banksys
end-to-end transactions
Technologies & Products

Haachtsesteenweg 1442
1130 Brussels
Belgium

DEP Documentation

NCR Self-Signed Certificate User Manual

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

COPYRIGHT

LEGAL DISCLAIMER

JURISDICTION AND APPLICABLE LAW

1. TABLE OF CONTENTS

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

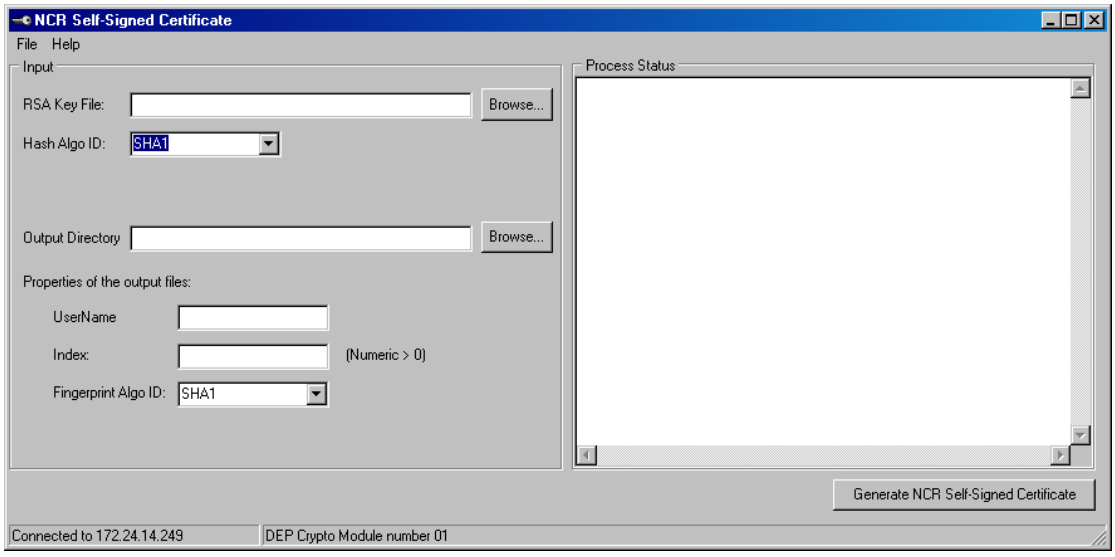
This is the default path. Possibly another path can be defined during the installation (paragraph 6 on page 13).

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:



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 self-signed certificate and the fingerprint,

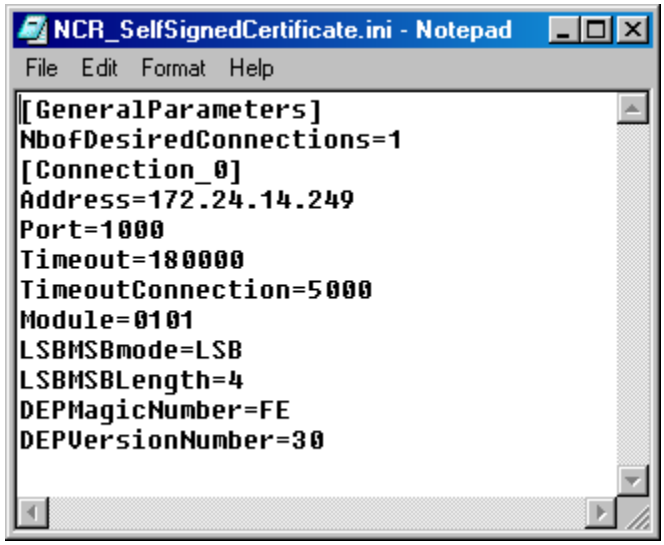
- A status bar contains the name or the TCP/IP address of the connected platform and the DEP Crypto Module number used for the generation of the self-signed certificate.

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

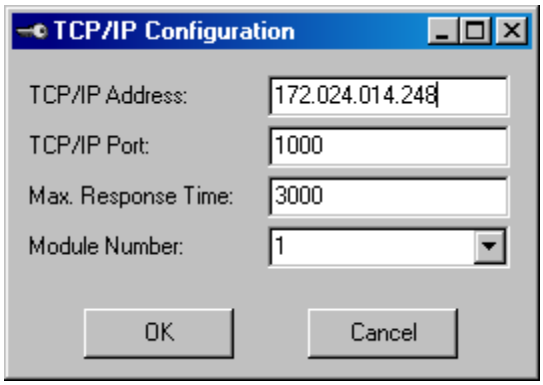


- *NbOfDesiredConnections* must be set to '1'.
- *Address* represents the IP address of the target DEP Platform.
- *Port* represents the TCP/IP port used for the communication with the DEP Platform.
- *TimeOut* represents in milliseconds the maximum waiting time for the response from the DEP Crypto Module.

- *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:



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.

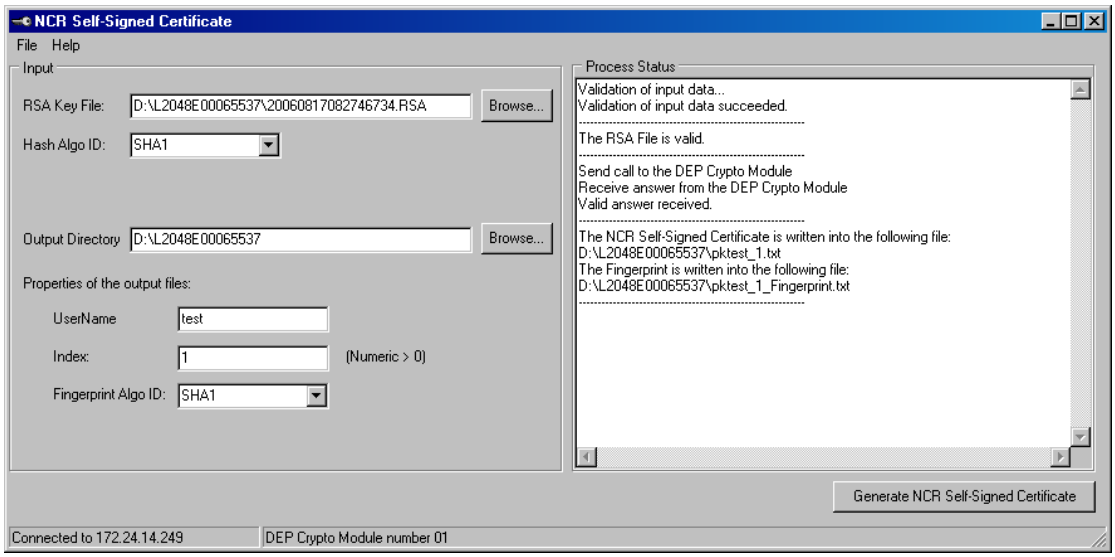
The input of the user is checked when he clicks on 'OK' and an error message appears if necessary:

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:



Description/format of the parameters:

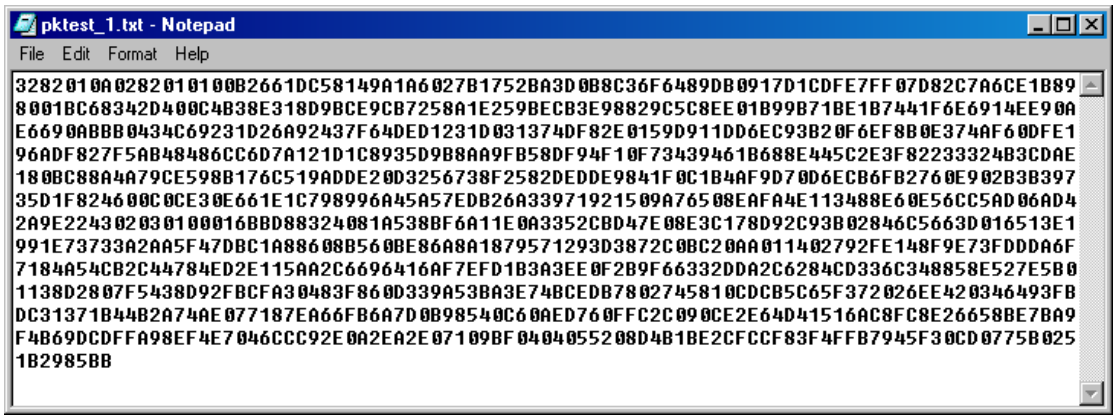
Field Name	Description
RSA Key File	This field contains the file name of the RSA Key to use.
Hash Algo ID	Identifier of the hash algorithm used for the generation of the Self-Signed Certificate. Accepted values are SHA1, SHA256 and MD5.
Output Directory	Directory used for writing the 2 output files. This 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.
Index	Represent the parameter “Index” of the output file.
Fingerprint Algo ID	Represents the hash algorithm used for the 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.

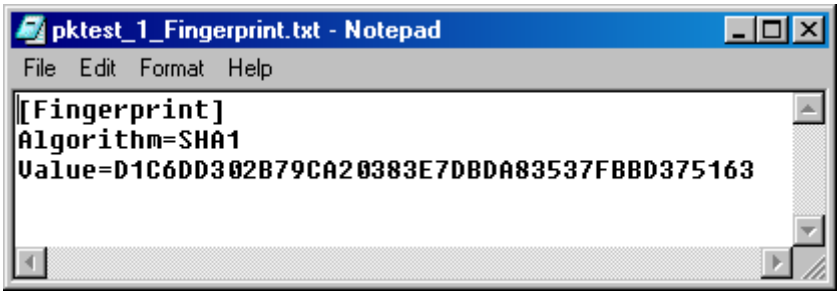
The right panel shows the progress of the import:

- 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



5.4.2. Fingerprint file

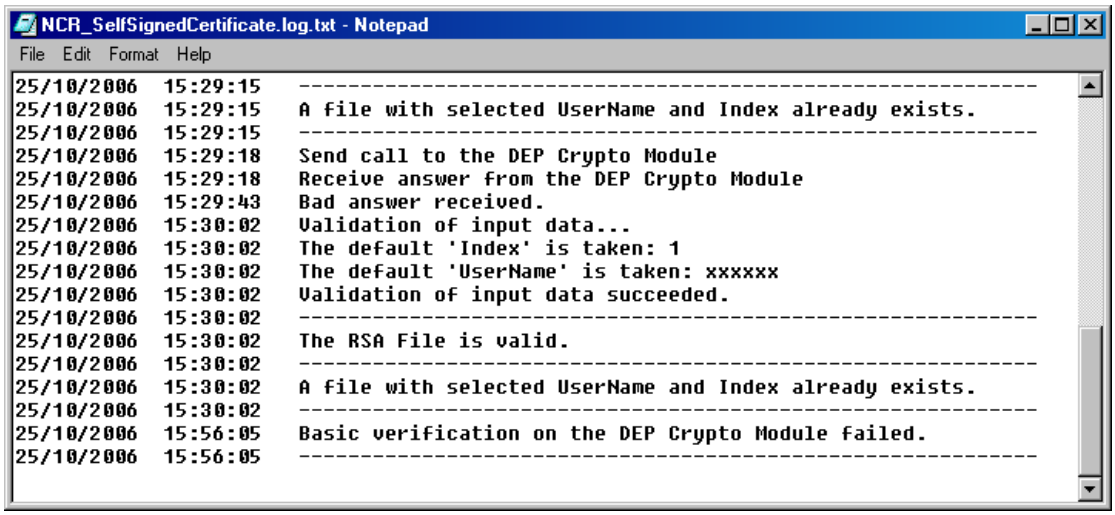


This file contains two fields:

- 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*".



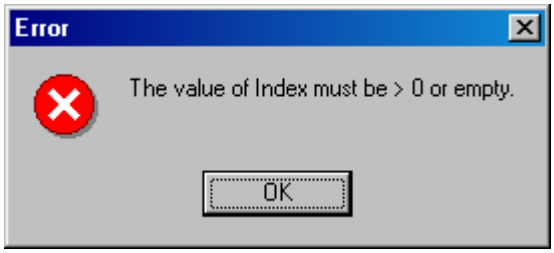
This file contains the copy of the right window.

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.

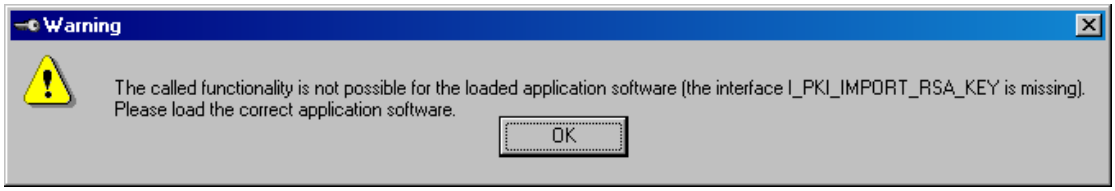
5.6.2. Validation of the DEP Crypto Module

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

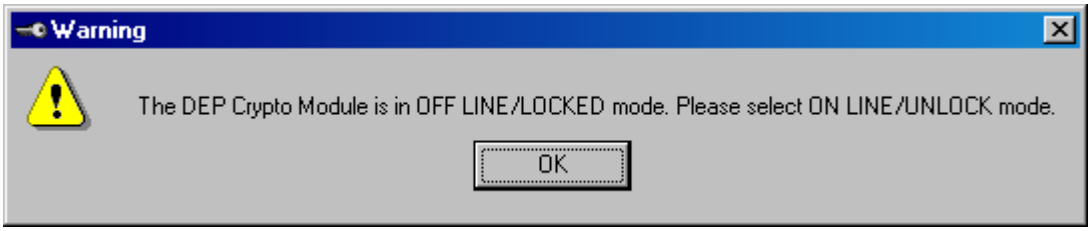
- Is the DEP Crypto Module on-line/unlocked?

- 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:



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.

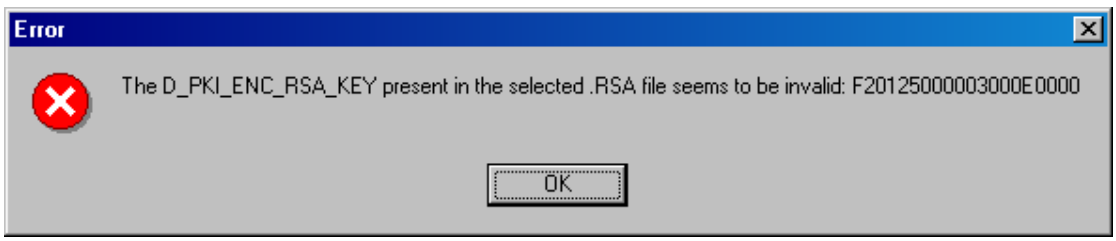


The user can also click on the "OK" button, solve the problem and click again on "Generate NCR Self-Signed Certificate" button.

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:



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.