

Technologies & Products

Haachtsesteenweg 1442 1130 Brussels Belgium

# **DEP Documentation**

# NCR Self-Signed Certificate User Manual

Versio	Version Management Report		
Version	Name(s)	Date	Comments
01.00	David Lheureux	26/10/2006	First version
01.01	David Lheureux	27/10/2006	After review.

#### CONFIDENTIALITY

The information in this document is confidential and shall not be disclosed to any third party in whole or in part without the prior written consent of Banksys S.A./N.V.

#### COPYRIGHT

The information in this document is subject to change without notice and shall not be construed as a commitment by Banksys S.A./N.V.

The content of this document, including but not limited to trademarks, designs, logos, text, images, is the property of Banksys S.A/N.V. and is protected by the Belgian Act of 30.06.1994 related to author's right and by the other applicable Acts.

The contents of this document must not be reproduced in any form whatsoever, by or on behalf of third parties, without the prior written consent of Banksys S.A./N.V.

Except with respect to the limited license to download and print certain material from this document for non-commercial and personal use only, nothing contained in this document shall grant any license or right to use any of Banksys S.A./N.V.'s proprietary material.

#### LEGAL DISCLAIMER

While Banksys S.A./N.V. has made every attempt to ensure that the information contained in this document is correct, Banksys S.A./N.V. does not provide any legal or commercial warranty on the document that is described in this specification. The technology is thus provided "as is" without warranties of any kind, expressed or implied, included those of merchantability and fitness for a particular purpose. Banksys S.A./N.V. does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product or process disclosed.

To the fullest extent permitted under applicable law, neither Banksys S.A./N.V. nor its affiliates, directors, employees and agents shall be liable to any party for any damages that might result from the use of the technology as described in this document (including without limitation direct, indirect, incidental, special, consequential and punitive damages, lost profits).

#### JURISDICTION AND APPLICABLE LAW

These terms shall be governed by and construed in accordance with the laws of Belgium. You irrevocably consent to the jurisdiction of the courts located in Brussels for any action arising from or related to the use of this document.

sa Banksys nv – Chaussée de Haecht 1442 Haachtsesteenweg B-1130 Bruxelles-Brussel - Belgium RPM-RPR Bruxelles-Brussel - TVA-BTW BE 0418.547.872

# 1. TABLE OF CONTENTS

1.	TABLE	C OF CONTENTS	4
2.	SCOPE	OF THE DOCUMENT	5
3.	REFER	ENCES	5
4.	PURPC	SE OF NCR SELF-SIGNED CERTIFICATE PROGRAM	5
5.	USE O	F NCR SELF-SIGNED CERTIFICATE	6
	5.1. St.	ART-UP	6
	5.2. De	SCRIPTION	6
	5.3. CO	MMUNICATION	7
	5.3.1.	INI File	7
	5.3.2.	TCP/IP Configuration window	8
	5.4. но	W TO GENERATE A NCR SELF-SIGNED CERTIFICATE ?	8
	5.4.1.	Certificate file	10
	5.4.2.	Fingerprint file	10
	5.5. Lo	GGING FILE	
	5.6. Er	RORS DURING EXECUTION	11
	5.6.1.	Validation of input data	11
	5.6.2.	Validation of the DEP Crypto Module	11
	5.6.3.	Error code from the DEP Crypto Module	
6.	ANNE	X 1: INSTALLATION PROCEDURE	

### 2. SCOPE OF THE DOCUMENT

This document describes the *NCR Self-Signed Certificate* program. This PC program can be used to generate a NCR Self-Signed Certificate and a Fingerprint on a RSA Public Key.

The document doesn't explain the functionalities of the DEP libraries on which this program is based.

## **3. REFERENCES**

This document contains references to other documents about the DEP. This paragraph gives a list of all the documents referred to:

- DEP Host Interface Protocol
- DEP/NMS User Manual
- DEP/NT DEP Handler Supervision Program User Manual
- DEP/Linux User Manual
- DEP/T6 Owner Manual

There are no references made to the following documents, but they could be useful to understand this document:

- PKI Library for DEP Reference DFS Manual
- DEP Introduction to DEP
- DEP General Architecture
- DEP Glossary
- DEP RSA Key Generation User Manual

# 4. PURPOSE OF NCR SELF-SIGNED CERTIFICATE PROGRAM

The purpose of this program is to generate a NCR Self-Signed Certificate and compute a Fingerprint on a RSA Public Key.

The program is intended to be used on a PC (running on Microsoft Windows 2000 or XP) that is connected to a DEP Platform loaded with a DEP Application Software that can import RSA Keys and generate a PKCS10 Self Sign Certificate.

## 5. USE OF NCR SELF-SIGNED CERTIFICATE

The installation procedure is reported to the Annex 1 on page 13.

#### **5.1. START-UP**

The NCR Self-Signed Certificate can be launched by executing:

#### C:\Program Files\Banksys\DEP\_NMS\_PlugIns\NCR\_SelfSignedCertificate\ NCR\_SelfSignedCertificate.exe

This is the default path. Possibly another path can be defined during the installation (paragraph 6 on page 13).

The application can also be launched directly from the *DEP/NMS program*. For more details please refer to the *DEP/NMS User Manual*.

Before starting the application (when the application is not launched from the *DEP/NMS*), the communication must be defined. (paragraph 5.3 on page 7).

#### **5.2. DESCRIPTION**

Once the NCR Self-Signed Certificate is started, the following window is opened:

- NCR Self-Signed Certificate				
File Help				
_ Input			Process Status	
RSA Key File:		Browse		~
Hash Algo ID: SHA1				
		1		
Output Directory		Browse		
Properties of the output files:				
UserName				
Index:	(Numeric > 0)			
Fingerprint Algo ID: SHA1	<b>•</b>			
				-
			1	<u> </u>
				Generate NCR Self-Signed Certificate
Connected to 172.24.14.249	DEP Crypto Module number 01			

In this window, the user can find:

• A memo (blank part) which will log the operations and their results,

- A menu at the top of the window, that allows to have a look at the program version (and also contact the DEP Hotline), the help files or to exit,
- The left panel contains the list of parameters needed to generate the NCR selfsigned certificate and the fingerprint,
- A status bar contains the name or the TCP/IP address of the connected platform and the DEP Crypto Module number used for the generation of the self-signed certificate.

#### **5.3.** COMMUNICATION

If the application is launched by the DEP/NMS the communication is automatically set by the DEP/NMS.

If the application is used as "stand alone" application, the user has two possibilities:

- use the file "NCR SelfSignedCertificate.ini".
- use the "TCP/IP Configuration" for that appears at the start of the application.

#### 5.3.1. INI File

🜌 NCR_SelfSignedCertificate.ini - Notepad	
File Edit Format Help	
[GeneralParameters] NbofDesiredConnections=1 [Connection_0] Address=172.24.14.249 Port=1000	A
Timeout=180000 TimeoutConnection=5000 Module=0101 LSBMSBmode=LSB LSBMSBLength=4 DEPMagicNumber=FE DEPVersionNumber=30	
1	V V

- *NbOfDesiredConnections* must be set to '1'.
- *Address* represents the IP address of the target DEP Platform.
- *Port* represents the TCP/IP port used for the communication with the DEP Platform.
- *TimeOut* represents in milliseconds the maximum waiting time for the response from the DEP Crypto Module.

- *TimeOutConnection* represents in milliseconds the maximum waiting time for establishing a connection.
- *Module* represents the DEP Crypto Module used to generate the self-signed certificate: the first byte will be always '01' and the second byte defines the target module: '01' to '04'.
- The four last parameters are described in the DEP Documentation (*DEP Host Interface Protocol*)

#### **5.3.2.** TCP/IP Configuration window

When the application starts in "stand alone" mode a configuration window appears with the last used parameters:

- TCP/IP Configural	tion 💶 🗵 🗙
TCP/IP Address:	172.024.014.248
TCP/IP Port:	1000
Max. Response Time:	3000
Module Number:	1
ОК	Cancel

The user can accept the parameters, define another or click on cancel. The 'Cancel' button corresponds to use the default parameters even though the fields are modified.

The signification of the different fields is available in the previous chapter.

The input of the user is checked when he clicks on 'OK' and an error message appears if necessary:



The values are stored in the ini file "*NCR\_SelfSignedCertificate.ini*" and will be reused as default value the next time that the application will be started.

5.4. HOW TO GENERATE A NCR SELF-SIGNED

#### **CERTIFICATE ?**

All the fields on the left panel must be filled in:

-• NCR Self-Signed Certificate	
File Help	
Input	Process Status
RSA Key File: D:\L2048E00065537\20060817082746734.RSA Browse	Validation of input data Validation of input data succeeded.
Hash Algo ID: SHA1	The RSA File is valid.
	Send call to the DEP Crypto Module Receive answer from the DEP Crypto Module Valid answer received.
Output Directory D:\L2048E00065537 Browse	The NCR Self-Signed Certificate is written into the following file: D:\L2048E00065537\pktest 1.txt
Properties of the output files:	The Fingerprint is written into the following file: D:\L2048E00065537\pktest_1_Fingerprint.txt
UserName test	
Index: 1 (Numeric > 0)	
Fingerprint Algo ID: SHA1	
	Generate NCR Self-Signed Certificate
Connected to 172.24.14.249 DEP Crypto Module number 01	

Description/format of the parameters:

Field Name	Description
RSA Key File	This field contains the file name of the RSA Key to
	use.
Hash Algo ID	Identifier of the hash algorithm used for the
	generation of the Self-Signed Certificate. Accepted
	values are SHA1, SHA256 and MD5.
Output	Directory used for writing the 2 output files. This
Directory	value is stored and reused the next time the
	application is started as default output directory
UserName	Represent the parameter "UserName" of the output
	file.
T 1	
Index	Represent the parameter "Index" of the output file.
Fingerprint	Represents the hash algorithm used for the
Algo ID	generation of the fingerprint. Accepted values are:
	SHA1, SHA224, SHA256, SHA384, SHA512, MD5
	and MDC2.

When the user clicks on "Generate NCR Self-Signed Certificate" the TCP/IP connection to the DEP Crypto Module is established and the certificate is generated.

The right panel shows the progress of the import:

- The validation of the input data.
- The validation of the '.RSA' file.
- The status of the call sent to the DEP Crypto Module.
- The confirmation of the generation of the certificate.
- The eventual errors.

#### 5.4.1. Certificate file

🔊 pktest_1.txt - Notepad	
File Edit Format Help	
3282010A0282010100B2661DC58149A1A6027B1752BA3D0B8C36F6489DB0917D1CDFE7FF0	7D82C7A6CE1B89 📥
80018C68342D400C4838E318D98CE9C87258A1E2598EC83E98829C5C8EE018998718E1874 F6600ARB80434C69231D26A92437F64DFD1231D031374DF82F0159D911DD6FC93B20F6FF8	41F6E6914EE90A B0F374AF60DFF1
96ADF827F5AB48486CC6D7A121D1C8935D9B8AA9FB58DF94F10F73439461B688E445C2E3F	82233324B3CDAE
18 0BC88A4A79CE598B176C519ADDE20D3256738F2582DEDDE9841F0C1B4AF9D70D6ECB6FB	2760E902B3B397
35/01F8240806662386601616798996845757678268397192158987658866611686335268047688636178092693882846	0E50CC5HD00HD4 C5663D016513E1
991E73733A2AA5F47DBC1A88608B560BE86A8A1879571293D3872C0BC20AA011402792FE1	48F9E73FDDDA6F
7184A54CB2C44784ED2E115AA2C6696416AF7EFD1B3A3EE0F2B9F66332DDA2C6284CD336C	34885865276580
DC31371B44B2A74AE077187EA66FB6A7D0B98540C60AED760FFC2C090CE2E64D41516AC8F	C8E26658BE7BA9
F4B69DCDFFA98EF4E7046CCC92E0A2EA2E07109BF0404055208D4B1BE2CFCCF83F4FFB794	5F30CD0775B025
182985BB	
1	7

#### 5.4.2. Fingerprint file



This file contains two fields:

- The algorithm used for the generation of the fingerprint.
- The value of the fingerprint.

#### 5.5. LOGGING FILE

When the user closes the application a logging file is created/updated in the installation directory: "*NCR\_SelfSignedCertificate.log.txt*".

MCR_SelfSig	gnedCertificate.	log.txt - Notepad	_ 🗆 🗵
File Edit Forma	at Help		
25/10/2006 25/10/2006 25/10/2006 25/10/2006 25/10/2006 25/10/2006 25/10/2006 25/10/2006 25/10/2006 25/10/2006 25/10/2006	15:29:15 15:29:15 15:29:15 15:29:18 15:29:18 15:29:43 15:30:02 15:30:02 15:30:02 15:30:02	A file with selected UserName and Index already exists. Send call to the DEP Crypto Module Receive answer from the DEP Crypto Module Bad answer received. Validation of input data The default 'Index' is taken: 1 The default 'UserName' is taken: xxxxxx Validation of input data succeeded.	
25/10/2006 25/10/2006 25/10/2006 25/10/2006 25/10/2006 25/10/2006	15:30:02 15:30:02 15:30:02 15:30:02 15:56:05 15:56:05	The RSA File is valid. A file with selected UserName and Index already exists. Basic verification on the DEP Crypto Module failed.	· · ·

This file contains the copy of the right window.

#### **5.6.** ERRORS DURING EXECUTION

#### 5.6.1. Validation of input data

Some verifications are made before sending the call to the DEP Crypto Module and messages are displayed.

For example:



Selecting the "OK" button sets the focus to the erroneous field for correction.

#### 5.6.2. Validation of the DEP Crypto Module

After the input validation, the application performs a DEP Crypto Module validation:

• Is the DEP Crypto Module on-line/unlocked?

- Does the DEP Crypto Module contain a valid DEP Application Software ?
- Is the DEP Application Software able to import RSA Keys?
- Is the DEP Application Software able to generate PKCS10 self-signed certificate?
- Is the key K\_PKI\_RSA\_TRANSPORT\_KEY loaded in the DEP Crypto Module ?

If one of the verification failed, a warning window is displayed:

🗝 Warnir	ng X
1	The called functionality is not possible for the loaded application software (the interface I_PKI_IMPORT_RSA_KEY is missing). Please load the correct application software.

All warning windows disappear automatically when the problem is solved. For example: when the correct capability is loaded or when the DEP Crypto Module is set on-line/unlocked.

<b>⇒0</b> ₩arni	ng 🔀
	The DEP Crypto Module is in OFF LINE/LOCKED mode. Please select ON LINE/UNLOCK mode.
	<u> </u>

The user can also click on the "OK" button, solve the problem and click again on "Generate NCR Self-Signed Certificate" button.

#### **5.6.3.** Error code from the DEP Crypto Module

After all verifications are done successfully, a call is sent to the DEP Crypto Module. When no problem occurs the Self-Signed Certificate is generated, otherwise an error message is returned.

For example:

Error	×
8	The D_PKI_ENC_RSA_KEY present in the selected .RSA file seems to be invalid: F20125000003000E0000

# 6. ANNEX 1: INSTALLATION PROCEDURE

There exists an installation procedure for the *NCR Self-Signed Certificate Program*. To begin the installation wizard of the program, start the **Setup.exe**.

The "destination folder" window allows defining the path where the application is installed. The following default path is advised.

🔂 NCR Self-Signed Certificate - Insta	IIShield Wizard	×
<b>Destination Folder</b> Click Next to install to this folder, or clic	k Change to install to a different	t folder.
Install NCR Self-Signed Certif C:\Program Files\Banksys\DEl Certificate\	icate to: P_NMS_PlugIns\NCR Self-Signed	<u>C</u> hange
InstallShield	< <u>B</u> ack	Cancel