AN10992

Quick Startup Guide for RD710

Rev. 2.1 — 6 December 2011
198121

Application note
COMPANY PUBLIC

Document information

Info	Content
Keywords	RD710, RD852, Quick startup guide, SAM AV1, SAM AV2, RC523, RX852
Abstract	This document is intended for new users to start working with the Design-In Kit. It shows the basic functionality with MIFAREdiscover.

Revision history

Rev	Date	Description
2.1	20111206	Added in 5.1 the Activation of a MIFARE Classic Card.
2.0	20110803	Extended usecases for MIFAREdiscover
1.1	20110712	Update due to release of new usecases of MIFAREdiscover
1.0	20110411	Initial version
	20110105	Draft version

Contact information

For more information, please visit: http://www.nxp.com

For sales office addresses, please send an email to: salesaddresses@nxp.com

1. Introduction

The purpose of this document is to provide a set of guidelines to aid in the first operation of the RD710 reader. The MIFAREdiscover (ver.3.x.x) will be used as a user interface to communicate to the readers and cards, respectively.

The USB drivers are included in the CD package.

2. Installation

2.1 Required items

To use the MIFAREdiscover, the following items are required:

- MIFARE cards as MIFARE DESFire EV1, MIFARE Classic, MIFARE Ultralight
- Pegoda Reader (RD710 or RD710 as part of EV710) (see [32] – [36])
- MIFAREdiscover (see [37])
    - Public version available on NXP web (see [39])
    - Full version (see [40])

2.2 Installing USB driver for the Reader

The demonstrated installation is shown on Windows 7, but it is the same in Windows XP and Vista.

1) If you don't have a CD that was delivered with your Pegoda, open your web browser, go to see [38] and download and extract the zip file.
2) Connect the Pegoda RD710 with your computer.
3) Wait until Windows 7 installs a standard driver.
4) Open the Windows Device Manager and navigate to the installed Reader (see figure 1 below)

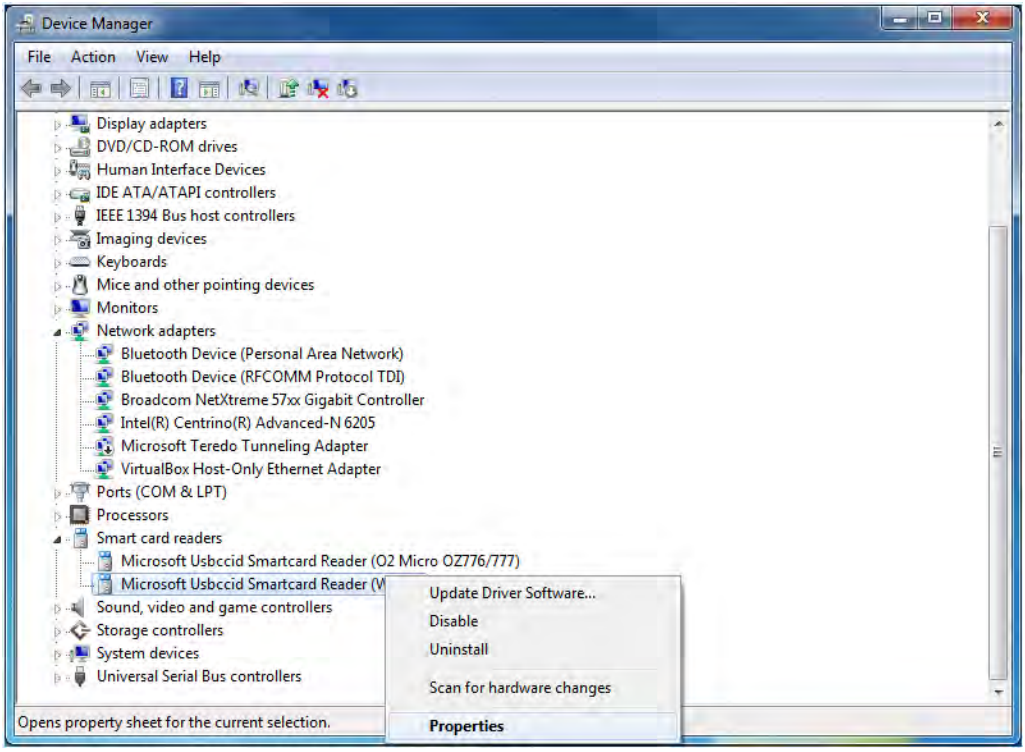


Fig 1. Device Manager

5) Click Smartcard Reader with the right mouse button and choose “Properties”.

6) Choose the tab driver and click “Update Driver”.

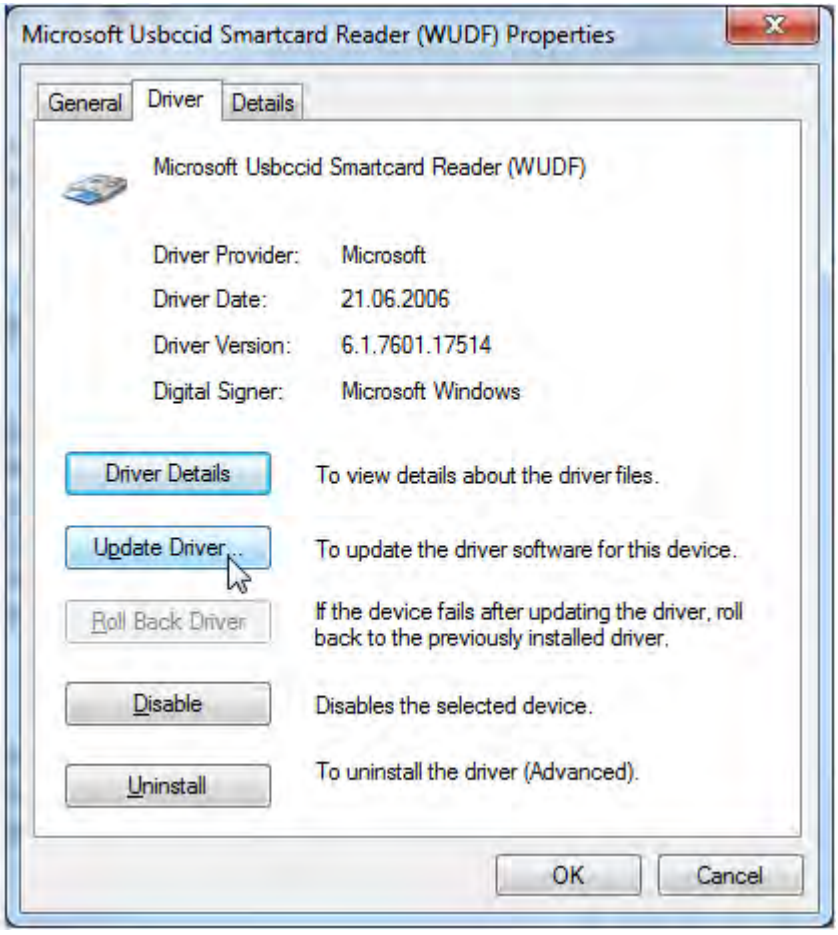


Fig 2. Update Driver

7) Windows will ask you how to search for the driver. Choose “Browse my computer for driver software”.

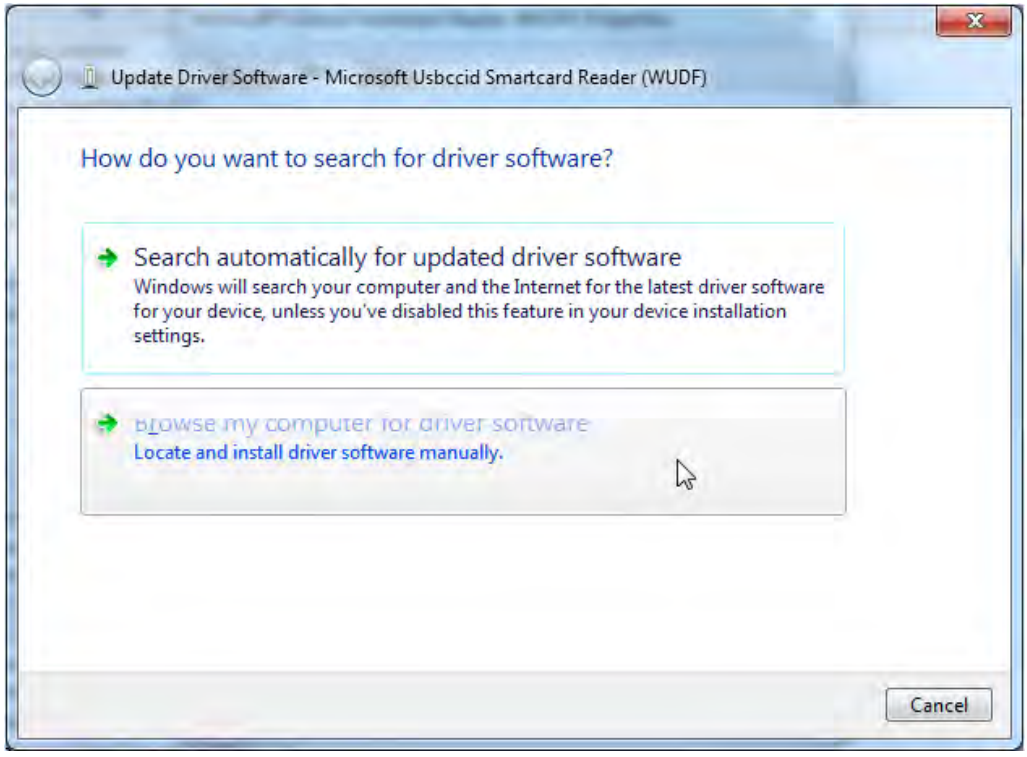


Fig 3. Browse Computer

8) Choose “Browse”, navigate to the root directory of the CD or the previous extracted content and click “Next”.

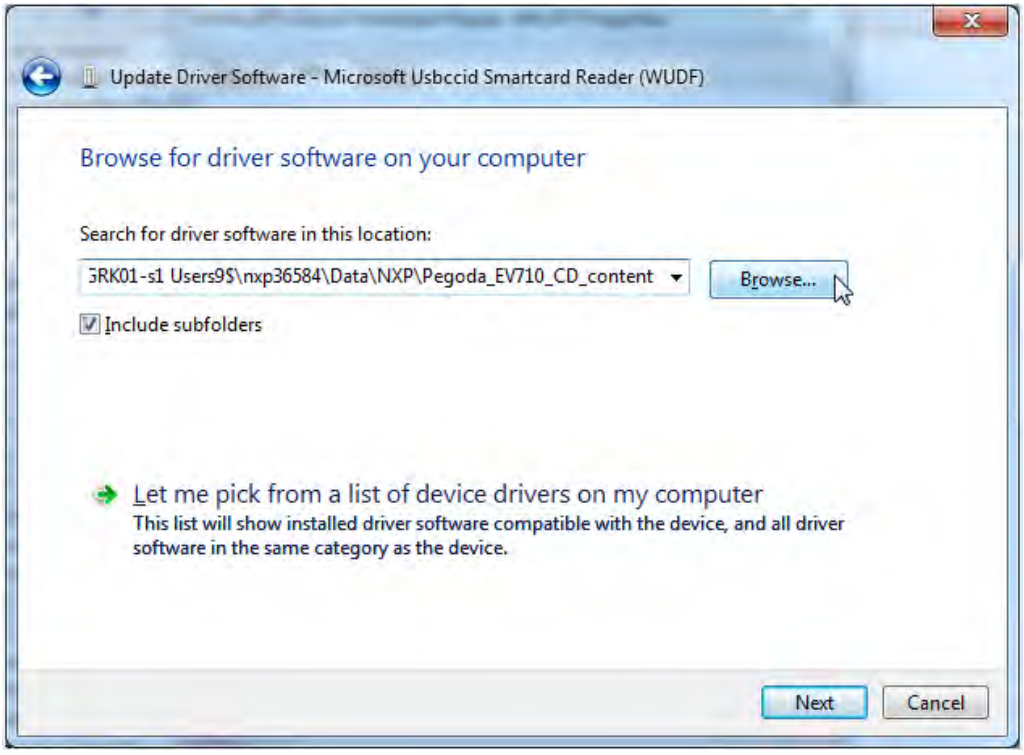


Fig 4. Browse for driver software on your computer

9) Wait until Windows has finished the installation.

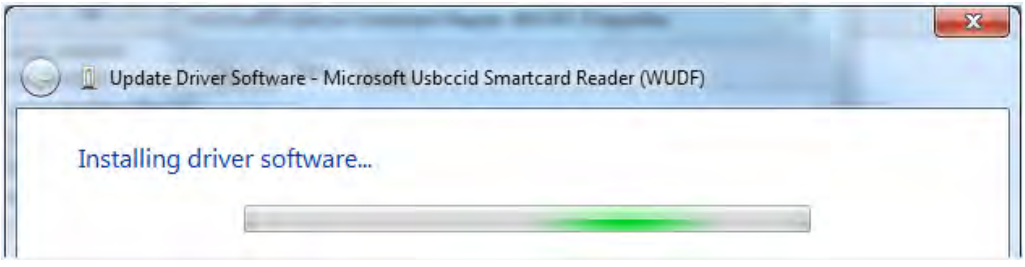


Fig 5. Installing driver software

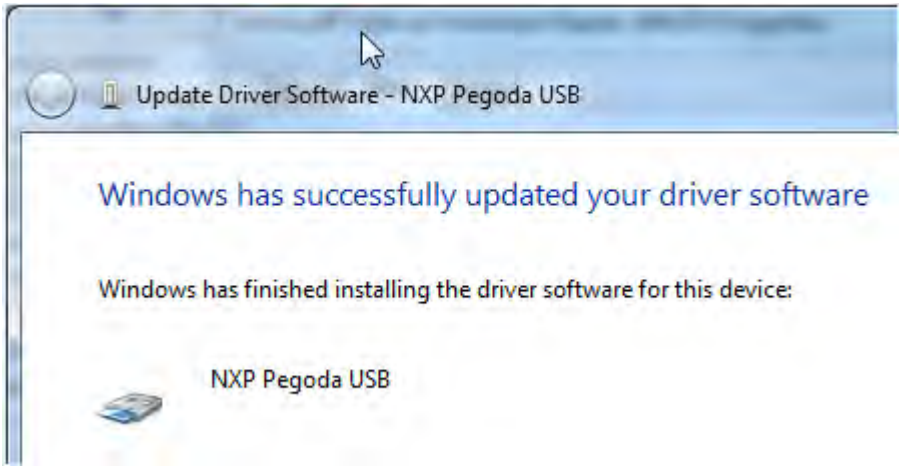


Fig 6. Finished installation

10) The installation is done.

2.3 Deactivate Smart Card Interface

For some customers it may be useful to deactivate the Smart Card Interface. This is especially important for users of Windows 7. If you see that Windows repeatedly tries to install a new Smart Card Interface you need to do the following steps.

1. Go to the Control Panel of your computer (Start – Control Panel)
2. Click “System” – “Device Manager” and then “Other devices”
3. Click “Smart Card” with your right mouse button and then disable.

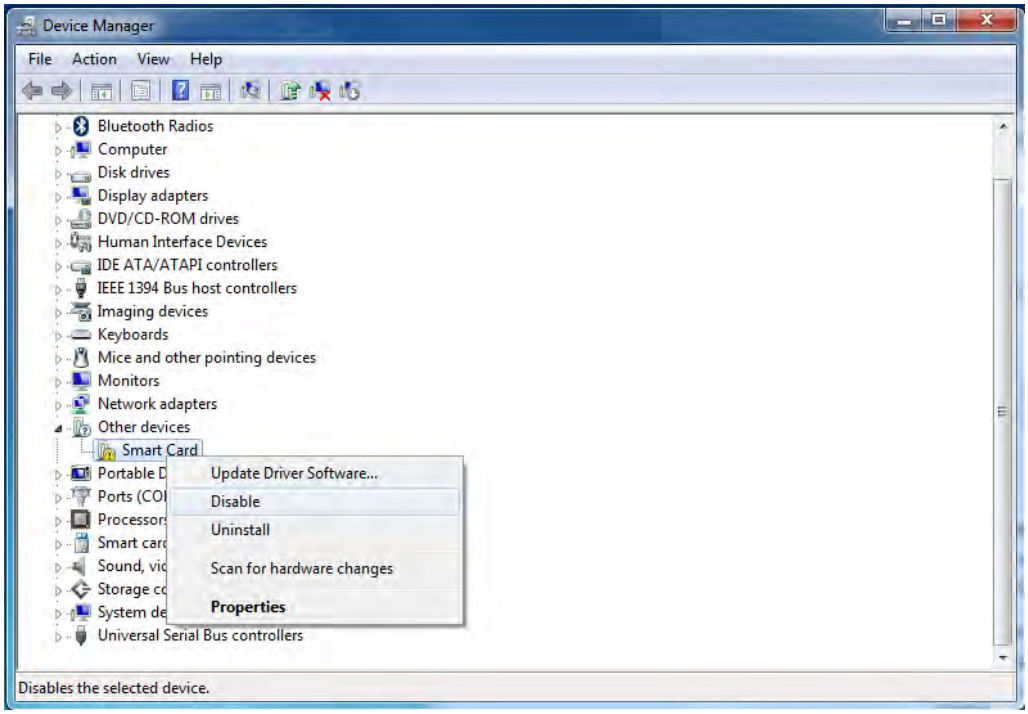


Fig 7. Deactivate Smart Card Interface

2.4 Installing MIFAREdiscover

There are two different versions of MIFAREdiscover; for once the full version can be retrieved from the doc store and the public version, which can be downloaded from the NXP Homepage.

The public MIFAREdiscover supports the functions for MIFARE Classic (see [1]) MIFARE Ultralight (see [13]), General ISO 14443-A (see [8]) protocol handling.

The full MIFAREdiscover supports the functions for MIFARE SAM AV2 (see [18]-[31]) support (X and conventional), MIFARE Plus (see [5]) MIFARE DESFire EV1 (see [4]), MIFARE Classic, MIFARE Ultralight, MIFARE Ultralight C (see [6]) and General ISO14443-A protocol handling.

2.4.1 System Requirements

- Microsoft Windows XP SP2 or higher
- Minimum screen resolution 1024x768 pixels
- Microsoft .NET Framework 3.5 Service Pack 1 or higher [will be installed along with this installer]
- Pegoda
- MIFARE SAM AV2 for X-mode

2.4.2 Installation process

Install Microsoft .NET Framework 3.5 SP1 (or higher if available)

- The Installer "SetupMIFAREdiscover" tries to install the Microsoft .NET Framework 3.5 Service Pack 1 by using a Net-Installer. If you have limited or no network connection to download and install the Microsoft .NET Framework the setup process is terminated and you have to install the Microsoft .NET Framework manually.

- .NET Framework can be found online (see [41])

- Install the "SetupMIFAREdiscover" package:

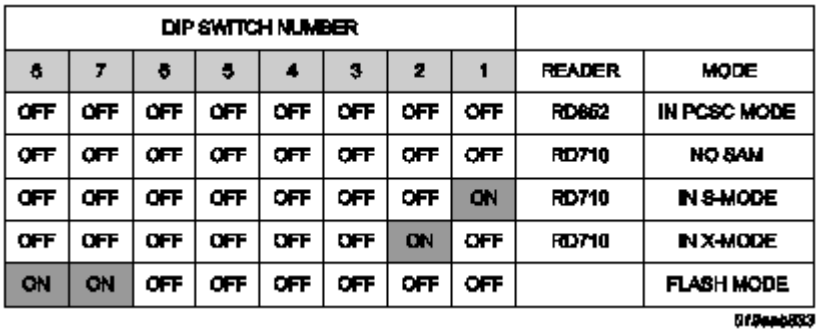
  Install the package and follow the instructions. The whole installation process requires administration rights. After you have successfully installed the program "MIFAREdiscover" and all of its required components you can start "MIFAREdiscover" via the link

  "Start -> All Programs -> NXP Semiconductors -> MIFAREdiscover -> MIFAREdiscover".

- Read “ReleaseNotes.txt” file that you received with the MIFAREdiscover package.

3. Demo mode and DIP switch configuration of the Pegoda

3.1 DIP switch configurations for various Reader modes



DIP SWITCH NUMBER									
8	7	6	5	4	3	2	1	READER	MODE
OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	RD662	IN PCSC MODE
OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	RD710	NO SAM
OFF	OFF	OFF	OFF	OFF	OFF	OFF	ON	RD710	IN S-MODE
OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF	RD710	IN X-MODE
ON	ON	OFF	OFF	OFF	OFF	OFF	OFF		FLASH MODE

Fig 8. Overview of important reader modi

You can find a photo with description on NXP web (see [35]) (table and figure 1)

3.2 Demo mode

To get into demo mode, configure the DIP switch as follows

8	7	6	5	4	3	2	1
OFF	ON	OFF	OFF	OFF	OFF	OFF	OFF

and connect the USB cable. Only power is provided by the USB cable, the reader itself works autonomously without interaction of the PC.

The demo mode is used to showcase some basic functionality of the reader. In this mode, ISO14443-3A activation loop is performed and an acoustic signal is generated based on the detected card and ***SAK-byte,*** respectively.

The following table depicts the default sound coding for different MIFARE cards:

Table 1. Card type according to SAK and number of beep

Card Type	beep
MIFARE 1K (0x08)	1
MIFARE Classic 4K (0x18)	2
MIFARE Ultralight (0x00)	3
MIFARE DESFire	4
MIFARE Plus	5

4. Public Version

All in this section explained steps are applicable to the full version as well.

4.1 Starting MIFAREdiscover

Connect the RD710 Reader with the PC by using the USB cable. Choose the desired DIP switch configuration on the mainboard of the reader (see chapter 3.1) as this tool does not support SAM. The DIP switches should all be set to “OFF”.

Start MIFAREdiscover from the Start menu.

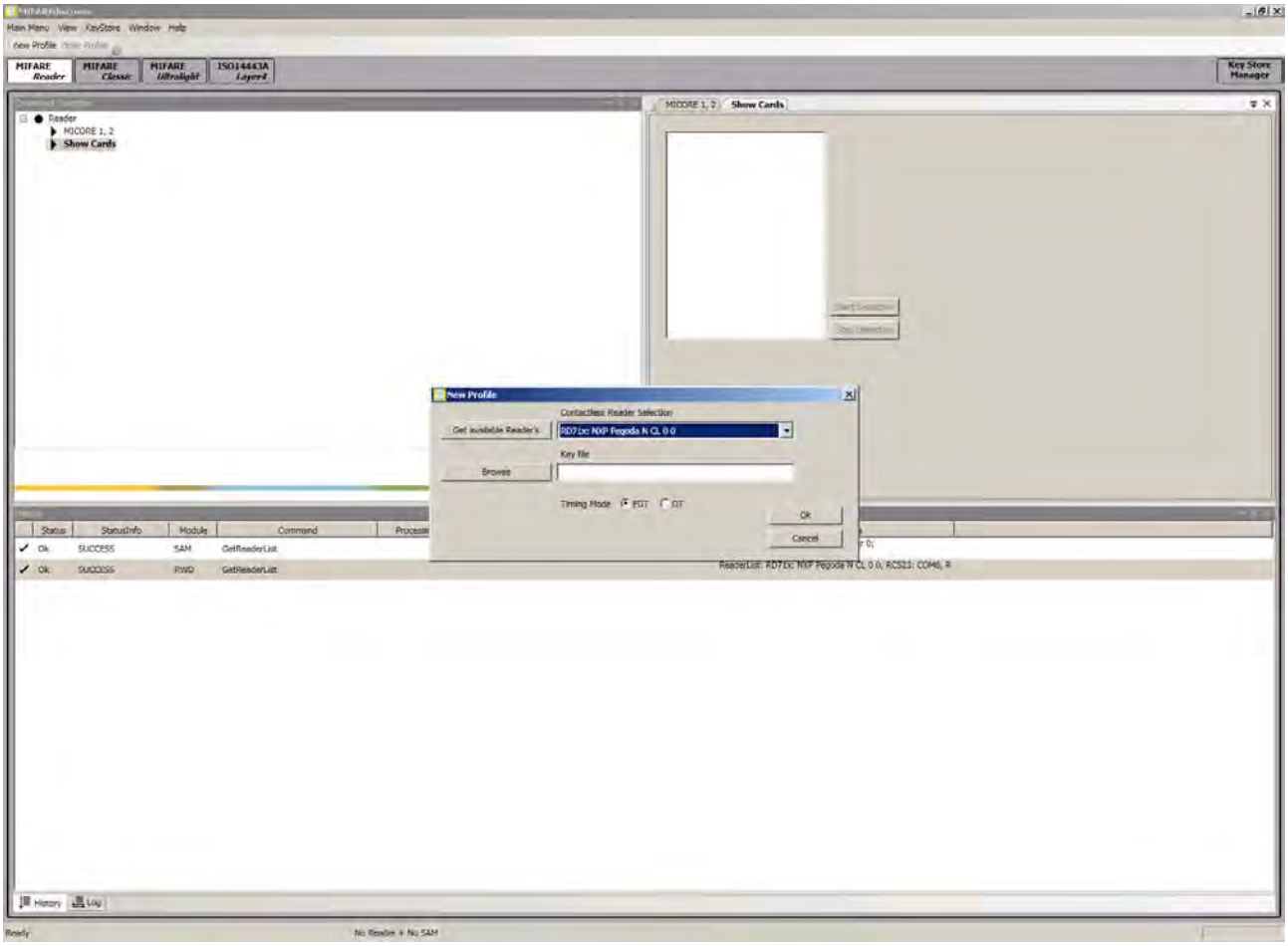


Fig 9. Press the "get available Reader´s" button

Press “Get available Reader’s” for the drop down field “contact- and contactless reader selection”. The available readers will be listed depending on the DIP switch configuration and the chosen reader.

Press “Ok” to open the mainframe of the MIFAREdiscover program for the specific reader configuration.

The following main window will appear. The History frame shows you that the reader has been opened successfully. The configured reader mode can be depicted from the history list as well.

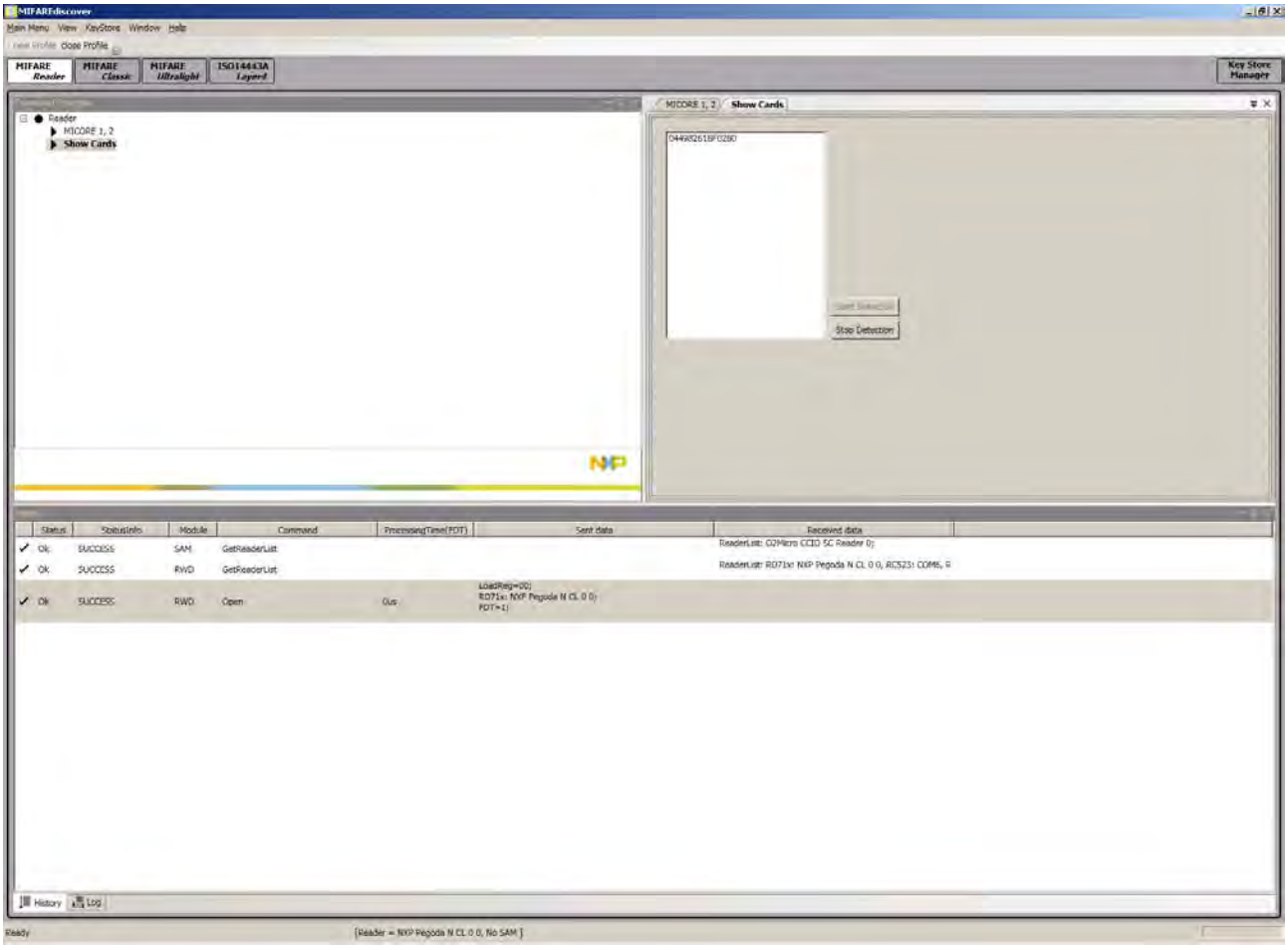


Fig 10. Interface to Reader has been opened successfully

The “command selection window” in the left upper sub window shows you the different possibilities of the current selected reader device. For instance in MIFARE Reader tab is the possibility of running ‘Show cards’ command, in which you can see UID of present cards in RF Field.

4.1.1 Mainframe general overview

The public MIFAREdiscover supports the functions for MIFARE Classic (see [1]), MIFARE Ultralight (see [13]), General ISO 14443-A (see [8]) protocol handling.

Therefore, the user interface is divided into functional blocks which are shown in different tabs.

In every block the history field shows the operations (send data and receive data). This history field can be cleared, or it can be stored in a text file. For an illustration see figure 15.

Note: The sequence of commands as described in ISO/IEC 14443 or in the relevant datasheet must be kept to be able to activate and operate a card. The MIFAREdiscover does not cross check the logical command flow.

5. Examples of some use cases for the public version

5.1 Accessing the MIFARE Classic

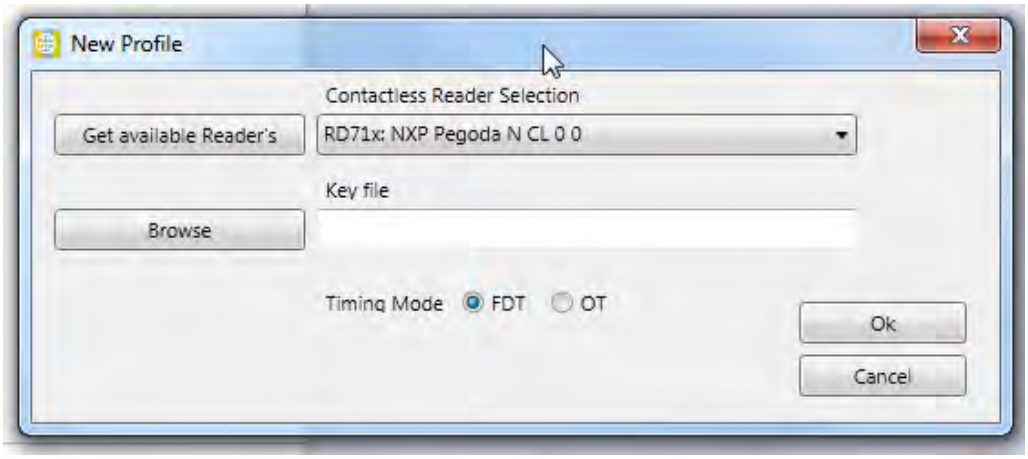


Fig 11. Choose Pegoda

Ensure that the Pegoda reader is set to “Normal Mode”.

Choose the Pegoda as shown in figure 11 and press OK.

Now open the ‘MIFARE Classic’ Tab and select ‘ISO 14443A Layer 3’. On the right side one can see a number of buttons for the activation of the card. The most convenient method is to push the ‘Activate Idle’ button.

Now open the Key Store Manager and select the following settings for the first Key:

Key Type: MIFARE, Entry PartA: FFFFFFFFFFFF, Version: 0

Leave the Key Store Manager and select “Data Processing”.

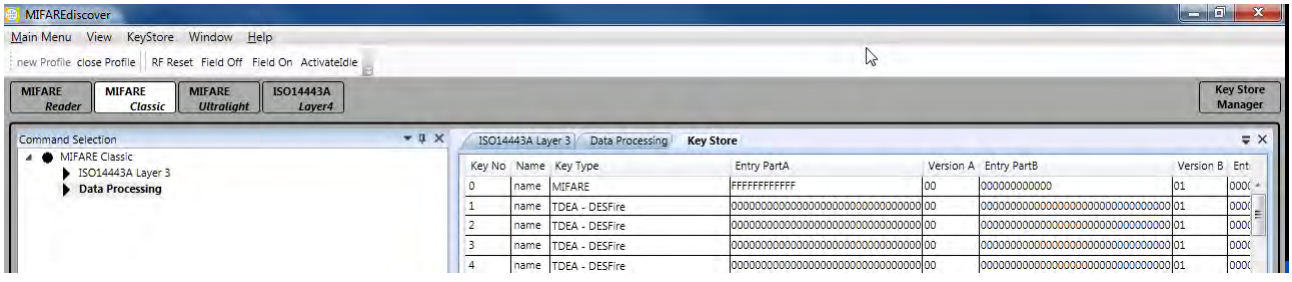


Fig 12. Key Store Manager

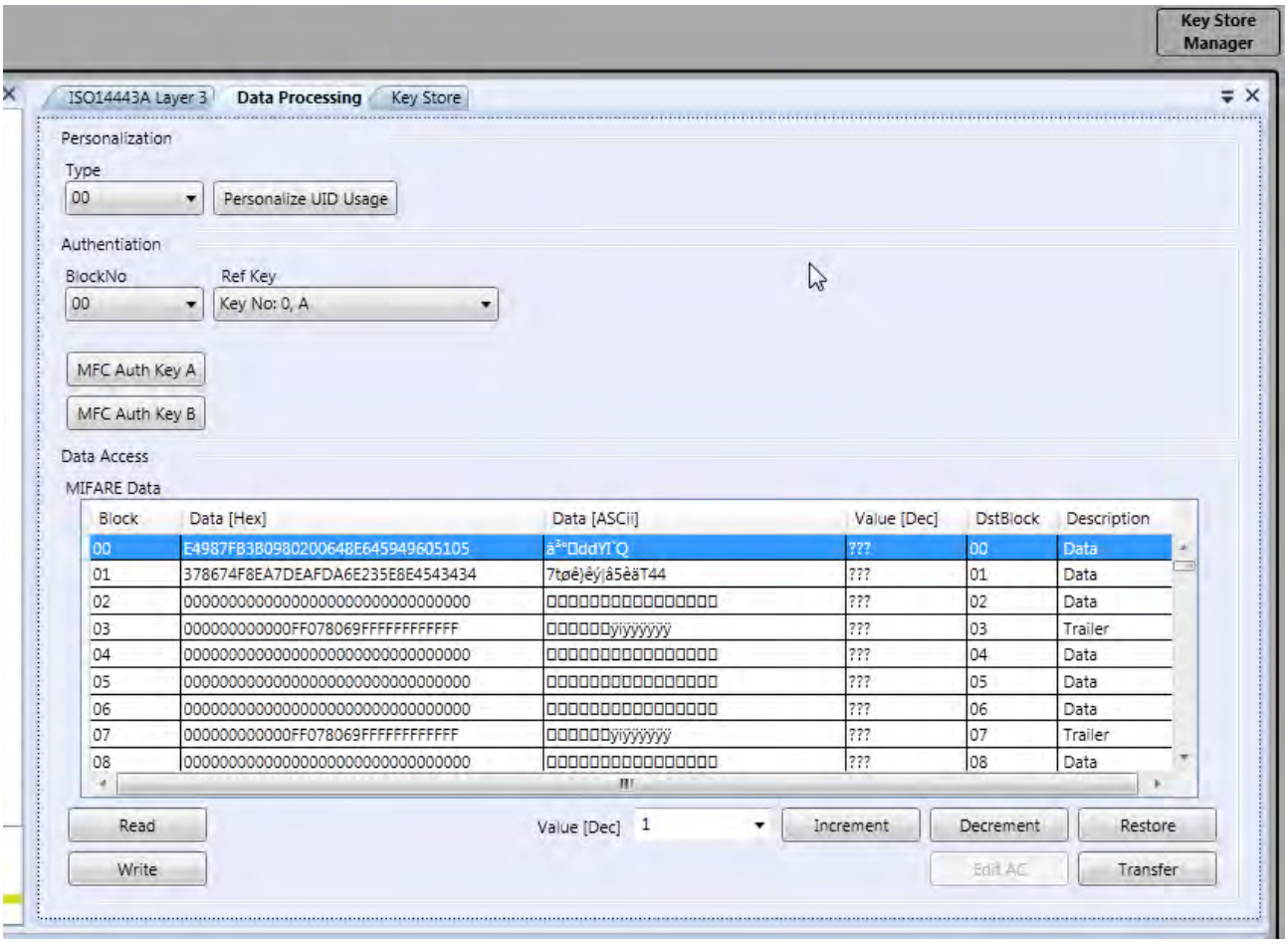


Fig 13. Data Processing

Select BlockNo 00, Ref Key 0, A and click "MFC Auth Key A"

Now you should be able to read and write in Sector 0 (Blocks 0-3).

6. Full Version

6.1 Starting MIFAREdiscover

Connect RD710 Reader to the PC with USB cable. Choose the desired DIP switch configuration on the mainboard of the reader (see figure 8). This can be

- Reader in X-Mode for RD710 with MIFARE SAM inserted in the slot
- Reader in No SAM-Mode
- Reader in S-Mode

In the following descriptions we need to have the DIP switch of the Pegoda set to X-Mode.

Start MIFAREdiscover from the Start menu.

You will be asked to select your reader connected to MIFARE AV2 SAM as shown in Fig.14.

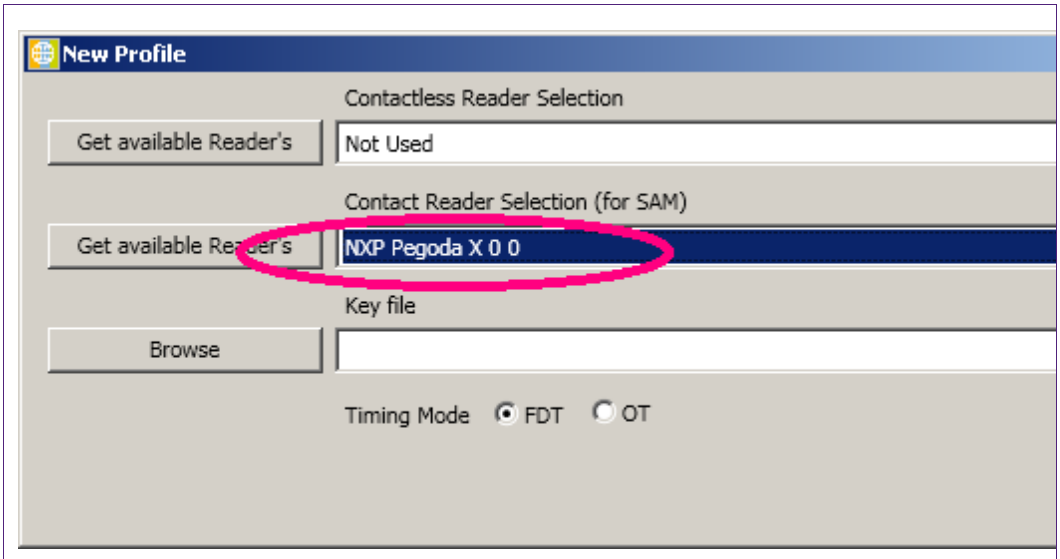


Fig 14. Select reader connected to SAM

Select the reader. Any time the profile can be closed or opened by using close and open profile respectively.

After selection of the reader the key file can be browsed if it is necessary. In the key file, the secret keys can be stored, which may be needed to authenticate MIFARE SAM AV2 with the host or to be changed later. Press OK button to validate the profile. If the MIFARE SAM AV2 is connected properly, the status field of the history window shows “SUCCESS”.

6.2 User Interface Overview

There are 5 areas in the main window, as shown in Fig 15.

1. Menu Bar and Buttons: for reader connection, display settings and help
2. Command Selection Window: list of commands
3. Configuration Window: for detailed configurations of commands
4. History Window: Showing the command execution histories
5. Status Bar: Showing the current command execution status

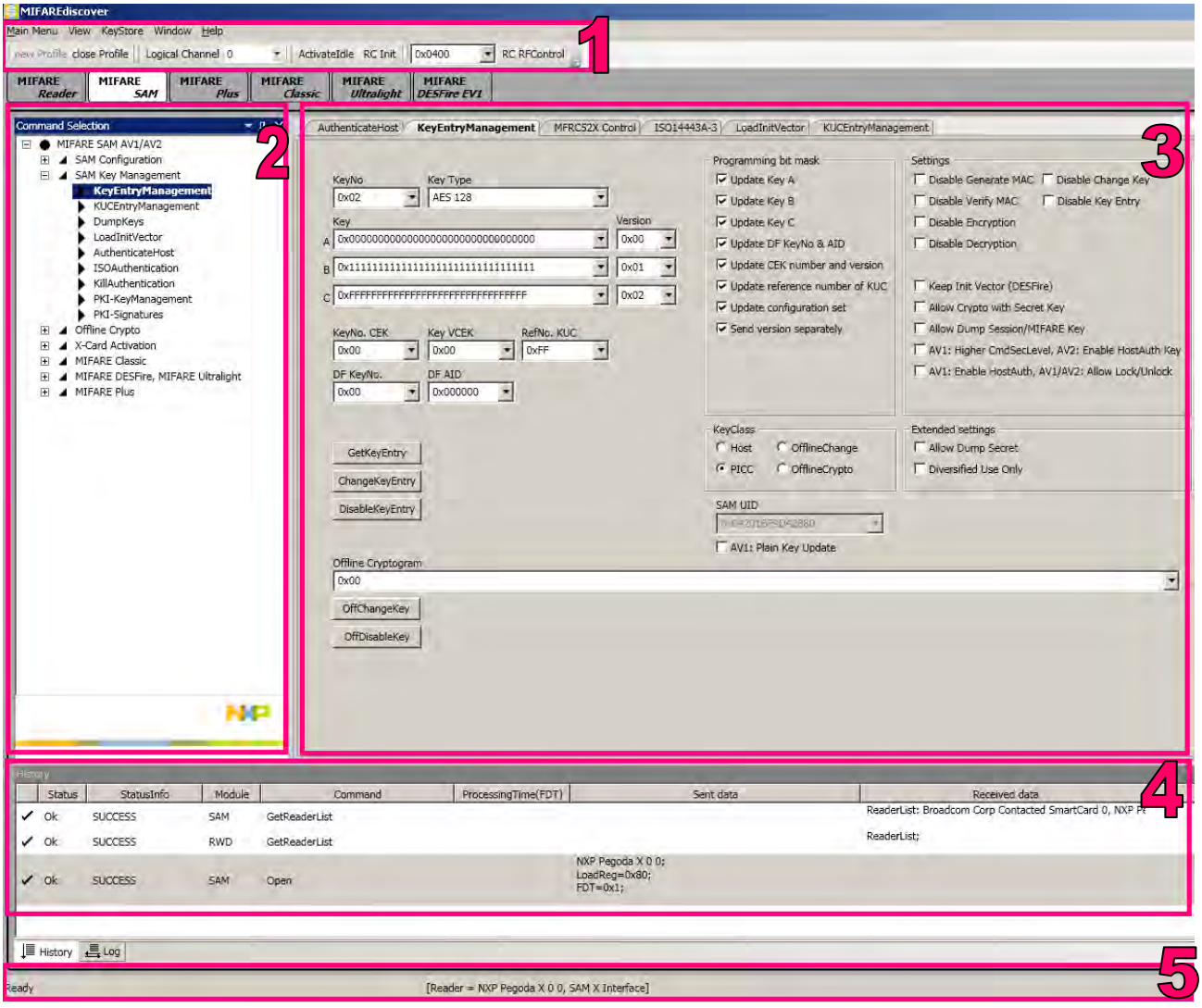


Fig 15. User Interface Overview

7. Examples of some use cases for the full version

In every use case (defined below) we need to have the DIP switch of the Pegoda reader set to **X-Mode**.

Overview

7.1. Checking the connected MIFARE SAM AV2

Here you will get some hardware and software related information about the installed SAM.

7.2. Switch the MIFARE SAM from AV1 to AV2 Mode

AV2 mode is recommended because of security reasons.

7.3. Authenticate host

This step is needed when operating with the SAM.

7.4. Operating the MIFARE DESFire EV1

7.4.1. Using MIFARE SAM AV2 for communication with MIFARE DESFire EV1

This example shows how to perform a basic authentication between SAM and MIFARE DESFire EV1.

7.4.2. Create Application and format MIFARE DESFire

7.4.3. Authenticate Application

7.5. Operating the MIFARE Plus S

7.5.1. Switch MIFARE Plus from Security Level 0 in Security Level 1

Security level 0 is the initial delivery configuration of the PICC. We have to pre-personalize the card to get into security level 1.

7.5.2. Switch MIFARE Plus from Security Level 1 in Security Level 3

Because security level 1 is the compatibility mode to the MIFARE Classic card, we want to use the enhanced security of security level 3.

7.5.3. Read/Write Actions of MIFARE Plus in Security Level 3

A short introduction of how to access blocks with read and write operation in security level 3.

7.1 Checking the connected MIFARE SAM AV2

Ensure that the Pegoda reader is set to “X-Mode”.

Let’s check the connected MIFARE SAM AV2. It can be done using the GetVersion command.

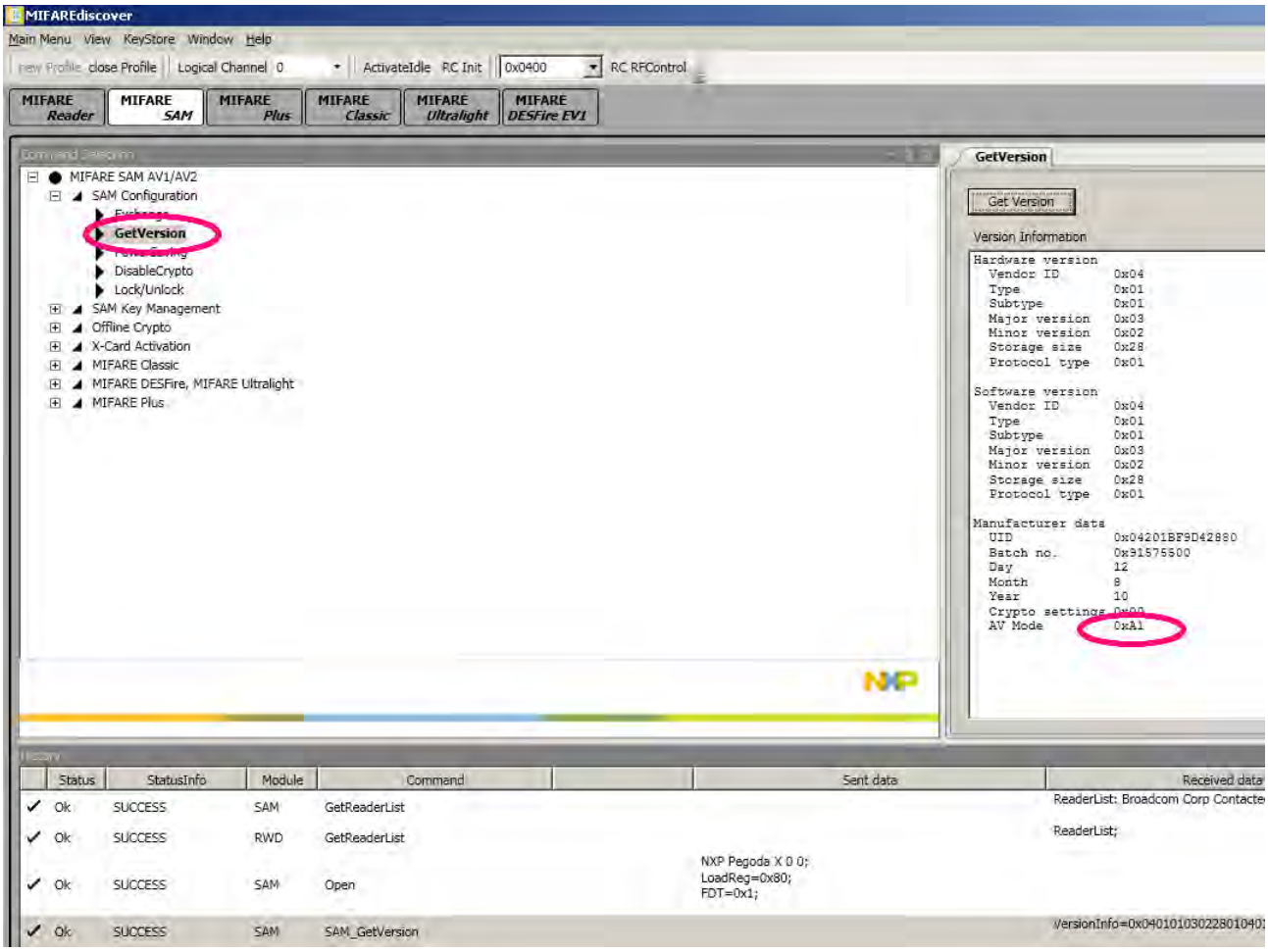


Fig 16. Get Version

The last byte of the “GetVersion” response will be “0xA1” for MIFARE SAM AV1 and will be “0xA2” for MIFARE SAM AV2.

7.2 Switch the MIFARE SAM from AV1 to AV2 Mode

The default MIFARE SAM is delivered from NXP semiconductor in MIFARE SAM AV1 mode. DIP switches should be set to “X-Mode” (see figure 8). For switching to AV2 mode follow the steps.

7.2.1 Authenticate host

Select the “AuthenticateHost” command at the command window. Set the reference key as shown in the following figure. The reference key here used is “Key No: 0, A” for the default setting, where you need to authenticate host using SAM Master key entry and version “00” to change the key.

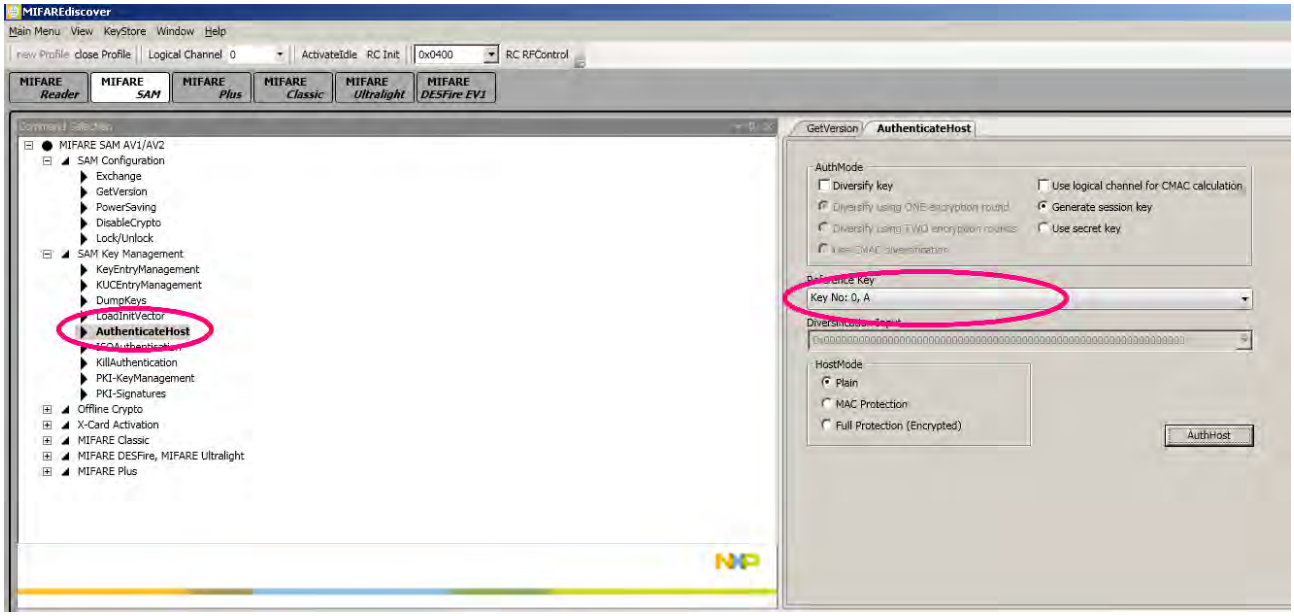


Fig 17. AuthenticateHost Key

7.2.2 Change SAM Master key to AES

SAM master key entry has to be changed to AES type to be able to switch the SAM mode.

Select the “KeyEntryManagement” Command from the command window and set the key “00” and key type “AES 128” (AES 192 is also ok). Set other field as shown in the following figure. We take the new key values and version all 00s, if you want, you can make your own keys as you like.

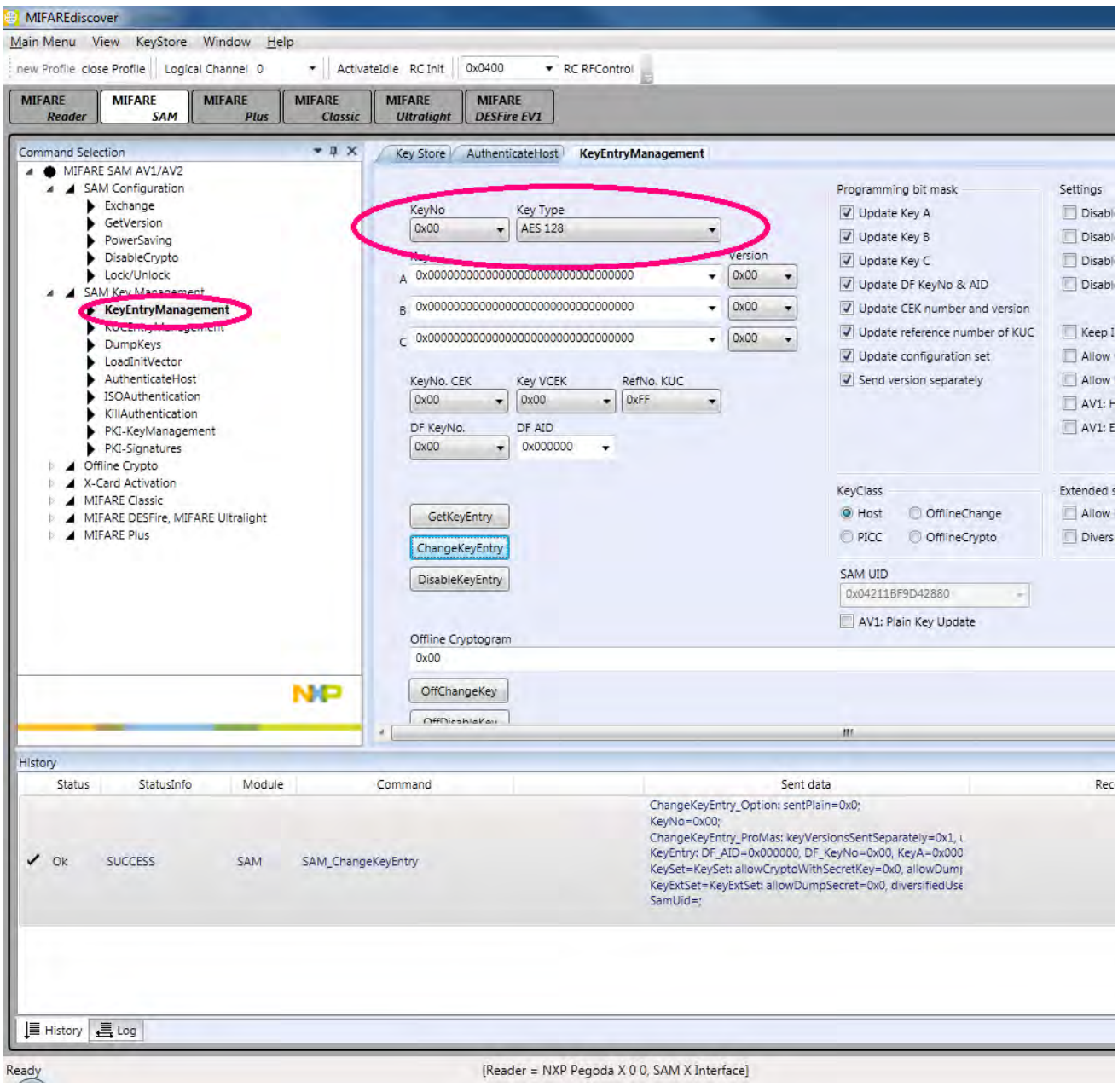


Fig 18. Change SAM master key to AES

If the SAM master key is already AES key type the steps 7.2.1 and 7.2.2 are not required.

Now change the key entry in the key file to have the same key as we have in the MIFARE SAM. Open the key file from menu. Change the key type and key values as we downloaded in previous command.

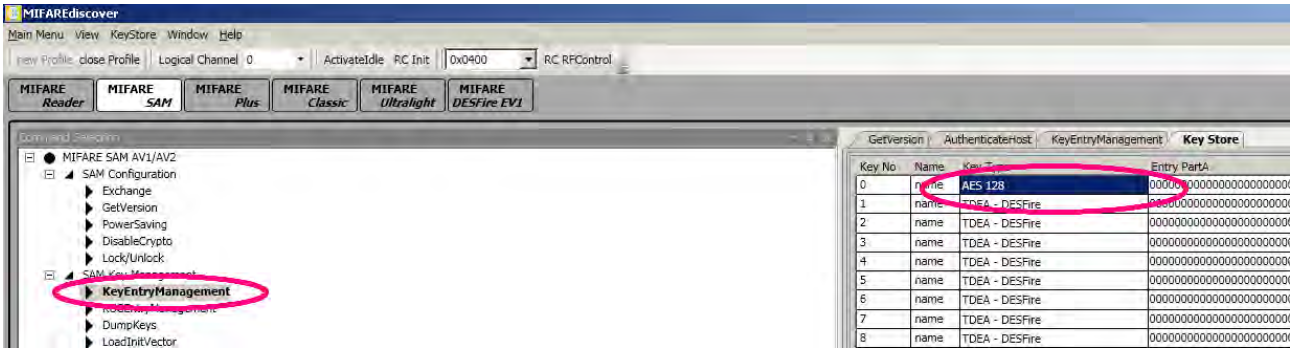


Fig 19. Change Key Type

7.2.3 Lock/Unlock Command

Now the MIFARE SAM AV2 is ready to accept the Activation of AV2 mode command.

Select the “Lock/Unlock” Command from the command window. Set the mode to “Activate AV2 mode” and refer to the key “key no: 0, A” of the key file as shown in the following figure, figure 20.

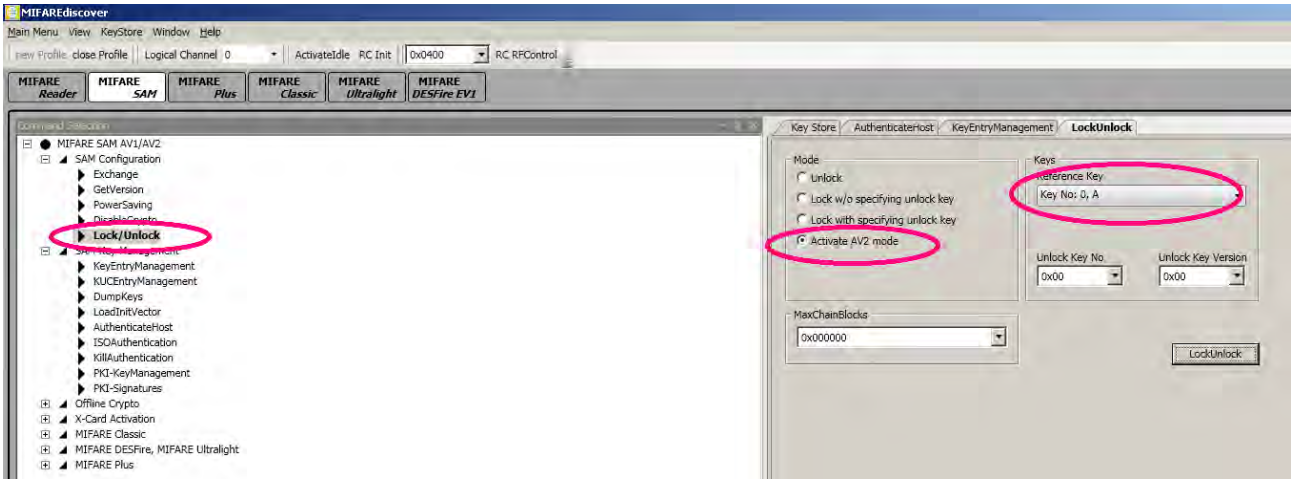


Fig 20. Lock/Unlock command

Now the MIFARE SAM is switched to AV2 mode.

7.3 Authenticate Host

Ensure that the Pegoda reader is set to “X-Mode”.

Select the “AuthenticateHost” command at the command window and open the Key Store Manager.

Fig 21. Key Store Manager

Change the settings:

KeyNo: 0, Key Type: AES 128, Part A: 00000000000000000000, VersionA: 00

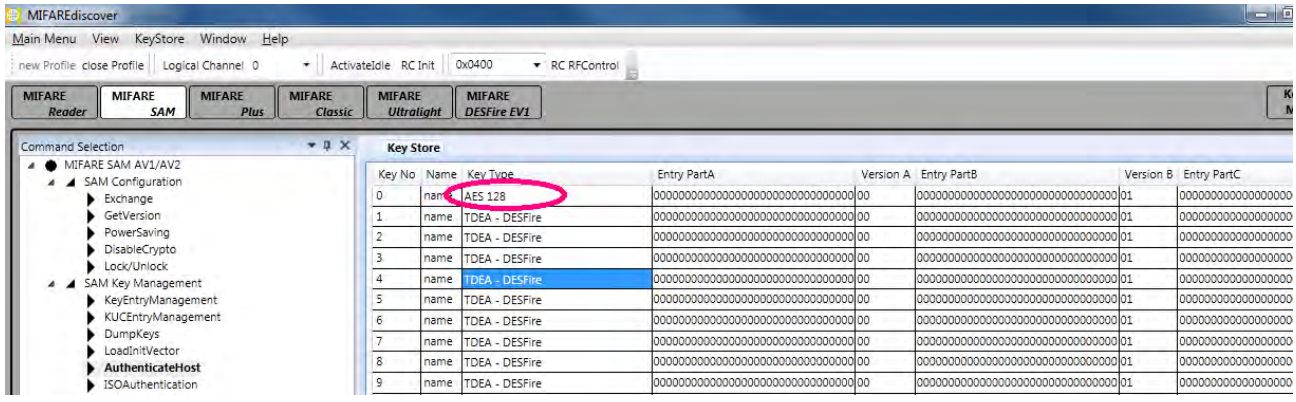


Fig 22. Change Key Type

Leave the Key Store manager and select “AuthenticateHost” again. Be sure to tick “Generate session key” at the AuthMode section and “Plain” at HostMode. Click “AuthHost”.

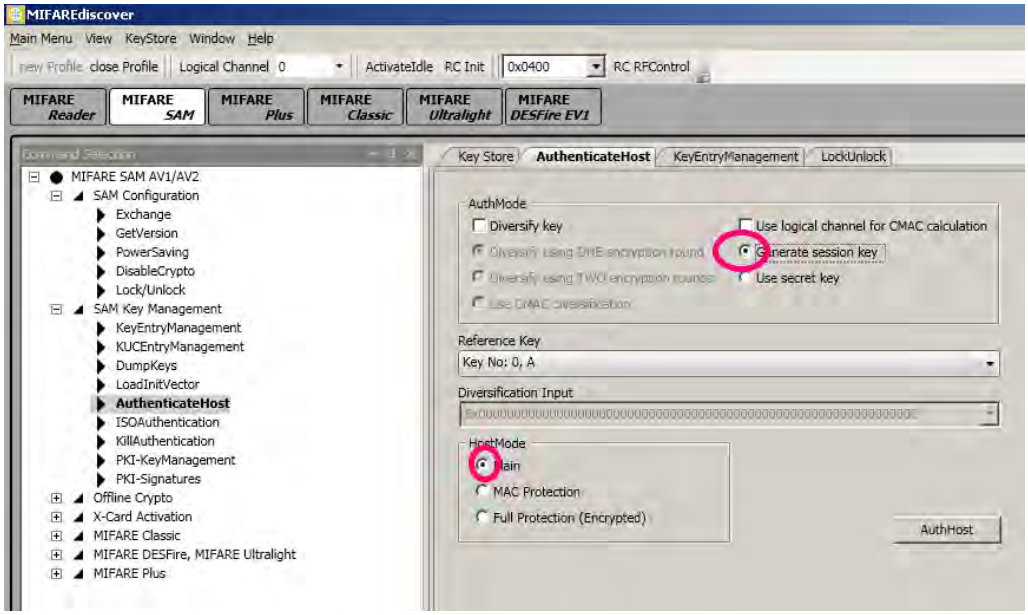


Fig 23. AuthHost

7.4 Operating the MIFARE DESFire EV1

The MIFARE DESFire EV1 answers every command with a status code. These codes can be found in MIFAREdiscover command selection at the Received data column. For example, if you enter an invalid command you will get “AppDataOut=0x1C”.

A list with useful status and error codes is provided:

Table 2. Useful status and error codes

Hex Code	Status
0x00	OPERATION_OK
0x0C	NO_CHANGES
0x0E	OUT_OF_EEPROM_ERROR
0x1C	ILLEGAL_COMMAND_CODE
0x1E	INTEGRITY_ERROR
0x40	NO_SUCH_KEY
0x7E	LENGTH_ERROR
0x9D	PERMISSION_DENIED
0x9E	PARAMETER_ERROR
0xA0	APPLICATION_NOT_FOUND
0xA1	APPL_INTEGRITY_ERROR
0xAE	AUTHENTICATION_ERROR
0xAF	ADDITIONAL_FRAME
0xBE	BOUNDARY_ERROR

Hex Code	Status
0xC1	PICC_INTEGRITY_ERROR
0xCD	PICC_DISABLED_ERROR
0xCE	COUNT_ERROR
0xDE	DUPLICATE_ERROR
0xEE	EEPROM_ERROR
0xF0	FILE_NOT_FOUND
0xF1	FILE_INTEGRITY_ERROR

7.4.1 Using MIFARE SAM AV2 for communication with MIFARE DESFire EV1

At first, the DESFire Key has to be downloaded to the MIFARE SAM if it is not already there. According to the steps done here, downloading a key to the MIFARE SAM requires host authentication as shown in § 7.3.

7.4.1.1 Uploading MIFARE DESFire EV1 AES key to SAM

Let's change the key entry number 1 to PICC DESFire EV1 AES key. To make it simple

Key A = "00000000000000000000000000000000", version 0x00

Key B = "11111111111111111111111111111111", version 0x01

Key C = "22222222222222222222222222222222", version 0x02

The other options are checked as shown in the following figure, figure 24.

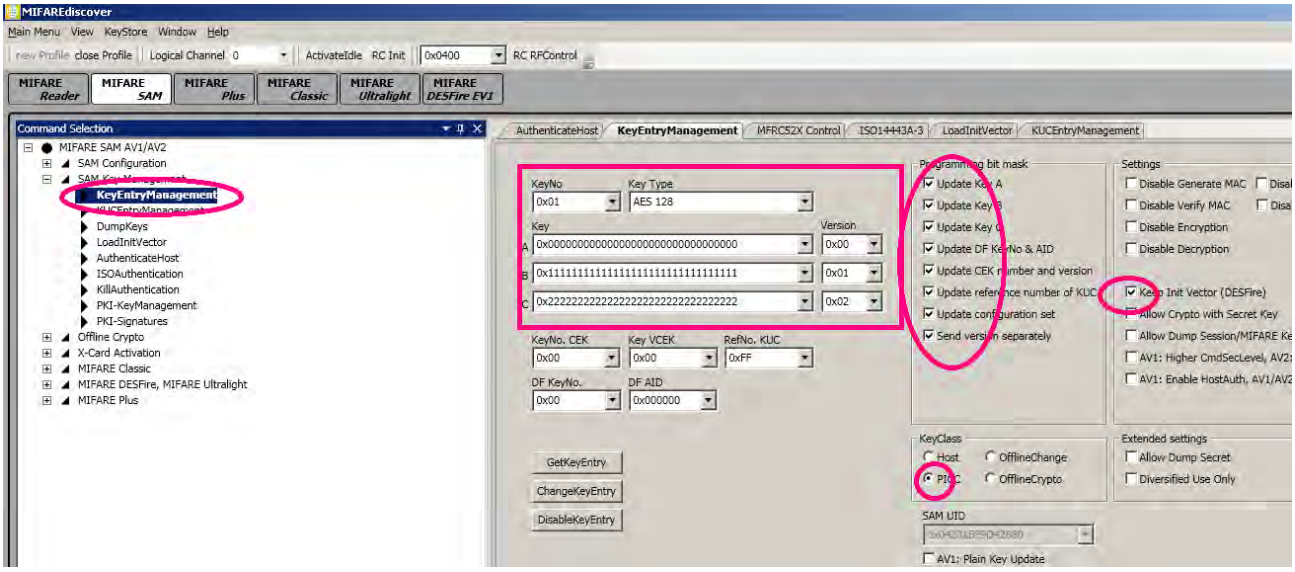


Fig 24. Downloading MIFARE DESFire EV1 AES key to SAM

Do not forget to tick the "keep Init Vector" option for DESFire EV1 AES and standard TDEA keys.

7.4.1.2 Accessing MIFARE DESFire EV1

The steps are as follows:

1. RC Init to initialize the I^2C communication (shown in fig. 25).
2. RC RFControl to turn on the RF field (shown in fig. 25).

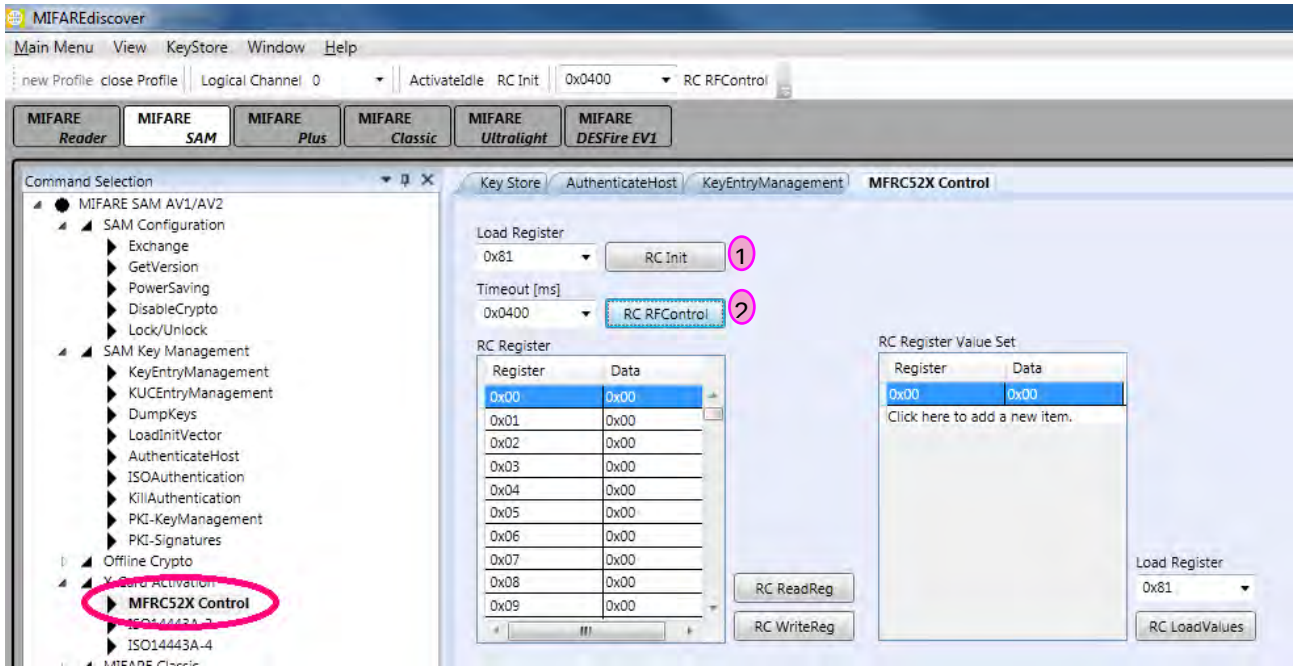


Fig 25. RC Init and RC RF Control

3. ActivateIdle to activate the MIFARE DESFire EV1 card to ISO/IEC14443 part 3 (shown in fig. 26).
4. RATS and PPS command to prepare the MIFARE DESFire EV1 card to ISO/IEC 14443-4 layer (shown in fig. 27).

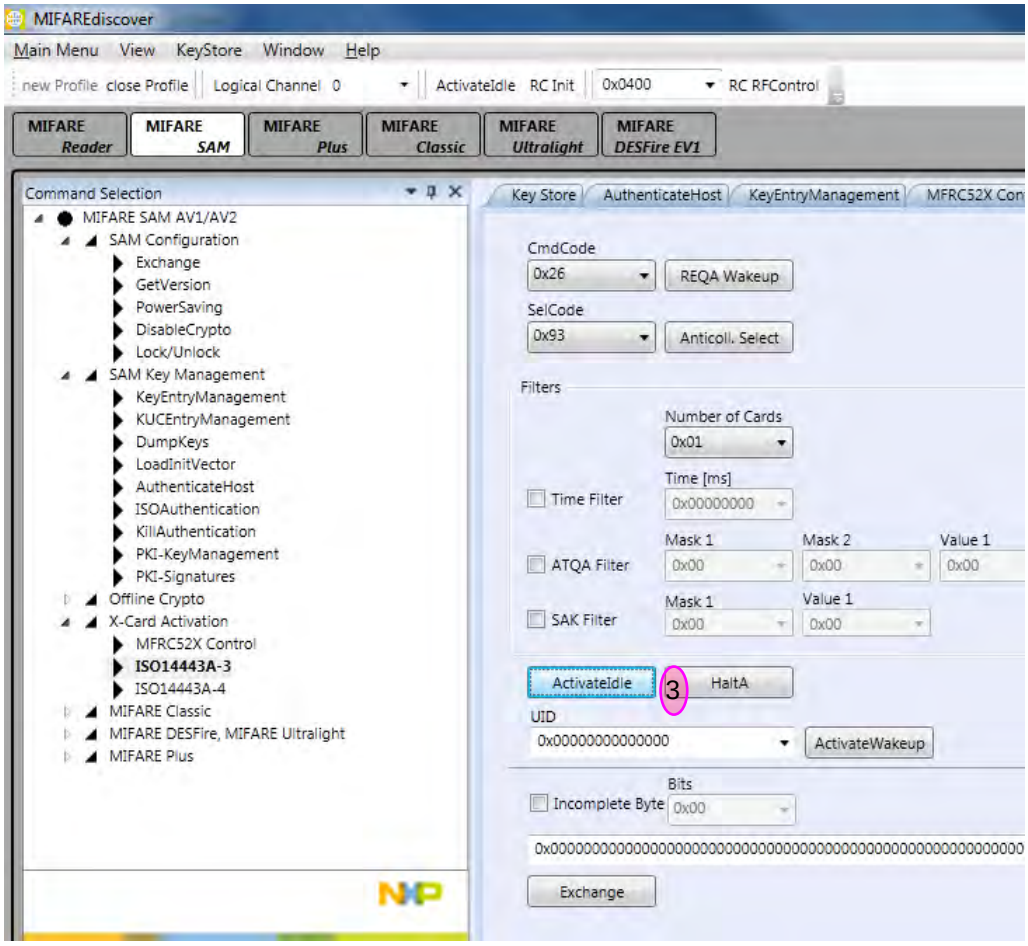


Fig 26. ActivateIdle

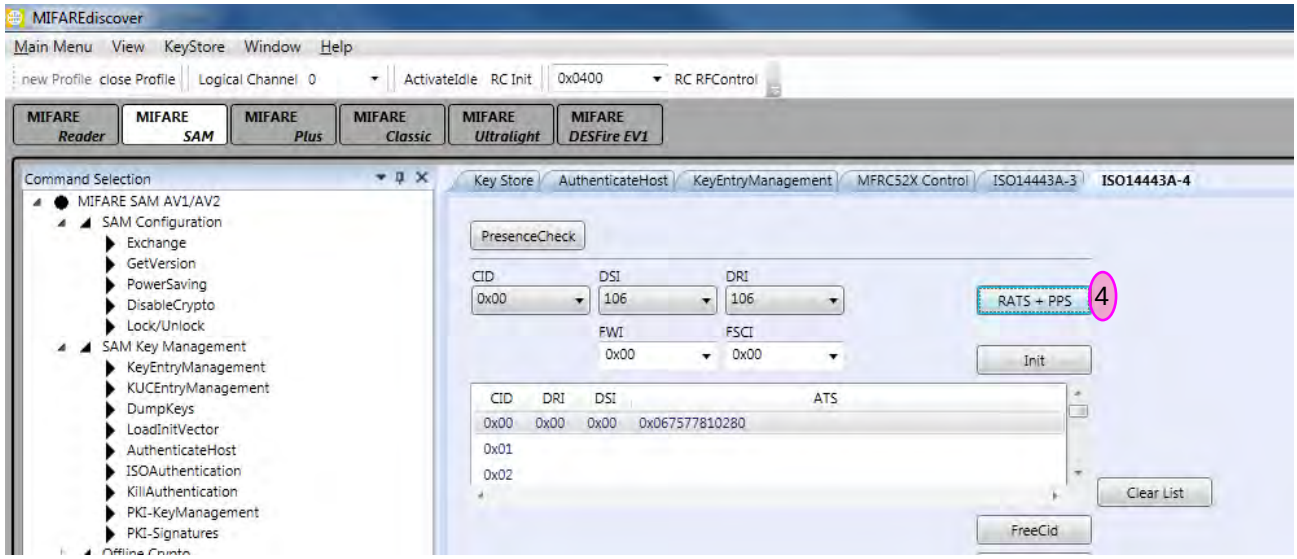


Fig 27. RATS + PPS

Sometimes, when opening RD710 with MIFARE SAM AV2 for the first time, ReqA and ActivateIdle commands fail. As a workaround, please execute the following steps.

Select “SAM Configuration” and “Exchange” at the Command Selection window and insert the following data:

CLA = 0x80, INS = 0x2E, P1 = 0x00, P2 = 0x00, Lc = 0x16

Tick „Use Data“

Data: 2A822BAA15401875194D265927F4283F29110C100100

And press “Exchange”.

Fig 28. Exchange Data

7.4.2 Create Application and format MIFARE DESFire

1. See § 7.3 and do the AuthenticateHost command
2. Open the “KeyEntryManagement” and change the Master Key to KeyNo: 03 if it is still “default”. The Key Type has to be TDEA – DESFire.

   All Keys and Versions are 0, KeyClass is PICC. Be sure to tick everything at Programming bit mask (see figure below).

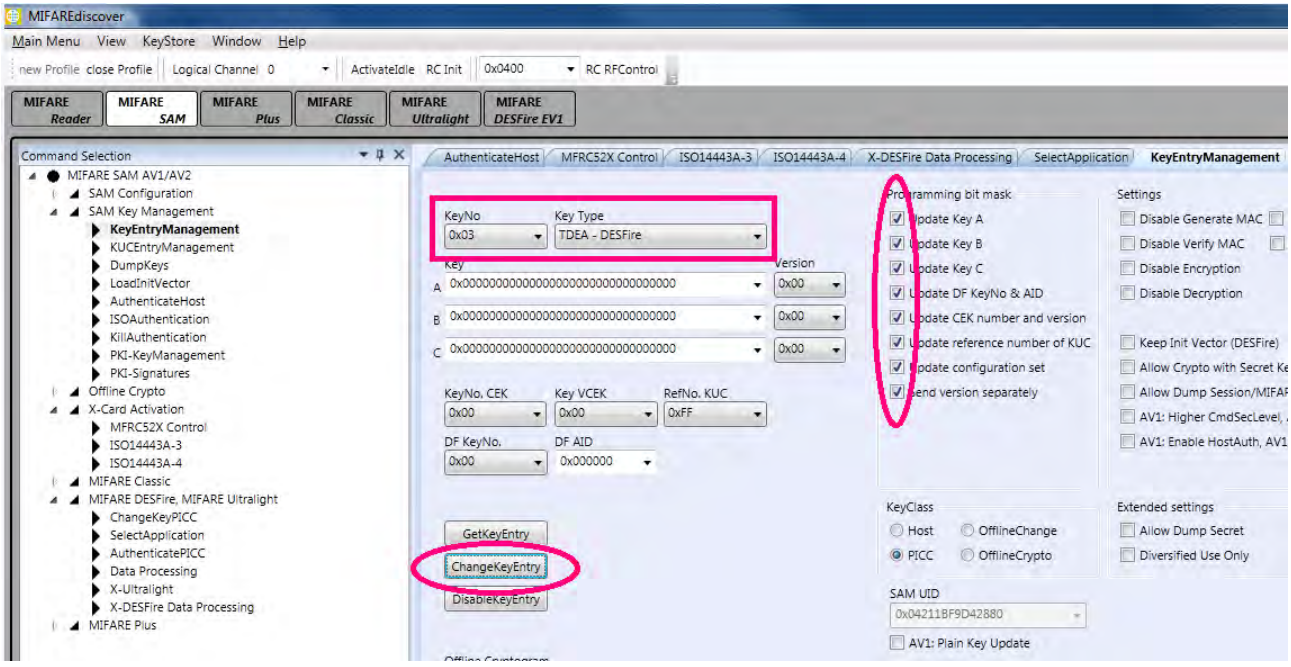


Fig 29. ChangeKeyEntry

3. Click “ChangeKeyEntry”
2. To get access to DESFire, do the steps described in § 7.4.1.2.
3. Then select “X-DESFire Data Processing” at the Command Selection and insert the following data:

   DESFire KeyNo:0

   “Selection by key entry number”

   Mode: Native

   Current Key KeyNo: 0x03, KeyVersion 0x00

4. Click “AuthPICC”.

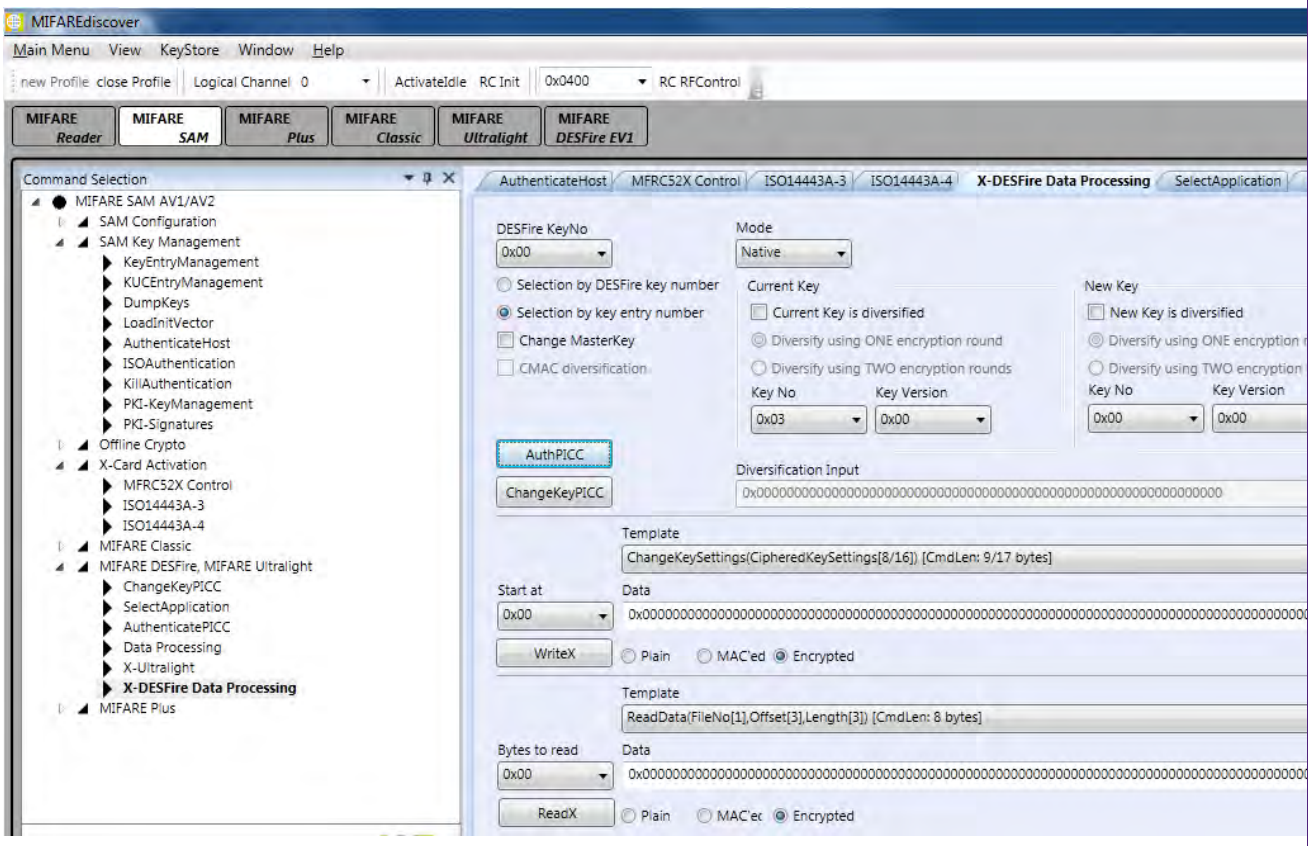


Fig 30. AuthPICC

5. Go to “ISO14443A-4”.
6. To see applications on the card, insert “0x6A” and click “Exchange”.

   To create a new application, insert “0xCaaaaaaa0f8e” and click “Exchange” (The repeated “a” describe the AID (Application ID))

   To format the card, insert “0xfc” and click “Exchange”.

7.4.3 Authenticate Application

1. Do the ApplicationHost command, as described in § 7.3.
2. Open the “KeyEntryManagement” and change the Master Key to “KeyNo: 01” if it is still “default”. The Key Type has to be AES 128.

   All Keys and Versions are 0, KeyClass is PICC. Be sure to tick everything at Programming bit mask and “Keep Init Vector (DESFire)”.
3. Click “ChangeKeyEntry”
4. To get access to DESFire, do the steps described in § 7.4.2.
5. Select Application with “5aaaaaaa” and click “Exchange”.

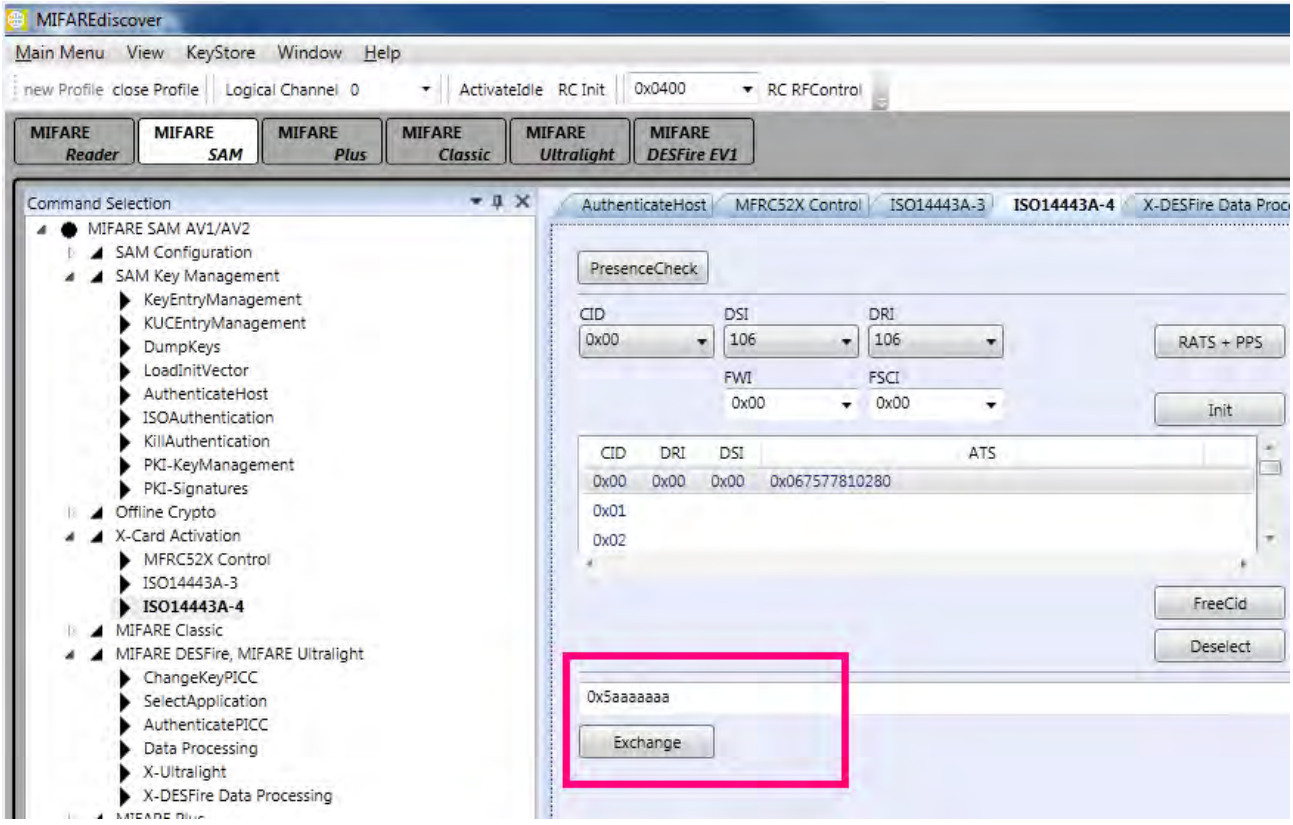


Fig 31. Select Application

6. Select “X-DESFire Data Processing” at the Command Selection
7. Insert the following data:

   DESFire KeyNo: 1

   "Selection by key entry number”

   Mode: Native

Current Key: Key No.: 01, Key Version: 0

8. Click “AuthPICC”.

Now you are registered with your first Application.

7.5 Operating the MIFARE Plus S

To get to MIFARE Plus, you have to set the DIP switches to X-mode (see figure 8) and switch the MIFARE SAM into AV2 mode.

7.5.1 Switch MIFARE Plus from Security Level 0 in Security Level 1

Select “MIFARE Plus” (below the Menu bar) and then “ISO14443A Layer 3” at the command selection. Click “RF Reset” first and “Activate Idle” afterwards.

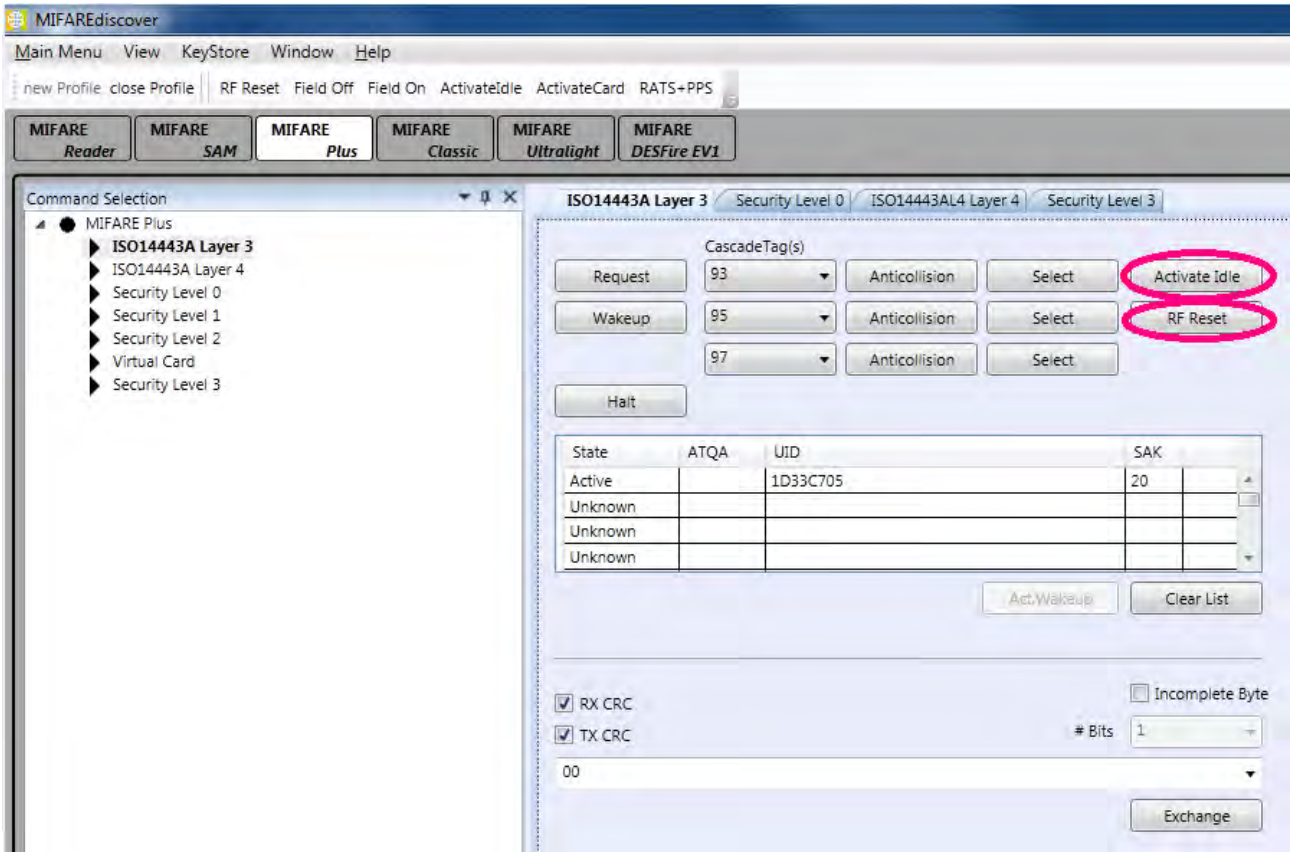


Fig 32. RF Reset and ActivateIdle

Go to “ISO14443A Layer 4” and click “ActivateCard”.

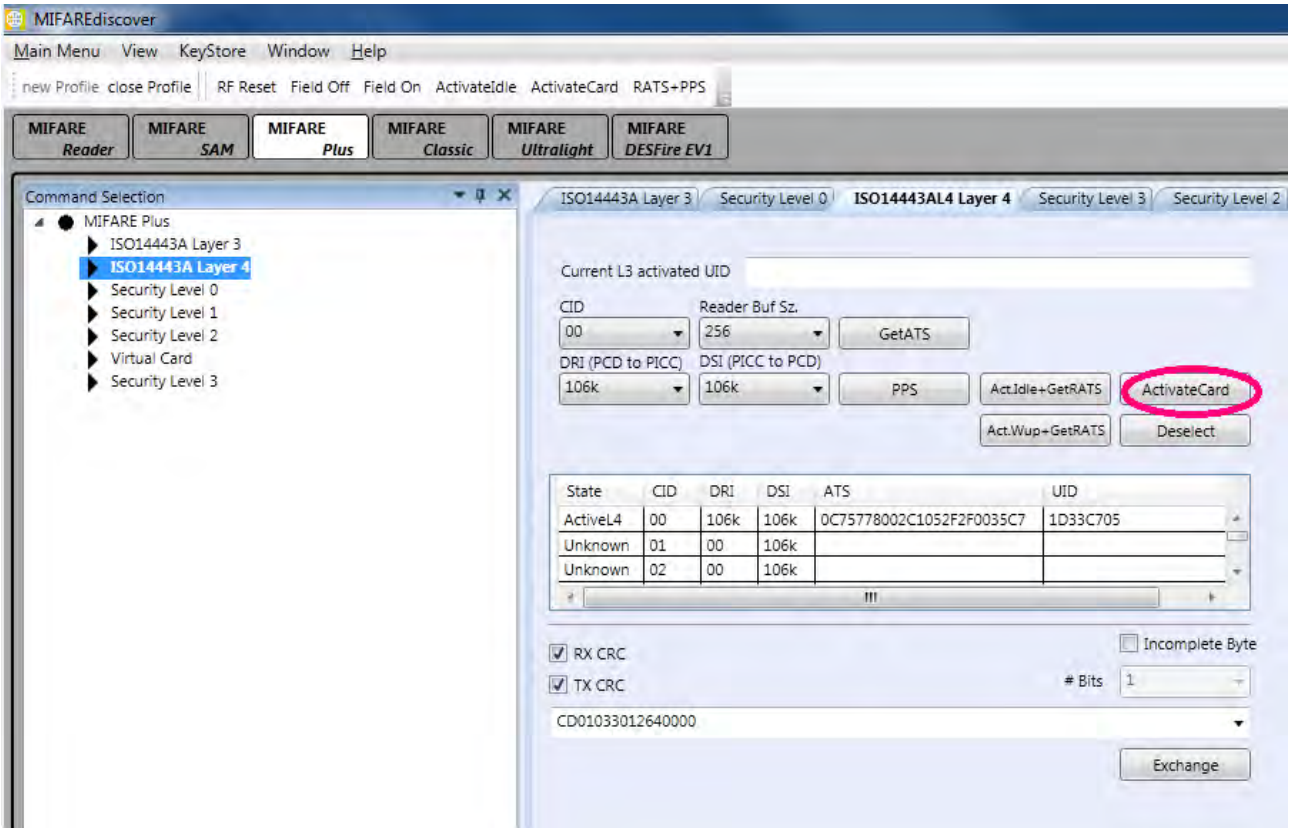


Fig 33. Activate Card

Select “Security Level 0” at the Command selection and insert the data as the next figure shows:

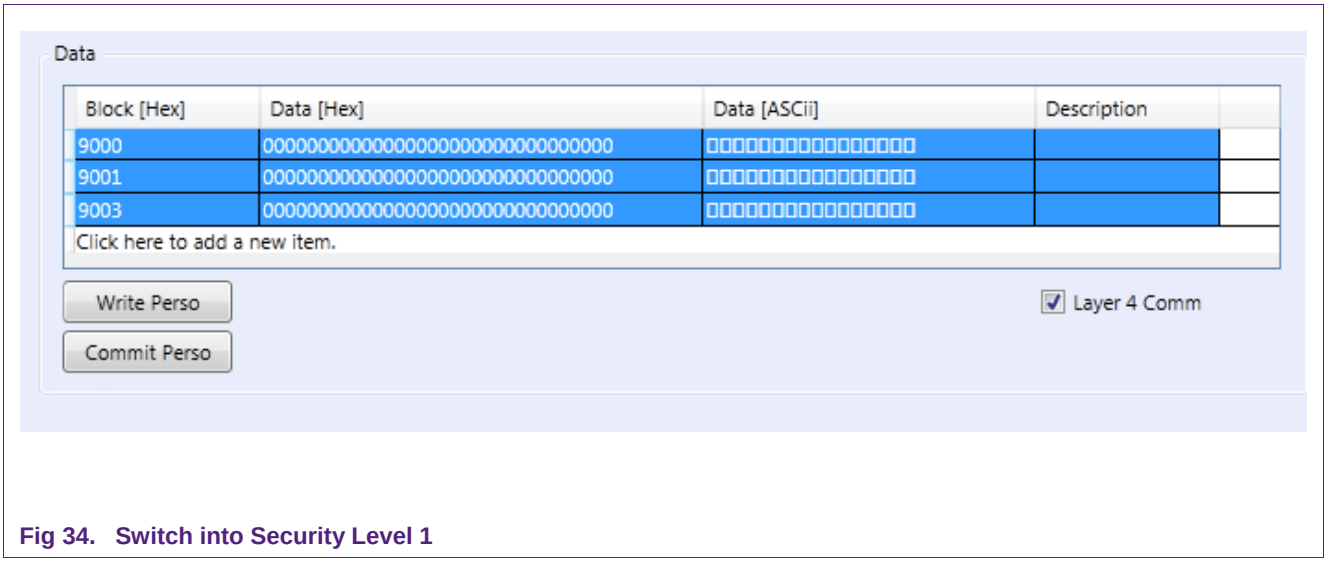


Fig 34. Switch into Security Level 1

Press Ctrl on your keyboard to select all 3 entries. Then click “Write Perso” and afterwards “Commit Perso”.

Then, press the following buttons (Menu bar) in this sequence: "RF Reset", "ActivateIdle", "ActivateCard".
Now, your card is in Security Level 1.

7.5.2 Switch MIFARE Plus from Security Level 1 in Security Level 3

After switching MIFARE Plus into Security Level 1, it is now possible to switch to Security Level 3.

Select “Security Level 1” at the Command selection and change the settings as shown in the following figure. Click “FirstAuth” after you are done.

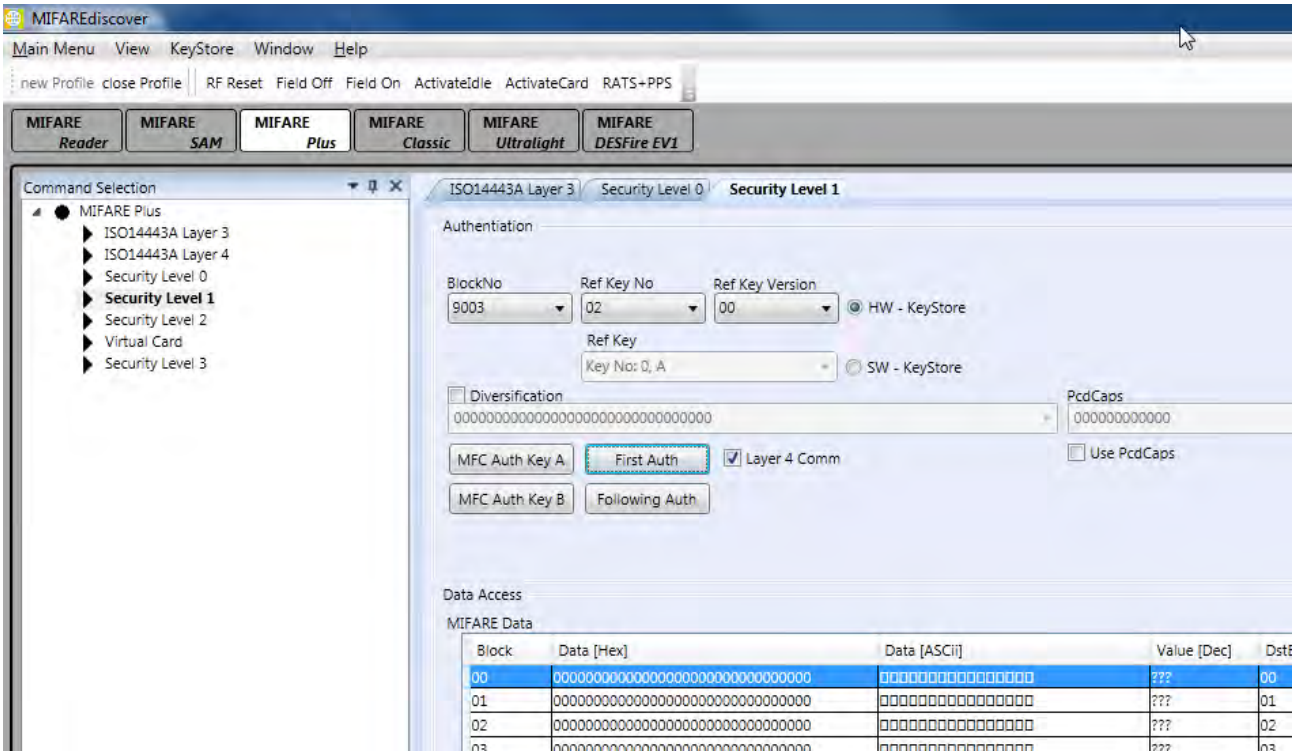


Fig 35. Switch into Security Level 3

Now your card is in Security Level 3.

You can check if the MIFARE Plus is in security level 3 by performing an “ActivateIdle” command. At the section “Received Data” in the command history you will see the SAK of the card afterwards. For example, if you have a 4KB MIFARE Plus card you will get 0x20 if it is in Security Level 3. See the Application note AN10833 for details. (http://www.nxp.com/documents/application_note/AN10833.pdf)

7.5.3 Read/Write Actions of MIFARE Plus in Security Level 3

Select “Security Level 3” at the Command selection.

Because the standard key for the blocks are the same as we inserted at the keystore at position 02, version 02, we can now use these to authenticate at different storage locations.

Change the settings:

Block/KeyNo: 4000

Ref Key No: 02

Ref Key Version: 02

“HW – KeyStore”

And click “FirstAuth”

If you click “Read” you can now read the individual blocks and if you click “Write” you can write beforehand edited blocks. Be sure to tick “MAC on Command” and “MAC on Response” (figure 35).

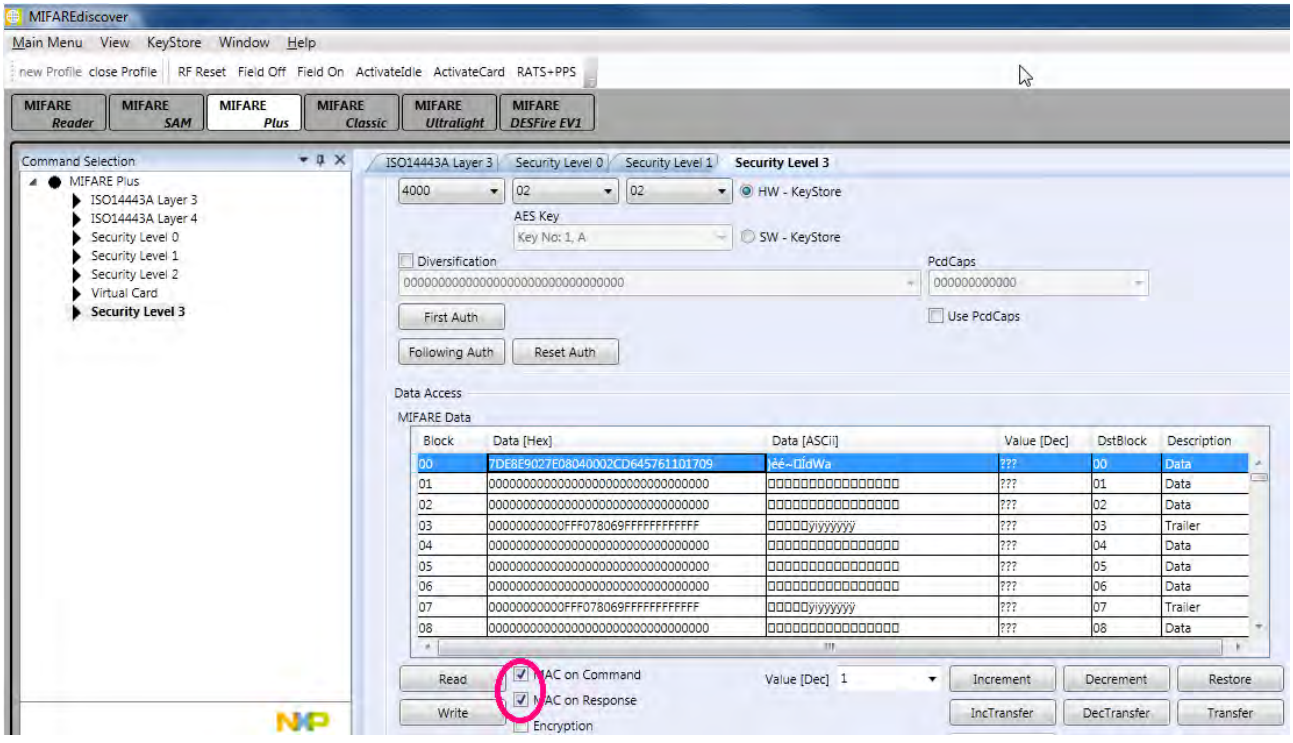


Fig 36. Read/Write Actions

7.6 Using MIFAREdiscover without MIFARE SAM AV2

Ensure that the Pegoda is set to „Normal Mode“.

All described accesses to MIFARE cards are also possible without the MIFARE SAM AV2. If you use a MIFARE SAM AV2 all keys that are needed to get access to MIFARE cards get stored on the SAM.

If no MIFARE SAM AV2 is used the keys have to be inserted at the Key Store Manager of MIFAREdiscover. At positions where a key is needed you have to insert “SW – KeyStore” and the suitable storage location instead of “HWKeyStore”.

8. Firmware download

In order to download firmware to the reader, the DIP switches have to be configured to “flash mode”. After a reset of the Pegoda reader it does response as mass storage device. The user can upgrade the Pegoda firmware by copying it (drag and drop) to the Pegoda mass storage device.

Important note: The file name of the binary file must be renamed to pegoda2x.bin, where x can be any character or letter or none; otherwise the Pegoda will refuse to copy the file and Windows will response with an I/O error (see 36).

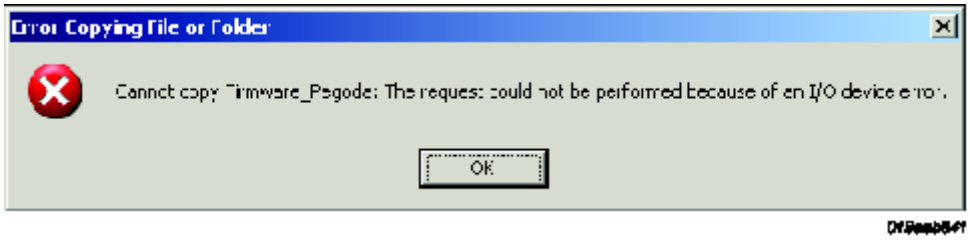


Fig 37. I/O Error when filename is not correct

After successfully copying the file, the Pegoda will start blinking and beeping; windows will response with the following message (see 37).

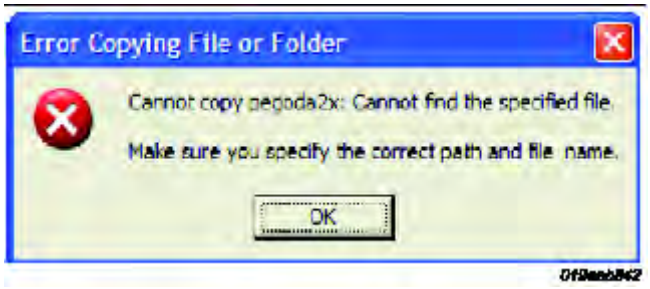


Fig 38. Firmware download successful

Now, the firmware has been updated; reset the device and choose the desired reader mode with the DIP switches.

9. Error Codes

In MIFAREdiscover, user will observe following error and component codes in the History window under Status Info. The definitions of the error codes will help user to understand the cause of error.

Error codes & definitions

Error Codes	Definition
SUCCESS	Returned in case of no error
SUCCESS_CHAINING	Rx chaining is not complete, further action needed
SUCCESS_INCOMPLETE_BYTE	An incomplete byte was received
IO_TIMEOUT	No reply received, e.g. PICC removal
INTEGRITY_ERROR	Wrong CRC or parity detected
COLLISION_ERROR	A collision occurred
BUFFER_OVERFLOW	Attempt to write beyond buffer size
FRAMING_ERROR	Invalid frame format
PROTOCOL_ERROR	Received response violates protocol
AUTH_ERROR	Authentication error
READ_WRITE_ERROR	A Read or Write error occurred in RAM/ROM or Flash
TEMPERATURE_ERROR	The RC sensors signal overheating
RF_ERROR	Error on RF-Interface
INTERFACE_ERROR	An error occurred in RC communication
LENGTH_ERROR	A length error occurred

INTERNAL_ERROR	An internal error occurred
INVALID_DATA_PARAMS	Invalid data parameters supplied (layer id check failed)
INVALID_PARAMETER	Invalid parameter supplied
PARAMETER_OVERFLOW	Reading/Writing a parameter would produce an overflow
UNSUPPORTED_PARAMETER	Parameter not supported
UNSUPPORTED_COMMAND	Command not supported
USE_CONDITION	Condition of use not satisfied
KEY	A key error occurred

Component codes & Identifiers

Component Code	Identifiers
GENERIC	Generic Component Code
BAL	BAL Component Code
HAL	HAL Component Code
PAL_ISO14443P3A	ISO14443-3A PAL-Component Code
PAL_ISO14443P3B	ISO14443-3B PAL-Component Code
PAL_ISO14443P4A	ISO14443-4A PAL-Component Code
PAL_ISO14443P4	ISO14443-4 PAL-Component Code
PAL_MIFARE	MIFARE(R) PAL-Component Code
PAL_FELICA	Open FeliCa PAL-Component Code
PAL_EPCUID	ICode EPC/UID PAL-Component Code
PAL_SLI15693	ICode SLI/ISO15693 PAL-Component Code
PAL_I18000P3M3	ISO18000-3 Mode3 PAL-Component Code
PAL_I18092MPI	ISO18092 passive initiator mode PAL-Component Code
AL_MFC	MIFARE(R) Classic AL-Component Code
AL_MFUL	MIFARE(R) Ultralight AL-Component Code
AL_MFP	MIFARE(R) Plus AL-Component Code
AL_VCA	Virtual Card Architecture AL-Component Code
AL_FELICA	Open FeliCa AL-Component Code
AL_I15693	ISO15693 AL-Component Code
AL_SLI	ICode SLI AL-Component Code
AL_I18000P3M3	ISO18000-3 Mode3 AL-Component Code
AL_MFDF	MIFARE DESFIRE EV1 AL Component Code

AL_P40CMDPRIV	P40 command libraryAL-Component Code
AL_P40CMDPUB	P40 command libraryAL-Component Code
DL_AMP	Amplifier DL-Component Code
DL_THSTRM	Thermostream DL-Component Code
DL_OSCI	Oscilloscope DL-Component Code
DL_RDFPGA	Reader FPGA Box DL-Component Code
DL_MSTAMPOSC	Master Amplifier Oscilloscope DL-Component Code
DL_STEPPERStepper	DL-Component Code
CIDMANAGER	Cid Manager Component Code
CRYPTOSYM	CryptoSym Component Code
KEYSTORE	KeyStore Component Code
TOOLS	Tools Component Code
CRYPTORNG	CryptoRng Component Code
LOG	Log Component Code

10. References

[1] **Datasheet** - MF1S50 MIFARE Classic 1K – Mainstream contactless smart card IC for fast and easy solution development, available on NXP web: http://www.nxp.com/documents/data_sheet/MF1S50YYX.pdf

[2] **Datasheet** – MFR523; Contactless reader IC, BU-ID Doc. No. 1152**[1)], available on NXP Web: http://www.nxp.com/documents/data_sheet/MFRC523.pdf

[3] **Datasheet –** MFEV710, Pegoda EV710, available on NXP Web: http://www.nxp.com/documents/short_data_sheet/MFEV710_SDS.pdf

[4] **Datasheet –** MIFARE DESFire; MF3ICDx21_41_81, MIFARE DESFire EV1 contactless multi-application IC, BU-ID Doc. No. 1340**, available on NXP docu control

[5] **Datasheet –** MIFARE Plus; MF1PLUSx0y1, Mainstream contactless smart card IC for fast and easy solution development, BU-ID Doc. No. 163734, available at NXP docu control http://www.nxp.com/documents/short_data_sheet/MF1PLUSX0Y1_SDS.pdf

[6] **Datasheet –** MIFARE Ultralight C; MF0ICU2, BU-ID Doc. No. 1714**, available on NXP Web: http://www.nxp.com/documents/short_data_sheet/MF0ICU2_SDS.pdf

[7] **Datasheet** – ICODE ILT , smart label IC; will be available on NXP Web

[8] **ISO/IEC Standard** — ISO/IEC14443 Identification cards - Contactless integrated circuit cards - Proximity cards

[9] **Datasheet** - MFRX852 Secure contactless reader solution, available on NXP web, Doc.-Id.: 1815** http://www.nxp.com/documents/short_data_sheet/MFRX852_SDS.pdf

[10] **Datasheet** - MF1ICS50 MIFARE 1K, available on NXP web, Doc.-Id.: 0010** http://www.nxp.com/documents/data_sheet/001056.pdf

[11] **Datasheet** - MF1ICS70 MIFARE 4K, available on NXP web, Doc.-Id.: 0435** http://www.nxp.com/documents/data_sheet/043544.pdf

[12] **Datasheet** - MF0ICU2 MIFARE Ultralight C, available on NXP web, Doc.-Id.: 1714** http://www.nxp.com/documents/short_data_sheet/MF0ICU2_SDS.pdf

[13] **Datasheet** - MF0ICU1 MIFARE Ultralight, available on NXP web, Doc.-Id.: 0286** http://www.nxp.com/documents/data_sheet/MF0ICU1.pdf

[14] **Datasheet** - MF1PLUSx0y1 MIFARE Plus X, available on NXP web, Doc.-Id.: 1635** http://www.nxp.com/documents/data_sheet/MF1PLUSX0Y1_SDS.pdf

[15] **Datasheet** - MF1SPLUSx0y1 MIFARE Plus S, available on NXP web, Doc.-Id.: 1870** http://www.nxp.com/documents/data_sheet/MF1SPLUSX0Y1_SDS.pdf

[16] **Datasheet** - MF3ICD21, MF3ICD41, MF3ICD81 MIFARE DESFire EV1, available on NXP web, Doc.-Id.: 1456** http://www.nxp.com/documents/short_data_sheet/MF3ICDX21_41_81_SDS.pdf

[17] **Datasheet** - P5DF072EV2/T0PD4090 MIFARE SAM AV1, available on NXP web, Doc.-Id.: 1897** http://www.nxp.com/documents/short_data_sheet/P5DF072EV2_T0PD4090_SDS.pdf

MIFARE SAM AV2:

[18] **Datasheet** - P5DF081 System Guidance, Delivery and Operation Manual http://www.nxp.com/documents/short_data_sheet/P5DF081_SDS.pdf

[19] **Software** - MIFARE SAM AV2/ P5DF081 PES Reader Library

[20] **Application note** - MIFARE SAM AV2 Quick Start up Guide

[21] **Application note** - MIFARE SAM AV2 Interface and Architecture

[22] **Application note** - MIFARE SAM AV2 Key Management and Personalization

[23] **Application note** - AN10980 MIFARE SAM AV2 - Host Communication

[24] **Application note** - AN10979 MIFARE SAM AV2 - For MIFARE Plus

[25] **Application note** - AN1826 MIFARE SAM AV2 - For MIFARE DESFire EV1

[26] **Application note** - AN1827 MIFARE SAM AV2 - For MIFARE Ultralight C

[27] **Application note** - AN10978MIFARE SAM AV2 - For MIFARE Classic

[28] **Application note** - AN10977 MIFARE SAM AV2 -X interface

[29] **Application note** - 1830 MIFARE SAM AV2 - General Purpose Cryptography

[30] **Software** - MIFARE discover PC demo software for MIFARE SAM AV2

[31] **Objective Datasheet** - User Manual MIFAREdiscover

Pegoda EV710:

[32] **Application note** - AN10990 Example Projects for NXP RD710/RD852 Readers, available on NXP web: http://www.nxp.com/documents/application_note/AN10990.pdf

[33] **Application note** - AN10993 Pegoda Software Design Guide, available on NXP web: http://www.nxp.com/documents/application_note/AN10993.pdf

[34] **Application note** - AN10992 Quick Startup Guide for RD852 and RD710, available on NXP web: http://www.nxp.com/documents/application_note/AN10992.pdf

[35] **Application note** - AN10991 RM710/RM852 Hardware Design Guide, available on NXP web: http://www.nxp.com/documents/application_note/AN10991.pdf

[36] **Application note** - AN11002 Pegoda Toolchain Information, available on NXP web: http://www.nxp.com/documents/application_note/AN11002.pdf

[37] **Software** - SW MIFARE discover, available on NXP web: http://www.nxp.com/documents/software/214410.zip

[38] **Software** - Pegoda RD710 Driver for 32 and 64 bit, available on NXP web: http://www.nxp.com/documents/software/RD710_Driver_214710.zip

[39] **Software** – MIFAREdiscover Public version, available on NXP web: http://www.nxp.com/pipMFEV710_SDS.html

[40] **Software** – MIFAREdiscover Full version, available on doc store with doc ID.: 1717**

[41] **Software** - .NET Framework, available online: http://www.microsoft.com/downloads/details.aspx?FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7&displaylang=en

[1)] … BU-ID document version number

11. Legal information

11.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

11.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

11.1 Licenses

Purchase of NXP ICs with ISO/IEC 14443 type B functionality

This NXP Semiconductors IC is ISO/IEC 14443 Type B software enabled and is licensed under Innovatron's Contactless Card patents license for ISO/IEC 14443 B.

The license includes the right to use the IC in systems and/or end-user equipment.

RATP/Innovatron Technology

11.2 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

MIFARE — is a trademark of NXP B.V.

DESFire — is a trademark of NXP B.V.

MIFARE Ultralight — is a trademark of NXP B.V.

MIFARE Plus — is a trademark of NXP B.V.

12. Contents

For more information, visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 6 December 2011
198121
Document identifier: AN10992