ABAP Digital Signature guide for NFE

Disclaimer

The Web sites listed on this page do not contain SAP content and SAP does not represent or endorse the accuracy or reliability of any of the information, content, or advertisements (collectively, the "Materials") contained on, distributed through, or linked, downloaded, or accessed from any of the services contained on these Web sites. The information listed makes no claim to completeness, is a snapshot of 01/01/2015 and can change at any time or expire.

1	PROLOGUE	2
1.1	Installing the SAP Cryptographic Library	2
1.2	Determine the current SAPCryptolib version and patch level	2
1.3	XML Signature Test Program	2
1.4	Required Notes	2
1.5	Check and Warn About Certificates that Expire in Near Future	2
2	NFE INCOMING	3
2.1	Creating the PSE for NFE Signature Check	3
2.2	Import CA certificates	5
3	NFE OUTGOING	12
3.1	Obtain the private certificate	12
3.2	Create PSE	12
3.3	Create SSF application	12
3.4	Set Application Parameters	14
3.5	Load the PSE	16

1 Prologue

1.1 Installing the SAP Cryptographic Library

For the digital signature of NF-e data in the SAP system using Secure Store and Forward (SSF) you must install the SAP Cryptographic Library (SAPCRYPTOLIB) as described in SAP Note 662340 - SSF Encryption Using the SAPCryptolib. This is the prerequisite for the instructions in this manual. To support certificates with SHA-2 hashes the patch level should be at least on PL29.

1.2 Determine the current SAPCryptolib version and patch level

- (1) Run program SSF02
- (2) Execute
- (3) "Determine Version"
- (4) Execute
- (5) Version information: "SSFLIB Version 1.555.34"
- (6) The last two digits are the patch level

1.3 XML Signature Test Program

The program SECXML_DSIGNATURE provides an UI for testing both Sign and Verify a XML source and takes the configured PSE application and a local XML file name as input.

SAPCRYPTOLIB with Patch Level 30 is needed as prerequisite.

1.4 Required Notes

To prevent that the XML signature check fails if inclusive canonicalization is specified the following Notes must be applied:

1866334 CL_SEC_SXML_DSIGNATURE: Inclusive C14N

1666950 XML Signature check fails for inclusive canonicalization

1736879 XML Signature check fails for inclusive canonicalization

1333974 Central Note for WS Security on 7.20

1.5 Check and Warn About Certificates that Expire in Near Future

SSF_ALERT_CERTEXPIRE is a dialog report to check the validity period of certificates (SAP Note 572035). The task of this report is to provide warnings in the desired time before the expiry of the validity of installed certificates. The warnings can be provided in a variety of ways, e.g. via email. You can also schedule this report as a daily background job.

2 NFE Incoming

Importing the CA certificates for verification of the digital signature of incoming NF-e's

2.1 Creating the PSE for NFE Signature Check

From the Administration workplace use transaction STRUST – SSF: Trust Manager and create a self-signed PSE for SSF NFE signature validation:

I Edit Certificate	En <u>v</u> ironment S <u>v</u> stem <u>H</u> elp
۵ 🔹 🗸	📙 🛠 🚱 🛄 🛗 월 한 🎝 왕 🛒 🖉 🍞 📑
Trust Manager	
X SNC SAPCryptolib X SSL server Standard	Own Certificate
SSL client SSL Client (Anonyr SSL client SSL Client (Standa SSL client WSSE Web Service	Owner <u>CN=15M</u> Image: CN=15M (Self-Signed)
 X WS Security Standard X WS Security Other System En X WS Security WS Security Keys File SSF NFE signature creation C SSF NFE construct validation SSF NFE signature solidation 	Certificate List
	Veri. PSE Assword
	Certificate
	Owner
	Issuer
	Serial Number (Dec.)
	Valid From to
	Algorithm Key Length
	Check Sum (MD5)
	Checksum (SHA1)
	Add to Certificate List

Confirming suggestion of PSE:

🖙 <u>P</u> SE <u>E</u> dit <u>G</u> oto <u>C</u> ertific	ate En⊻ironment S⊻stem <u>H</u> elp
•	4 ■ C G Q ⊒
Trust Manager	
🕨 💼 System PSE	System PSE
SNC SAPCryptolib	Own Certificate
SSL server Standard SSL client SSL Client (Anon)	Wr Owner CN=15M
 X SSL client SSL Client (Stand 	(Self-Signed)
• 💥 SSL client WSSE Web Servi	Cf
K WS Security Standard WS Security Other System E	Certificate List
X WS Security WS Security Key	ys Owner
• 🔗 File	
SSF NEE cignature creation Soft Provide PSE	
Name IS	IN SSENEE signature validation
Comp (Org	3020179812
Country	
CA	=SAP Trust Community, C=DE
Algorithm D	DSA V
Key Length 1	024 💌
	Valid From to
	Algorithm Key Length
	Check Sum (MD5)
	Checksum (SHA1)
	Add to Certificate List

2.2 Import CA certificates

After receive the message "Data saved successfully", import the CA certificate of the issuer (the certification authority, e.g. AC CERTISIGN or SERASA) of the signing certificate (encoded in the XML tag <X509Certificate>). You can download the CA certificates as described here:

http://www.iti.gov.br > ICP-BRASIL > Repositório

You have to import all CA certificates of the signers of the NF-e you get in your Inbound scenario, and that might be a double digit number. Still, you don't need the whole certificate chain, only the lowest intermediate certificate from each CA.

You can restrict the number by finding out the CA's of your partner. To speed up a particular case with a particular partner, you can ask him for the certification provider he used.

Or to find the CA in the XML of the Inbound-NF-e take the Certificate between the tags <X509Certificate> and </X509Certificate> and copy the content of X509Certificate tag to a notepad file between two fixed lines below:

----BEGIN CERTIFICATE-----MIIGWjCCBUKgAwIBAgIIe94LRpgIoVYwDQYJKoZIhvcNAQEFBQAwdTELMAkGA1UEBhMCQlIxEzARBgNVBAoTCklDUC1CcmFzaWwx NjAOBgNVBAsTLVNlY3JldGFyaWEgZGEgUmVjZWl0YSBGZWRlcmFsIGRvIEJyYXNpbCAtIFJGQjEZMBcGA1UEAxMQQUMgU0VSQVNB IGRvIEJyYXNpbCAtIFJGQjEWMBQGA1UECxMNUkZCIGUtQ05QSiBBMTESMBAGA1UECxMJQVIgU0VSQVNBMTYwNAYDVQQDEy1VTklM TOcgVU5JVkVSU08gTE9HSVNUSUNBIExUREE6MDUyOTY10TAwMDAxNjUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKn+Ghn9 B8WMXA1E+kb9Xg87bzVmCBz312RWmP4IMpY0TGCoHe8ncVTPysiQovwMvJjrXXRZhlCSt1UBCazpYVNY/cdkBiljGg24/S0Yn4N8 xc+XJC2AhpC9dx9MvpbIA9t0WjNsgxTpXBZuYBxPj/7yQbs43T5th5tFy2tH2HzICi91fI03D1sAdxtGKaDmii9LMIQ== ----END CERTIFICATE-----

Then save it as .cer-file and double click on the file. Windows will show the certificate:

Certificate
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
 Proves your identity to a remote computer Protects e-mail messages
* Refer to the certification authority's statement for details.
Issued to: UNILOG UNIVERSO LOGISTICA LTDA:05296590000165
Issued by: AC SERASA RFB v1
Valid from 22/07/2011 to 21/07/2012
Install Certificate Issuer Statement Learn more about <u>certificates</u>
ОК

If you have the full chain inside your computer you can also see the path and the name of the CA:

Certificate
General Details Certification Path
Certification path
View Certificate
Certificate status:
This certificate is OK.
Learn more about <u>certification paths</u>
ОК

Import the CA certificate of the certification authority in STRUST:

E <u>P</u> SE <u>E</u> dit <u>G</u> oto	<u>C</u> ertificate	Environment	System <u>H</u> elp
Ø	<u>I</u> mport <u>E</u> xport		
Trust Manager	<u>D</u> ataba <u>A</u> ddres	ise is Book	_
 System PSE SNC SAPCryptolib SSL server Standar SSL client SSL Clie SSL client SSL Clie SSL client WSSE W SSL client WSSE W SSL client WSSE W WS Security Other 5 WS Security Other 5 WS Security WS Service File SSF NFE signature SSF NFE signature p246191_5M_0 	d nt (Anonyr nt (Standa eb Servicc rd cystem En curity Keys creation C validation	ortal <u>C</u> A (DSA) SSF NFE signature Own Certificate Owner Image: Certificate List Certificate List Image: Certificate Overi. PSE Certificate	Validation CN=I5M SSF NFE signature validation, OU=I0020179812, OU=SAP (Self-Signed) Owmer Owmer Password

SE <u>E</u> di	it <u>G</u> oto	<u>C</u> ertificate	e En <u>v</u> ironment System <u>H</u> elp
		- <	
SE Edi UST Ma System SSL Clie SSL clie	PSE PCryptolib ver Standa ent SSL Clie ent S	C:TEM	Engronment System Help
	SE Edi	SE Edit Qoto	SE Edit Goto Certificate

If receive an error like "SSF kernel error: invalid parameter" try to change file format:



The certificate will be shown on Certificate box:

로 <u>P</u> SE <u>E</u> dit <u>G</u> oto <u>C</u> ertifica	e En <u>v</u> ironment System	Help
 The second second	4 🔲 😋 🙆 🚱 昌 🛛	📲 😵 🔍 💥 C2 C2 C4 C4 C4
Trust Manager		
 System PSE SNC SAPCryptolib SSL server Standard SSL client SSL Client (Anonyr SSL client SSL Client (Standa SSL client WSSE Web Service WS Security Standard WS Security Other System En WS Security WS Security Keys File SSF NFE signature creation C SSF NFE signature validation p246191_I5M_04 	SSF NFE signature validati Own Certificate Owner Certificate List	on Description Description Owner Owner The second se
	🔄 Veri. PSE 🔒	Password
	Certificate Owner Issuer Serial Number (Hex.) Serial Number (Dec.) Valid From Algorithm Check Sum (MD5) Checksum (SHA1)	CN=Autoridade Certificadora Raiz Brasileira v1, OU=Instituto Nacior CN=Autoridade Certificadora Raiz Brasileira v1, OU=Instituto Nacior 01 ? 29.07.2008 19:17:10 to 29.07.2021 19:17:10 ? Key Length ? 93:F1:AD:34:0B:2B:E7:A8:54:60:E2:73:8C:A4:94:31 705D2B4565C7047A540694A79AF7ABB842BDC161

Click on Add to Certificate List



Repeat the same step for other CA certificates

Import one by one the CA certificates for all certification authorities of your business partners.

🖙 <u>P</u> SE <u>E</u> dit <u>G</u> oto <u>C</u> ertifica	te En <u>v</u> ironment System	Help
 The second second	4 📙 😋 😳 🚱 昌 🛛	비 🎼 최 한 유 외 🛒 🗾 🍞 📑
Trust Manager	1	
 System PSE SNC SAPCryptolib SSL server Standard SSL client SSL Client (Anonyr SSL client SSL Client (Standard) SSL client WSSE Web Service 	SSF NFE signature validati Own Certificate Owner	on <u>DN=I5M SSF NFE signature validation, OU=I0020179812, OU=SAP</u> (Self-Signed)
WS Security Standard WS Security Standard WS Security Other System En WS Security WS Security Keys	Certificate List	Owner Image: CN=Autoridade Certificadora Raiz Brasileira v1, OU=Instituto Na CN=AC Certisign Multipla G3, OU=Certisign Certificadora Digits CN=AC Certisign G3, OU=Instituto Nacional de Tecnologia da II CN=Autoridade Certificadora da Justica v3, OU=Instituto Nacion
	🔄 Veri. PSE 🔒	Password
	Certificate Owner Issuer Serial Number (Hex.) Serial Number (Dec.) Valid From Algorithm Check Sum (MD5) Checksum (SHA1)	CN=Autoridade Certificadora da Justica, O=ICP-Brasil, C=BR CN=Autoridade Certificadora Raiz Brasileira, SP=DF, L=Brasilia, OL 15 ? 19.12.2005 13:00:00 to 19.06.2011 23:59:00 ? Key Length ? DC:04:12:2D:35:70:52:DB:D2:9C:0B:08:93:1A:52:88 77658057E59110EB29C13A38931866AEF2794775

After import and add all certificates to list, save it to persist the changes



3 NFE Outgoing

In the following the customizing of the private certificate for digital signature of outgoing NF-es is described.

3.1 Obtain the private certificate

In order to issue electronic invoices the xml must be signed using a digital certificate compliant with ICP-Brasil standards securing the access between the NFE system and the government's servers.

To obtain the digital certificate you must interact with a Certification Authority. You can find a completed and updated list of Certificating Authorities on the National Information Technology Institute (ITI Brazil) website http://www.iti.gov.br. The main Certification Authorities are: Caixa, Serasa, Certisign, Valid, Digitalsign, Boa Vista.

The Certificating Authorities can issue both certificates as well as certificates in the form of a physical token; so make sure you request the digital certificate that can be used for e-commerce transactions in PKSC#12 format with the file ending .pfx.

Hints:

- The certificate can also be used for the client authentication using https in PI.
- For signing you can also use the physical token and connect it via PI using enhancement spot /XNFE/CORE_SIGNATURE_CREATE_EN

3.2 Create PSE

Use tool SAPGENPSE to create PSE on the Command Prompt from existing private certificate as described in <u>Importing a PKCS#12 File</u>:

sapgenpse import_p12 -p <path>file.pse bras.pfx

Hints:

 In case of an error that the pfx is missing the certification chain you can complete the chain by adding the missing certificates with option '-r'. Then the command line should look like this:

sapgenpse import_p12 -r SerasaACPv2.cer -r ICPBrasilv2.cer -p <path>file.pse bras.pfx

- Inform the full path for the PSE to be created.
- If asked for a PSE PIN enter one or click Return.

3.3 Create SSF application

From the Administration workplace use application *SSF: Define Application.* With this administration UI SSF applications are created and also all attributes are set correctly in the SSFAPPLIC table. You need a separate SSF application for each private certificate that you use for signing the NF-e (e.g. for each own tax number). This step has to be done in all three the dev, test and production systems (no transport).

Existing SSF Applicat	ons	
New Entry		
SSF Application	SSF Application Description	
DFAULT	Standard Application	
ELEARN	Create an SSF Application	
HTTPCS		
NFESIG	SSF Application: * NFE001	
NFE_IN	SSF Application Description: * NFE signature creation CNPJ 12345678	
DFX		
PLMCPR		
PPPI		
	OK Cancel	

The SSF applications have also to be customized in IMG activity Outbound > "Maintain System Response for Own Tax Numbers".

3.4 Set Application Parameters

From the Administration workplace use transaction SSFA – SSF: Set Application Parameters

¢	<u>T</u> able View	<u>E</u> dit	<u>G</u> oto	<u>S</u> election	Utilities(<u>M</u>)) S <u>v</u> stem	<u>H</u> elp			
6			•	• 4 📙	😋 😧 🚷		🎝 🔁	10 XI	₩ 🏹	🔞 🖪
	Change V	liew "	Appli	cation-S	pecific S	SSF Para	meters	": Ove	rview	
60 4	🖉 🕄 🛛 New B	Entries	D 📑	🗠 🖪 🖪						
	Application-S	pecific S	SF Parar	neters						
	Appl.			SS	F prod.	SSF format				
										-
_										

Create the configuration for ZNFE01 (for sign NF-es)

Ż <u>T</u> able View	<u>E</u> dit <u>G</u> oto	<u>S</u> election	Utilities(<u>M</u>)	System	<u>H</u> elp	
0		- 4 目	😋 🙆 🚷	l h k	12002	🕱 🗾 🔞 🛯
New Entri	es: Details	of Adde	ed Entries			
🎾 📑 🔂 🗟						
SF Application	PAY(PPPI ELE# HTTF SSO NFE NFE OFX	CRD Digital S ARN E-Learr PCS HTTP cl 2 Logon 1 201 NFE sig _IN NFE sig Open Fl	Signatures Adh ning ontent Server Ficket gnature creation gnature validati inancial Exchai	ering to FDA 1 CNPJ 123 201 1 ge Applicat	A Requirements 45678 iion Level 1	
	PLM PSR	CPR PLM cP M Public S	rojects Sector Records	Manageme	ent	* *

Filling data:

Ø	▾ ◁ 📙 ✿ ֎ ֎ 📮 🗑 🖧 활 앱 ይ ֎ 🛒 🔊 😵 星	
New Entries: D	etails of Added Entries	
🦅 📑 🔂 🗟		
3SF Application	NFE001 NFE signature creation CNPJ 12345678	
Application-Specific SSF	Parameters	
Security Product	SAPSECULIB	
SSF Format	PKCS7 International standard PKCS#7	
Private Address Book	NFE_SAP12345678.pse	
SSF Profile Name	NFE_SAP12345678.pse	
SSF Profile ID (Opt)		
Hash Algorithm	SHA1	
Encryption Algorithm	AES128-CBC 🗖	
Include Certificates		
Digital Signature with Data		

3.5 Load the PSE

From the Administration workplace use transaction STRUST – SSF: Trust Manager and load the PSE: Double click on *File*:

	e En <u>v</u> ironment System <u>H</u> elp
 The second second	4 📙 🛠 🚱 😫 📇
Trust Manager	File
SNC SAPCryptolib SSL server Standard SSL client SSL Client (Anonyr SSL client SSL Client (Standa SSL client SSL Client (Standa SSL client WSSE Web Service	Own Certificate Owner Image: Comparison of the second s
 XWS Security Standard XWS Security Other System En XWS Security WS Security Keys File XSF NFE signature creation C XSF NFE signature validation 	Certificate List
	Veri. PSE Password
	Certificate
	Owner Issuer
	Serial Number (Hex.)
	Serial Number (Dec.)
	Algorithm
	Check Sum (MD5)
	Checksum (SHA1)
	Add to Certificate List



Informing the .pse which is copied from server to local machine

Inform the password of PSE

 X WS Security Standard 	Certificate List		
🔸 💥 WS Security Other System En	Owner		
🔸 💥 WS Security WS Security Keys			
• 🔗 File			
 X SSF MEE cignature creation () 			
🔸 🗶 SSF 🗁 File			
Password ******	······································		

Choosing PSE -> Save as...

G	7	<u>PSE</u> dit <u>G</u> oto	<u>C</u> ertificate	En <u>v</u> ironment System <u>H</u> elp	
	6	<u>I</u> mport <u>E</u> xport	1	I 📙 🕸 🚱 🛄	
		<u>S</u> ave as			
		Create <u>V</u> erification P	SE		
		Check <u>A</u> ll	F5		
		Distribute A <u>I</u> I	F6	File	
		E <u>x</u> it Sł	hift+F3	Own Certificate	
	•	 SSL client SSL Clier SSL client SSL Clier SSL client WSSE We 	nt (Anonyr nt (Stands eb Servic:	Owner EMAIL=bruno.renzo@sap.com, CN=SAP Brasil Ltda, OU=(EM BRAN QE Email_=bruno.renzo@sap.com, CN=SAP Brasil Ltda, OU=(EM BRAN	
	•	X WS Security Standar	rd	Certificate List	
		X WS Security Other S X WS Security WS Sec File X SSF NFE signature of SSF NFE signature of	iystem En curity Keys creation C validation	Owner	
				Veri. PSE Password	

Select SSF application on Save PSE as box, and select and confirm the proper SSF for signature which are being created:

Data saved successfully...

 ▼ SSF NFE signature creation C ■ p246191_I5M_04 ■ 005 NFE is in the matrix 	
Image: PSE Edit Goto Certificat Image: PSE Manager Image: PSE System PSE	e Environment System Help 4 🕒 😋 🚱 📮 🎁 🛍 😩 管 🖧 🏝 🛒 💽 🎯 📑 SSF NFE signature creation CNP
 SNC SAPCryptolib SSL server Standard SSL client SSL Client (Anonyr SSL client SSL Client (Standa SSL client WSSE Web Service WS Security Standard WS Security Other System En WS Security WS Security Keys ST FITE SSF NFE signature creation (Own Certificate Owner Email_=bruno.renzo@sap.com, CN=SAP Brasil Ltda, OU=(EM BRAN) Certificate List Owner Image: Comparison of the second
	Certificate Owner Issuer Serial Number (Hex.) Serial Number (Dec.) Valid From Algorithm Key Length Check Sum (MD5) Checksum (SHA1) Image: Construction of the construction of t