCRYPTOLIB 8

Figure 1-3 SAPCRYPTOLIB DOWNLOADS Option

4. Download COMMONCRYPTOLIB8.

#### Note:

This is the latest cryptography software and it is also backward compatible with all prior cryptographic software versions.

lownloads						
SAP CRYPTOGRAPHIC SOFTWARE / SAPCRYPTOL COMMONCRYPTOLIB 8 DOWNLOADS INFO ECCN INFO	IB /					
Multispanning: Packages that are larger than 4 GB multispanning and how to extract the multi-part.exe	will be packed in an a archive on UNIX Se	archive, whic ae SAP Note	ch is split into 4 GB parts. All archives need 888535.	to be downloaded	l and unpacked. For r	nore details on
Items Available to Download (13)			AIX 64BIT			E 1↓
Selected Items (0)						
Name	Patch Level	File Type		ease Date	Change Date	Related Info
SAPCRYPTOLIBP_8510-20011699.SAR SAPCRYPTOLIBP	8510	SAR	LINUX ON IA32 32BIT	8.02.2017	28.02.2017	Ш.
SAPCRYPTOLIBP_8509-20011699.SAR SAPCRYPTOLIBP	8509	SAR	LINUX ON IA64 64BIT LINUX ON POWER BE 64BIT	0.02.2017	10.02.2017	Ê
SAPCRYPTOLIBP_8508-20011699.SAR SAPCRYPTOLIBP	8508	SAR	LINUX ON X86_64 64BIT LINUX ON ZSERIES 64BIT	2.02.2017	02.02.2017	Ŵ
SAPCRYPTOLIBP_8449-20011699.SAR SAPCRYPTOLIBP	8449	SAR	OS/400 SOLARIS ON SPARC 64BIT	4.03.2016	14.03.2016	Ê
SAPCRYPTOLIBP_8448-20011699.SAR	8448	SAR	SOLARIS ON X86_84 64BIT WINDOWS SERVER ON IA32 32BIT	3.02.2016	03.02.2016	Ê
SAPCRYPTOLIBP_8447-20011699.SAR	8447	SAR	WINDOWS ON IA64 64BIT WINDOWS ON X64 64BIT	3.12.2015	03.12.2015	Ê
SAPCRYPTOLIBP_8442-20011699.SAR	8442	SAR	Z/OS 64BIT	8.09.2015	28.09.2015	Ê

Figure 1-4 Downloading COMMONCYPTOLIB 8

5. Select your platform.

命 <	SAP Software	Downloads						
		SAP CRYPTOGRAPHIC SOFTWARE / SAPCRYPTOL COMMONCRYPTOLIB 8	IB /					
		DOWNLOADS INFO ECCN INFO						
		Multispanning: Packages that are larger than 4 GB multispanning and how to extract the multi-part .exe	will be packed in an archive on UNIX Se	archive, whi e SAP Note	ch is split into 4 GB parts. All archives a 888535.	need to be downloaded	d and unpacked. For r	nore details on
		Items Available to Download (12)			WINDOWS ON X64 64BIT	~		`⊟ _t
		Selected Items (0)						
		SAPCRYPTOLIBP_8510-20011729.SAR SAPCRYPTOLIBP	Patch Level 8510	SAR	File Size	28.02.2017	28.02.2017	Related Into
		SAPCRYPTOLIBP_8509-20011729.SAR SAPCRYPTOLIBP	8509	SAR	7584 KB	10.02.2017	10.02.2017	â
		SAPCRYPTOLIBP_8508-20011729.SAR SAPCRYPTOLIBP	8508	SAR	7592 KB	02.02.2017	02.02.2017	Ê
		SAPCRYPTOLIBP_8449-20011729.SAR SAPCRYPTOLIBP	8449	SAR	7306 KB	14.03.2016	14.03.2016	Ĥ
		SAPCRYPTOLIBP_8448-20011729.SAR SAPCRYPTOLIBP	8448	SAR	7288 KB	03.02.2016	03.02.2016	ê
		SAPCRYPTOLIBP_8447-20011729.SAR SAPCRYPTOLIBP	8447	SAR	7275 KB	03.12.2015	03.12.2015	Ê
		SAPCRYPTOLIBP_8442-20011729.SAR	8442	SAR	6790 KB	28.09.2015	28.09.2015	₩
		Figure 1	-5 Select	ing Y	our Platform			

6. Download the latest version.

# **1.3 Installing the SAP Cryptography Software**

To install the cryptography software, follow these steps.

- 1. You need the SAPCAR utility, available from the SAP download site, to extract the file you downloaded in 1.2 Downloading SAP Cryptography Software.
- 2. Extract the contents of the SAP Cryptographic Library installation package. The SAP cryptography is in this directory:

👔 nt-x86_64				
	_64		💌 🚱 Search	<b>P</b>
🕑 Organize 🔻 🏢 Views 🔻				0
Favorite Links Documents File Pictures Wusic More >>	Name A sapcrypto.dll sapcrypto.lst sapcrypto.pdb sapgenpse sapgenpse,pdb	•         Date modified         •         Type         •         Size           10/7/2014 3:31 PM         Application Extern.         2           10/8/2014 3:31 PM         Application Extern.         2           10/7/2014 3:31 PM         PDB File         1           10/7/2014 3:31 PM         Application         1           10/7/2014 3:31 PM         PDB File         1	▼   Tags   ▼ ,285 KB 1 KB ,531 KB 16 KB 131 KB	

Figure 1-6 Extracting SAP Cryptographic Library Contents

- 3. Copy the library file and the configuration tool (sapgenpse.exe) to the directory specified by the application server's profile parameter DIR\_EXECUTABLE. In the following example, this directory is represented with the notation \$(DIR\_EXECUTABLE).
- 4. Copy these library files to two locations:
  - D:\usr\sap\GE2\DVEBMGS00\exe
  - D:\usr\sap\GE2\SYS\exe\uc\NTAMD64
- 5. For both copies of the library files, follow these steps to check the permissions:
  - a. Right-click sapcrypto.dll and select **Properties**.

b. Click the **Security** tab.



Figure 1-7 Checking DLL Permissions

- c. Check the file permissions for the SAP Cryptographic Library. Make sure that <sid> adm (or SAPService <sid> under Windows) can execute the library's functions.
- 6. Locate the ticket <DRIVE>:\usr\sap\<SID>\<instance>\sec\ticket.

🔐 sec					
G D:\usr\sap\GE2\DVEBMG500\sec			I	🕶 🛃 Search	
🕒 Organize 🔻 🏢 Views 🔻					
Eavorite Links	Name 🔺	▼ Date modified ▼	Туре	▼ Size	🔹 🔻 Tag
	cred_v2	11/16/2015 9:49	File		1 KB
Documents	LASVerify.pse	11/9/2015 10:34	PSE File		1 KB
E Pictures	SAPSNCS.pse	11/17/2015 11:5	PSE File		3 KB
Nusic	SAPSSLS.pse	11/17/2015 11:5	PSE File		2 KB
More »	SAPSYS.pse	11/17/2015 11:5	PSE File		2 KB
	TEMP_E58A5980EBB83CF1925A00155D0204B2.pse	11/13/2015 4:54	PSE File		2 KB
Folders 🗸	TEMP_E587D30E31810FF1925A00155D0204B2.pse	11/10/2015 11:4	PSE File		2 KB
	TEMP_E5888FCF097D47F1925A00155D0204B2.pse	11/11/2015 4:01	PSE File		2 KB
Floppy Disk Drive (A:)	TEMP_E58700B02FCAF6F1925A00155D0204B2.pse	11/9/2015 10:41	PSE File		9 KB
🚢 OS (C:)	TEMP_E589654C434108F1925A00155D0204B2.pse	11/12/2015 11:4	PSE File		2 KB
Applications (D:)	ticket 🥢	2/28/2012 6:36 PM	File		1 KB

Figure 1-8 Locating the Ticket

7. Copy the ticket file to the sec subdirectory in the instance directory \$(DIR\_INSTANCE), which is DIR\_INSTANCE:

<DRIVE>:\usr\sap\<SID>\<instance>

8. Set the environment variable SECUDIR to the sec subdirectory.

The application server uses this variable to locate the ticket and its credentials at runtime. If you set the environment variable using the command line, the value may not be applied to the server's processes. Therefore, setting SECUDIR in the startup profile for the server's user or in the registry is recommended.

Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp
	New Edit Delete
ystem variables Variable	New Edit Delete
ystem variables Variable PSModulePath	Value C:\Windows\system32\WindowsPower5
ystem variables Variable PSModulePath SECUDIR	New         Edit         Delete           Value         C:\Windows\system32\WindowsPower5         D:\usr\sap\GE2\DVEBMG500\sec
ystem variables Variable PSModulePath SECUDIR SNC_LIB	New         Edit         Delete           Value         C:\Windows\system32\WindowsPower5         D:\usr\sap\GE2\DVEBMG500\sec           D:\usr\sap\GE2\DVEBMG500\sec         D:\Program Files (x86)\SAP\FrontEnd\5
ystem variables Variable PSModulePath SECUDIR SNC_LIB TEMP	New     Edit     Delete       Value     C:\Windows\system32\WindowsPower5       D:\usr\sap\GE2\DVEBMG500\sec       D:\Program Files (x86)\SAP\FrontEnd\S       C:\Windows\TEMP

Figure 1-9 Setting the Environment Variable

# **1.4 Creating the PSE for the Server**

To create the PSE for the server, follow these steps.

1. Start transaction **RZ10** and select the instance profile used by the server startup.

Parameter Name	Parameter value
(-util lanis uf-	1
shc/excld_login_ric	1
<pre>snc/extid_login_diag</pre>	1
<pre>snc/permit_insecure_start</pre>	1
<pre>snc/accept_insecure_rfc</pre>	0
<pre>snc/accept_insecure_r3int_rfc</pre>	1
<pre>snc/accept_insecure_gui</pre>	1
<pre>snc/accept_insecure_cpic</pre>	1
<pre>snc/data_protection/min</pre>	2
<pre>snc/data_protection/max</pre>	3
snc/gssapi_lib	D:\usr\sap\GE2\SYS\exe\uc\NTAMD64\sapcrypto.dll
snc/enable	1
icm/HTTPS/verify_client	1
ssl/ssl_lib	D:\usr\sap\GE2\SYS\exe\uc\NTAMD64\sapcrypto.dll
sec/libsapsecu	D:\usr\sap\GE2\SYS\exe\uc\NTAMD64\sapcrypto.dll
icm/server_port_2	PROT=HTTPS, PORT=8100, TIMEOUT=60, PROCTIMEOUT=60
ssf/ssfapi_lib	D:\usr\sap\GE2\SYS\exe\uc\NTAMD64\sapcrypto.dll
ssf/name	SAPSECULIB
snc/identity/as 🦰	p:CN=sap00.housapbw01v, OU=IT, O=GE2, C=US
SAPSYSTEMNAME	GE2
SAPGLOBALHOST	housapbw01v
SAPSYSTEM	00
INSTANCE_NAME	DVEBMGS00

Figure 1-10 Selecting the Instance Profile for the Server Startup

- 2. Add the instance parameter snc/identity/as.
- Set the instance parameter snc/identity/as to the specific name of the server. For example:

```
snc/identity/as P:CN=sap00.housapbw01v; OU=IT. 0=G2, C=US
```

Do not forget to add *p*: in front of the name.

#### Note

While specifying the distinguished name for your Client/Server P:CN=sap00.housapbw01v, ou-IT. 0=G2, c=us, the cryptographic tool validates the country code for the C=xx attribute.

4. Restart your server.

5. Create the SNC PSE.



Figure 1-11 Creating the SNC PSE

- 6. Start the **STRUST** transaction.
- 7. Right-click SNC (SAPCryptolib) and select Create.

Create	9 PSE	<b>X</b>
SNC ID	CN=IDS, OU=IT, O=CSW, C=DE	
<b>X</b>		

Figure 1-12 Selecting SAPCryptolib for the SNC

- 8. Accept the **SNC ID**, which is taken from the instance parameter snc/identity/as.
- 9. Double-click **SNC (SAPCryptolib)** and select **Assign Password** to add a password for the SNC (SAPCryptolib) PSE.

Password (New)	*****
Repeat Password	*****

Figure 1-13 Assigning a Password for the SNC PSE

- 10. Type in a password. The password can contain both letters and numbers. Without the password, the server will not start when you set the instance parameter snc/enable to 1.
- 11. Save the settings.
- 12. Create the server cred\_v2 file.
- 13. After setting up the server PSE, create a file named *cred\_v2*, which is used to give SAP secure access to the PSE without providing the password for the PSE.

C:\SAPCrypto>sapgenpse seclogin -p SAPSNCS.pse -O DV\SAPServiceGE2

#### Note:

DV\SAPServiceGE2 should be the account SAP runs under on the server.

14. At the text **Please enter PIN:**, type in your PIN.

15. At the text Added SSO-credentials for PSE <your path>/SAPSNCS.pse, enter

"P:CN=sap00.housapbw01v, OU-IT. O=G2, C=US

# **1.5 Setting SNC Additional Parameters**

Follow these steps to enable Add Additional SNC parameters.

1. Start transaction **RZ10**.

G	<u>P</u> rofile	<u>E</u> dit	<u>G</u> oto	Utilities	Syst	tem	<u>H</u> elp								
Ø				- 4 (		۵ و	<table-cell></table-cell>		H	K	2	Û	Ð	8	<u>*</u>
E	dit Pr	ofiles	5												
	Create	🔓 Cł	neck	🗎 Сору	🔁 In	nport									
	Profile Version	n	GE2_DV	EBMGS00_	HOUSA	PBW01	v	(Ir (S	istar aved	ice p I, act	orofile tivate	e ed			
	Edit Pr	ofile													
	⊖ Adn ⊖ Basi [• Exte	ninistrat c maint ended r Displa	ion data enance maintena y Ø	ance Change	<b>-</b>										

Figure 1-14 Starting Transaction RZ10

2. Select the instance profile used by the server startup.



Figure 1-15 Selecting the Instance Profile

3. Click the **Change** button.

🔄 <u>P</u> rofile P <u>a</u> rameter	<u>G</u> oto S <u>y</u> stem <u>H</u> elp
Ø	🔹 🔇   💐 🕄 😫   🚢 🏭 🔐   🏭 🕄 🕄 🔜
Maintain Profile	'GE2_DVEBMGS00_HOUSAPBW01V' Version '000012'
Copy 🞾 🖆 🗋 Parar	neter 🖉 Parameter 🖓 Parameter 🅨
18.11.2015	Active parameters 12:08:10

*Figure 1-16 Changing the Parameter* 

4. Click Create Parameter.



Figure 1-17 Creating the Parameter

5. Add the **Parameter** name and value.

Table 1-1 SNC Profile Parameters

Profile Parameter	Value	Example
snc/enable	1	1
snc/gssapi_lib	Path and filename where the SAP Cryptographic Library is located	UNIX: usr/sap/ <sid>/SYS/ exe/ run/libsapcrypto.so Windows: D:\usr\sap\<sid>\SYS\exe \run\sapcrypto.dll</sid></sid>
snc/identity/as	Application server's SNC name Syntax: p: <distinguished_name> The Distinguished Name part must match the Distinguished Name that you specify when creating the SNC PSE.</distinguished_name>	p:CN=ABC, OU=Test, O=MyCompany, C=US

Profile Parameter	Value	Example
<pre>snc/data_protection/max</pre>	1: Authentication only 2: Integrity protection 3: Privacy protection	3
<pre>snc/data_protection/min</pre>	1: Authentication only 2: Integrity protection 3: Privacy protection	1
snc/data_protection/use	1: Authentication only 2: Integrity protection 3: Privacy protection 9: Use the value from snc/ data_protection/max	9
<pre>snc/accept_insecure_cpic</pre>	0: do not accept 1: accept	1
<pre>snc/accept_insecure_gui</pre>	0: do not accept 1: accept	1
<pre>snc/accept_insecure_r3int_rfc</pre>	0: do not accept 1: accept	1
snc/accept_insecure_rfc	0: do not accept 1: accept	1
<pre>snc/r3int_rfc_secure</pre>	0: Internal RFCs are unpro- tected 1: Internal RFCs are protected with SNC	1
snc/r3int_rfc_qop	1: Secure authentication only 2: Data integrity protection 3: Data privacy protection 8: Use the value from snc/ data_protection/use 9: Use the value from snc/ data_protection/max	8

#### Table 1-1 SNC Profile Parameters (Continued)

- 6. Repeat steps 2 to 5 for all parameters.
- 7. Save the settings.
- 8. Restart the SAP Application server.

# **1.6 Creating PSE for RFC Client i-e for ERP-link iNet Connection Service**

This section contains steps for configuring SAP cryptography on the RFC Client side (i.e., ERP-link Connection Service).

## **1.6.1 Installing SAP Cryptography on the Gimmal Connection Service** Machine

Follow these steps.

1. Log on to the ERP-link server machine where the Connection Service is running.



Figure 1-18 Logging onto the ERP-Link Server

2. Create a directory named *SAPCrypto* and make sure the login account has full permission to the directory.

3. Make sure you set the SECUDIR environment variable to the directory SAPCrypto and copy the library to a different directory.

l	Environment Variables	>		
User variables for FV	Vajeehullah			
Variable	Value			
TEMP	%USERPROFILE%\AppData\Local\Temp			
TMP %USERPROFILE%\AppData\Local\Temp				
	New Edit Delete			
System variables				
Variable	Value	~		
RFC_TRACE	1			
RFC_TRACE_DIR RFC_TRACE_DU	C:\RFCTrace			
SECUDIR	C:\SAPCrypto	~		
	New Edit Delete			
	OK Cancel			

*Figure 1-19 Setting the Environment Variable* 

4. Add this path to your **PATH** environment variable.

## **1.6.2 Creating Client PSE**

Follow these steps to create the client PSE.

- 1. Launch the cmd process as an admin.
- 2. Change the directory to c:\sapcrypto directory.
- 3. Issue the following command:

```
C:\SAPCrypto>sapgenpse gen_pse -v -p RFC.pse
```

4. You will have to provide the PIN and the distinguished name (DN) of the user.

```
Got absolute PSE path "C:\SAPCrypto\RFC.pse".
Please enter PIN:
Please reenter PIN:
get_pse: Distinguished name of PSE owner: CN=RFC, OU=IT, O=GE, C=US
    Supplied distinguished name: "CN=RFC, OU=IT, O=GE, C=US"
Creating PSE with format v2 (default)
Generating key (RSA, 2048-bits) ... succeeded.
Certificate creation... ok
```

```
PSE update... ok
 PKRoot... ok
Generating certificate request... ok.
PKCS#10 certificate request for "C:\SAPCrypto\RFC.pse":
----BEGIN CERTIFICATE REQUEST----
MIICejCCAWICAQAwNTELMAkGA1UEBhMCVVMxCzAJBgNVBAoTAkdFMQswCQYDVQQL
EWJJVDEMMAOGA1UEAXMDUkZDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA/+xt00KoMapkf7GThg0FEBM620SZU6ptDd6/dr0m/HLvYNVtBF9bWTp67NAt
o4qhLwF0YEvRhT+1b5Ac5G7a4CppW0rFyew81naPa01yGqjCQTTesM44QXC5pBrj
PP+Om6Q8FtLRfnpBGiKu1MsABFnIln/R3rTXj9mLEAd43nvN8w7LL+mL9g/1ZyC8
KGGsG74oKsPM5jP5/FBBzlh8jgjMtCWJWPOV9qunToTWwBV1drXmOpJy2xcfA7Qy
n+H3yh08wrBVQb85IsEy3udeJEeZqKyM363GEiaiXn5ZqsBYJb1dqxMM7nVkTpOs
eF0ftzMau6HbThg29NjACsD5aQIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAEX+
xdvffsiCP7112N/U3/s511/E5ws7aFRfxX86tcuVEFx+QRkoMAxVRwQu6tfGTCY2
EPTagbNFx1+Txjks48j/sbgzrv4y11Kdf9Nw1pDcjYAZRzTYrbyj6HNqNWUdaphS
+Inc/HP5Tn4CEwHI6yvOBcVuT2wANJOQV5e+b6LHwUC+9OwER+Jq4p2VmH/oI2zf
/sHNyWYNnKmQuvGpA3eI5gtlscU10ZzrWQT+1MLiR411pJI1DcaS0eZQDLbBczm5
ftNMGIdRq5xU+hYG4VaCVGH2R70B3mIOrc+2hpRI7hnf2pqmtTxkn0XQ07wdfaNq
81+6GH6D0QpvosSpKyU=
----END CERTIFICATE REQUEST---
```

# 1.6.3 Importing and Exporting Client Certificates between Client PSE and SAP Application Server

For the Client RFC to communicate successfully with the SAP Application server, you must take the application server's certificate in STRUST and put it into the client's PSE. You must also take the RFC client's user certificate and add it to the server's PSE (typically via STRUST).

You can retrieve the certificates by following these steps.

1. Log in to cmd as an admin and issue the following command:

C:\SAPCrypto>sapgenpse export\_own\_cert -v -p RFC.pse -o RFC.crt

2. The following text displays.

```
Opening PSE "C:\SAPCrypto\RFC.pse"...
No SSO credentials found for this PSE.
Please enter PIN:
PSE (v2) open ok.
Retrieving my certificate... ok.
Writing to file (PEM-framed base64-encoded)... ok.
```

#### Note:

The RFC.pse file is under the c:\sapcrypto directory.



Figure 1-20 Location of the RFC.pse File

### Importing the Client Certificate to Server PSE

You can import the client certificate via transaction STRUST.

1. Open the Node SNC (SAPCryptolib).



Figure 1-21 Opening the Node SNC

2. Provide the password set when prompted.



Figure 1-22 Selecting Import Certificate

3. Click the **Import certificate** button.

File	Directory service	Database	SAP System
Filo nath	DUREC ort		
nie pauli	Jancar		
File forma	at		
and the second se			
OBinary			

Figure 1-23 Importing the Certificate

4. Select **File format** *Base64* and select the file.



5. Click **Add to Certificate List**. The certificate displays in the certificate list in SNC (SAP-Cryptolib).

Certificate List							
	Owner						
	CN=RFC, OU=IT, O=GE, C=US						
	CN=RFC, OU=IT, O=GE, C=US						
	· · · · · · · · · · · · · · · · · · ·						
	▼						
🔄 🛛 Veri. PSE	Password						
Certificate							
Owner	CN=RFC, OU=IT, O=GE, C=US						
Issuer	CN=RFC, OU=IT, O=GE, C=US						
Serial Number	0A20151109185555						
Valid From 09.11.2015 18:55:55 to 01.01.2038 00:00:01							
Check Sum							

*Figure 1-25 Verifying the Certificate* 

#### Note:

Two different certificates in the certificate list.sap.

## Exporting the Server Certificate

To export the server certificate, follow these steps.

- 1. In the STRUST node SNC (SAPCryptolib), double-click on your server's certificate to display it in the **Certificate** field.
- 2. Click Export certificate.
- 3. At node **SNC (SAPCryptolib)**, double-click your server's certificate to display it in the **Certificate** field.
- 4. Click Export certificate.
- 5. Click the **File** tab.

🔄 Export Certificate	×
File Directory service Database	
File path C:\sec\ServerCert.crt	
File format         Binary         Base84	
	<ul><li>✓ ×</li></ul>

Figure 1-26 Exporting the Certificate

- 6. Select **Base64** for the **File format** and provide a name for the file.
- 7. Click the **Ok** button.

## Importing the Server Certificate to the Client PSE

To import your server's certificate to the client PSE, follow these steps.

1. Copy the server certificate that you saved in Exporting the Server Certificate to the ERPlink iNet Connection Service machine. 2. Issue the following command from the command prompt:

#### Note:

You have to provide the pin you set earlier. //?

### **1.6.4 Creating the cred\_v2 File**

After setting up the client PSE, you must create a file called cred\_v2, which is used to give the RFC Program (iNet CS) secure access to the PSE without providing the password for the PSE.

#### Note

The cred\_v2 file is created through calling sapgenpse using the seclogin parameter. It is created in the same directory as the .pse file.

```
1. Run this operating:
```

C:\SAPCrypto>sapgenpse seclogin -p RFC.pse -O DV\ConnectorService

#### Note:

pv\connectorservice should be the account that the iNetRemote service or the Connector 5.0 Application pool account is using.

2. Enter information as you are requested to do so.

```
Please enter PIN: *******
Added SSO-credentials for PSE "<your path>/RFC.pse"
"CN=RFC, OU=IT, O=CSW, C=DE
```

Run this operation for each user account that might need to access the PSE file.

# **1.7 Configuring SAP for Secure Network Communications**

Now you need to map the x.509 certificates that were created for the user accounts on the SAP Server.

## 1.7.1 Allowing SNC Connection with RFC

Perform these steps to allow Secure Network Communications to connect with the RFC.

1. Start transaction **SM30**.

🗞 🛛	▼ 4 🗎 ble Views: Init	i C @ Q   🗅 H	1643668	<u>*</u>
聞 Find Maintenance	e Dialog			
Table/View	VSNCSYSACL	-		
Restrict Data Range				
●No Restrictions				
O Enter conditions		1		
Ovariant				
🗞 Display	🖉 Maintain	Transport	Customizing	
[□=> Info	rmation		Ì	×
			٦	
	aution: The table is o	ross-client	L.	
				3
			🛩 🔇	2

Figure 1-27 Starting Transaction SM30

- 2. Enter the **View** *VSNCSYSACL*. This view restricts the SNC RFC Connections by an Access Control List (ACL).
- 3. When an alert displays, click the **right** button on the bottom.



Figure 1-28 Selecting ACL Entry

4. Select *E* for the **Type of ACL entry** and click the **right** button on the bottom. 

System IP	IDS		
SNC name	p:CN=RFC, OU=IT, O	=CSW, C=DE	
Entry for RFC	activated		
Entry for CPI	C activated		
Entry for DIA	G activated		
Entry for cer	tificate activated		
Entry for ext	. ID activated		
SNC data		Administrative	data
🖌 Canonical	Name Determined	Created by	G.WOLF

Figure 1-29 Selecting Type of ACL Entry

#### 5. Enter System ID and SNC name.

T

100

#### Note:

Do not forget the p: in front of the DN.

- 6. Select the following check boxes:
  - Entry for RFC activated
  - Entry for CPIC activated
  - Entry for certificate activated
  - Entry for ext. ID activated
- 7. Save the entry.

#### Note:

When trying to edit the entry, you might see an alert window display. Click the **right** symbol and make your changes.

## 1.7.2 Mapping X.509 Certificate to User

To map the X.509 Certificate to the user for a successful login, follow these steps.

- 1. Start **Transaction SM30**.
- 2. Enter VUSREXTID and click Maintain.
- 3. Using the view **VUSREXTID**, set up a mapping between the **DistinguishedName** provided by an X.509 Certificate and an ABAP User.

C Determine Work Area: Entry	6	×
External ID type	Work Area	
✓ Further select cond. Append	Pi 🗙	

Figure 1-30 Setting Mapping

4. Select the **Distinguished Name** for the **External ID type**.

5. Create a new entry and activate it.



Figure 1-31 Activating Mapping

6. Save the entry.

# **1.8 Configuring Connection Service for SNC**

This section contains the steps necessary to configure the Connection Service to use SNC.

## **1.8.1 Configuring SNC for iNet Connection Service**

Before starting these steps, make sure that the ERP-link product has been installed and configured. Refer to the latest version of the *ERP-link Installation and Administration Guide* for more information.

- 1. Log in to the iNetCSAdmin Console.
- 2. Click the Connection Pool to configure the connection settings.

Figure 1-32 Selecting the Connection Pool

3. To configure SNC settings to be used by iNet CS, provide this information:

Destination string: ASHOST=housapbw01v SYSNR=00 SNC\_PARTNERNAME="p: CN=sap00.housapbw01v, OU=IT, O=GE2, C=US" SNC\_MYNAME="p: CN=RFC, OU=IT, O=GE, C=US" SNC\_QOP="8" SNC\_MODE="1" SNC\_LIB=C:\SAPCrypto\sapcrypto.dll

#### Note:

SNC\_MODE =1 means that SNC is enabled

Select and enter all the other settings on the screen, such as Logon mode and the SAP credentials.

e Action view ravontes window	nep	
) 🖄 📰 🛿 🗊		
onsole Root		Actions
ERP-Link CS Administration	Pool #01; SAP BW system	01: Pool #01: SAP BW sv
CS Hubs	Destination String ="8" SNC_MODE="1" SNC_LIB=C:\SAF System GE2	Connection pool details
⊿ 🛁 Connection Pools	Logon control	Access control
00: Pool #00;SAP 01: Pool #01; SAP BW s	Logon Mode SAP credentials	Validate
02: Pool #02; (unconfig 02: Pool #02; (unconfig	Shared & anonymous     Client     800	Save & Activate
▷ 100 HO3; (unconfig ▷ 100 HO4; (unconfig =	User fwajeehu	Save w/o Activation
05: Pool #05; (unconfig	Password	
Vb: Pool #06; (unconfig Vb: Pool #07; (unconfig	Language en	New Window from Here
▶ 🔏 08: Pool #08; (unconfig		7 Help
09: Pool #09; (unconfig 10: Pool #10; (unconfig	Pool size	
11: Pool #11; (unconfig	Max. number of live connections 5 Min. 1	
▷ 12: Pool #12; (unconfig		
13: Pool #13; (unconfig 14: Pool #14; (unconfig	Testing configuration	
15: Pool #15; (unconfig		
⊳ 🚡 16: Pool #16; (unconfig	Configuration successfully validated. System discovered: GE2	
17: Pool #17; (unconfig)		
Fig. 10: Pool #10; (unconfig 19: Pool #19: (unconfig)		
⊳ 🚡 20: Pool #20; (unconfig	ОК	
21: Pool #21; (unconfig		
22: Pool #22; (unconfig) 3: Pool #23; (unconfig)		

5. After completing all the configuration details, click **Validate**.

Figure 1-33 Validating the Connection

- 6. If the SNC is properly configured, you should see the message *Configuration successfully validated. System GE2.* Click **OK**.
- 7. **Save** and then **Activate** to save the configuration.

## Configuring Connector 5.0 for SNC

- 1. Display the Admin console settings,
- 2. Make sure the RFC.PSE and the cred\_v2 files are copied to:

## **1.8.2 Testing SNC Using the Gimmal Connection Service**

Follow these steps to test if SNC is correctly set up.

1. Run the transaction **RZ10**.



Figure 1-34 Running the RZ10 Transaction

- 2. Make sure the parameter snc/accept\_insecure\_rfc is set to 0 (zero), which means do not accept any insecure connections.
- 3. From the iNetCs administration console, set the SNC\_MODE =1 to disable SNC.
- 4. Now attempt to validate a connection. A message similar to the following displays:

-	Description Pool #01; SAP BW system
	Destination String ="8" SNC_MODE="0" SNC_LIB=C:\SAF System (?)
	Logon control
	Logon Mode SAP credentials
	Shared & anonymous     Client     800
	O Shared w/ SAP Auth. User [fwajeehu
	O User Password ••••••
	Language en
	Pool size Max. number of live connections 5 Min. 1
-	Configuration could not be validated
	Connection attempt has failed. Details: SNC required for this connection
	ОК

Figure 1-35 Validating the Connection

This message indicates that SNC must be active on the RFC client, and in this case, iNet CS service can make a connection to SAP.

5. Click **OK**.

6. When you enable the SNC on iNet Cs service, the connection should be successful.

ow Help	
<ul> <li>▲ Description</li> <li>Destination Stri</li> <li>Logon contro</li> <li>Logon Mod</li> <li>④ Sharee</li> <li>○ Sharee</li> <li>○ User</li> </ul>	Pool #01: SAP BW system         ng       ="8" SNC_MODE="1" SNC_LIB=C:\SAF       System         e       SAP credentials         d & anonymous       Client       800         d w/ SAP Auth.       User       Fwajeehu         Password       •••       Language         e       e       e
Pool size Ma	ax. number of live connections 5 Min. 1
	Testing configuration X
	Configuration successfully validated. System discovered: GE2
	ОК

Figure 1-36 Successful Connection Message