Open NFC - NFC Controller Simulator - User's Manual

Document Type:	Manual
Reference:	MAN_NFC_0905-114 Version 1.3 (14516)
Release Date:	June 23, 2011
File Name:	MAN_NFC_0905-114 Open NFC - NFC Controller Simulator - User's Manual.pdf
Security Level:	General Business Use

Copyright © 2009-2011 Inside Secure

Disclaimer

This document is licensed under the Creative Commons Attribution 3.0 license (http://creativecommons.org/licenses/by/3.0/). (You may use the content of this document in any way that is consistent with this license and if you give proper attribution (http://www.open-nfc.org/license.html#attribution).

Copyright © 2009-2011 Inside Secure

Open NFC and the Open NFC logo are trademarks or registered trademarks of Inside Secure.

Other brand, product and company names mentioned herein may be trademarks, registered trademarks or trade names of their respective owners.

History

Version	Date	Comments
0.1	May 16, 2009	First Draft
1.0	Dec. 15, 2009	Release for Open NFC 3.4
1.1	Dec. 8, 2010	Release for Open NFC 4.0
1.2	Jan. 27, 2011	Release for Open NFC 4.2 Updated for the new version of the NFC Simulator.
1.3	June 23, 2011	Release for Open NFC 4.3 Updating the functionalities and the screen shots.

Copyright © 2009-2011 Inside Secure

Summary of Contents

Summary of Contents 4

1 Introduction 5

2 NFC Simulator Tool 6

2.1 Installation 6

2.2 Main Window 6

2.2.1 General description 6

2.2.2 Menu bar 7

2.2.3 Device Window 9

2.2.4 Object Catalog Window 10

2.2.5 Presenting a virtual card in front of the antenna 11

2.1 Reader-Writer Functions 15

2.1.1 Read and Write 15

2.1.1 Collision 16

2.2 Multiple Device Interaction 17

2.2.1 NFC Device #2 17

2.2.2 External NFC Device 19

Copyright © 2009-2011 Inside Secure

1 Introduction

The NFC Controller Simulator is a Windows application that is part of the Open NFC tool kit that giving a way to run and debug NFC applications without the availability of a hardware NFC controller.

The NFC Controller Simulator provides simulation of the following features:

- Another NFC controller.
- Peer 2 Peer (target & initiator, passive & active, connected & connection less)
- Card Reader with the following protocol:
  - ISO14443-4-A/B
  - ISO14443-3-A/B
  - Jewel/Topaz protocol
  - ISO 15693-3
  - FeliCa
- Card emulation with following protocols
  - ISO14443-4-A/B
- Virtual Presentation Robot Service,

The NFC Controller Simulator support theses virtual cards:

- Mifare UL, Mifare UL C
- Mifare Classic (for detection)
- Mifare DesFire (in Type 4)
- Topaz 96
- Topaz 512
- Picopass 2k
- Picopass 32k
- Micropass (in type 4)
- Tag It
- LRI 512
- Icode
- NFC Forum Tags type 1, 2, 4A, 4B, 5, 6

The ***NFC Controller*** is used to develop applications, on top of Open NFC, without having a NFC Controller connected to the computer.

The ***Virtual cards***, gives possibility to develop user applications with card interaction. An antenna area is displayed and virtual card can be presented in front of them. The user selects the card among the list of virtual cards. Once presented in front of antenna the application can communicate with the card.

The ***Card emulation*** is used to develop application emulating card. The emulated card may be presented in front of another virtual NFC controller.

The ***Virtual Robot Service*** is used to drive automatically the card's presentation in front of the antenna without user interaction.

Copyright © 2009-2011 Inside Secure

2 NFC Simulator Tool

2.1 Installation

The NFC Controller Simulator ***NFCSimulator.exe*** can be installed in any folder.

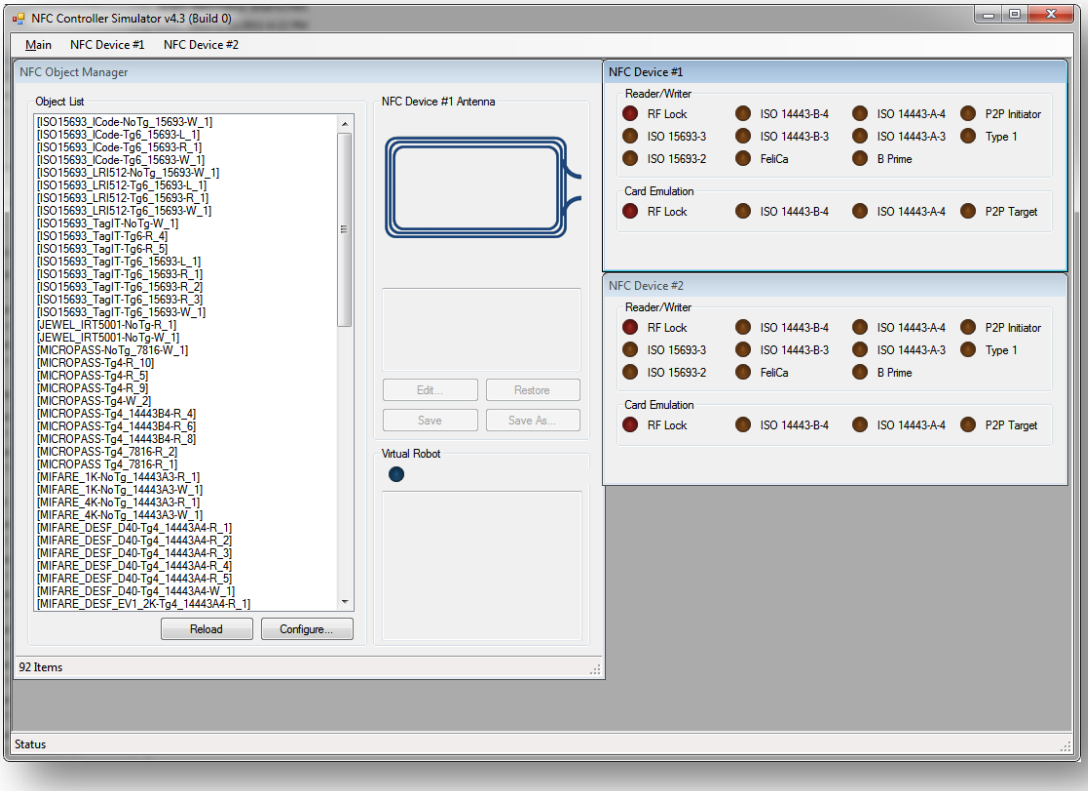
There is no installation procedure; just ensure that the following files are in the destination directory:

- NFCSimulator.exe
- InitSettings.xml (see below for description)
- PersistantData.xml (see below for description)
- Require DLLs (see below for list)
- “virtualcards” directory

2.2 Main Window

2.2.1 General description

After launching the executable, the following window is displayed:



Notice the 4 areas in this screen application:

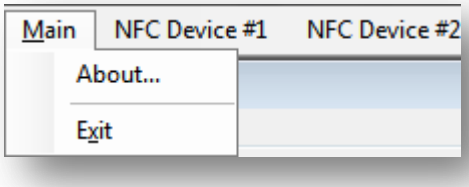
- Menu bar at the top
- NFC Device #1 and NFC Device #2 at the right side
- NFC Object Manager at the left side

Copyright © 2009-2011 Inside Secure

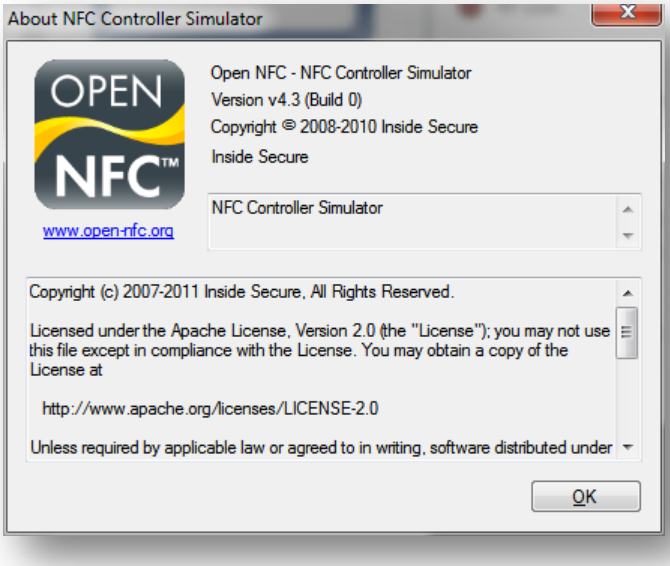
2.2.2 Menu bar

The menu bar has 3 items:

- Main:

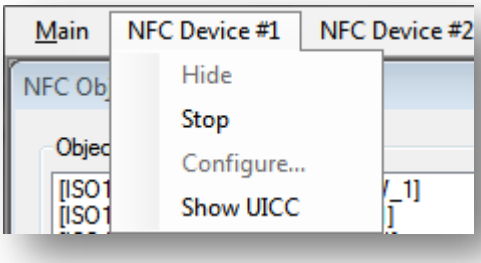


You can see the version and license policy about the simulator application by "About…" option:



You can exit application by "Exit" option

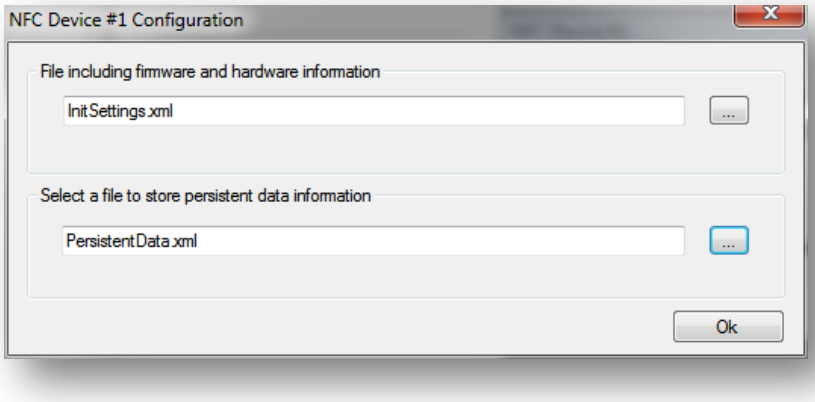
- NFC Device #1(representing the first NFC Device controller)



You can:

- Hide/Show the device #1 window
- Stop/Start the device #1.
- Configure the device by selecting the xml files containing the configuration and persistent data from NFC device controller.
  The device must be stopped before accessing the Configuration menu.

Copyright © 2009-2011 Inside Secure



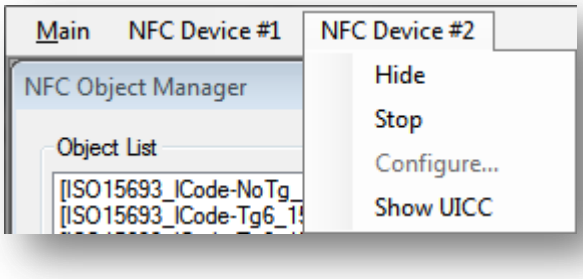
The file PersistentData.xml represents the persistent data stored in the device and contains theses information:

- <PersistantMemory> → the connection data used for device authentication during the HCI protocol initialization.
- <PersistentPolicy> Default access rights of the NFC device.

The InitSettings.xml represents the capabilities of the device and contains theses information:

- <HardwareInfo> → Description of device functionalities.
- <FirmwareInfo> → Description of firmware functionalities.
- <UICCCardMode> → Card mode configuration.
- <UICCReaderMode> → Reader mode configuration.
- UICCSwpMode> → SWP status.

- NFC Device #2 (represents the second NFC Device controller)

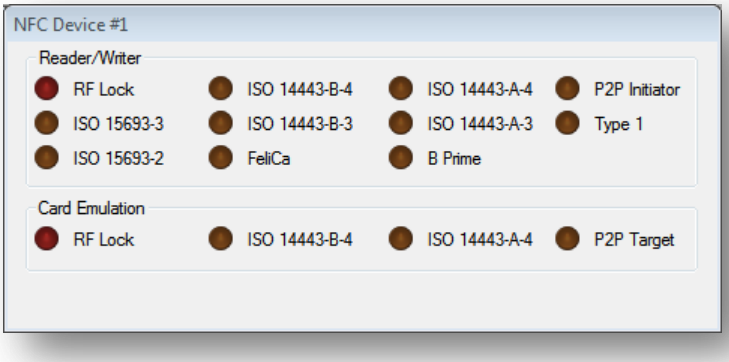


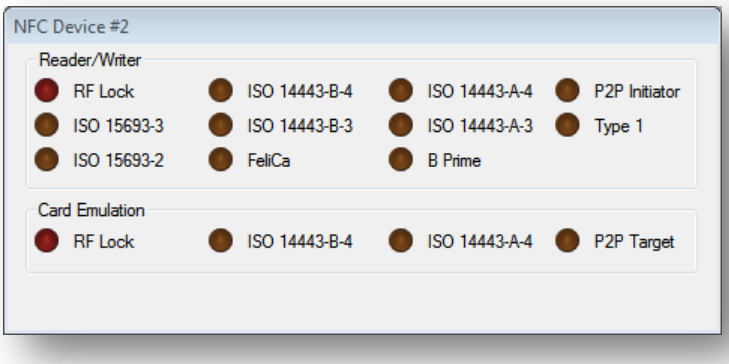
Device 2 has the same functionality as NFC Device #1.

The simulation of the NFC Device #1 and #2 are started automatically at the start of the simulator.

Copyright © 2009-2011 Inside Secure

2.2.3 Device Window



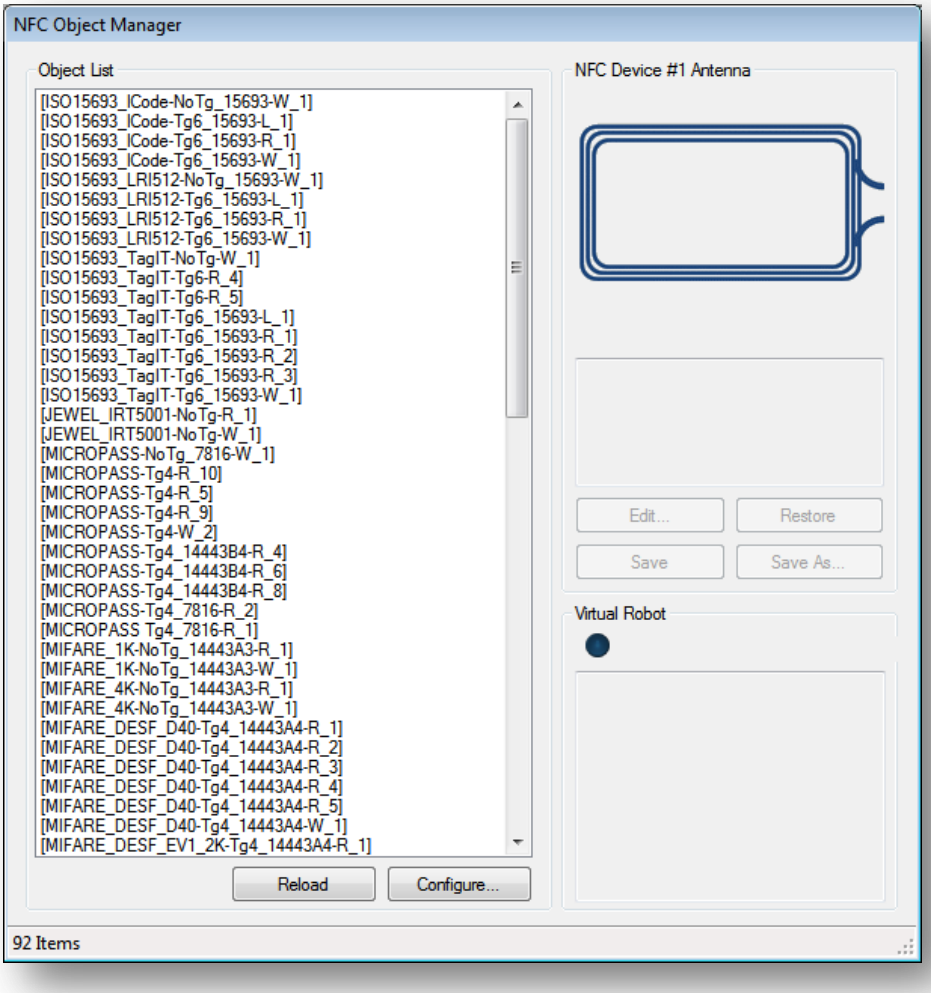


The window “NFC Device #1” and “NFC Device #2” represent the activity of the virtual NFC Controllers: The protocols used for the polling are displayed in orange, if a protocol collision occurs; the corresponding led is displayed in bright red. When a protocol is selected for communication in reader mode, card emulation or Peer 2 Peer, the protocol is displayed in green.

Copyright © 2009-2011 Inside Secure

2.2.4 Object Catalog Window

The figure below shows the NFC Object Manager Window without a card in front of antenna of the device #1:



The object catalog window contains several areas. On the left hand side, a list of virtual objects is used to select the object to present to the virtual NFC Controller:

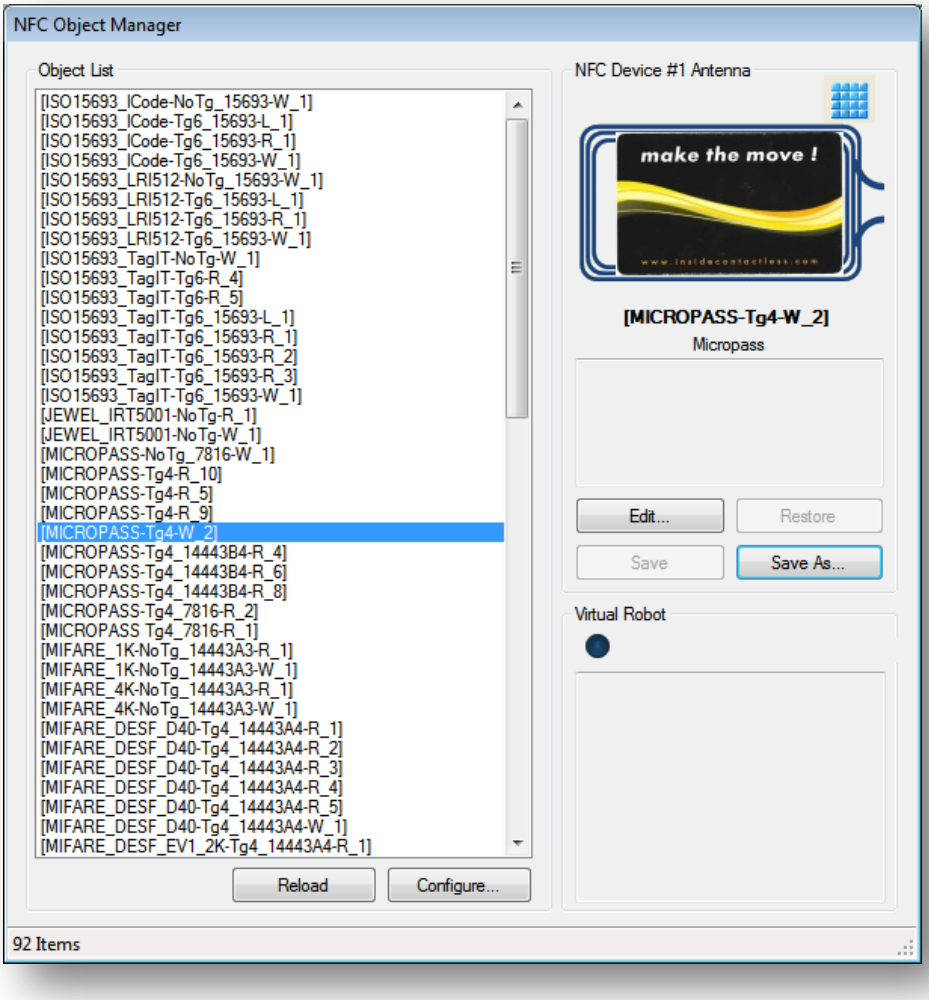
- Virtual Cards are simulation of physical card based on a XML file.
- Collision objects represent a set of conflicting cards causing a protocol collision.
- NFC Device #2 represents a second instance of simulated NFC Device.
- External NFC Device represents a third NFC device optionally connected to the NFC Controller Simulator.

All objects in the list are stored in the “virtualcards” directory and each of them is represented by a XML file description.

Copyright © 2009-2011 Inside Secure

2.2.5 Presenting a virtual card in front of the antenna

The object catalog contains also an area representing the antenna of the NFC Device #1. You can put object in front of this antenna by double clicking on the object from the object list. Double click on the object to remove it from the antenna.
The figure below shows the NFC Object Manager window with an example of MICROPASS card in front of antenna:



When you put an object in front of antenna of the NFC Device #1, you can edit the properties of the object and copy or save it in another xml file.

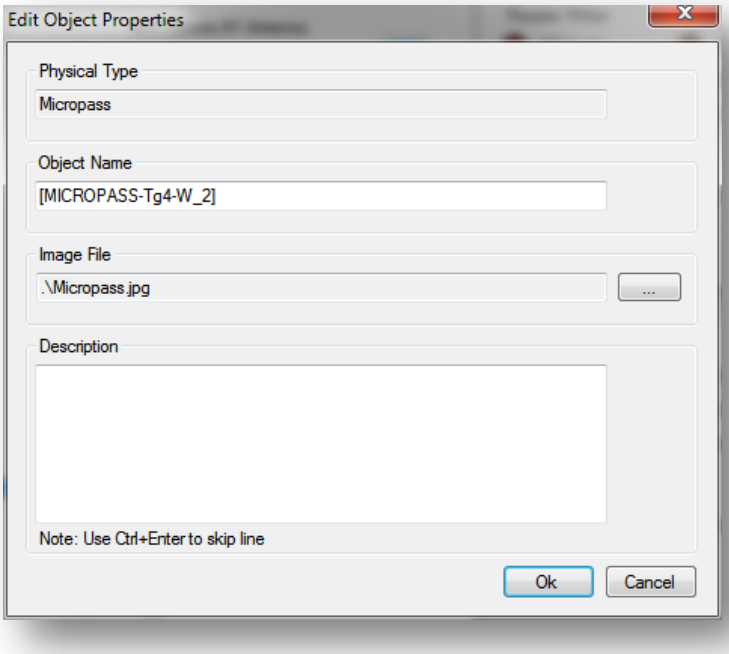
Copyright © 2009-2011 Inside Secure

2.2.5.1 Edit object properties

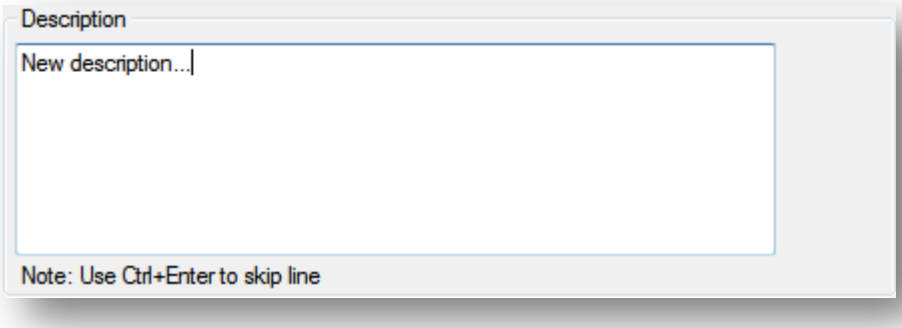
Clicking on “Edit”, a dialog box appears to edit/change the following object properties:

- name
- Image file
- Description

The figure below shows the object properties:

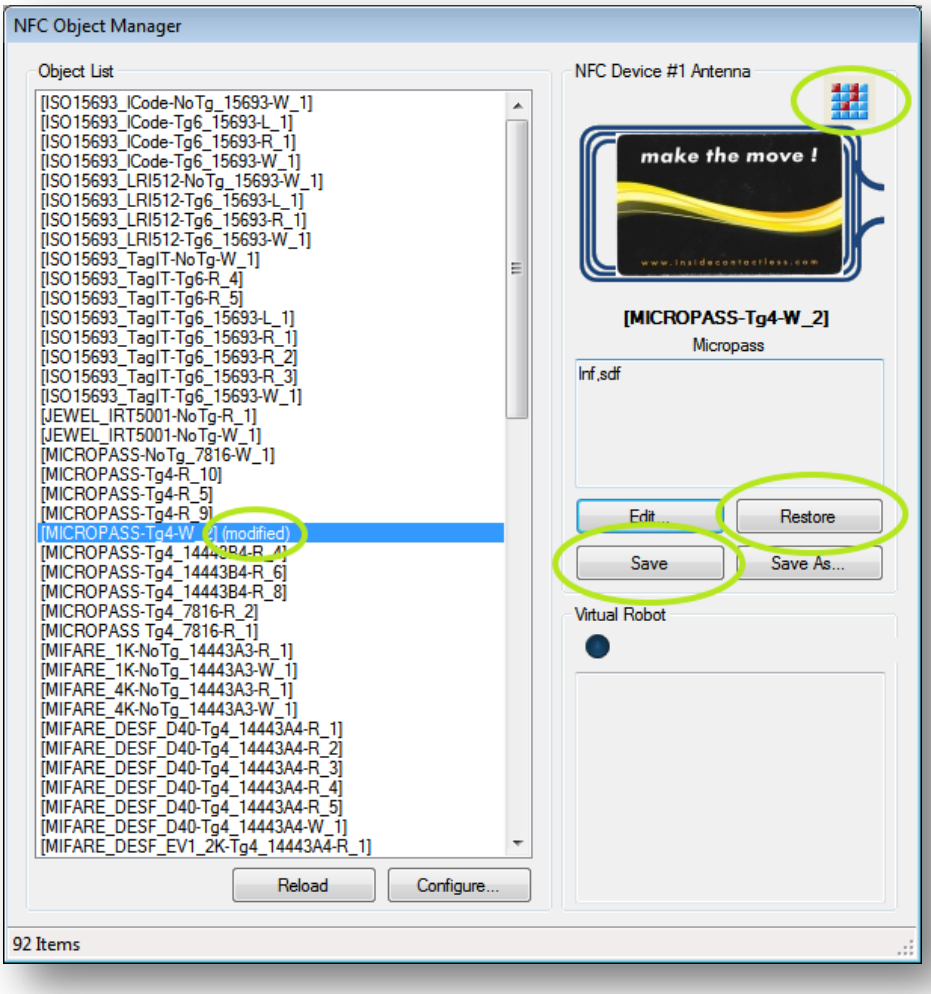


When you modify one of the properties of an object, for example the description,



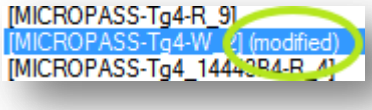
Copyright © 2009-2011 Inside Secure

After validation, the changes are visible in the object manager window.



Description of modifications:

- The object in the list is tagged as being modified.



- A specific icon in the top of antenna is displayed to notify a modified object.

- Button “Restore” enabled. This button restores the original properties and content of an object. The unsaved modifications are discarded.
- Button “Save” enabled. This button saves the current modifications in the original object file. Then the object is no longer tagged.

Copyright © 2009-2011 Inside Secure

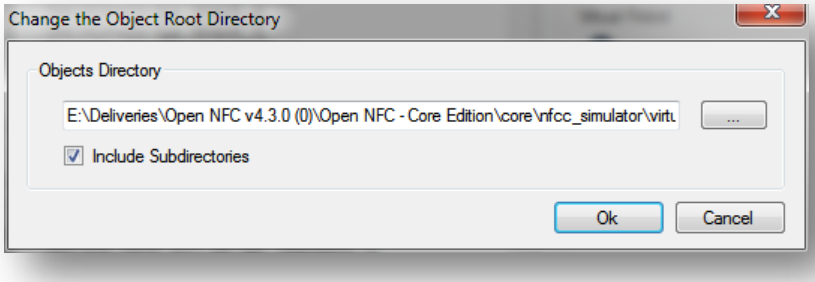
2.2.5.2 Virtual robot area

The virtual robot area is used for automating presentation of object. It is used in conjunction with an automatic test tool.

2.2.5.3 Manage virtual card repository

2 buttons are used to manage the virtual card repository:

- The reload button to reload all cards from original files. All modifications will be lost.
- The configure button to browse any folder and modified the path of the Object directory where are save the cards used by the simulator.

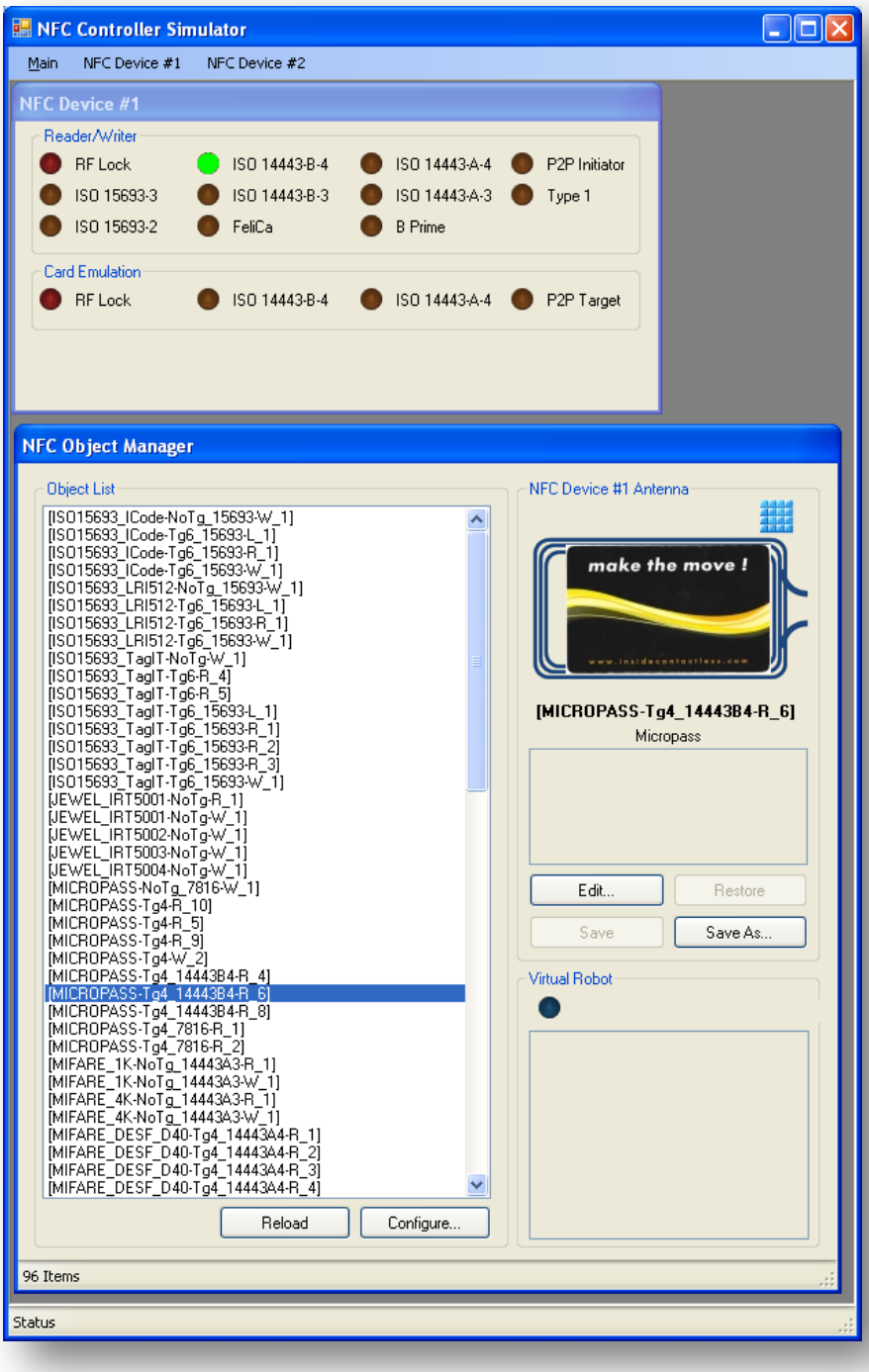


Copyright © 2009-2011 Inside Secure

2.1 Reader-Writer Functions

2.1.1 Read and Write

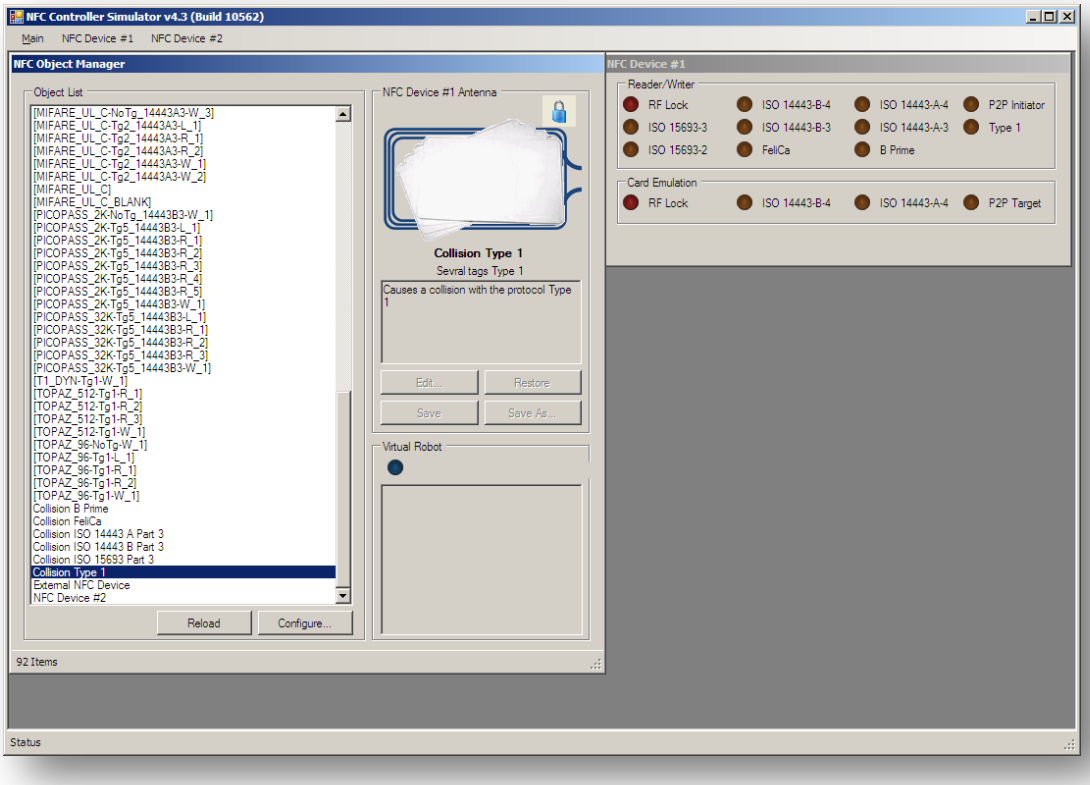
Figure below describes an ongoing reading operation on a virtual card.



Copyright © 2009-2011 Inside Secure

2.1.1 Collision

As shown in the figure below, presenting one of the collision objects will simulate a collision for the given protocol.



Copyright © 2009-2011 Inside Secure

2.2 Multiple Device Interaction

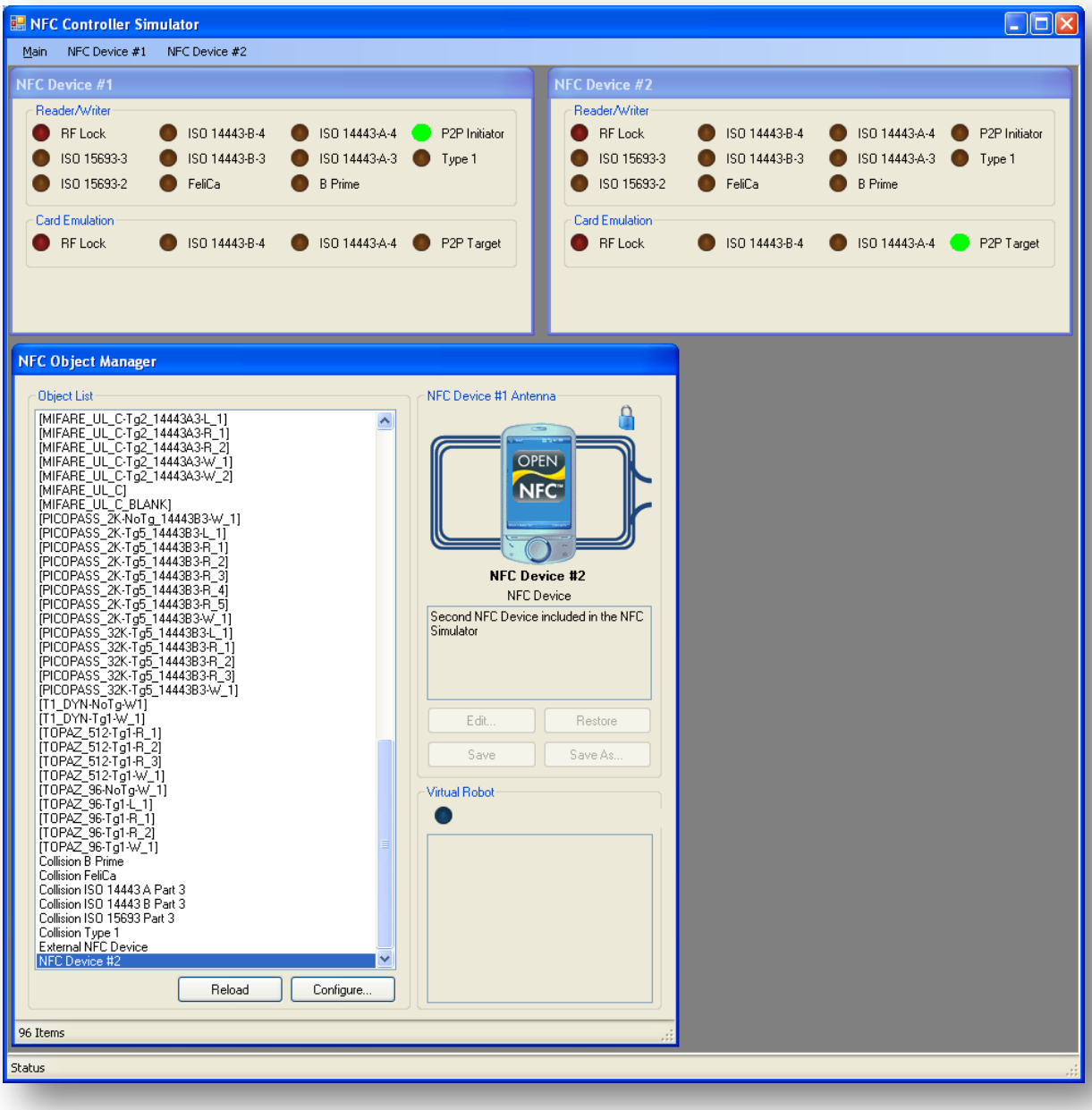
The NFC Simulator Tool includes the simulation of two NFC Devices. The two NFC devices can be controlled by two different NFC stacks so the interaction of two applications executed on two different devices can be simulated.

The second device can be presented or removed from the antenna of the first device like any other virtual object listed in the object catalog.

2.2.1 NFC Device #2

The simulation can be done with one device in reader mode and one device in card emulation mode. A peer 2 peer communication can also be simulated.

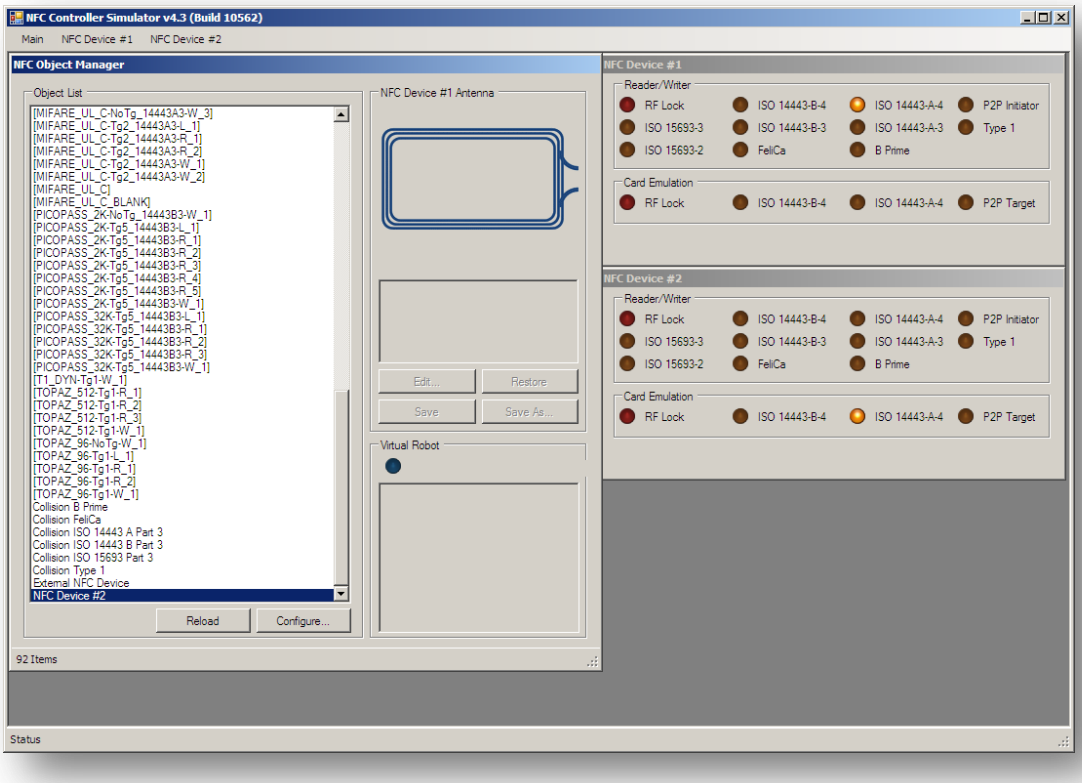
The following figure shows a scenario of Peer 2 Peer communication.



Copyright © 2009-2011 Inside Secure

Copyright © 2009-2011 Inside Secure

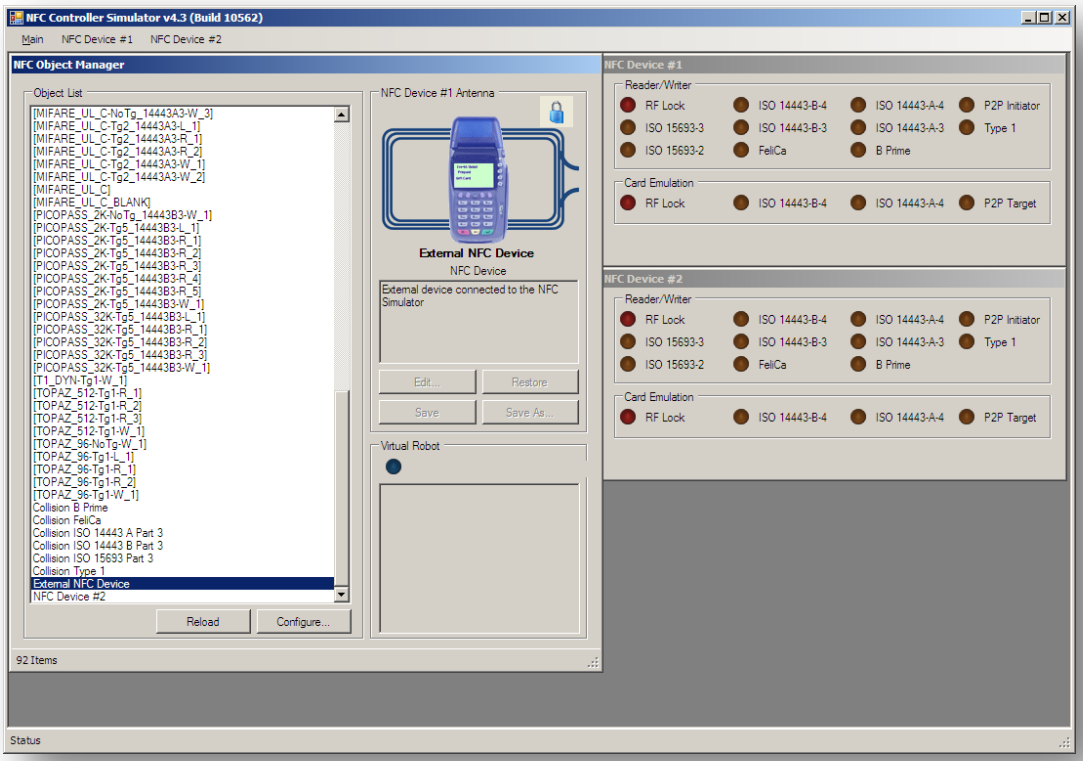
The following figure shows a scenario of Card Emulation communication



2.2.2 External NFC Device

External NFC device used for POS device simulation (Point Of Sale)

Copyright © 2009-2011 Inside Secure



Copyright © 2009-2011 Inside Secure