MAX32590/MAX32550

HSM User Guide

UG25T03
Revision A
10/13/2014

Maxim Integrated, Inc.
160 Rio Robles
San Jose, CA 95134

MAXIM Integrated PROPRIETARY – CONFIDENTIALITY

Revision History

Rev A	2014-Oct-13	1st release

Disclaimer

To our valued customers

We constantly strive to improve the quality of all our products and documentation. We have spent an exceptional amount of time to ensure that this document is correct. However, we realize that we may have missed a few things. If you find any information that is missing or appears in error, please contact us. We appreciate your assistance in making this a better document.

Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Maxim Integrated Office.

Maxim Integrated Technologies may only be used in life-support devices or systems with the express written approval of Maxim Integrated, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Table of Contents

Glossary

ACS	Administrator Card Set
CRK	Customer Root RSA Key
HSM	Hardware Security Module
MRK	Maxim Integrated Root RSA Key
OCS	Operator Card Set
SCP	Secure Communication Protocol
SoC	System On Chip

References

[1] PCI-PTS modular security requirements. V4.0 Jun-2013

[2] nShield Edge User Guide.

[3] UG21T24. MAX32590 Secure ROM User Guide. Rev A.

[4] UG25H04. MAX32550 Secure ROM User Guide. Rev D.

1 INTRODUCTION

This document explains how to use the HSM from an operator point of view. More particularly, it describes the security procedures to enforce in order to be compliant with security standards like PCI-PTS (see [1]). It also describes the way to use it. For more details about the HSM installation, refer to the Thales nShield Edge documentation (see [2]).

This document describes the procedure for the MAX32590 (RSA keys) and MAX32550 (ECDSA keys).

The HSM is used for four purposes:

- For nCipher Tools installation, see section 2.
- For CRK generation and certification, see section 3.
- For SCP packets signature and generation, see section 4.
- For customer application signature, see section 5.

2 nCipher Tools installation

Maxim Integrated has developed a suite of tools in order to use the **THALES nShield EDGE** HSM.

This suite is called: ***nCipher Tools***.

2.1.1 Installation requirements

- Supported OS: Windows XP, 7.
- Supported HSM: **Thales nShield Edge**

2.1.2 Thales nShield Edge HSM installation

The first step consists of HSM installation. Simply use the CD (so called “ncss-win-Edge-11”) from the THALES installation package.

2.1.2.1 Software installation

DO NOT PLUG THE HSM BEFORE INSTALLING SOFTWARE AND DRIVERS!!!

- Supported OS: Windows XP/ Windows 7
- JRE installation is required before going ahead. “The nCipher software supports JRE/JDK version 1.4.2, 1.5, and 1.6. The nCipherKM JCA/JCE CSP supports JRE/JDK 6.0” extract from THALES documentation.
- Launch setup.exe at root path.
- Follow the guide lines and choose default choice each time.

2.1.2.2 Configuration

Before to continue with ***nCipher Tools*** installation, it’s required to perform following operations referring to the Thales nShield Edge HSM documentation:

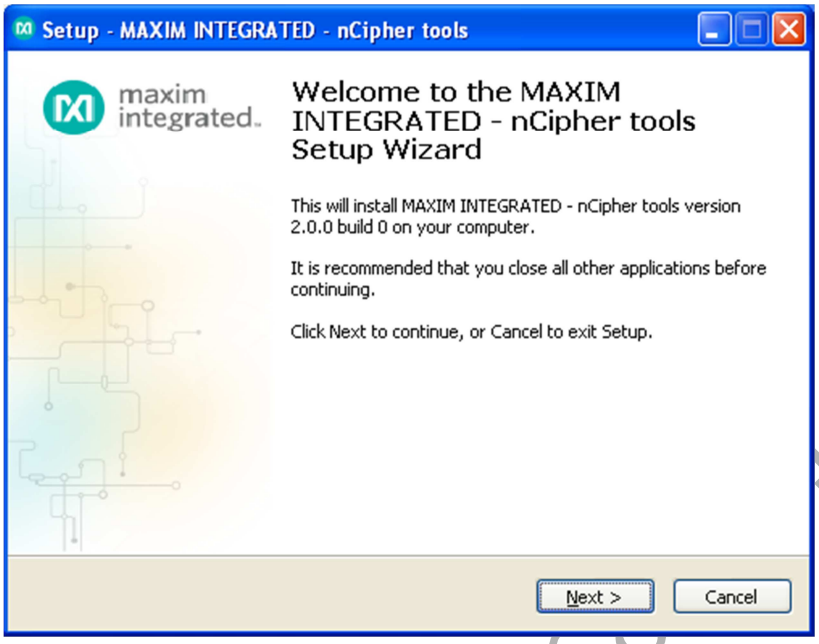
1. Create a Security World (***new-world.exe*** command line tool).
2. Create OCS (***createocs.exe*** command line tool).

Remark:
These two operations require the user to define a quorum k/n for ACS cards, during Security world creation step, and another one for OCS cards. Achieving a quorum requires a defined chosen number of smart cards (k) from a total set (n) be brought together for an operation to be authorized. For compliance with PCI PTS, we recommend at least a dual control so that means “k” value equal or superior to 2. The “n” value can be defined as follow “n” >= “k”+1.

2.1.3 Installation package

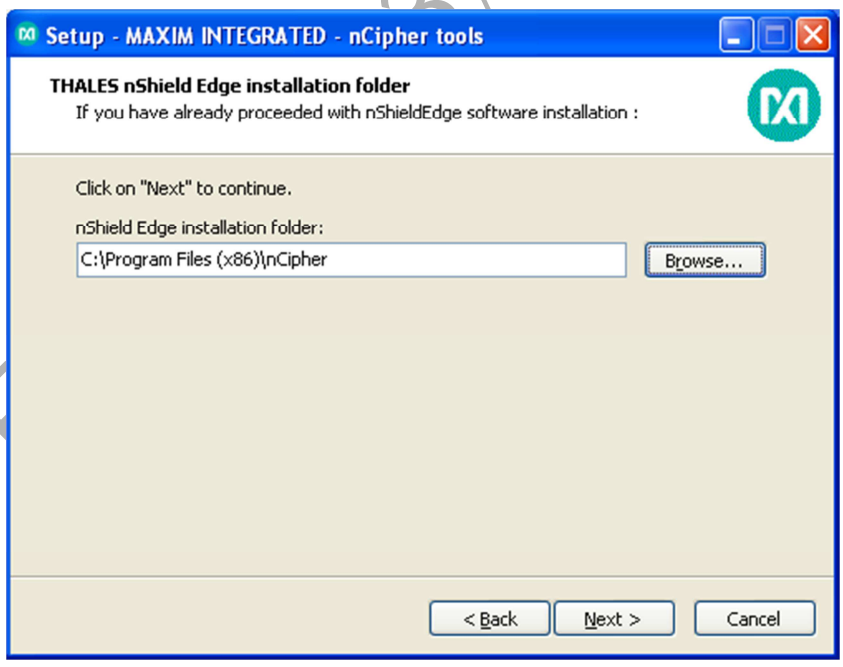
Depending on the targeted chip, the following package has to be installed:

- Installation package name:
  - For MAX32590: ***mxim_ncipher_tools_setup.exe***
  - For MAX32550: ***mxim_ncipher_tools_MAX32550_setup.exe***
- Launch installation:

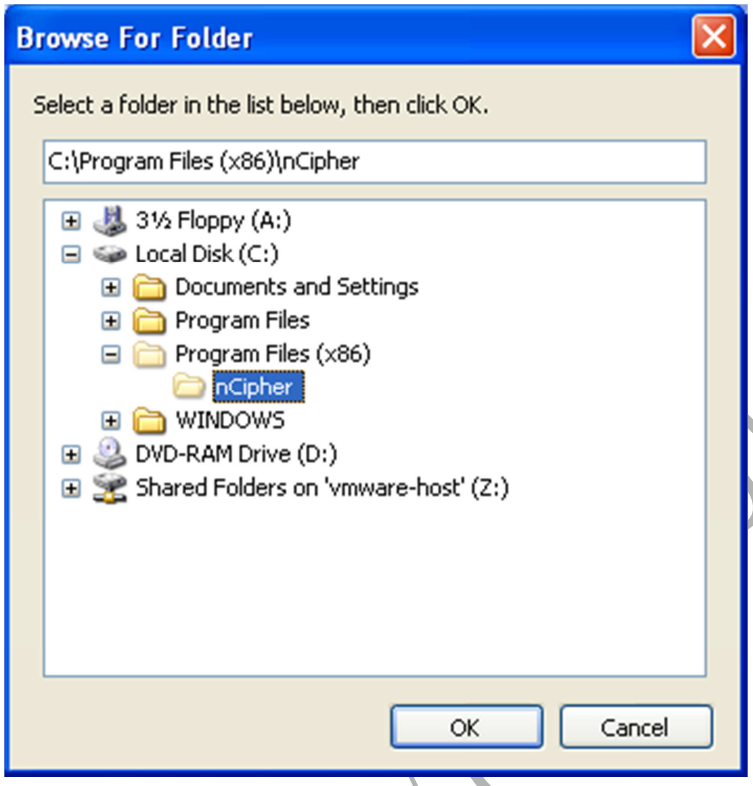


- Click on “Next”, enter **Thales nShield Edge** Installation folder:

  Select the folder where you installed **Thales nShield Edge** software.

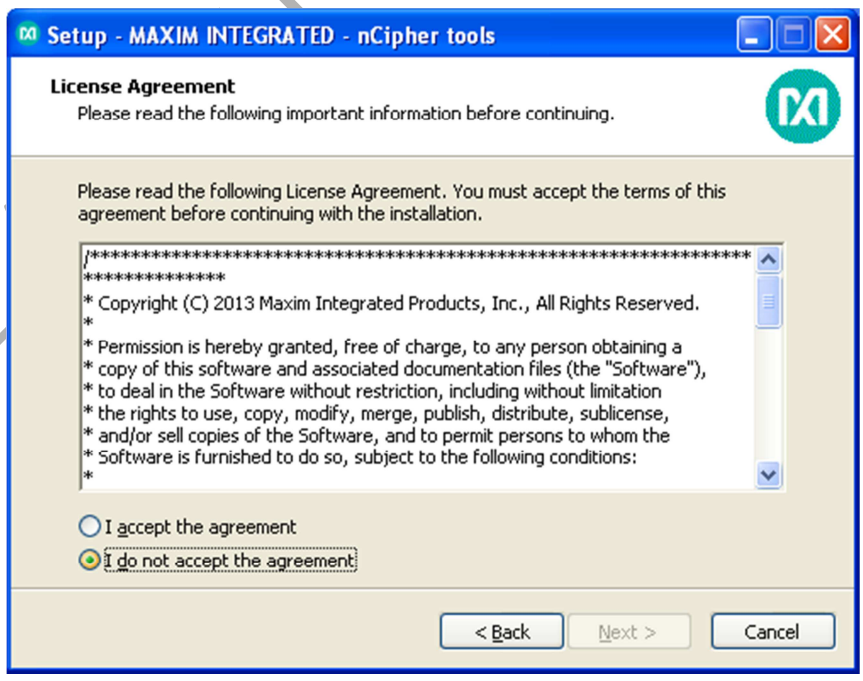


- Browse Thales nShield Edge software installation:

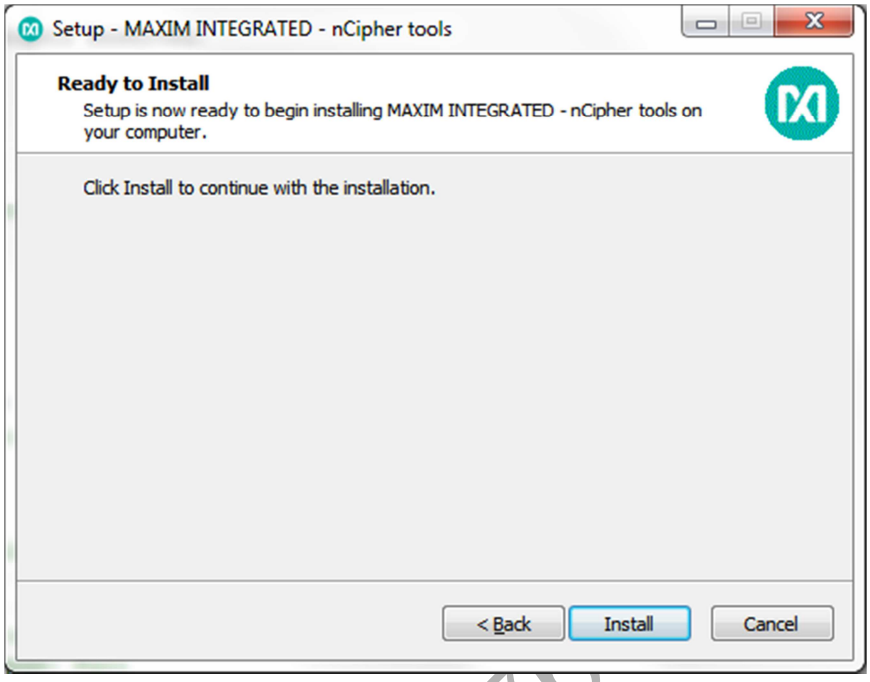


Click on **OK** to validate the choice.

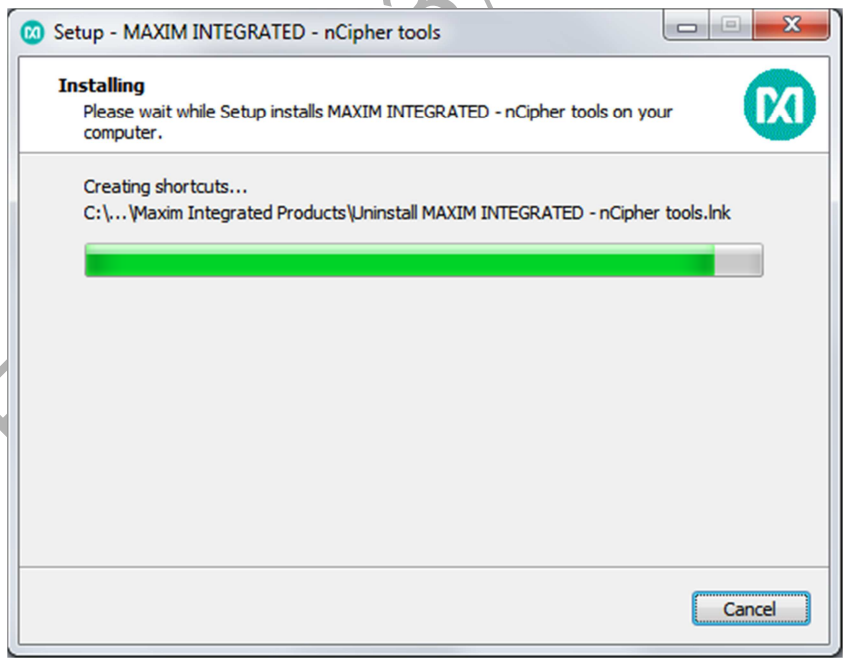
- Read and accept license agreement. Finally click on **Next**:



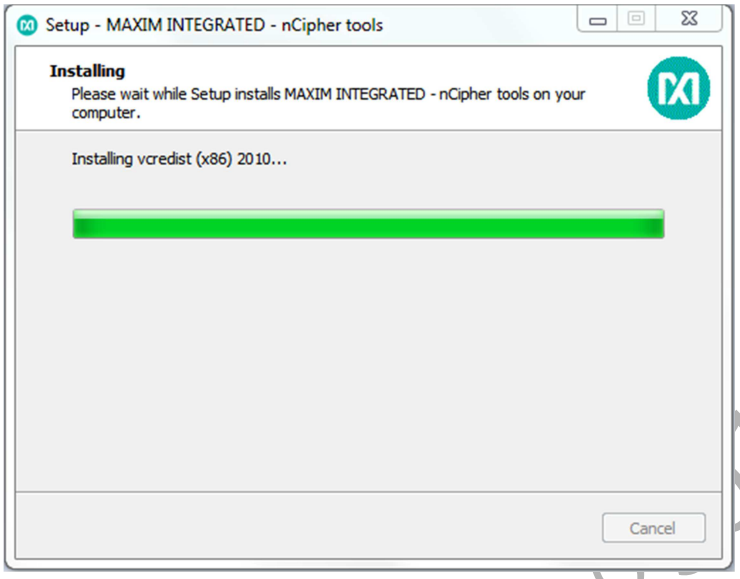
- Click on “Install”:



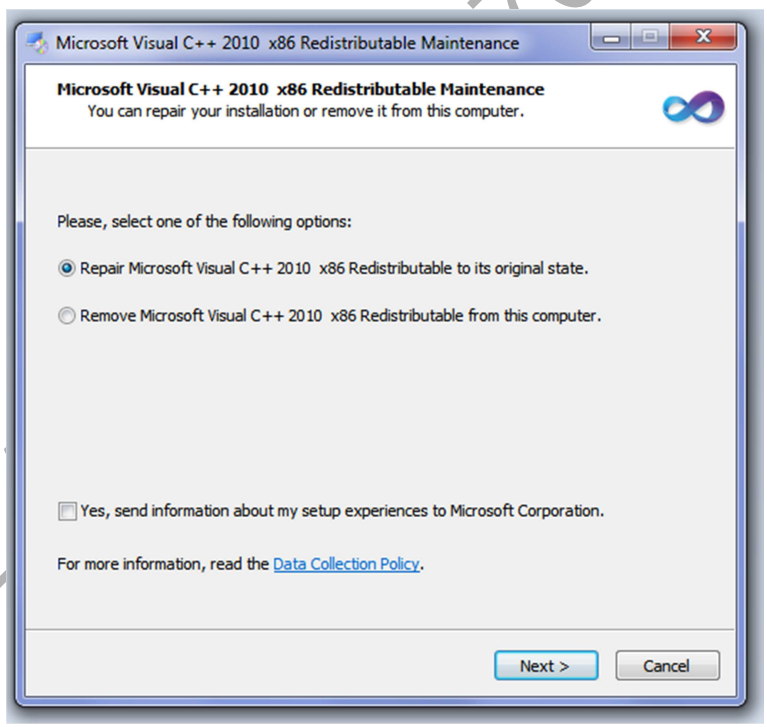
The setup first has to stop Thales nShield Edge services: “nFast Edge” and “nFast Server”.



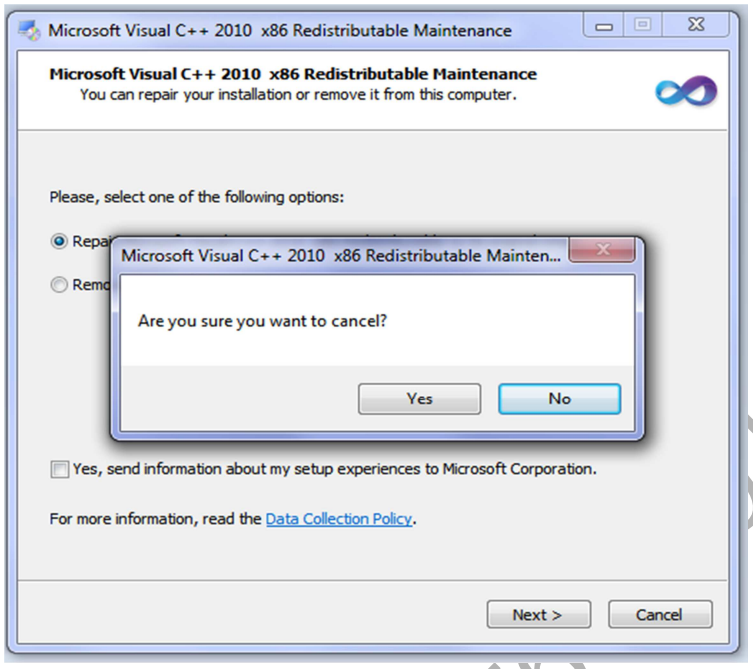
- Redistributable Visual Studio C++ package installation:



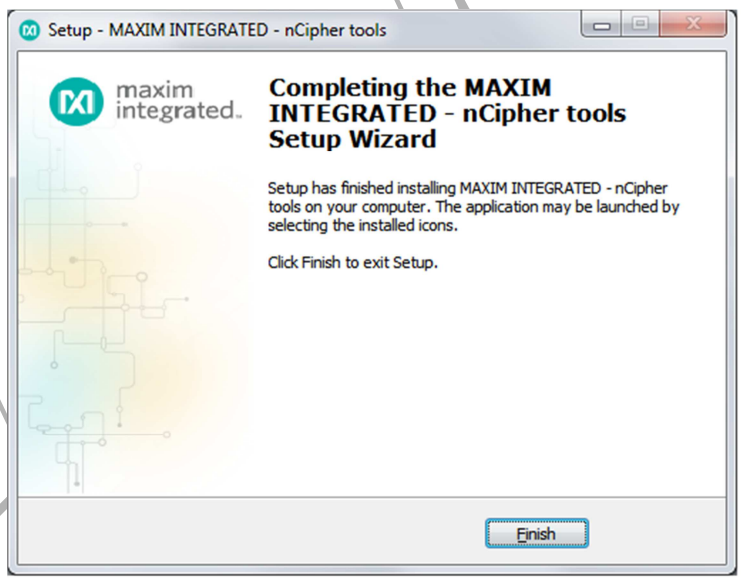
The package will proceed with the components installation but it will stop if it has been already installed and display the following window:



Ignore this window and click on **Next**. The installer requires you to confirm, so click **Yes**:



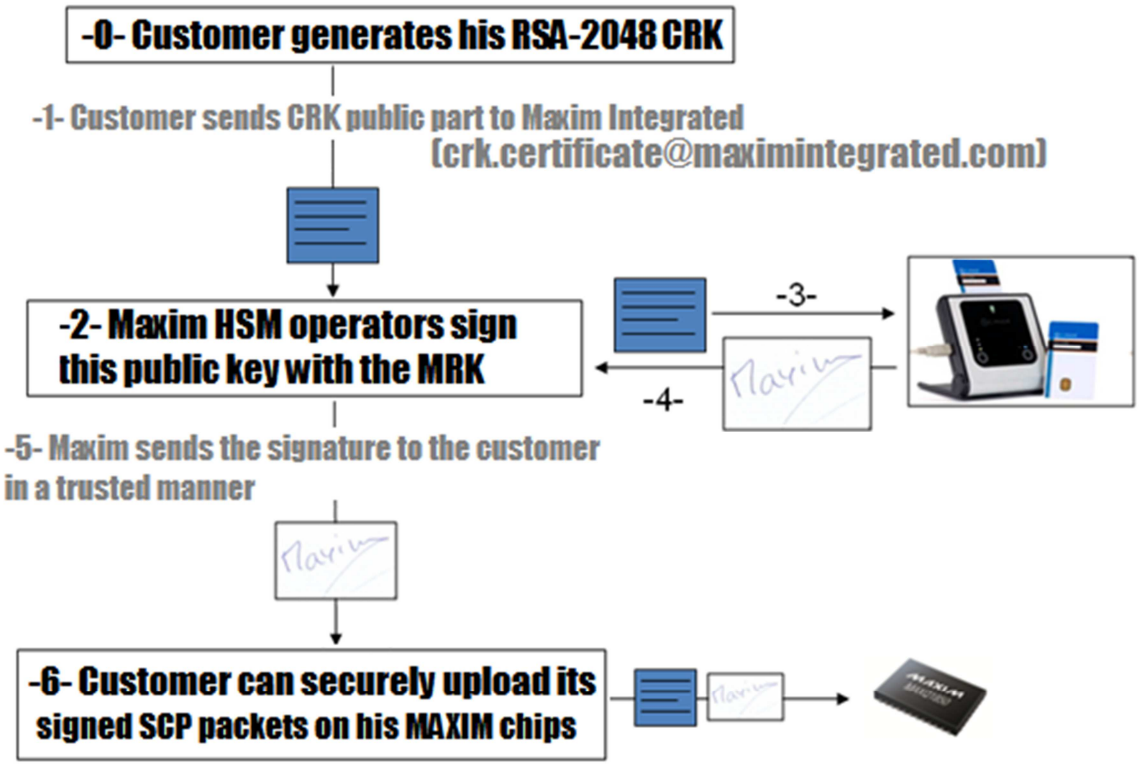
- Wait for the end and click on **Finish**:



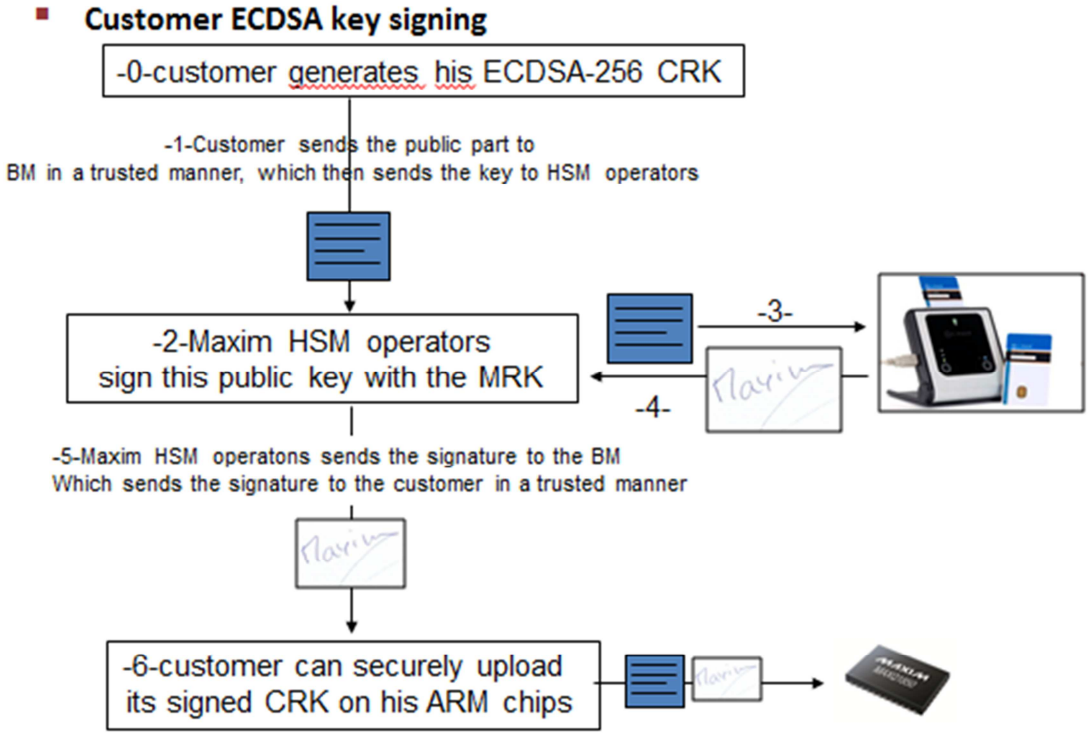
3 CRK generation

Customers have to generate their own key, the CRK and ask Maxim Integrated to certify this key, by issuing certified (i.e. signed) SCP packets, which include the CRK, signed by the MRK.
The diagram below describes this process, to be performed once per CRK.

- For MAX32590 (RSA key process):



- For MAX32550 (ECDSA key generation process)



3.1 mxim_hsm_manager application

This application belongs to **nCipher Tools** suite. This command line allows to generate the CRK.

First of all, ***run as administrator*** Windows console and type following commands:

- `cd <ncipher_tools_installation_folder>\bin`
- `mxim_hsm_manager.exe --help`

The last command displays the help information.

3.2 MAX32590

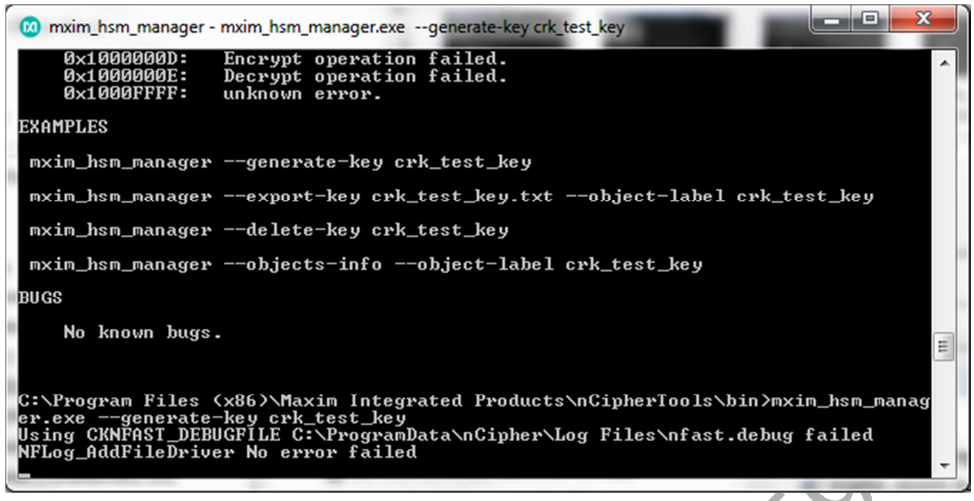
3.2.1 Generate new RSA key pair

Considering a security world (see section 2.1.2.2) is present on the PC and all ***OCS*** cards required accordingly to the quorum are available, you have to plug the**Thales nShield Edge** in. Then, in Windows console, type the following command and follow the instructions:

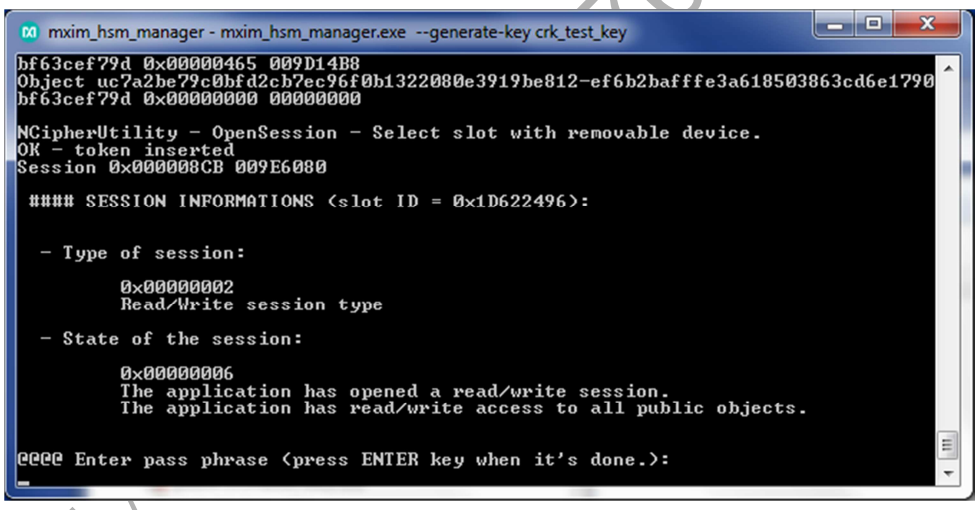
- `mxim_hsm_manager.exe –-generate-key <name_of_rsa_key_pair>`

Example:

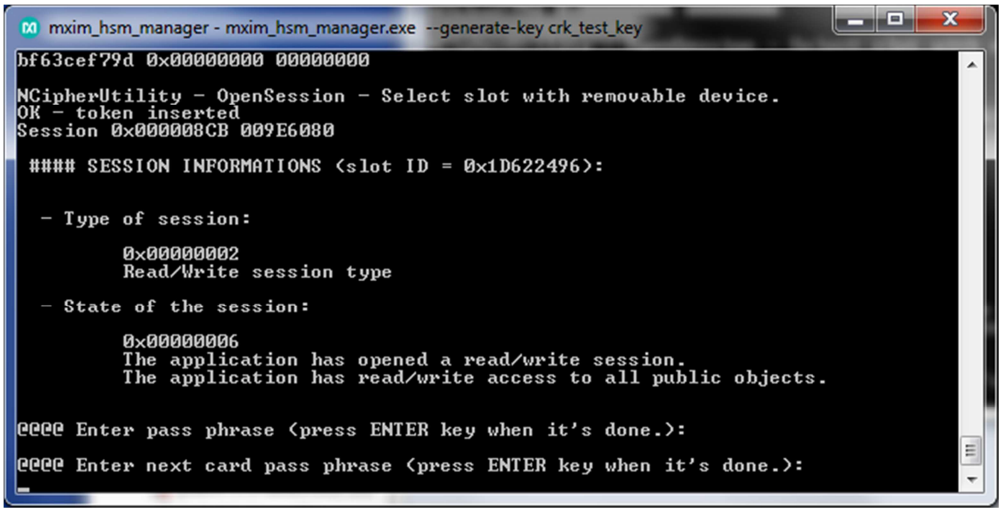
Type following command: ***mxim_hsm_manager.exe --generate-key crk_test_key***



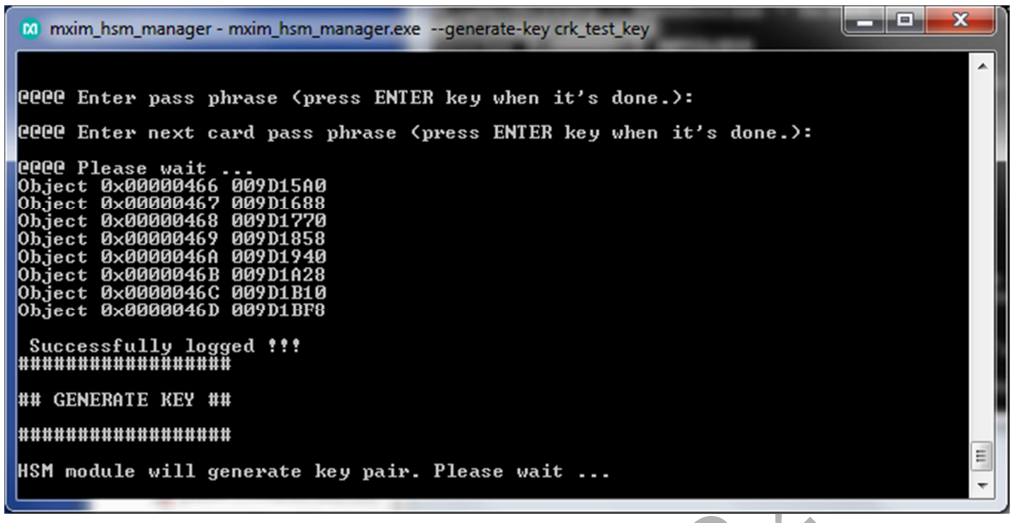
Insert first OCS card, so called ***token***, type the password and validate with ENTER:



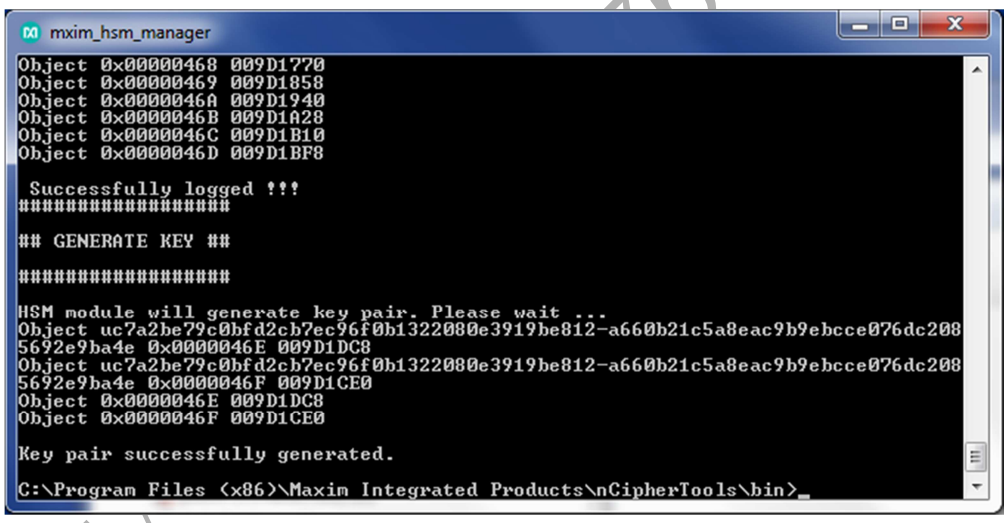
Insert next OCS card(s), type the password and validate with ENTER (repeat this operation accordingly to the quorum):



HSM will generate RSA key pair. The operation takes some time.



And finally …



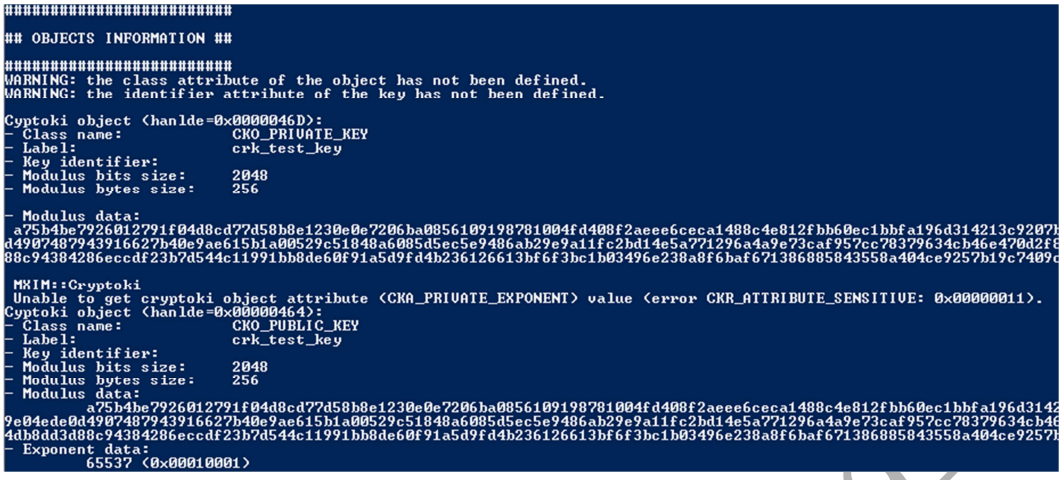
3.2.2 Export public RSA key

Considering a security (see section 2.1.2.2) is present on the PC, all ***OCS*** cards required accordingly to the quorum are available, and one RSA key has already been created (see section 3.2), you have to plug the**Thales nShield Edge** in. Then, in Windows console, type the following command and follow the instructions:

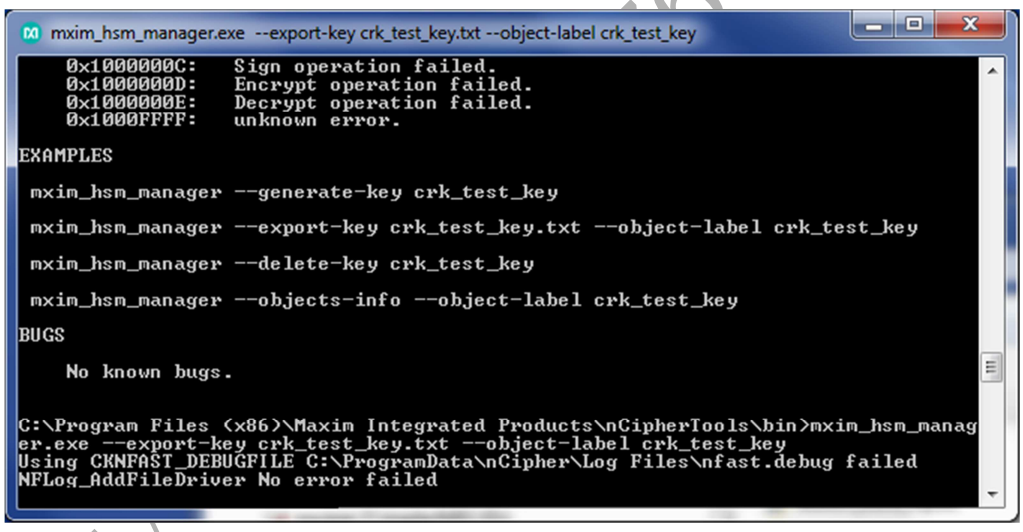
- `mxim_hsm_manager.exe --export-key <path_and_file_name> --object-label <name_of_rsa_key>`

Example:

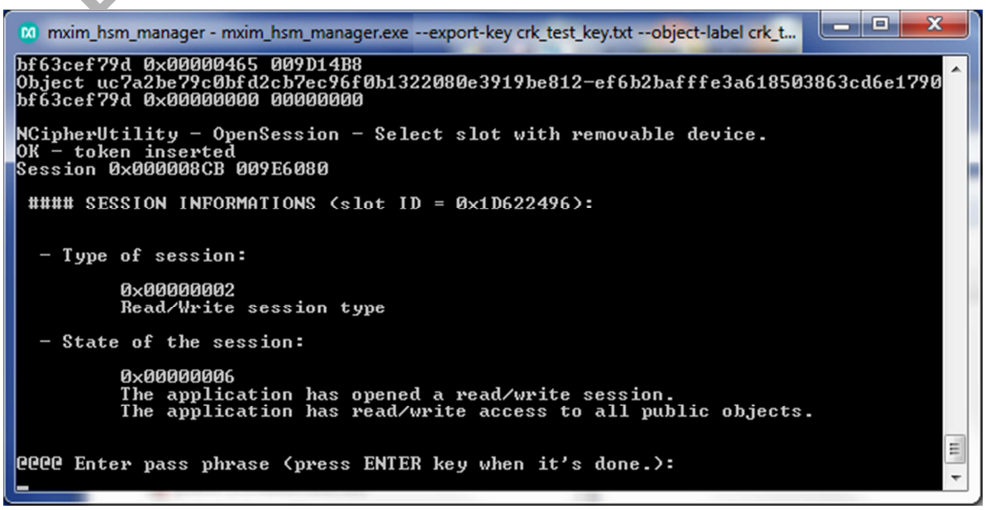
To check that the RSA key exists:
`mxim_hsm_manager.exe --objects-info --object-label crk_test_key`



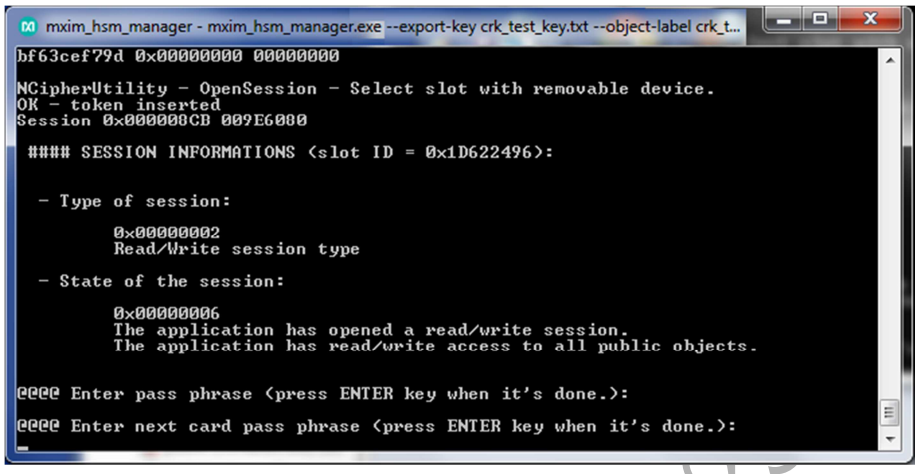
Then type following command:
`mxim_hsm_manager.exe --export-key crk_test_key.txt --object-label crk_test_key`



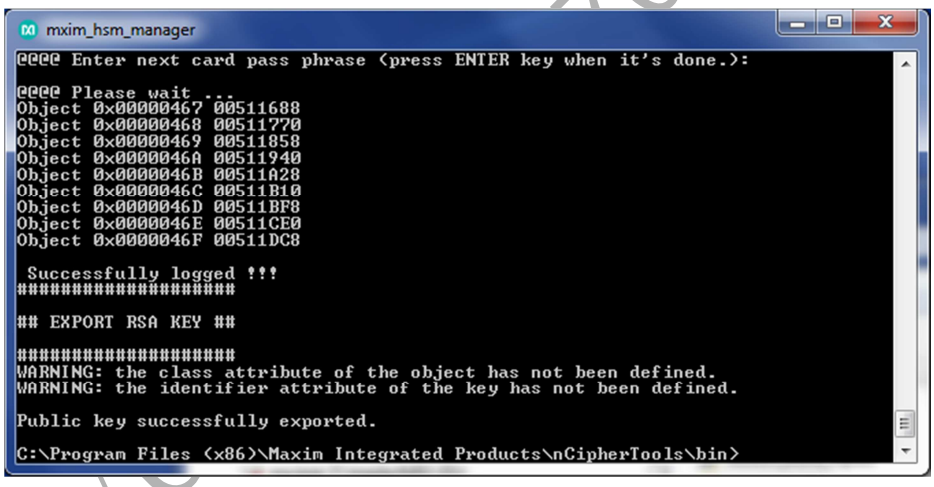
Insert first OCS card, so called ***token***, type the password and validate with **ENTER**:



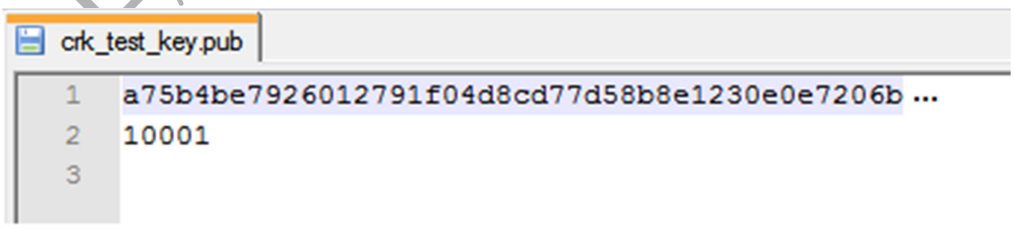
Insert next OCS card(s), type the password and validate with **ENTER** (repeat this operation accordingly to the quorum):



HSM will export public RSA key.



The exported file result:



First line is corresponding to the modulus of the public RSA key.
Second line is corresponding to the exponent of the public RSA key.

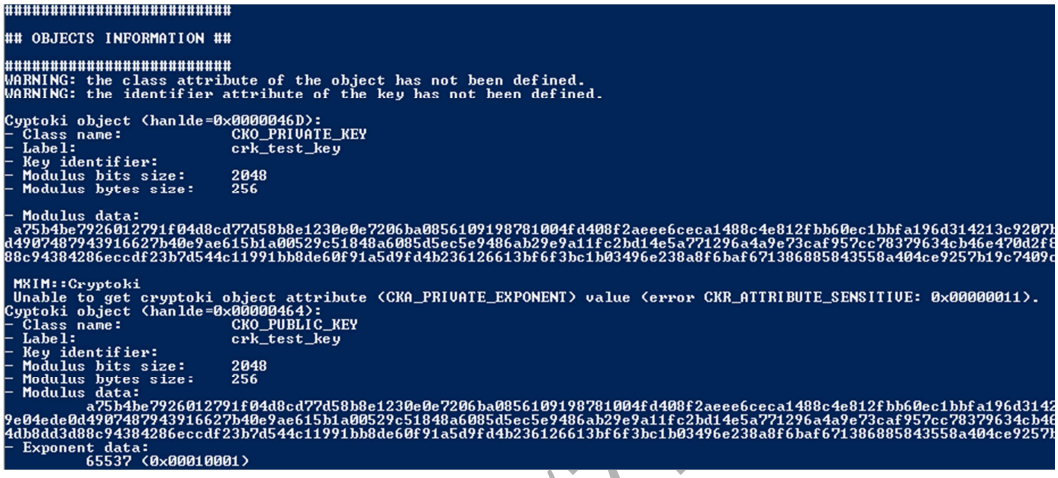
3.2.3 Remove RSA key pair

Considering a security (see section 2.1.2.2) is present on the local machine, all ***OCS*** cards required accordingly to the quorum are available, and one RSA key has already been created (see section 3.2), you have to plug the**Thales nShield Edge** in. Then, in Windows console, type the following command and follow the instructions:

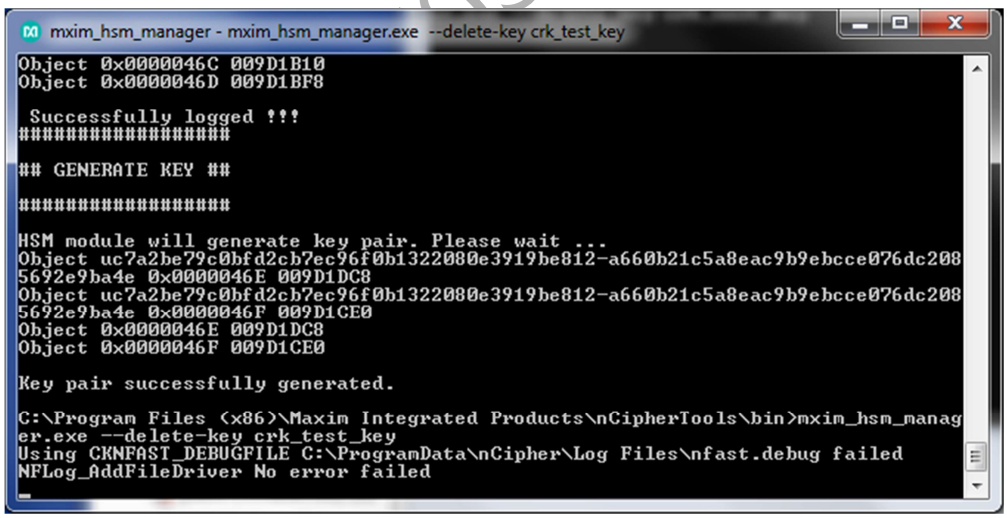
- `mxim_hsm_manager.exe --delete-key <name_of_rsa_key>`

Example:

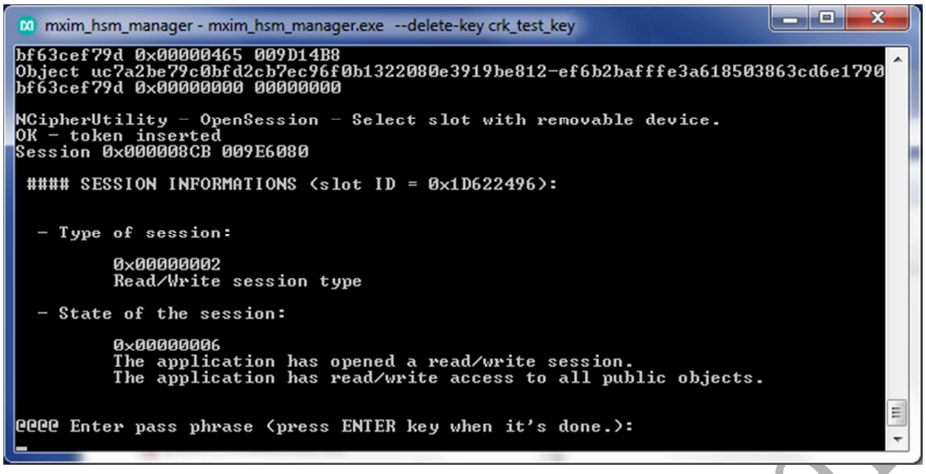
To check that the RSA key exists:
`mxim_hsm_manager.exe --objects-info --object-label crk_test_key`



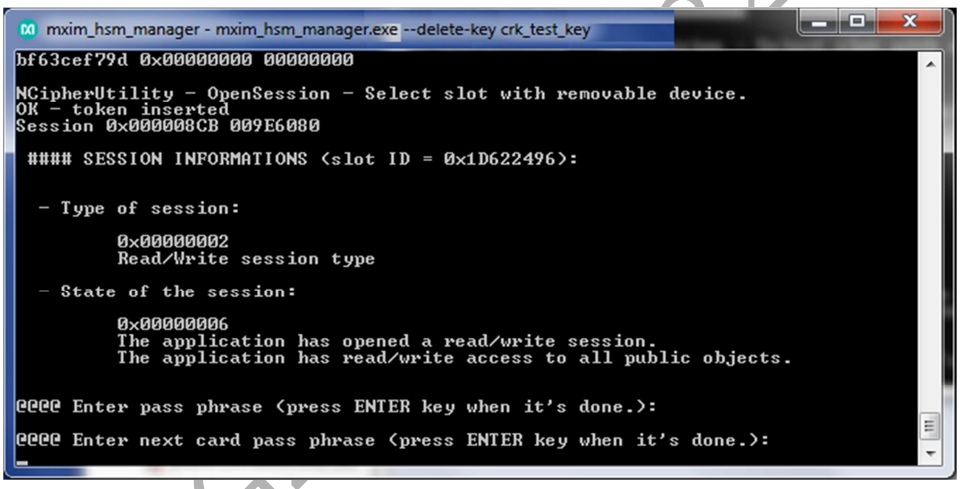
Type following command: `mxim_hsm_manager.exe –delete-key crk_test_key`



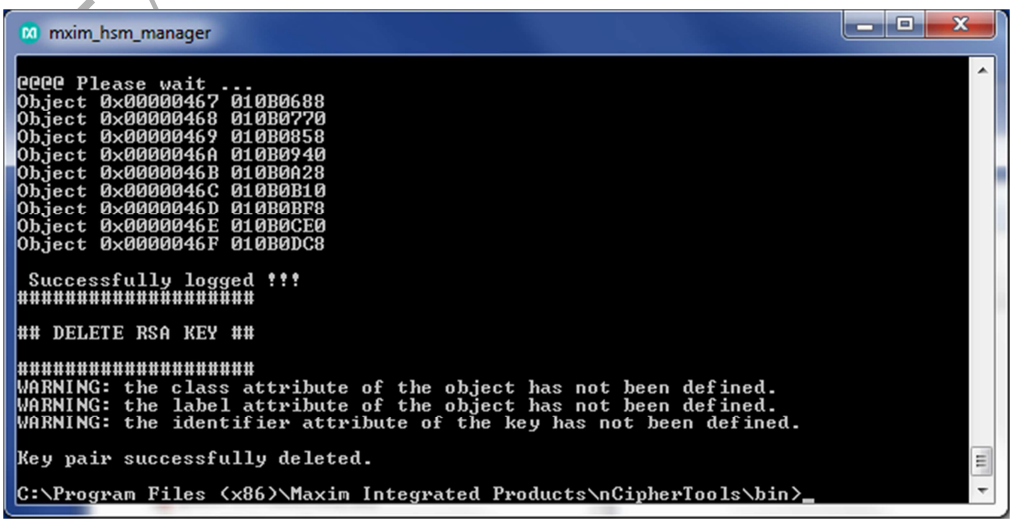
Insert first OCS card, so called ***token***, type the password and validate with **ENTER**:



Insert next OCS card(s), type the password and validate with **ENTER** (repeat this operation accordingly to the quorum):



HSM will delete RSA key pair.



3.3 MAX32550

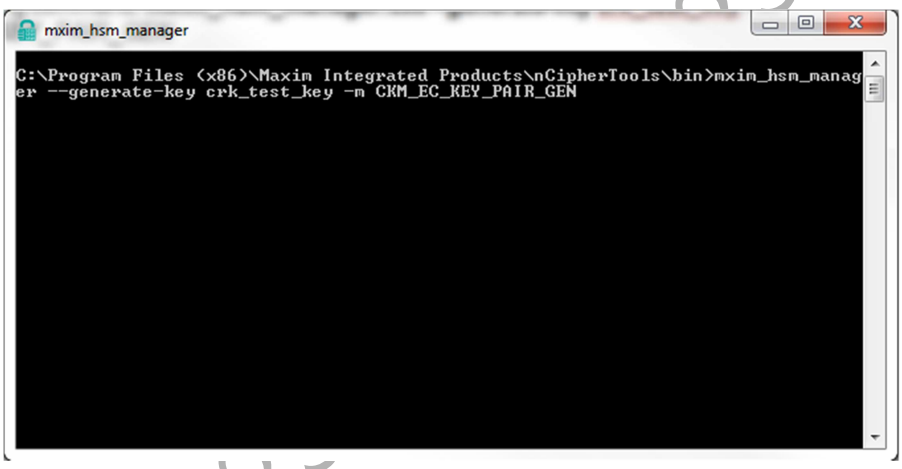
3.3.1 Generate new ECDSA key pair

Considering a security world (see section 2.1.2.2) is present on the PC and all ***OCS*** cards required accordingly to the quorum are available, you have to plug the**Thales nShield Edge** in. Then, in Windows console, type the following command and follow the instructions:

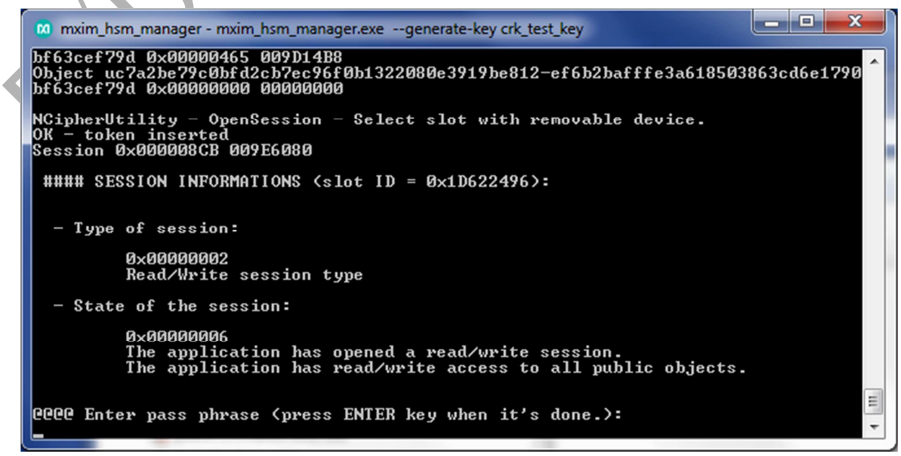
- `mxim_hsm_manager.exe –-generate-key <name_of_ecdsa_key_pair> -m [CKM_EC_KEY_PAIR_GEN|CKM_ECDSA_KEY_PAIR_GEN]`

Example:

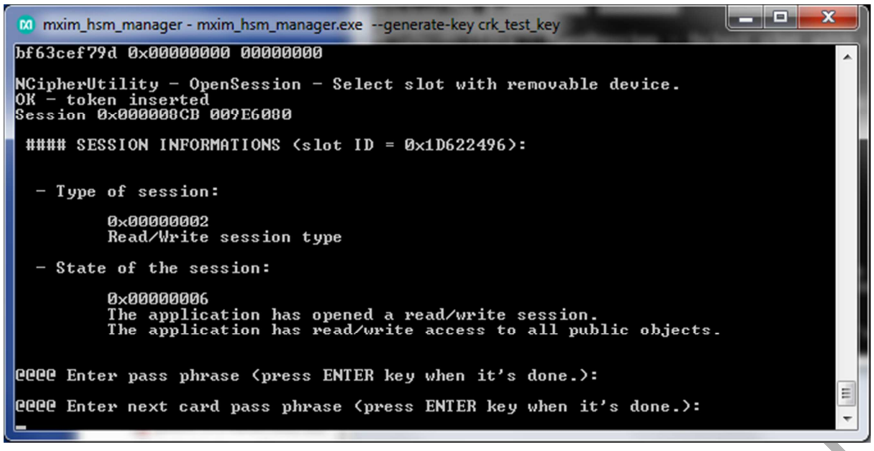
Type following command: ***mxim_hsm_manager.exe --generate-key crk_test_key –m CKM_EC_KEY_PAIR_GEN***



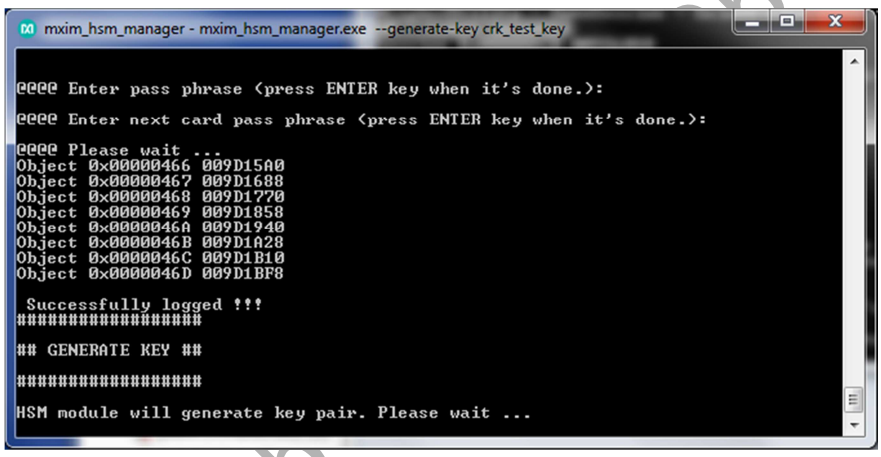
Insert first OCS card, so called ***token***, type the password and validate with ENTER:



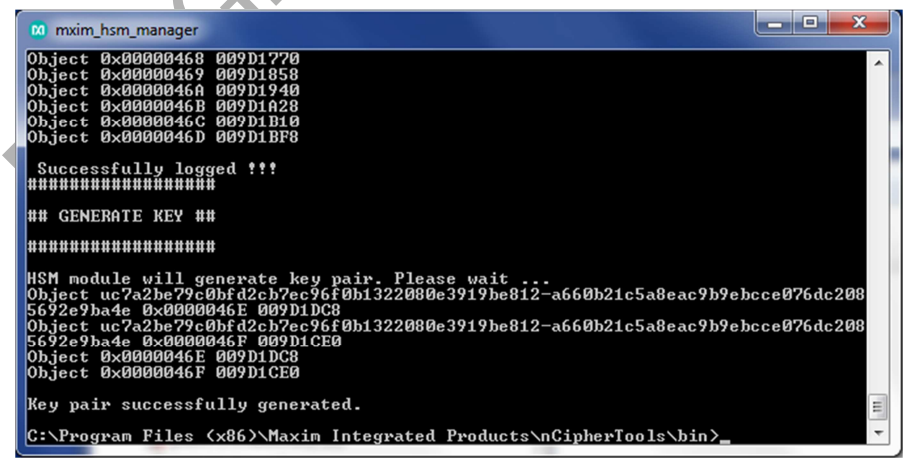
Insert next OCS card(s), type the password and validate with ENTER (repeat this operation accordingly to the quorum):



HSM will generate ECDSA key pair. The operation takes some time.



And finally …



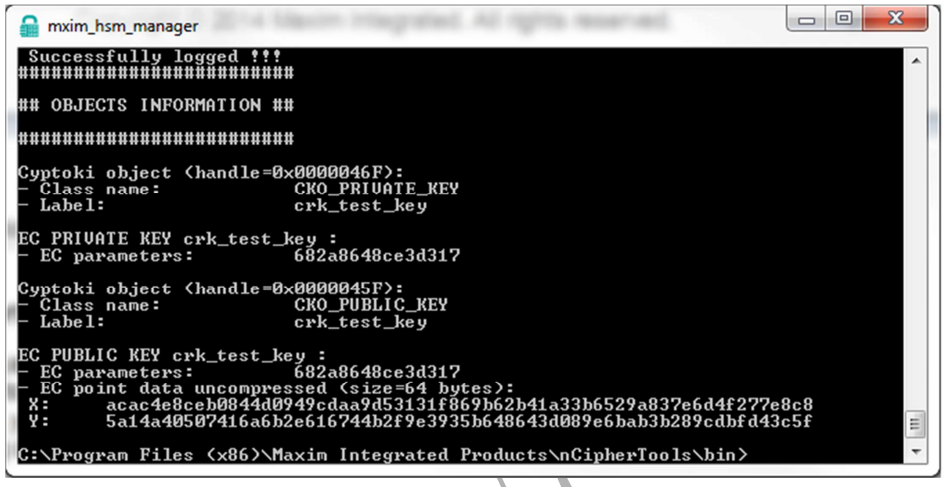
3.3.2 Export public ECDSA key

Considering a security (see section 2.1.2.2) is present on the PC, all ***OCS*** cards required accordingly to the quorum are available, and one ECDSA key has already been created (see section 3.2), you have to plug the**Thales nShield Edge** in. Then, in Windows console, type the following command and follow the instructions:

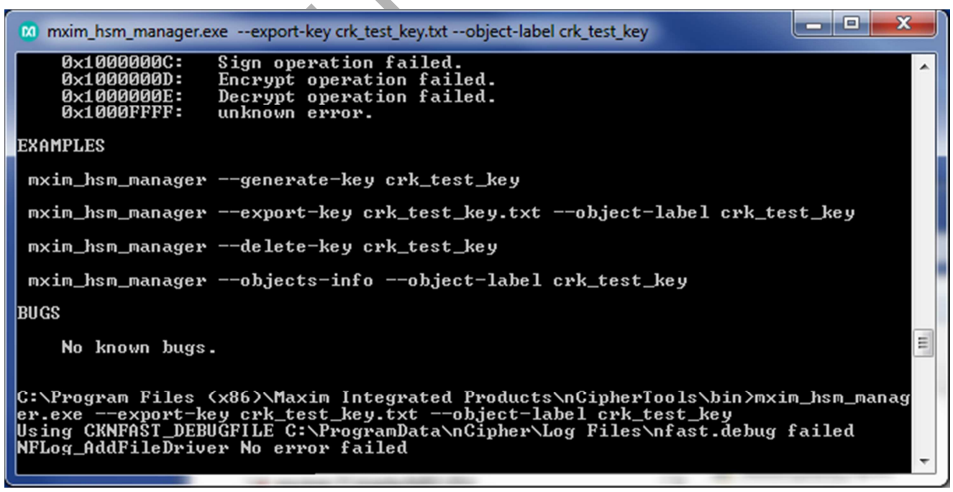
- `mxim_hsm_manager.exe --export-key <path_and_file_name> --object-label <name_of_ecdsa_key>`

Example:

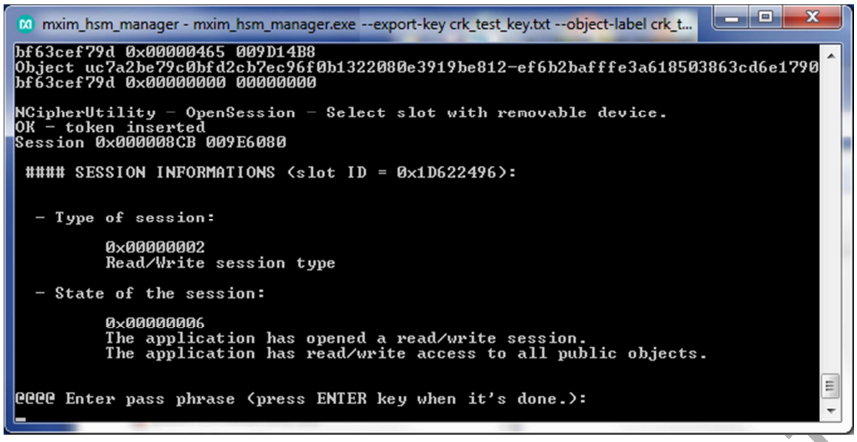
To check that the ECDSA key exists:
`mxim_hsm_manager.exe --objects-info --object-label crk_test_key`



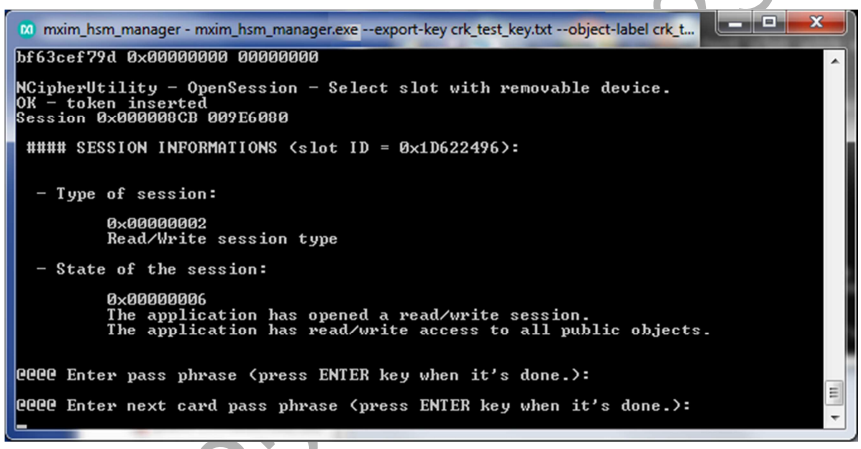
Then, type following command:
`mxim_hsm_manager.exe --export-key crk_test_key.txt --object-label crk_test_key`



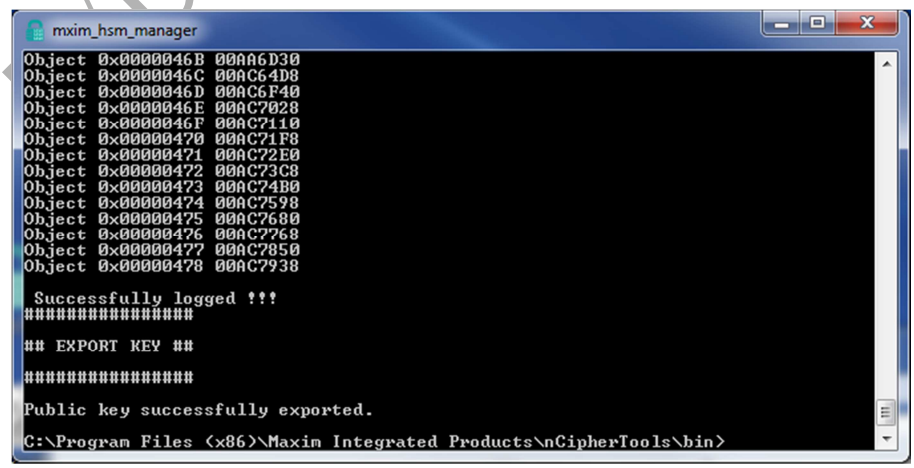
Insert first OCS card, so called ***token***, type the password and validate with **ENTER**:



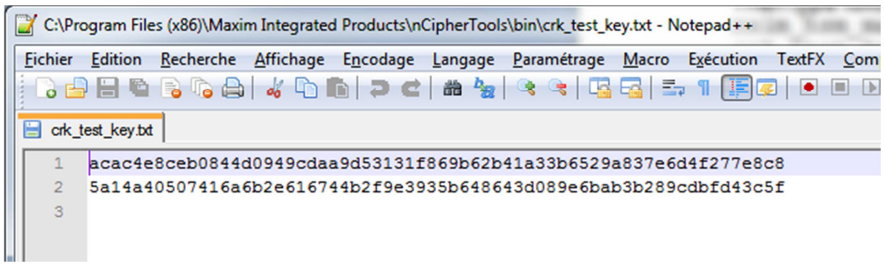
Insert next OCS card(s), type the password and validate with **ENTER** (repeat this operation accordingly to the quorum):



HSM will export public ECDSA key.



The exported file result:



First line is corresponding to the modulus of the public ECDSA key.
Second line is corresponding to the exponent of the public ECDSA key.

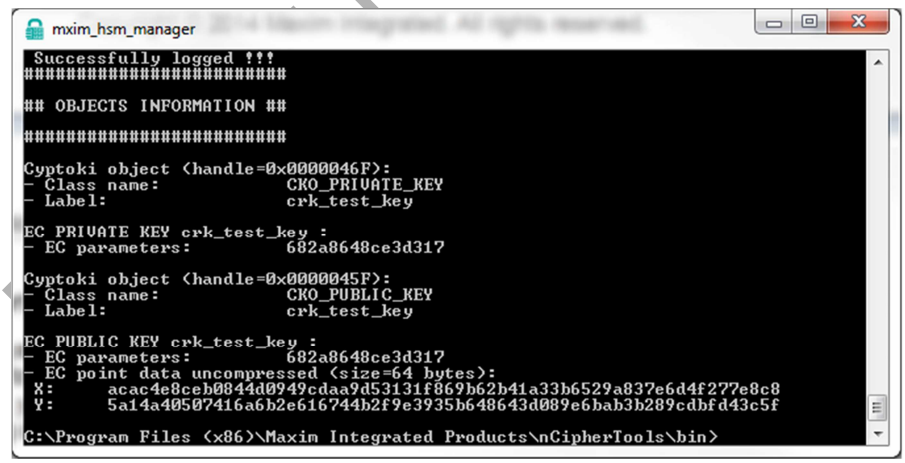
3.3.3 Remove ECDSA key pair

Considering a security (see section 2.1.2.2) is present on the local machine, all ***OCS*** cards required accordingly to the quorum are available, and one ECDSA key has already been created (see section 3.2), you have to plug the**Thales nShield Edge** in. Then, in Windows console, type the following command and follow the instructions:

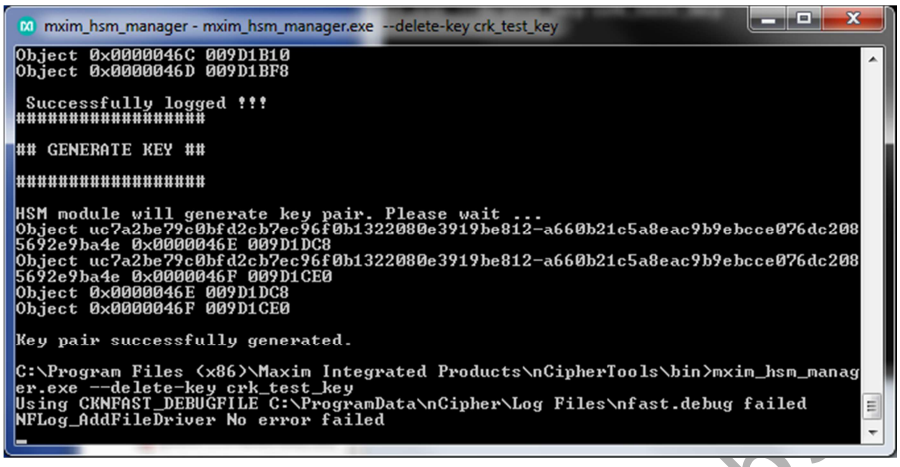
- `mxim_hsm_manager.exe --delete-key <name_of_ecdsa_key>`

Example:

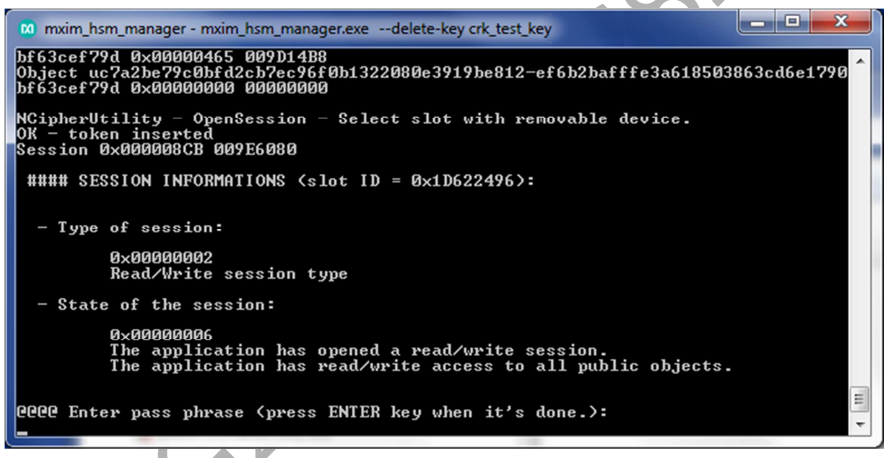
To check that the ECDSA key exists:
`mxim_hsm_manager.exe --objects-info --object-label crk_test_key`



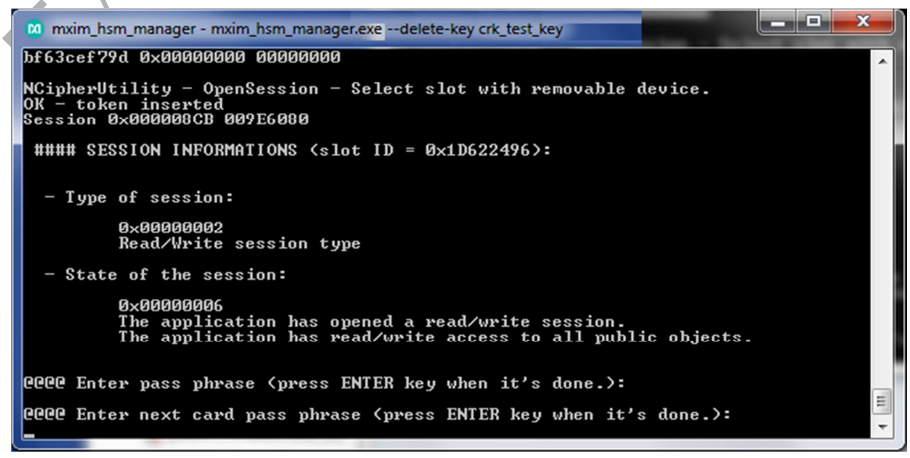
Type following command: `mxim_hsm_manager.exe –delete-key crk_test_key`



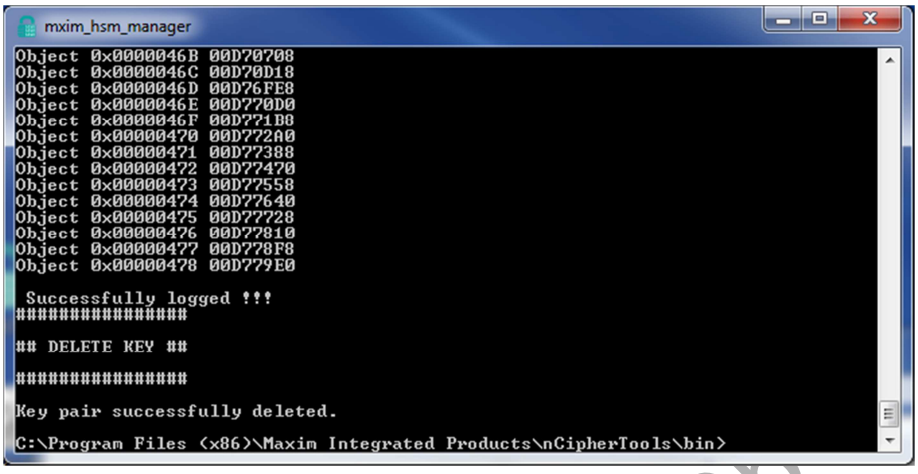
Insert first OCS card, so called ***token***, type the password and validate with **ENTER**:



Insert next OCS card(s), type the password and validate with **ENTER** (repeat this operation accordingly to the quorum):



HSM will delete ECDSA key pair.



4 SCP packets generation

Maxim Integrated has sent signed CRK public key to the customer who can securely upload its SCP packets on his Maxim integrated chip.

4.1 nCipher_session_build application

It is strongly recommended to read the UG21T24 (see [3]) for MAX32590 and UG25H04 (see [4]) for MAX32550 and notably the part dedicated to `session-build` tool and details related to its configuration file. `ncipher_session_build` application use the same configuration file except new parameters related to the use of HSM (see section 4.1.1).

4.1.1 Configuration file

The application program and the configuration file shall be located in the same directory. Accordingly to the `session_build` tool documentation set the parameters in the "session-build.ini" file. Then configure the parameters related to HSM:

```
#-----------------------------------------
#-- HSM ECDSA KEY
#-----------------------------------------
name_of_ecdsa_key=CRK_PROD
quorum_k=2
quorum_n=3
#-------------------------------------
#-- HSM RSA KEY
#-------------------------------------
name_of_rsa_key=CRK_PROD
quorum_k=2
quorum_n=3
#-------------------------------------
```

- "name_of_rsa_key": MAX32590 RSA key label used to sign SCP packets. The key has been generated by **Thales nShield Edge** HSM (see section 3.2).
- "name_of_ecdsa_key": MAX32550 RSA key label used to sign SCP packets. The key has been generated by **Thales nShield Edge** HSM (see section 3.2).
- "quorum_k" and "quorum_n": OCS cards quorum values (see section 2.1.2.2).

This operation has to be done once.

4.1.2 SCP packets building

Considering a security (see section 2.1.2.2) is present on the PC, all ***OCS*** cards required accordingly to the quorum are available, and one RSA or ECDSA key has already been created (see section 3.2), you have to plug the**Thales nShield Edge** in. Then, in Windows console, type the following command and follow the instructions:

- `cd <ncipher_tools_installation_folder>\bin`
- `ncipher_session_build.exe`

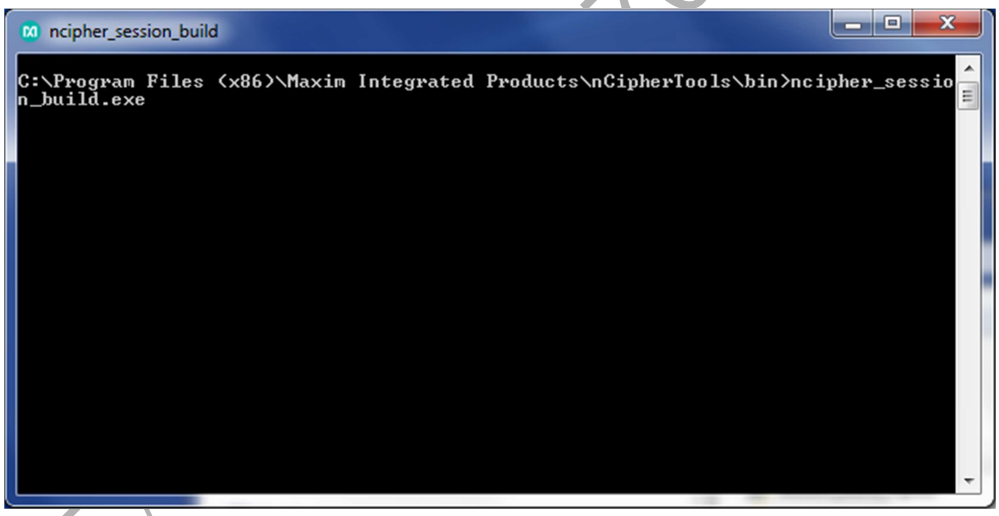
Example:

The configuration has default parameters used to perform a test:

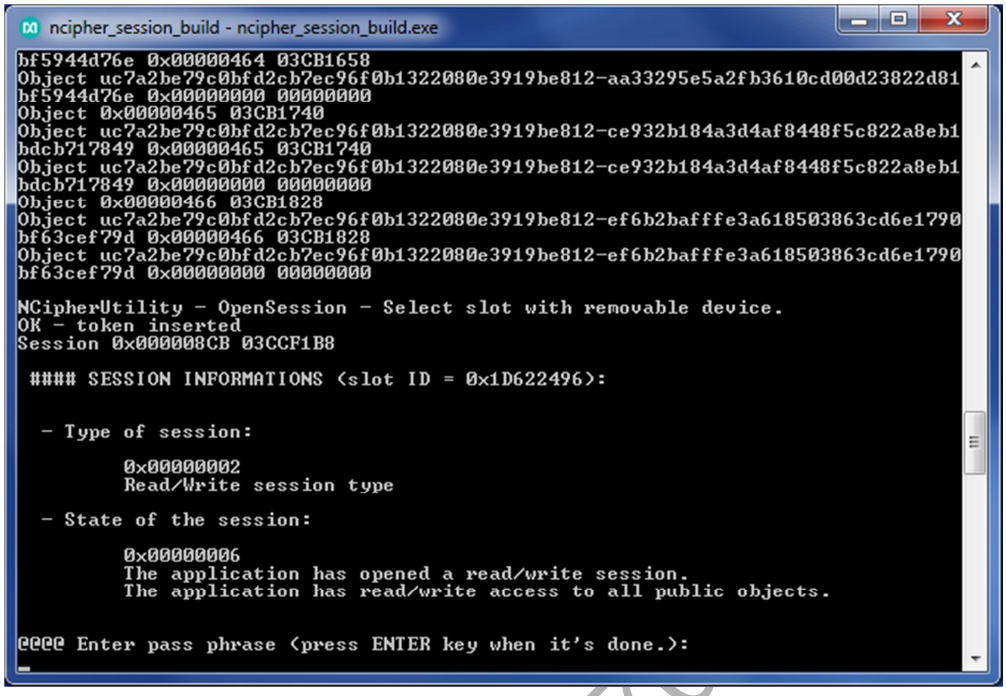
- `output_file`: define where are saved the SCP packets files: `<ncipher_tools_installation_folder>\bin\session_build_outputs`.

- `script_file`: corresponding to the script file used to generate SCP packets: `<ncipher_tools_installation_folder>\bin\session_build_inputs\script.txt`

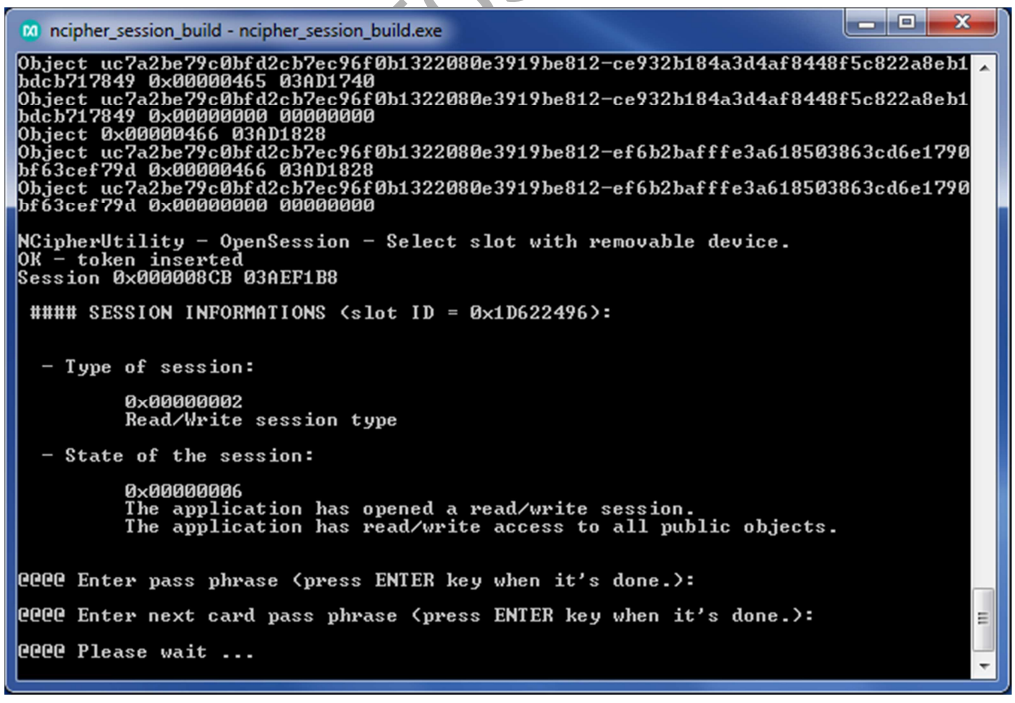
Type following command: `ncipher_session_build`



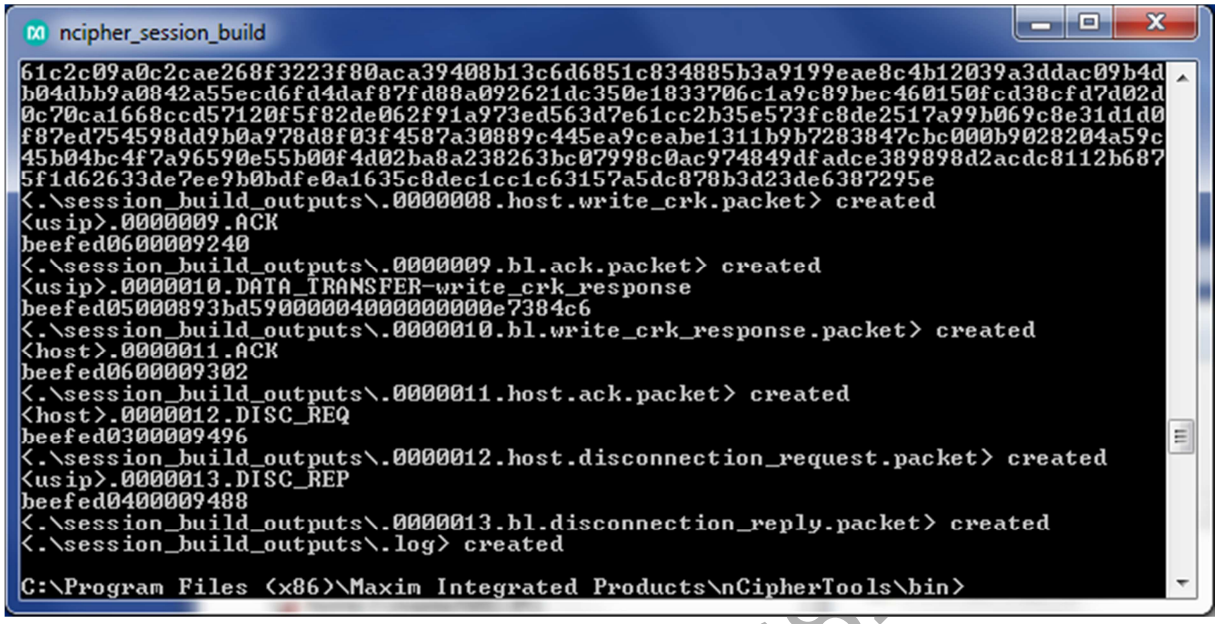
Insert first OCS card, so called ***token***, type the password and validate with **ENTER**:



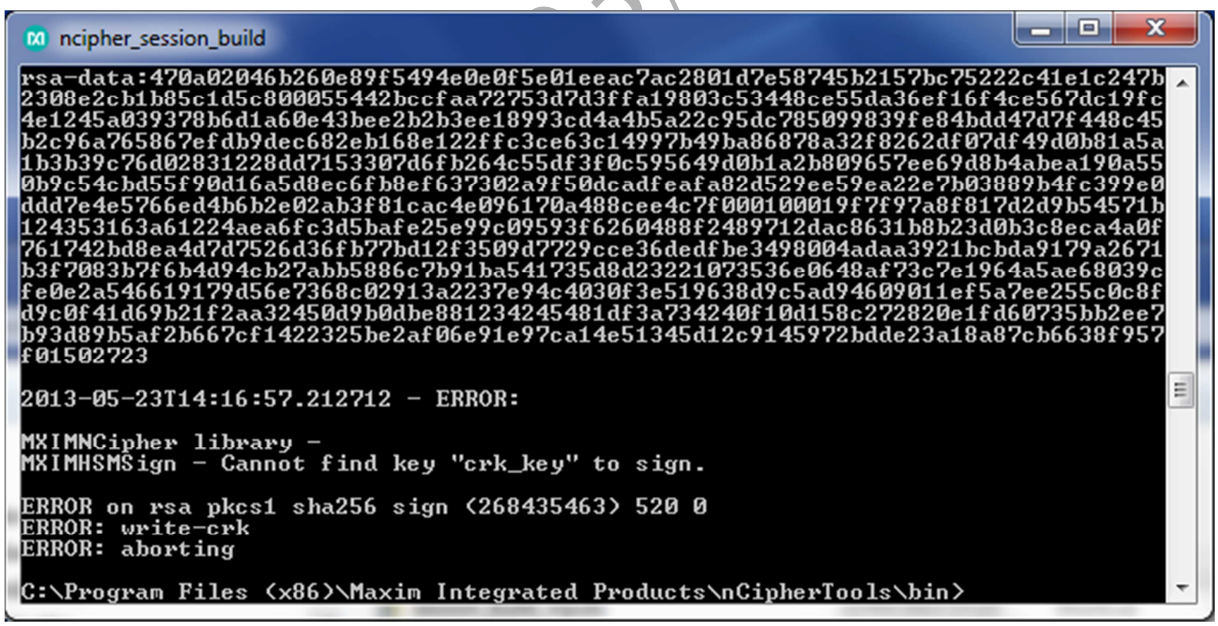
Insert next OCS card(s), type the password and validate with **ENTER** (repeat this operation accordingly to the quorum):



Application successfully ended:



Errors:
If the RSA or ECDSA key name is wrong or it has not been generated (see 3.2) in the configuration file:



5 Customer application signature

Customer application that is launched by the MAX32590 or the MAX32550 Secure ROM code has to be signed by the CRK as the ROM code performs digital signature verification with this key before agreeing to run the application.

5.1 nCipher_ca_sign_build application

It is strongly recommended to read the UG21T24 for MAX32590(see [3]) and UG25H04 (see [4]) for MAX32550 and notably the part dedicated to `ca-sign` tool and details related to its configuration file. `ncipher_ca_sign_build` application use the same configuration file except new parameters related to the use of HSM (see section 4.1.1).

5.1.1 Configuration file

The application program and the configuration file shall be located in the same directory. Accordingly to the `ca_sign_build` tool documentation set the parameters in the "ca_sign_build.ini" file. Then configure the parameters related to HSM:

```
#----------------------------------------
#-- HSM ECDSA KEY
#----------------------------------------
name_of_ecdsa_key=CRK_PROD
quorum_k=2
quorum_n=3
#----------------------------------------
#-- HSM RSA KEY
#----------------------------------------
name_of_rsa_key=CRK_PROD
quorum_k=2
quorum_n=3
#----------------------------------------
```

- "name_of_rsa_key": for MAX32590, RSA key label used to sign binary file. The key has been generated by **Thales nShield Edge** HSM (see section 3.2).
- "name_of_ecdsa_key": for MAX32550, key label used to sign binary file. The key has been generated by **Thales nShield Edge** HSM (see section 3.2).
- "quorum_k" and "quorum_n": OCS cards quorum values (see section 2.1.2.2).

This operation has to be done once.

5.1.2 Application signature

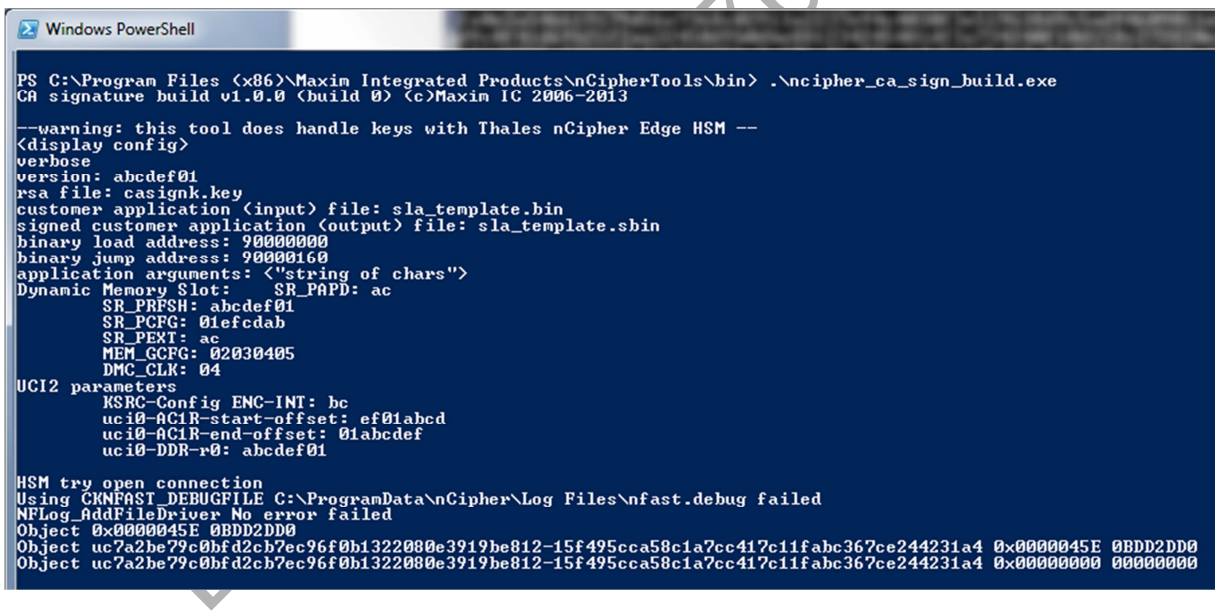
Considering a security (see section 2.1.2.2) is present on the PC, all ***OCS*** cards required accordingly to the quorum are available, and one RSA or ECDSA key has already been created (see section 3.2), you have to plug the**Thales nShield Edge** in. Then, in Windows console, type the following command and follow the instructions:

- `cd <ncipher_tools_installation_folder>\bin`
- `ncipher_ca_sign_build.exe`

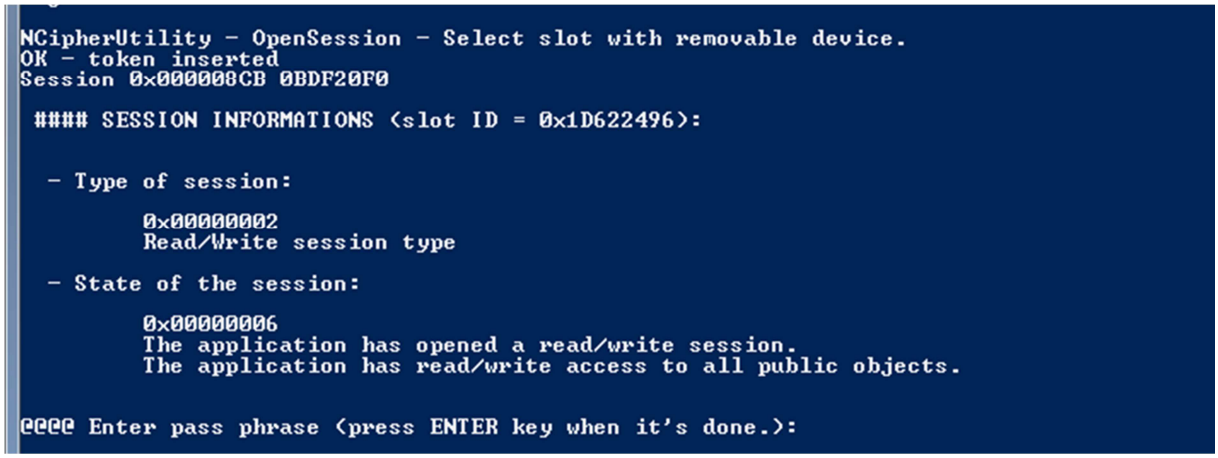
Example:

The configuration has default parameters used to perform a test (see ca_sign_build.ini file).

Type following command: `ca_sign_build`



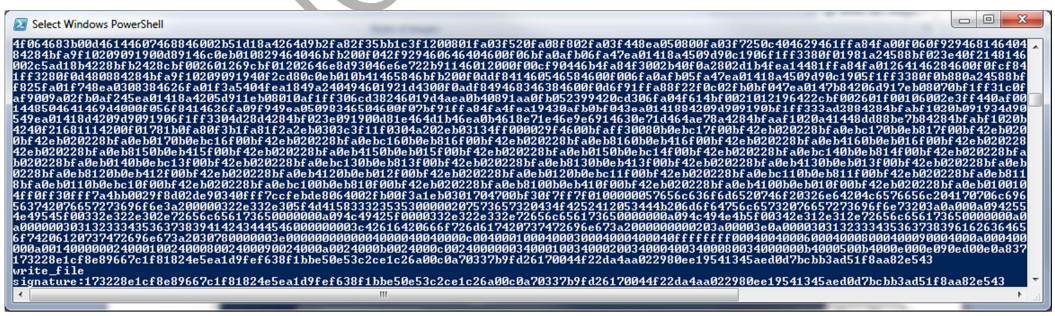
Insert first OCS card, so called ***token***, type the password and validate with **ENTER**:



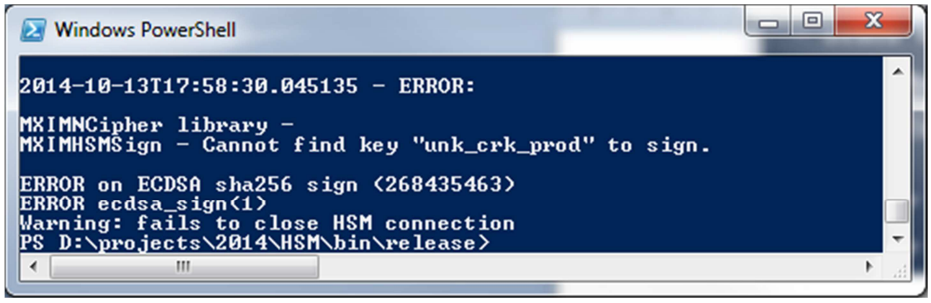
Insert next OCS card(s), type the password and validate with **ENTER** (repeat this operation accordingly to the quorum):

```
#### SESSION INFORMATIONS (slot ID = 0x1D622496):

 - Type of session:

        0x00000002
        Read/Write session type

 - State of the session:

        0x00000006
        The application has opened a read/write session.
        The application has read/write access to all public objects.

@@@@ Enter pass phrase (press ENTER key when it's done.):

@@@@ Enter next card pass phrase (press ENTER key when it's done.):
```

Application successfully ended:



Errors:
If the RSA or ECDSA key name is wrong or it has not been generated (see 3.2) in the configuration file:

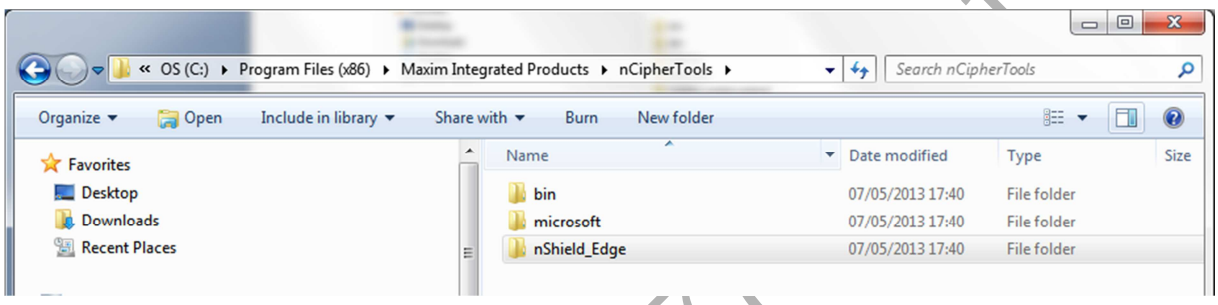


6 ANNEX: THALES nShield Edge USB FTDI drivers

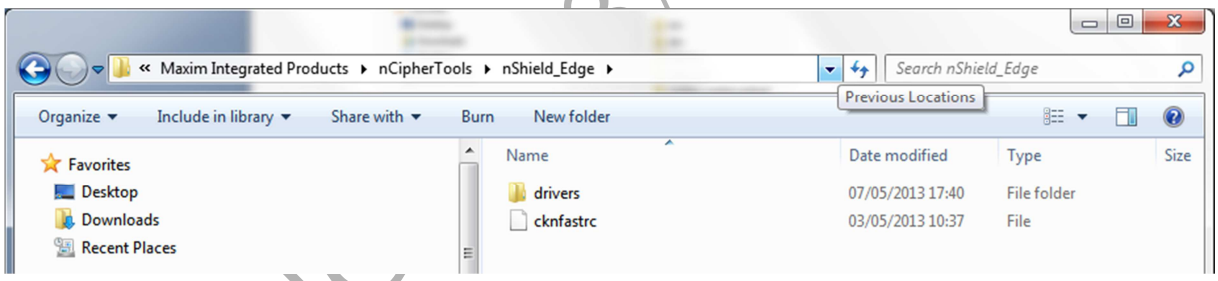
During THALES nShield Edge installation (problem already seen on Windows 7, 64 bits architecture), the HSM may not be recognized by the system due to USB pilots incorrect installation.

Follow this procedure:

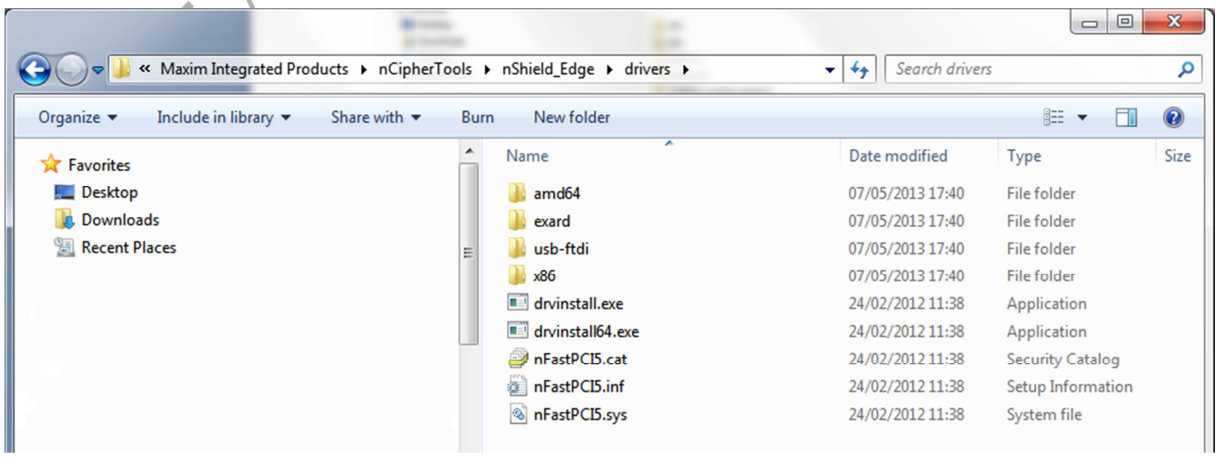
- Go into “MAXIMINTEGRATED nCipherTools” installation directory:



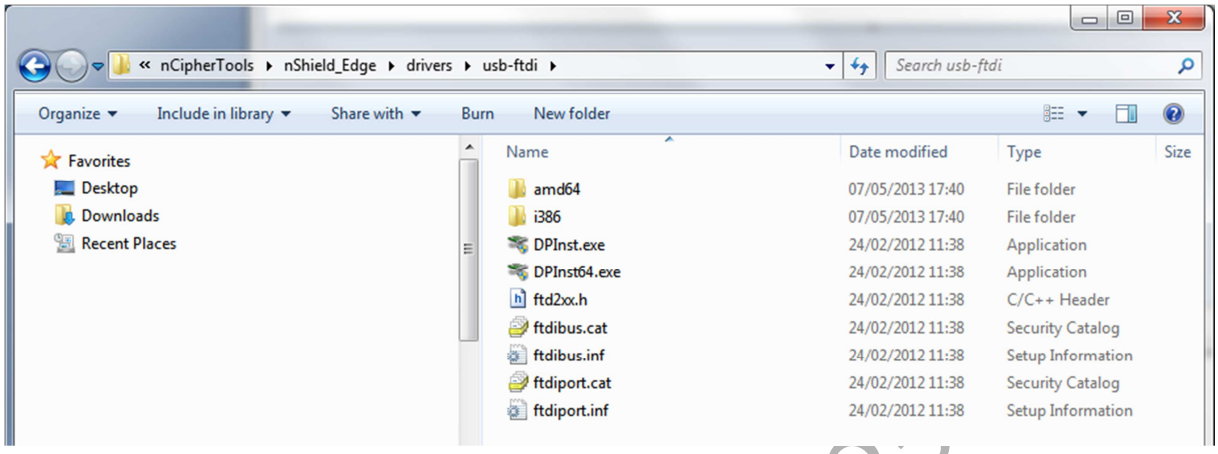
- Then into “nShield_Edge” installation directory:



- In “drivers” directory:



- Finally, in “usb-ftdi”:



- Click on “DPinstall.exe” in case of 32 bits architecture or on “DPinstall64.exe” in case of 64 bits architecture and follow instructions.

Maxim Integrated Reference

MAXIM Integrated

http://www.maximintegrated.com

for support, go to www.maximintegrated.com/support

