UG10039

CLRD730 Quick start guide

Rev. 1.1 — 6 November 2023 **User guide**

Document information

Information	Content
Keywords	Reader, CLRD730, MFEV730, User Guide, Quick startup guide, MIFARE SAM AV3, PN7642, Design In Kit MFEV730, Pegoda, NFC Cockpit, RFIDDiscover, Card Test Framework
Abstract	This document is intended for new users to start working with the Design-In Kit. It shows the basic functionality with RFIDDiscover GUI and its support to NFC Cockpit GUI and Card Test Framework GUI.

Revision history

Revision history

Rev	Date	Description
1.1	20231106	Section 1.1 and Section 3.7: Added the Note**:** Do not update the PN7642 Firmware to a version greater than 1.x. or the Pegoda reader will become unusable.
1.0	20230706	Initial version

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

1 Introduction

The purpose of this document is to provide a set of guidelines to aid in the first operation of the CLRD730 reader, simply named Pegoda from now onwards. RFIDDiscover (ver.5.3.0) will be used as a guided user interface to communicate to the Pegoda and between this reader to cards. A complete description of Pegoda is shown in the CLRD730 data sheet (see [1]). Also, other application software is mentioned to support Pegoda (like NFC Cockpit tool [4] and Card Test Framework [6]), including Pegoda operation mode as “mass storage device” (allowing to update the binary application stored in PN7642 built-in M33 flash memory).

The default operation of Pegoda does not require any special installation of USB drivers since by default Windows OS identifies it as a PC/SC reader. For more details, see [1].

In this document, the terms „MIFARE Classic card“ and "MIFARE DESFire card" refer to a MIFARE Classic or a MIFARE DESFire IC-based contactless card.

1.1 Firmware information

The Pegoda is based on the PN7642 NFC controller with the FW version v01.00.

Note: Do not update the PN7642 firmware to a version greater than 1.x. or the Pegoda reader will become unusable.

More info can be found in PN7642 data sheet [5]. All PN7642 product support package can be found on the https://nxp.com/PN7642 landing page. Updated firmware can be downloaded from NXP website: PN7642 Firmware.

1.1.1 Firmware version installed on the reader

You can check the firmware version on Pegoda reader by following instructions described in [1].

1.1.2 Pegoda firmware update

For new projects and implementations, the usage of the latest Pegoda firmware is recommended. Pegoda firmware can be found under Software on https://www.nxp.com/design/:CLRD730.

This is as well the case for projects using the reader both in PC/SC mode as well as in VCOM mode (see [1]).

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

2 Installation

2.1 Required items

In order to use RFIDDiscover GUI, the following items are required:

- MIFARE sample cards, such as MIFARE Classic, MIFARE Plus, MIFARE DESFire, MIFARE Ultralight or NTAG products (NTAG I^2C *plus*, NTAG 21x tags, NTAG 424 DNA) or vicinity products (NTAG 5, ICODE family).
- Pegoda (CLRD730), which are available for ordering from buy direct website:

https://www.nxp.com/webapp/ecommerce.secure_home.framework

- RFIDDiscover version 5.3.0 or later (NDA protected version) available at “Secure Files”, through the My NXP Account portal: https://www.nxp.com/security/login

Also, it is possible to test Pegoda with Card Test Framework GUI, while on PC/SC mode. More information can be found in [6]. More information about Card Test Framework usage can be found in Section 3.5.

Alternatively, it is also possible to test Pegoda with NFC Cockpit GUI; it is suggested then:

- Install NFC Cockpit version version 7.1.0.0 or superior; such GUI can be downloaded from: https://www.nxp.com/webapp/swlicensing/sso/NFC-COCKPIT
- Use MIFARE sample cards as mentioned above.
- Follow instructions in Section 3.6 and Section 3.7, in order to upload Pegoda with suitable binary firmware to test it with the NFC Cockpit tool. Such binary can be found at the NFC Cockpit installation directory.

2.2 Installing USB driver for the reader

As mentioned before, by default CLRD730 works as a PC/SC reader, therefore Windows detects it without the need to manually install its driver. In order to verify the presence of CLRD730, consider that it will be identified by Windows as contactless (multi-ISO/IEC standard reader) as well as contact (ISO/IEC7816 reader) ports.

2.2.1 Steps to detect the Pegoda connected via USB-Type C cable to Windows OS PC/tablet/ laptop

1. Run Windows Device Manager and check presence of USB port as below:

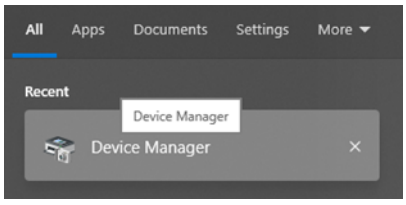


Figure 1. Running Windows Device Manager for USBCCID Reader detection

2. Check in tab smart card readers the presence of any reader:

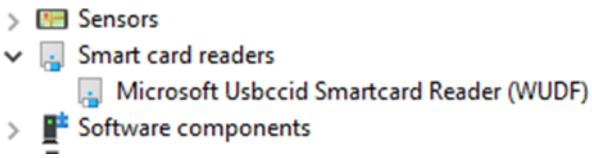


Figure 2. Running Windows Device Manager for USBCCID Reader detection – Smart card reader section

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

As seen above, many laptops often have also a built-in reader which is shown as “Smart card reader”, generally to allow user authentication with an ISO/IEC7816 contact card.

3. Connect Pegoda to your computer: by default, connect USB-Type C cable to port “USB 1” (explanation is given in [1])

Figure 3. Connecting Pegoda using USB-Type C on USB 1 port

4. Check again in the Device Manager after refreshing: you should see two extra smart card readers, named as “Microsoft USBCCID Smartcard Reader (WUDF)”. One of them will be contactless reader, the other one will be ISO/IEC7816 contact reader, both of them built in Pegoda HW.

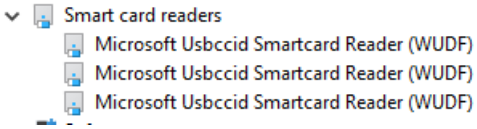


Figure 4. Inspection of new USBCCID Smartcard Readers detected by Windows OS

5. In terms of hardware, the contactless reader antenna is located below the top surface, the contact reader is the slot found in short side area below the NXP logo.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Figure 5. Frontal aspect of Pegoda CLRD730, showing ISO/IEC7816 slot and contactless antenna near NXP logo

2.3 Installing RFIDDiscover

So far, there have been two different versions of RFIDDiscover; the full version, protected by NDA and working with former CLRD710 (former Pegoda version), which can be retrieved by registering and entering in My NXP Account portal. The public version, named as RFIDDiscover Lite (supporting former CLRD710) can be downloaded directly from the NXP homepage without NDA.

RFIDDiscover Lite supports only the functionality of non-secure MIFARE, NTAG, and ICODE product families (see [3]).

On the other hand, RFIDDiscover full version (released only under NDA) supports also the functionalities of strong authentication products (like MIFARE DESFire, MIFARE Plus at security level 3, MIFARE Ultralight AES, NTAG 424 DNA, NTAG 22x DNA, and ICODE DNA).

RFIDDiscover 5.3.1 and above currently supports CLRD730 and it is available through My NXP Account portal, at the tab “Secure Files” (see [2]).

Customers that would like to qualify to download confidential documents and software available in My NXP Account, should follow instructions available on these links:

https://www.nxp.com/docs/en/user-guide/nxp-secure-access-rights-registration.pdf

https://www.nxp.com/support/support/secure-access-rights-overview:SEC-ACCESS

2.3.1 System requirements

- Microsoft Windows 10 or higher
- Pegoda (CLRD730) connected via USB-Type C
- Optional MIFARE SAM AV3 sample (in ID1 card format) to test ISO/IEC7816 interface.
- MIFARE product-based card samples, which may be requested to your local NXP Sales representative.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

2.3.2 Installation process

1. Download the PDF containing RFIDDiscover.exe package encapsulated in it
2. Select “attached file” logo and highlight zip file, which has been uploaded in PDF with a file extension different than “*.zip” (this is necessary to avoid email spam/junk filtering actions)
3. Save encapsulated file, by changing extension to zip
4. unzip it in any temporary directory
5. Double click *.exe to install the "RFIDDiscover" package

Install the package and follow the instructions. The whole installation process requires administration rights. After you have successfully installed the program "RFIDDiscover" and all of its required components, you can start "RFIDDiscover" via respective shortcut link created in Windows desktop.

Figure 6. RFIDDiscover shortcut link after installation under Windows OS

Alternatively you can browse this path to get to RFIDDiscover.exe.

C:\Program Files (x86)\NXP Semiconductors\RFIDDiscover\V5.3.1.0\Bin\RFIDDiscover.exe

Read the “ReleaseNotes.txt” file that you have received with the RFIDDiscover package.

As soon as you double click previously mentioned desktop link, you see the following message:

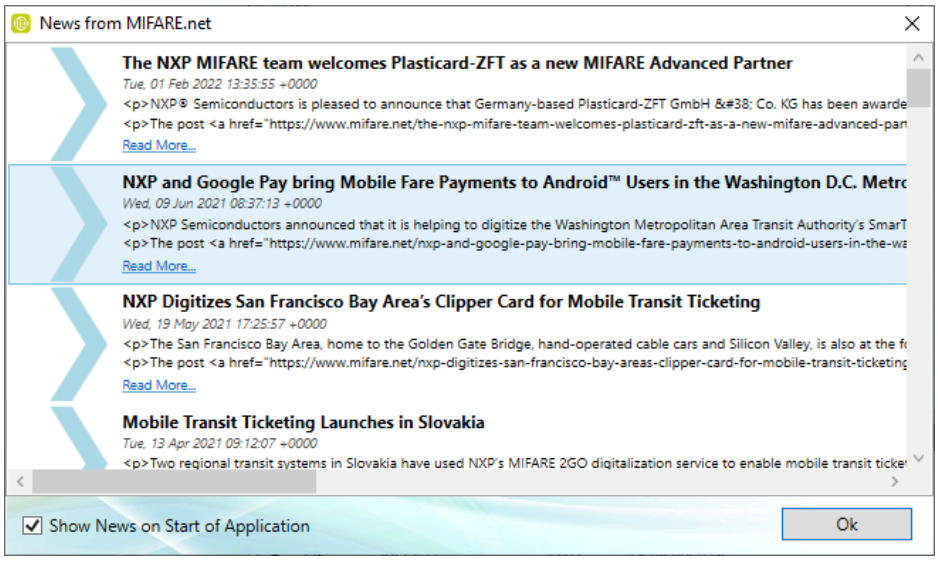


Figure 7. News from MIFARE.net at first run of RFIDDiscover

This News snapshot keeps the audience aware about important NXP press releases and SW updates. You can remove it from every RFIDDiscover start, by unticking bottom left corner square.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

3 Manual insertion of the Pegoda name in reader list of RFIDDiscover

3.1 First run of RFIDDiscover, CLRD730 in PC/SC mode

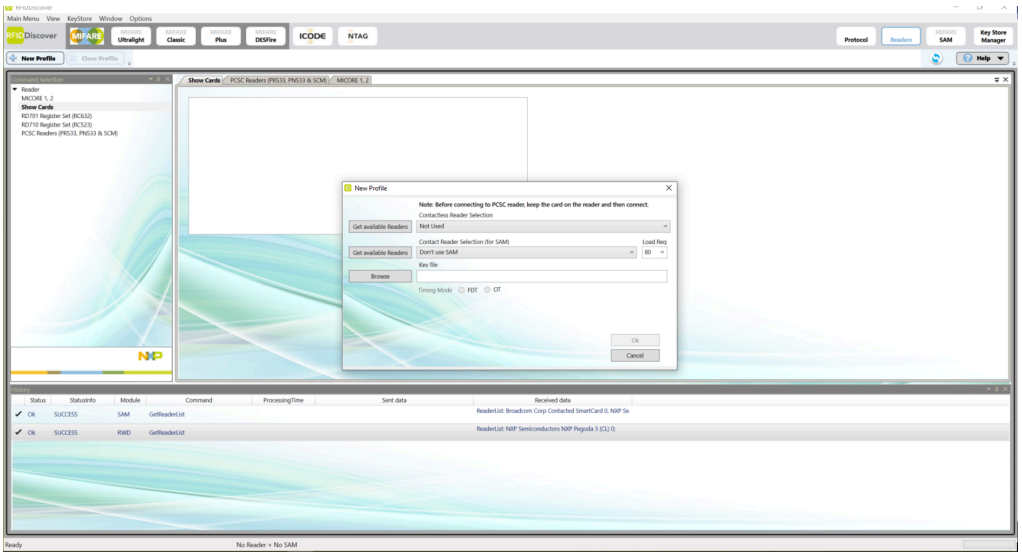


Figure 8. Aspect of RFIDDiscover at first run

The first time you run RFIDDiscover, GUI prompts for presence of smart card readers attached to your laptop/ PC.

3.2 Getting available readers

Since the Pegoda is by default delivered in PC/SC mode, it is possible to interact only with ISO/IEC-14443-4 cards (like MIFARE DESFire family, MIFARE Plus in SL3, NTAG DNA family tags (NTAG 424 DNA, NTAG 223 DNA, NTAG 224 DNA), JCOP etc. cards by default. Therefore it is necessary to place contactless card on top of Pegoda antenna before opening a “New (reader) Profile” (top left button in RFIDDiscover GUI). After a card is placed on Pegoda antenna, you will see “COMM” LED turned from on to green on the readers top side. In the default mode, ISO/IEC 14443-4A activation loop is performed each time one card is detected.

You can recognize that Pegoda is in PS/SC mode by looking to POWER LED (constantly red colored), MODE LED (white colored) and COMM LED, which is off, when no card is in the field, and green colored when there is an ISO/IEC14443-4 card in the field (see below):

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Figure 9. Aspect of Pegoda leds when in default (PS/SC) mode. Presence of card both in contactless interface as well as in contact interface turns COMM LED from off to colored green

This functionality can be extended to other cards (ISO/IEC-14443-3, ISO15693 and other non-ISO14443-4 contactless products) by changing operation mode (see Section 3.4).

Pay attention to the dialog area, named "History" (choice by default). The GUI gets automatic response from “Get available readers” and shows the following:

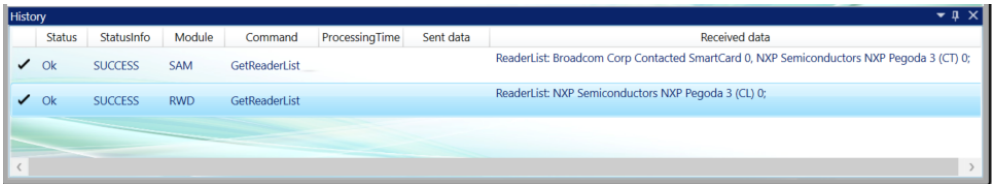


Figure 10. History dialogue window and detection of two smart card readers (CL and CT).

Notice that on first “History” line there are two silicon vendor names, including NXP. Main reason is that this windows laptop also contains an ISO/IEC7816 slot allowing use of contact smartcards.

On the second “History” line, you see the text description “ReaderList: NXP Semiconductors NXP Pegoda 3 (CL) 0;” (bottom right). This means that contactless reader has been detected (it refers to PN7642 open NFC controller, operating in contactless active interface).

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

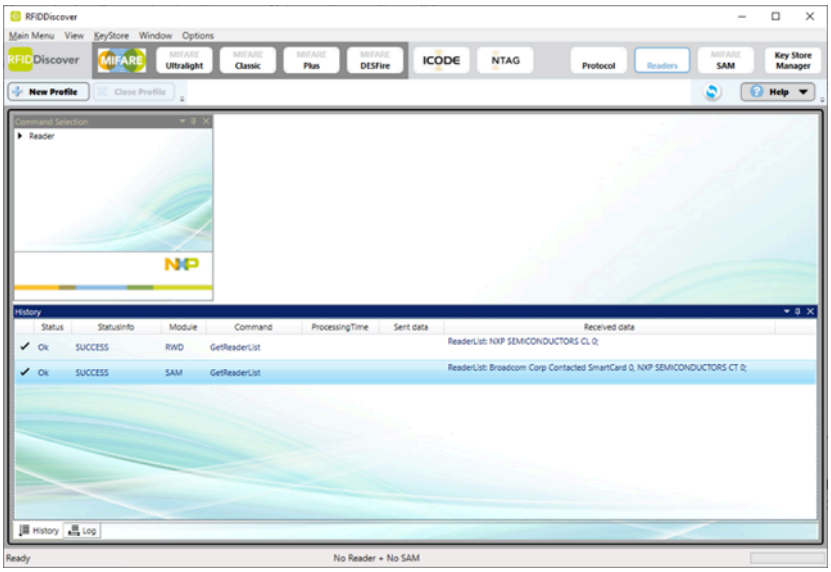
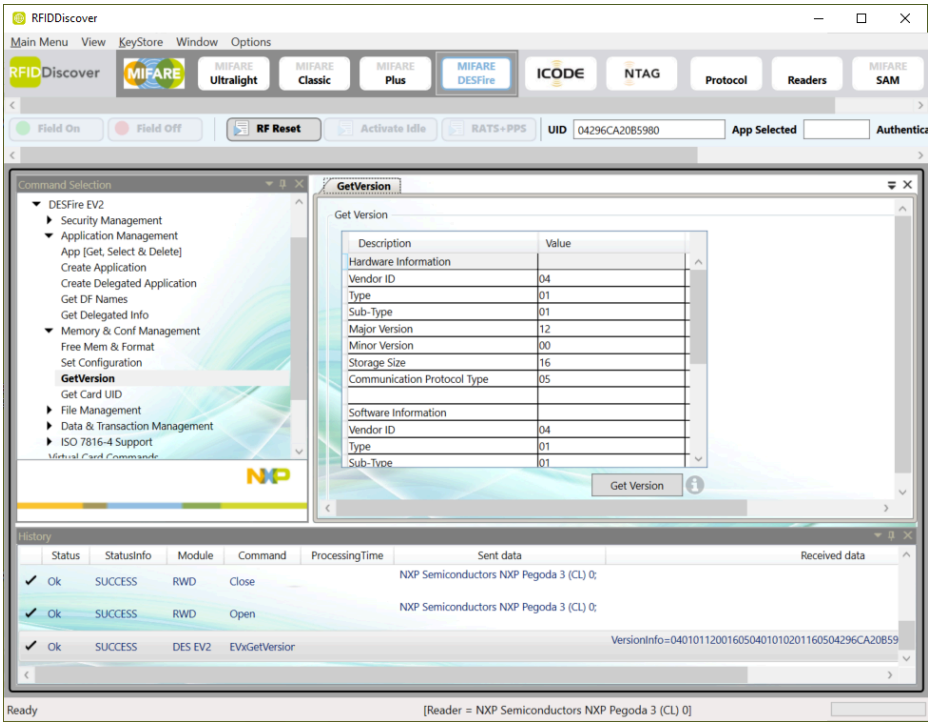


Figure 11. History dialogue window and detection of two smart card readers

Besides this automatic detection, you see also a prompt for a “New Profile” each time you run RFIDDiscover; place a ISO14443-4 card on the reader antenna, select “NXP Semiconductors NXP Pegoda 3 (CL) 0”, then press OK (see below).



All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

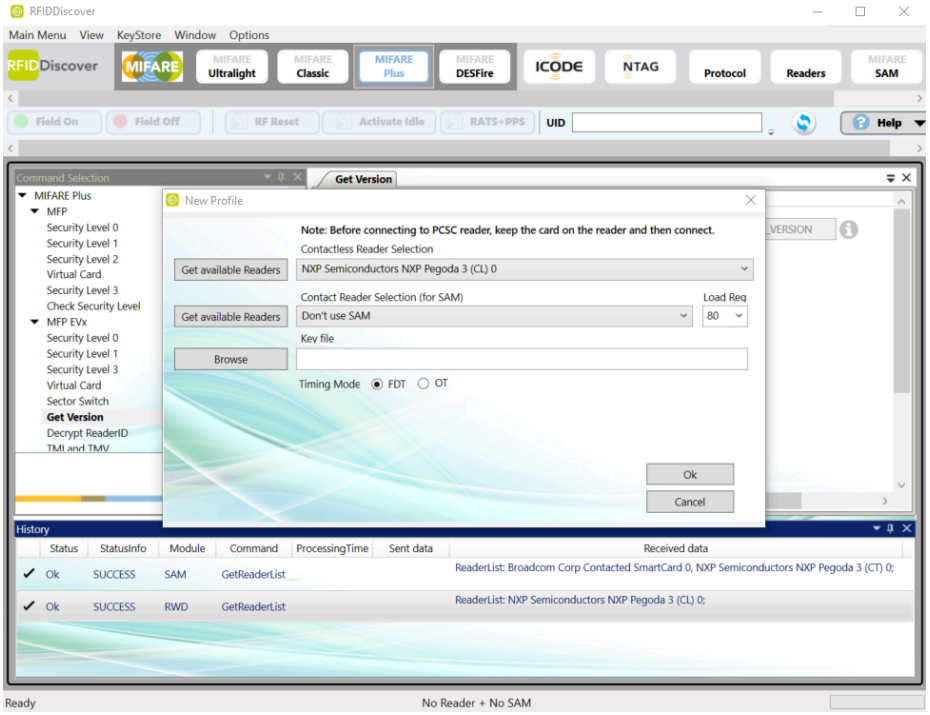


Figure 12. Contactless interface selected for Pegoda. Example of MIFARE DESFire EV2 detection

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

3.3 In case RFIDDiscover does not list Pegoda reader

If you cannot find the Pegoda reader in the list in the "New Profile" dropdown, then follow these instructions.

Select the button named “Readers” (top 9th button from left to right, or third from top right to left):

Figure 13. “Readers” button and available menu on left part – Pegoda belongs to “PC/SC Readers (PR533, PN533 and SCM)”

Now, on the left corner, select last position menu, named “PCSC Readers (PR533, PN533, and SCM).

You see a scrollable window; by clicking the right sliding tab, scroll it until the extreme bottom.

There you find a list of Readers.

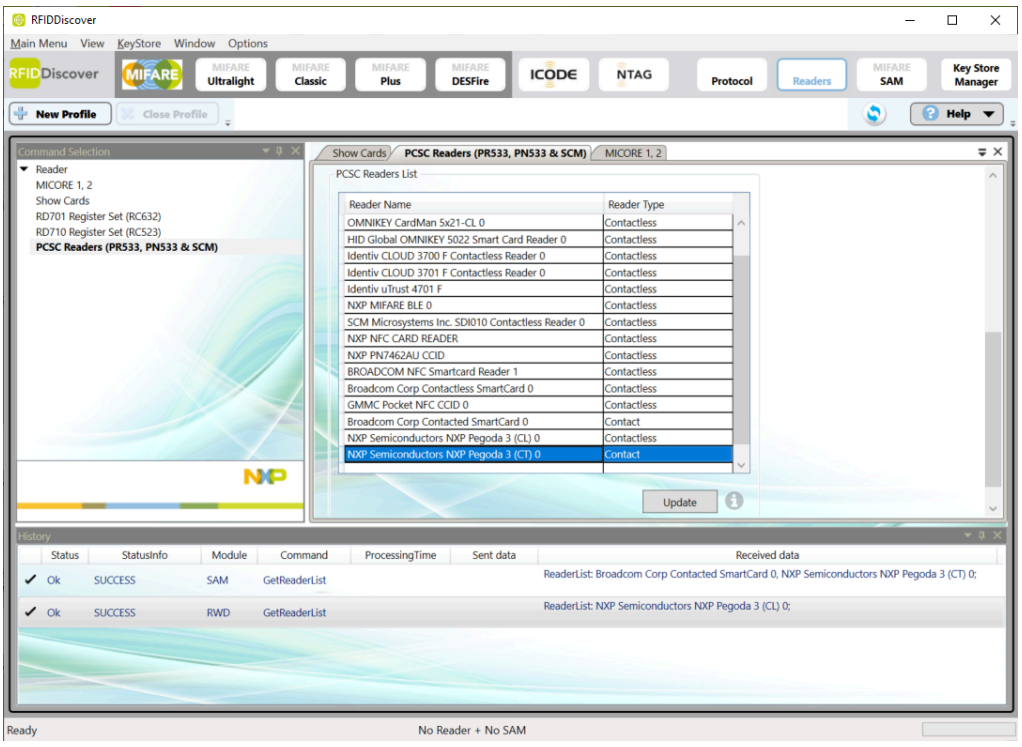


Figure 14. Table containing PC/SC Readers – Pegoda includes one contactless interface and one contact interface.

If you do not find “**NXP Semiconductors NXP Pegoda 3 (CL) 0**” on the left part of referred table click the line and start writing exactly this reader text (it is case-sensitive); on the right part of table (under “Reader Type”) select option “Contactless” for (CL) 0.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Go to below line, and do the same with text “**NXP Semiconductors NXP Pegoda 3 (CT) 0**” (consider it is case-sensitive too). On right part of table, select “Contact” for (CT) 0.

Then press “Update”. You notice these two smart card reader descriptors will univocally detect Pegoda respectively contactless and contact part.

3.4 Support to other products (ISO/IEC 14443-3, ISO/IEC 15693, etc.)

The CLRD730 Pegoda reader has a small hole on the lateral side of the plastic case, which gives access to different operation modes. Use a needle or tip of a paper clip to access this pushbutton through the hole. When the Pegoda is attached to USB, the pushbutton toggles between two modes of operation, VCOM mode and PS/SC mode. When pressed during a power cycle of the reader, this allows the Pegoda to be identified as “mass storage device" by a Windows computer. This allows flashing of different binaries and using the CLRC730 also with the NFC Cockpit tool (see Section 3.7).

Figure 15. Pegoda has a lateral access to an internal PCB pushbutton: while in PS/SC, pressing this button toggles VCOM mode with PC/SC mode.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

3.4.1 Pegoda in VCOM mode

After pressing the pushbutton, notice all three leds will blink for a while (between dark blue and red) and will toggle to VCOM operation (see new LED status below). In this operation mode, the CLRD730 can also support interaction with ISO14443-3 products (non-secure MIFARE products, e.g., MIFARE Ultralight family), NTAG products (like NTAG21x family, NTAG I^2C Plus family, NTAG 5 family), ICODE products (SLIX family, DNA, ILT, etc).

This mode of operation will be recognized by Device Manager with a different USB descriptor (see below).

As this mode provides the most flexibility, it is recommended to use VCOM mode as much as possible.

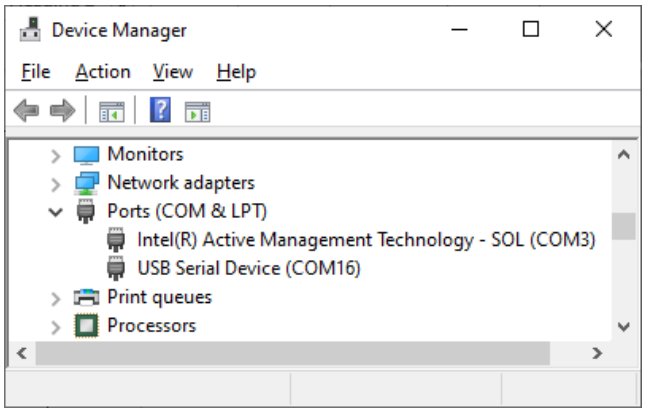


Figure 16. Pegoda in VCOM mode (POWER LED is red, MODE LED is light blue, COMM LED is dark blue); on the right, USB descriptor while in VCOM Mode (in this case, COM16).

3.4.2 Pegoda support of ISO/IEC14443-3 products and ISO/IEC15693 on RFIDDiscover

While in VCOM mode, RFIDDiscover supports all 13.56 MHz transponder supplied by NXP (including ISO/IEX14443-4 cards). After the mode switch is done (Section 3.4.1) is done, if you inspect the Device Manager, you will find a USB descriptor like “USB Serial Device (COMxy)”.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

3.4.3 RFIDDiscover using Pegoda in VCOM mode

If you run again RFIDDiscover, one is able to notice the following reader detection window.

On the top drop-down list, select “PEGODA 3: USB Serial Device COMxy” and press ok. Note, that in VCOM mode, no card must be on top of the reader to establish the connection.

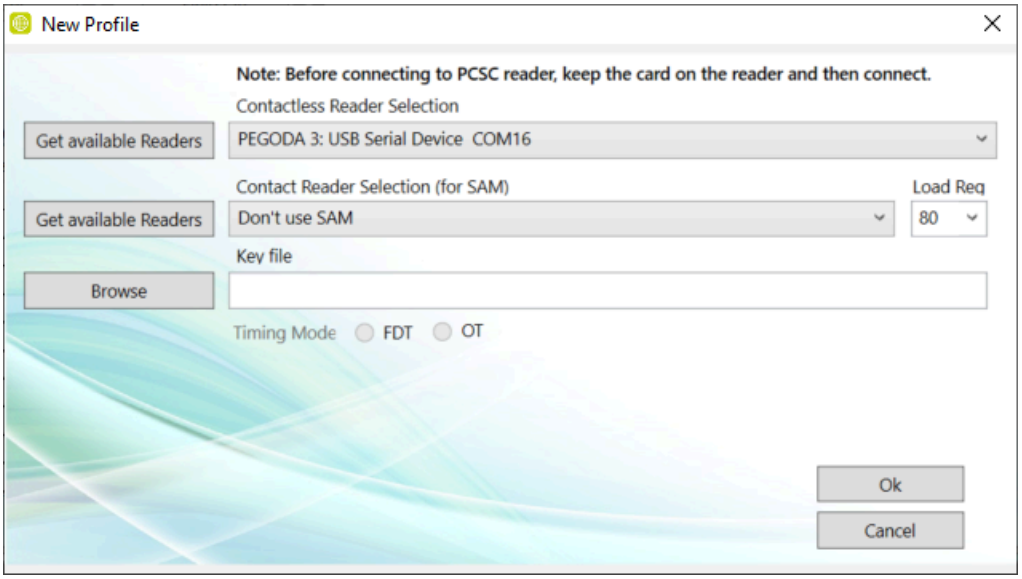


Figure 17. RFIDDiscover in VCOM mode

Place a card on the reader antenna, for instance, a MIFARE Ultralight EV1 card. Select MIFARE Ultralight button (first selectable rectangular tab from top left to right). Then select MIFARE Ultralight EV1, press Activate Idle (fourth tab from middle top left to right). Check the 7 bytes UID of card shown in central window (see picture below).

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

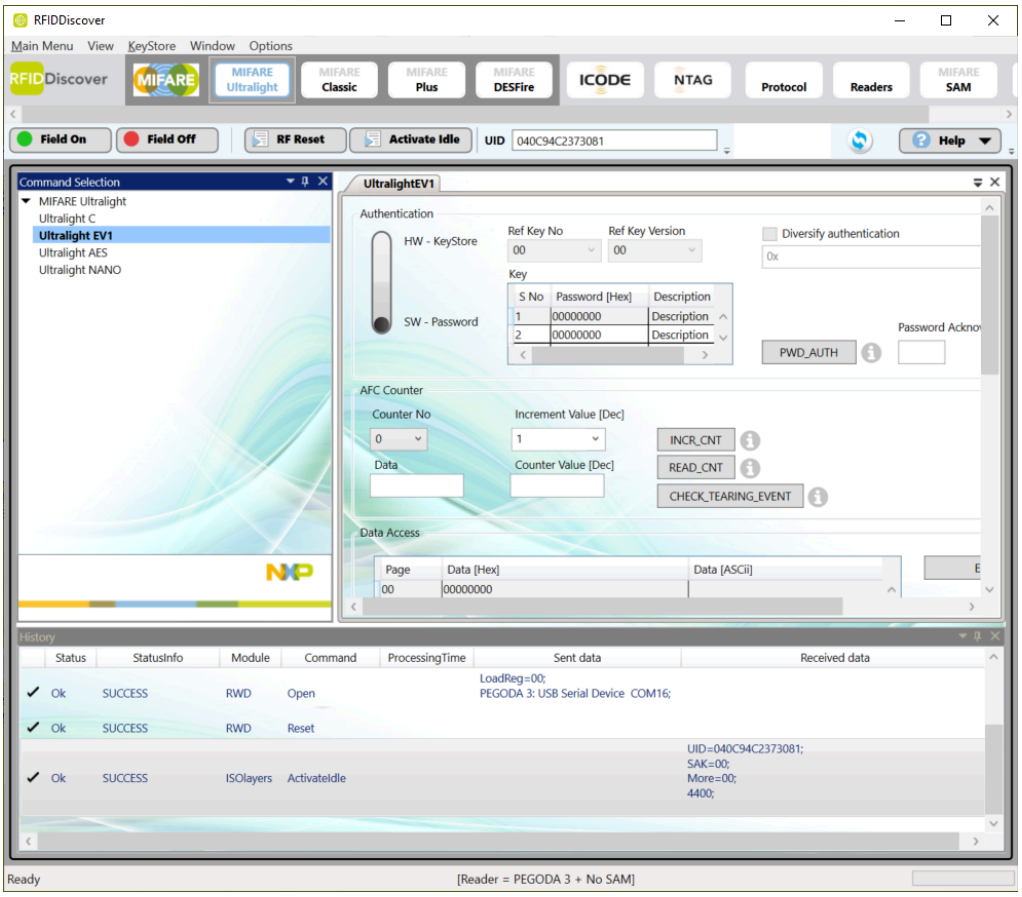


Figure 18. MIFARE Ultralight detection of Pegoda in VCOM mode.

Now try to place a MIFARE Classic card on Pegoda antenna and try to interact with it (see below example with 1 kbit 7 bytes UID). In SW Keystore tab, it is possible to set keys on specified table address. In this case, Crypto1 keys were set to 0xFFFFFFFFFFFF, at address 0A, on Software Key storage.

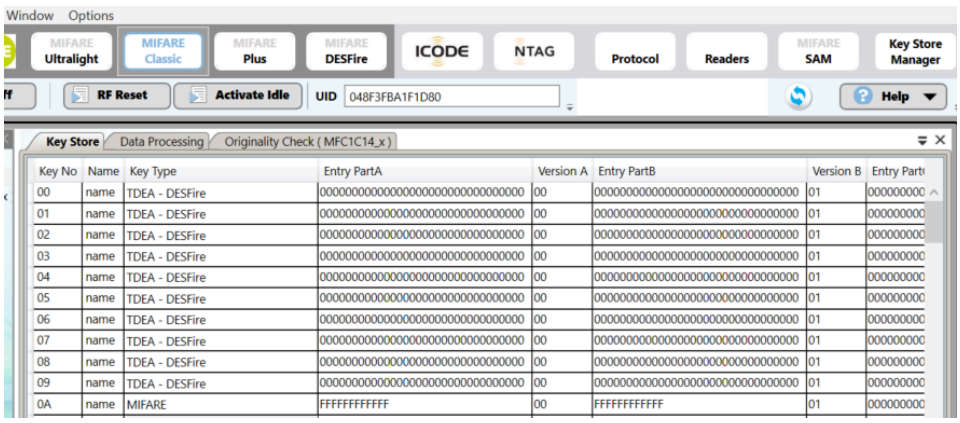


Figure 19. MIFARE Classic Crypto1 keys set in address A0

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

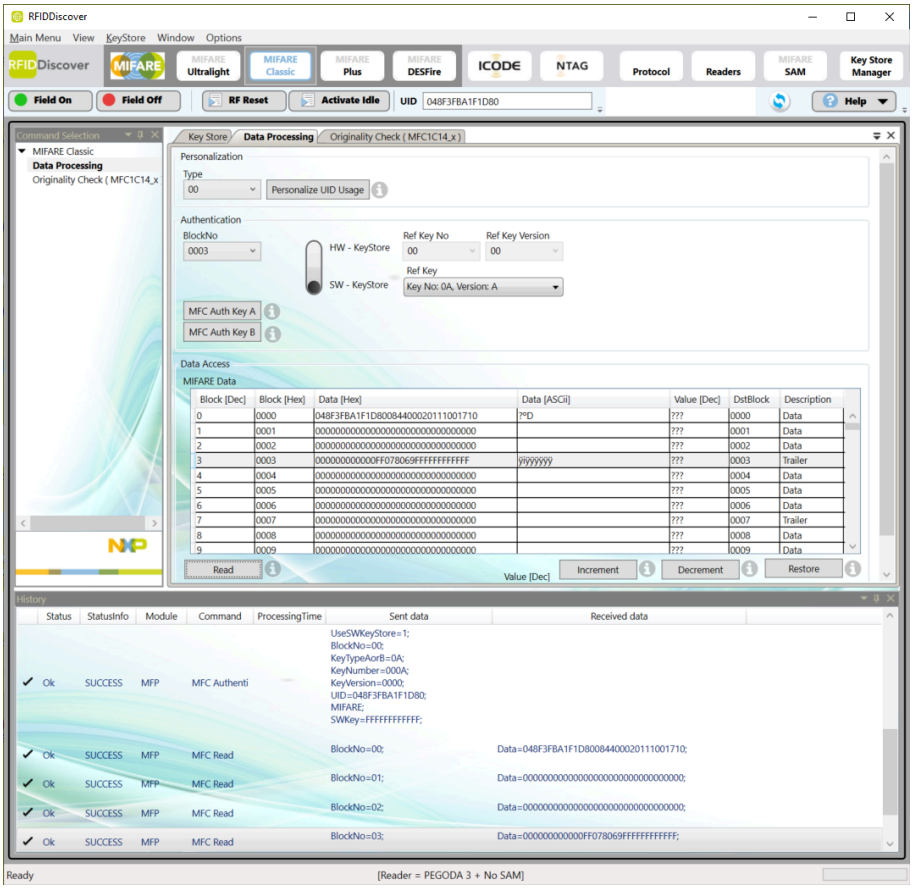


Figure 20. MIFARE Classic detection and authentication of first sector blocks with Pegoda in VCOM mode.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

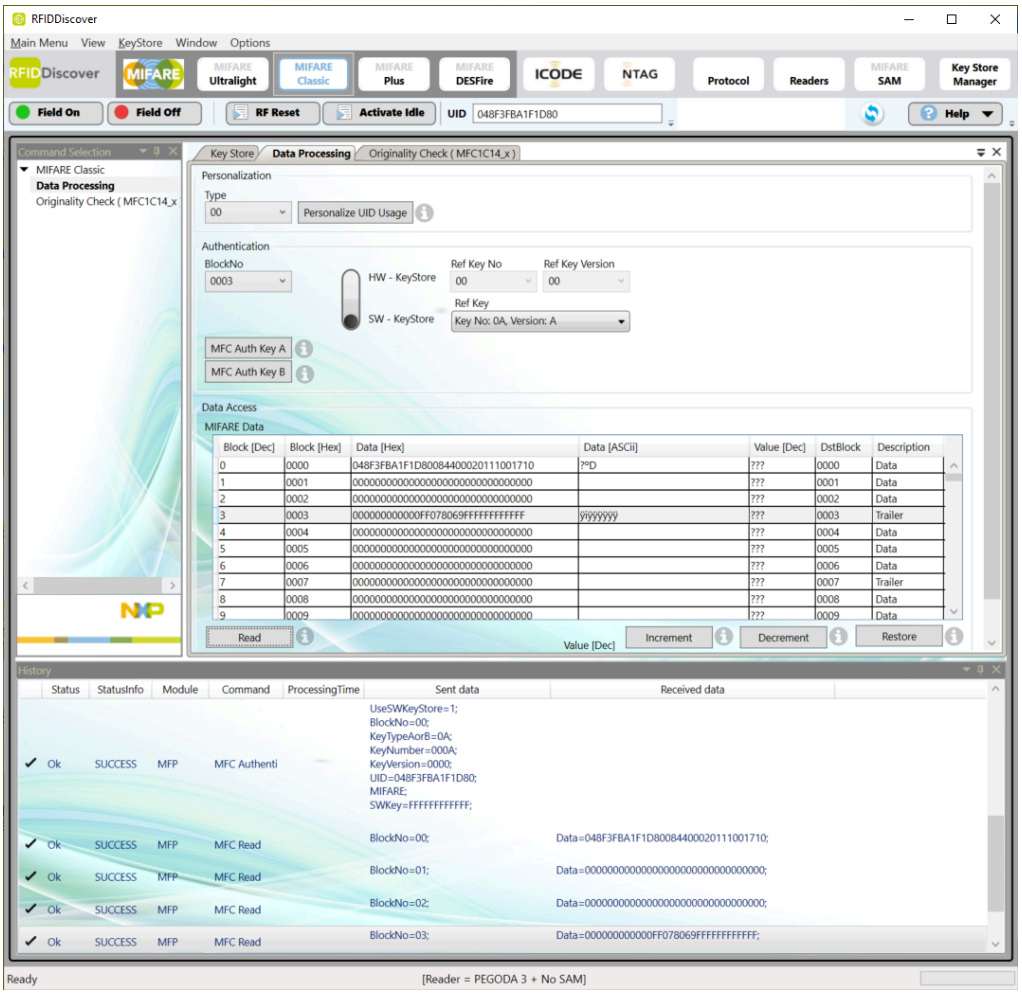


Figure 21. MIFARE Classic reading of first sector blocks with Pegoda in VCOM mode.

3.5 Support of Pegoda to Card Test Framework GUI

NXP delivers another Software GUI consisting of a Windows application which runs scripts containing transponder commands. It is named Card Test Framework and it is particularly useful to test key provisioning and personalization of smartcards, because a script may contain all necessary operations to initialize/configure cards that are received with default keys and their memory completely empty.

One can obtain Card Test Framework if you have a valid NDA with NXP. Like all other NDA-protected documents and application software, One may download Card Test Framework by enrolling and qualifying to My NXP Account. Installation and documentation can be obtained by clicking “Secure Files” and by selecting option “Product”, then type “Card Test Framework” on space and press “ok”. You see three secure files that you may download: Card Test Framework application executable (SW installation under Windows computers), user manual, and application note.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

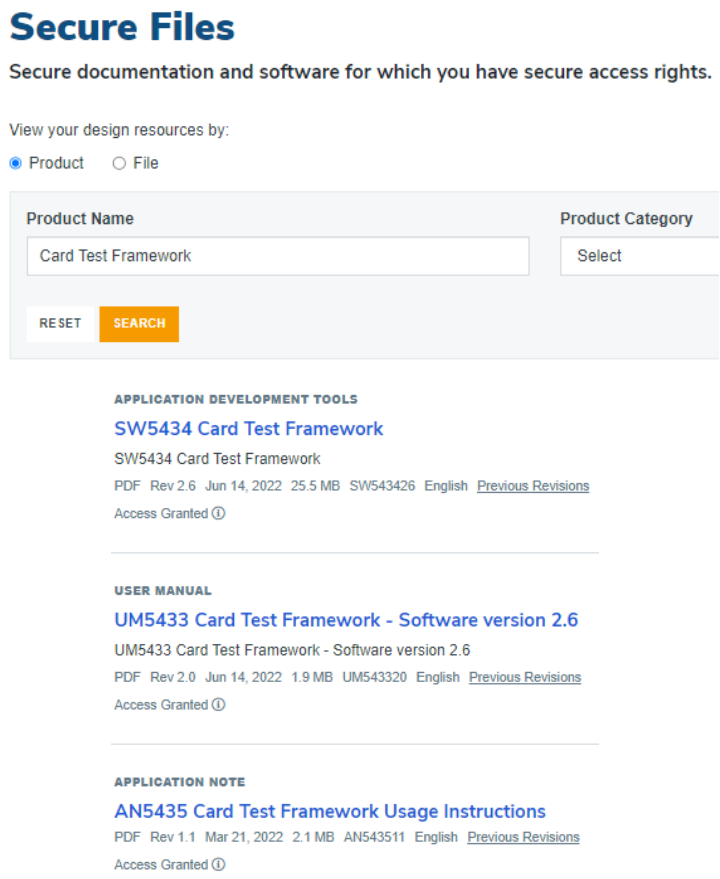


Figure 22. Card Test Framework search in Secure Files.

Then, after configuring reader in “equipment list”, (Configuration → Equipment) it is possible to select a script, and run it.

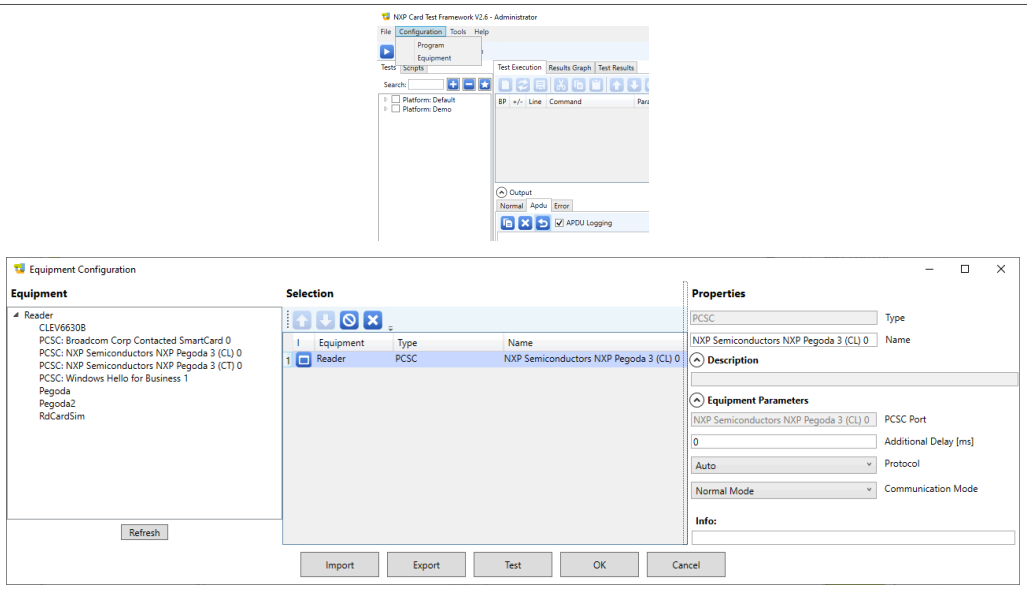


Figure 23. How to configure “equipment” before using Card Test Framework

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Certificate Propagation service is by default enabled on Windows computers, therefore you might get a Service Warning advising user to disable it to avoid interference with operation of PCSC smart card reader. You can access this service and disable it, by opening Control Panel → Administrative Tools → Services.

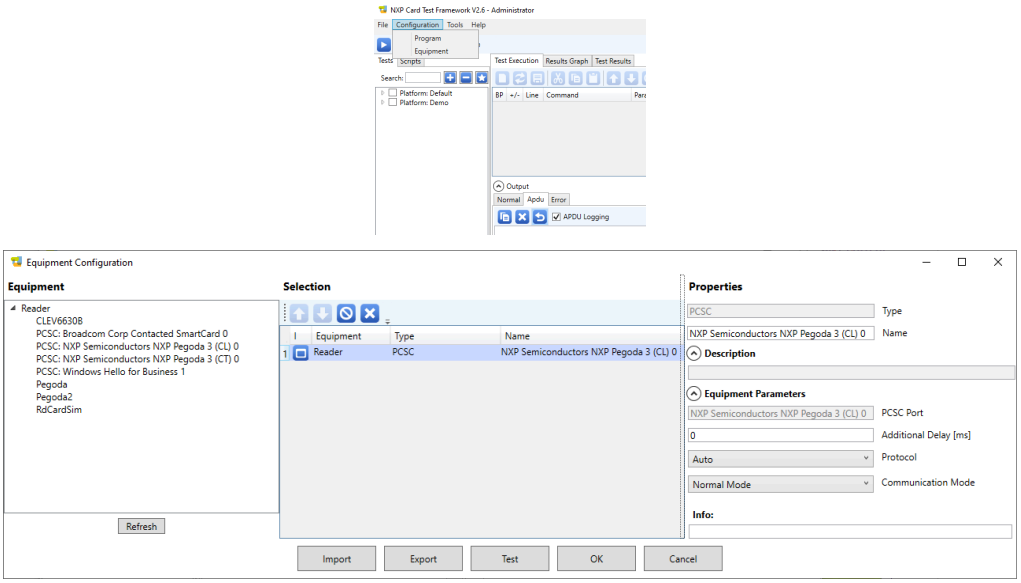
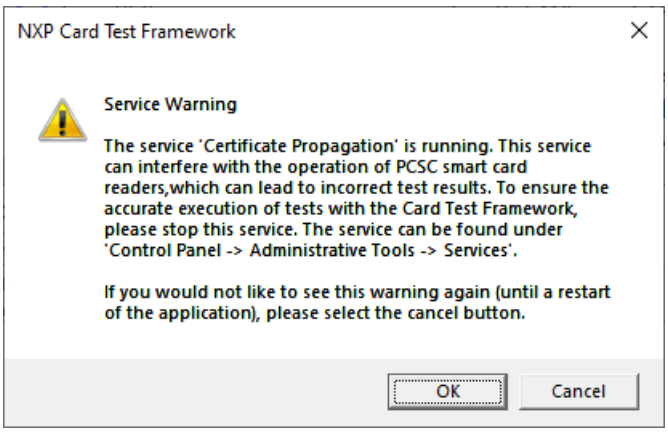


Figure 24. How to configure “equipment” before using Card Test Framework



All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

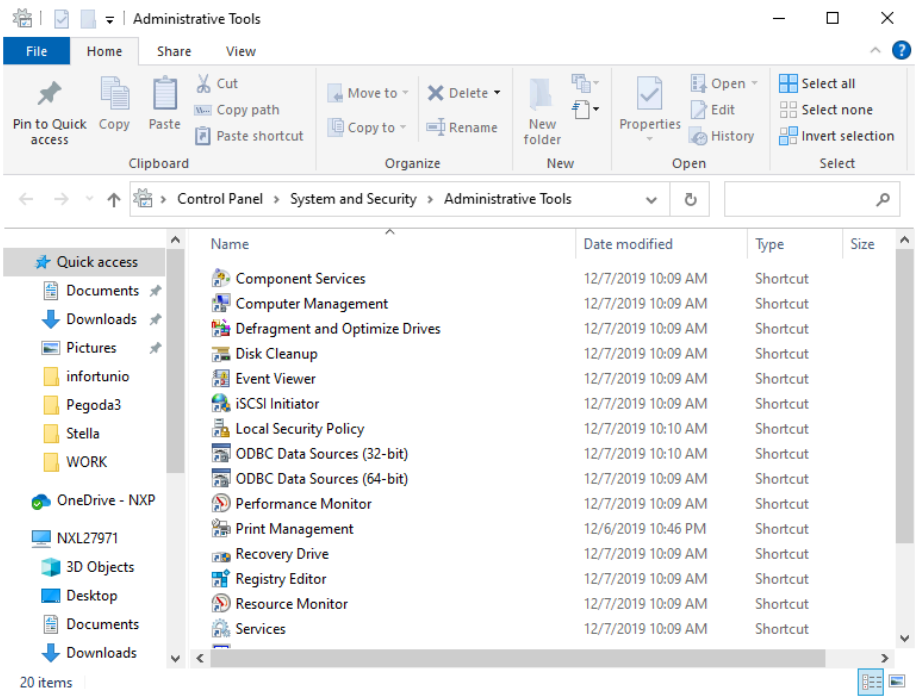


Figure 25. “Propagation of Certificates” warning and access from Control Panel

As an example, a MIFARE DESFire card formatting script is demonstrated in picture below, after having placed one MIFARE DESFire EV3 card on top of Pegoda.

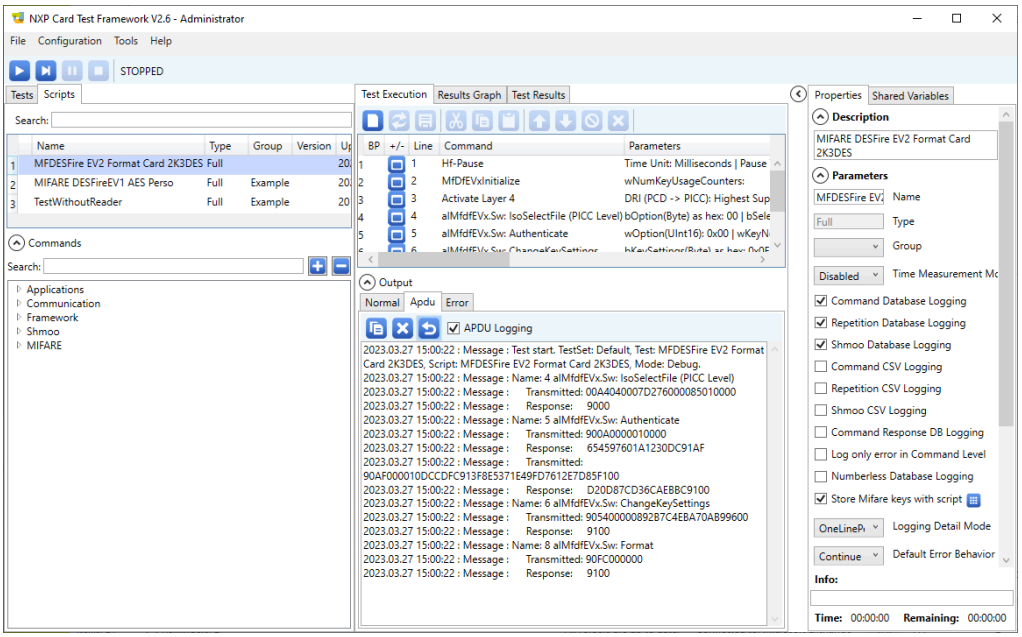


Figure 26. Simple MIFARE DESFire card formatting example to demonstrate CTF usage

One may find instructions on how to detect/include Pegoda in reader list and on how to use Card Test Framework in this application note: AN5435 Card Test Framework Usage Instructions. For more info, see [6].

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

3.6 Pegoda configured as mass storage device

When in mass storage mode, it is possible to overwrite the current Pegoda binary, which actually is the PN7642 binary contained in built-in MCU flash. By default, CLRD730 is delivered with PS/SC-VCOM binary, which is used to support RFIDDiscover, aiming to allow customers to get familiarity with NXP transponder technologies at 13.56 MHz (ISO/IEC 14443A - proximity tags - and ISO/IEC 15693 - vicinity transponders).

Nevertheless, it is possible to upload the binary delivered with NFC Cockpit and available inside its installation directory:

C:\nxp\NxpNfcCockpit_v7.1.0.0\firmware\PN7642\

Currently it is named NxpNfcCockpit_05_03_00_Flash.bin.

Before writing new binary, it is necessary to delete the previous one (see next picture).

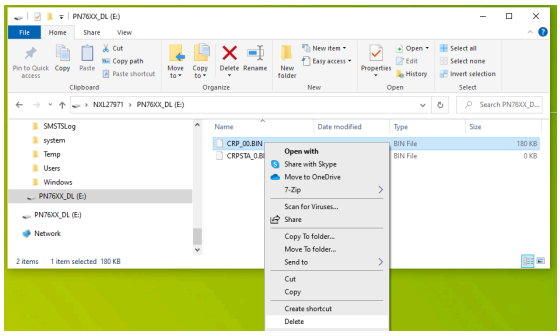


Figure 27. How to change Pegoda application – first delete current binary file then drag and drop new binary.

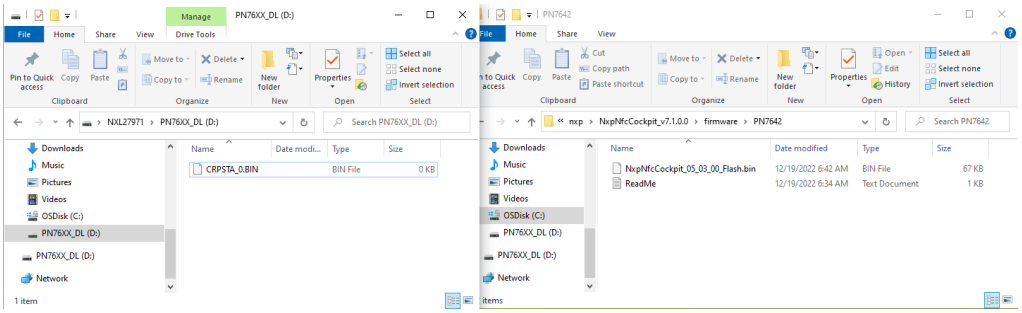


Figure 28. Example above shows uploading PN7642 binary available in NFC Cockpit installation directory: C:\nxp \NxpNfcCockpit_v7.1.0.0\firmware\PN7642

You recognize that Pegoda is in mass storage mode by looking to all three leds which are on: “POWER” LED is blue colored on; “MODE” LED is white-colored on and “COMM” LED is white-colored on (see below).

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Figure 29. Pegoda in mass-storage mode

3.7 Pegoda configured to support NFC Cockpit

Note: Do not update the PN7642 Firmware to a version greater than 1.x. or the Pegoda reader will become unusable.

When the NFC Cockpit binary is dragged and dropped to “mass storage” location, it is necessary to reset CLRD730 (unplug and plug again USB-C cable).

Then one notices that Device Manager changes USB description as shown below.

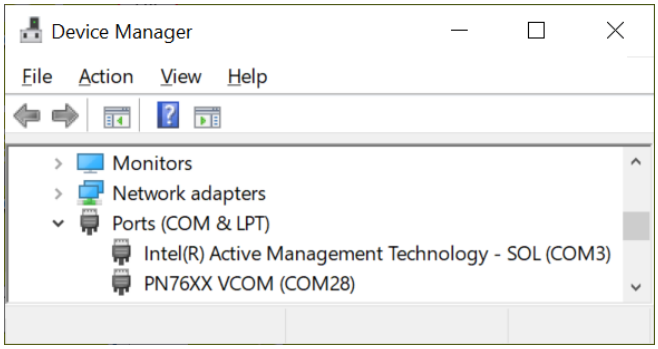


Figure 30. Device manager USB descriptor: there is no entry when CLRC730 is in mass-storage mode but there is “PN76XX VCOM”, able to support NFC Cockpit GUI

It is possible to recognize Pegoda in VCOM functionality looking to RED POWER LED always on (while other two leds are off). Under this condition, it is possible to run NFC Cockpit and get familiarity with all functionality of PN7642 NFC controller (all documentation, SDK, and product support package is available on this landing page https://nxp.com/PN7642)

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

As mentioned before, NFC Cockpit can be downloaded from NXP public website (see [4]):

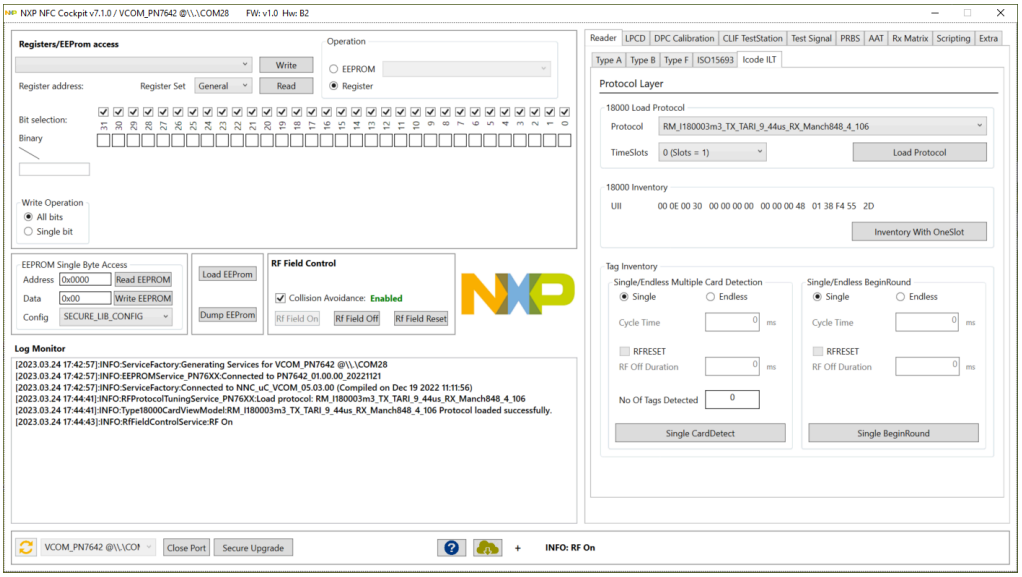


Figure 31. Aspect of NFC Cockpit GUI – it is important to have a display resolution equal or bigger than 1920x1080 to have full GUI window inside screen

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

4 Public version of RFIDDiscover

4.1 RFIDDiscover Lite installation

In order to get to know all available functions of public version of RFIDDiscover, go to NXP website and type RFIDDiscover Lite in “search” field:

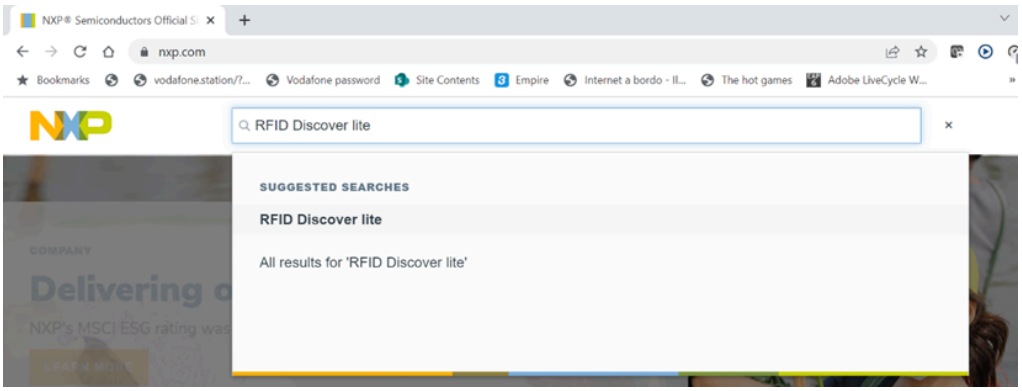


Figure 32. NXP search engine and how to locate RFIDDiscover Lite GUI

One finds two links: “Documentation” and “Downloads”

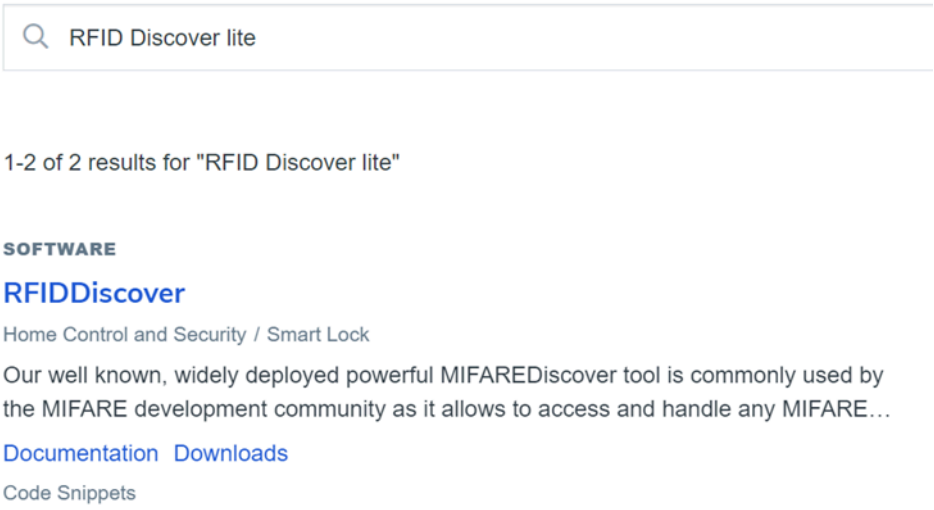


Figure 33. RFIDDiscover Lite download link

Click in “Downloads”, one is able then to see following item:

Figure 34. RFIDDiscover Lite download

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Alternatively, this is the link to get to RFIDDiscover lite location: https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-desfire/rfiddiscover:RFID-DISCOVER#downloads

After unzipping until the level of RFID installer, the installer will ask for administrator rights to install it in your machine:

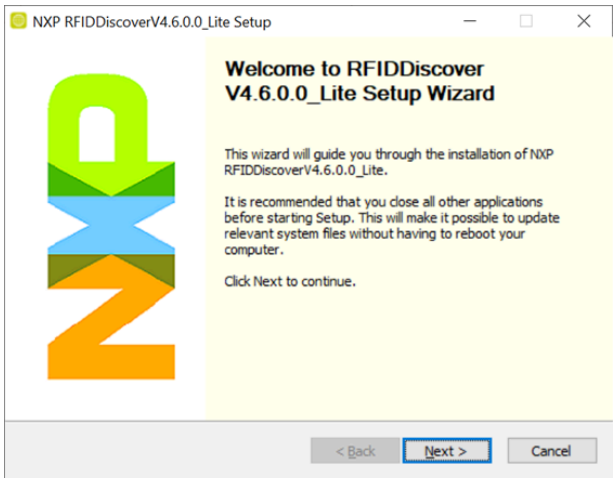


Figure 35. RFIDDiscover lite GUI installation

After installation, you will find this directory in your machine:

C:\Program Files (x86)\NXP Semiconductors\RFIDDiscover\V4.6.0.0_Lite\

The ReleaseNotes.pdf can be found in the directory "Doc".

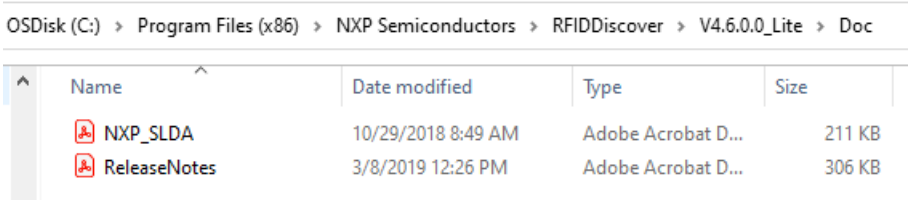


Figure 36. RFIDDiscover lite installation directory in Program Files

RFIDDiscover user manual currently is only available if you download it from “Secure Files” repository, therefore upon signature of mutual NDA with NXP.

4.2 Main frame general overview

The public RFIDDiscover Lite supports the functions for non-secure MIFARE, NTAG, and ICODE families.

Therefore, the user interface is divided into functional blocks which are shown in different tabs in Figure 37 (1).

They open the so-called ‘Command selection’ window (2) which allows to select a command window in (3).

At the bottom (4) Figure 37 shows the history field where all the operations are displayed. For a more detailed view on the sent data and received data, a switch to the log window is possible. Both fields can be cleared, or can be stored in a text file.

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

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

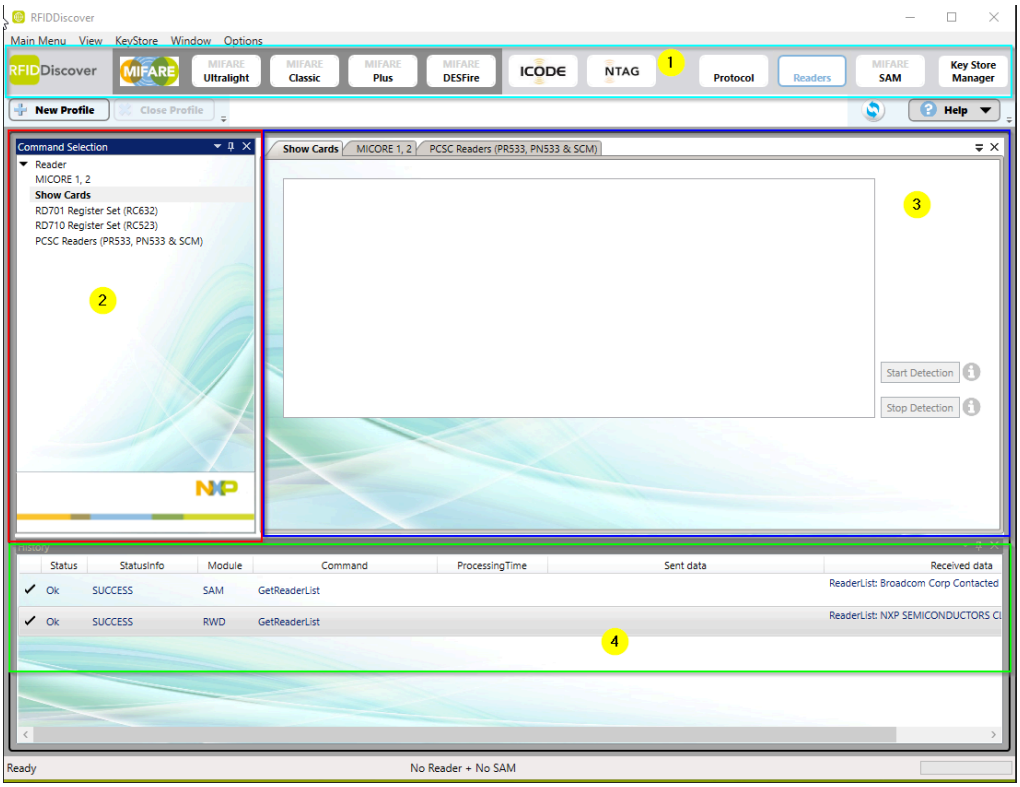


Figure 37. Interface to reader has been opened successfully

4.2.1 Readers window

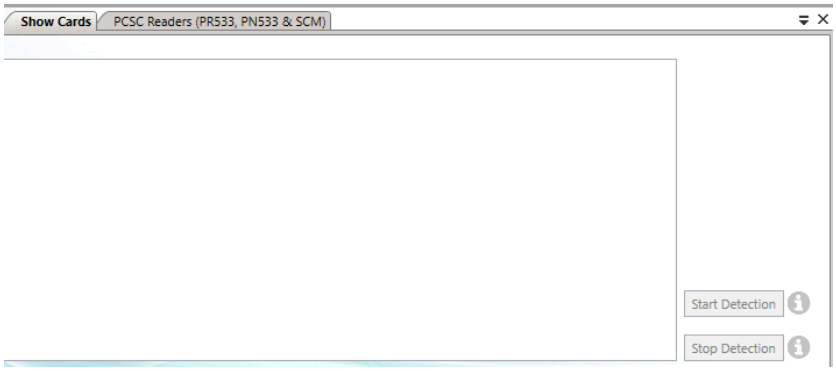


Figure 38. Show Cards command window

The ‘Show Cards’ command window in Figure 38 allows you to detect all cards which are present in the reader field. With ‘Start Detection’, the reader starts to poll for cards (ISO 14443 Type A and B) and you get the UID of the cards presented to the Pegoda as well as the card type. With ‘Stop Detection’, the polling is stopped again.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

4.2.2 Protocol window

The command window related to protocol is shown in Figure 39.

1. This part of the panel allows you to activate a number of cards and perform the anti-collision protocol according to ISO/IEC 14443. The most convenient method is to push the ‘Activate Idle’ button. After that, in the table a UID appears in section 2 and its State is ‘Active’.
2. This section allows you to manage multiple cards in the reader field. Select a specific card that you want to communicate with. Therefore this card has to be in ‘Active’ State. To switch to another card in the reader field choose the current ‘Active’ card and with ‘Halt’ you can change the State from ‘Active’ to ‘Halt’ state (and work with another card in the meantime). Pick a ‘Halt’ UID and the button ‘Act.Wakeup’ changes the State back to ‘Active’ and you can work with the card again. ‘Clear List’ deletes all data in the table
3. With the control elements it (3) section, you can send individual commands and data to the card in an ISO 14443-3 message frame. Thereby the input format is hex coded. The checkboxes there indicate if you want to append a CRC code to the command and if you expect that the card to append a CRC to the response. The answer of the card is then displayed in the log windows. For a list of available command, refer to cards data sheet.

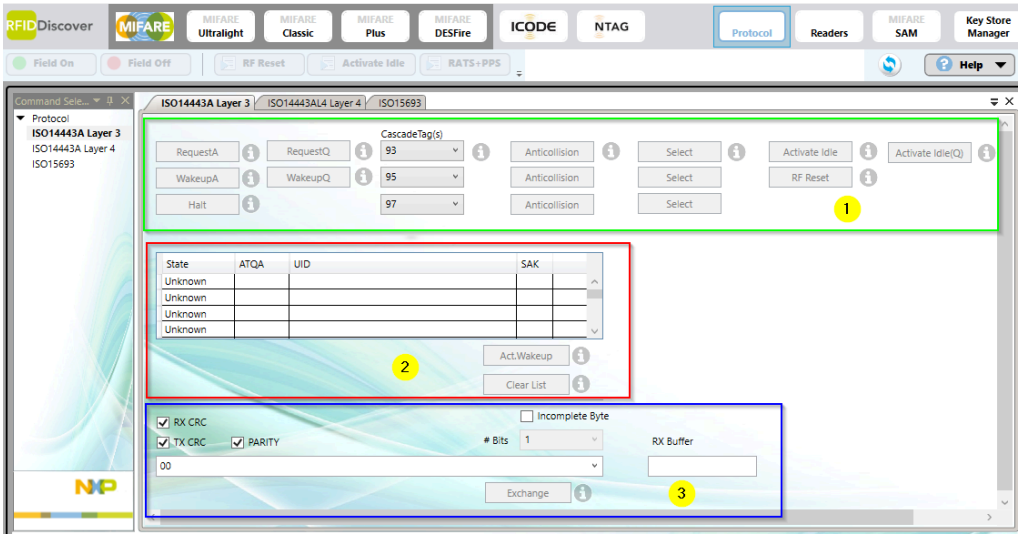


Figure 39. ISO14443A Layer 3

This view is ideal to understand the basic concepts from ISO14443-3 and can be used to evaluate scenarios on a very low level.

4.2.3 MIFARE Classic window

After pressing "MIFARE Classic" on middle text area (on right side of MIFARE logo), the dialogue with MIFARE Classic cards is opened on the left side. It includes Data Processing and Originality Check tabs.

Figure 40 shows the "Data Processing" window. With this window you can process the data stored on the MIFARE Classic card:

1. "Personalization UID Usage" allows you to configure the type of UID the card should use.
2. To gain access to the different storage sectors of the card, you first must authenticate with a Key. Therefore you can choose a "BlockNo" and the "Ref Key" (prepared in the KeyStore Section 4.2.6) and use the button "MFC Auth Key A" or "MFC Auth Key B".
3. With "Read", you can read a block from the card and with "Write" you can write the block on the card then is selected in the data grid. Use "Increment" to increase and "Decrement" to decrease the contents of a block.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

The results are stored in an internal data-register. The "Restore" button move the contents of a block into an internal data-register. Use "Transfer" to write contents of the temporary internal data-register to a value block.

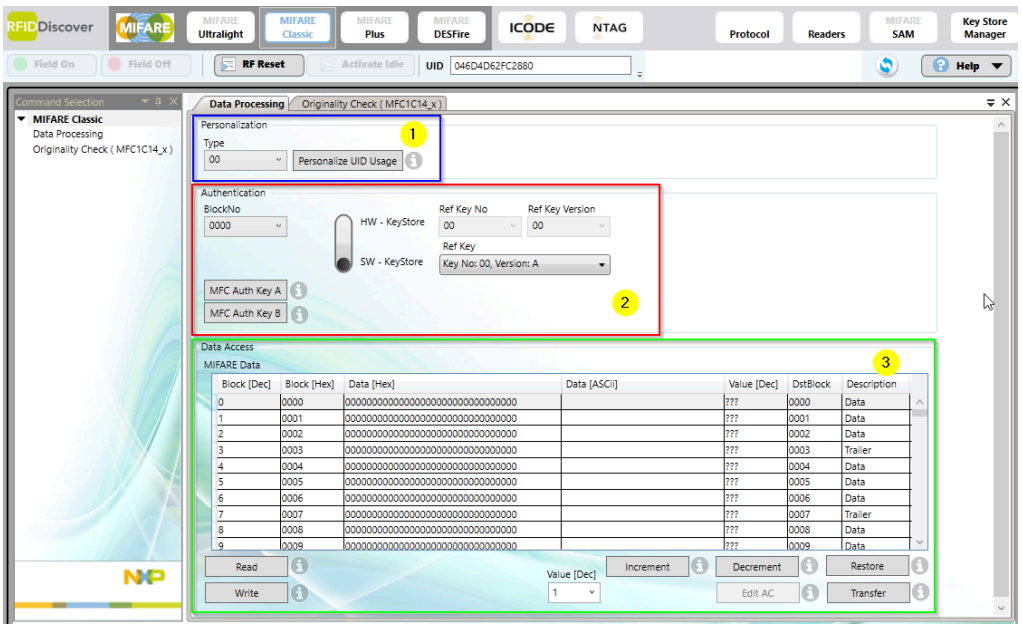


Figure 40. Data Processing

4.2.4 MIFARE Ultralight windows

By pressing MIFARE Ultralight button, then it is possible to operate with all MIFARE Ultralight product types. It is necessary to execute following commands in order to perform ‘ISO14443A Layer 3’ sequence and operate with one of above mentioned technologies: “Field On” (or “RF Reset”) and “Activate Idle”.

The "Ultralight AES" command window allows:

1. To read and write data on a chosen page of the card.
2. To edit lock bits/user configuration (refer to MIFARE Ultralight AES data sheet).

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

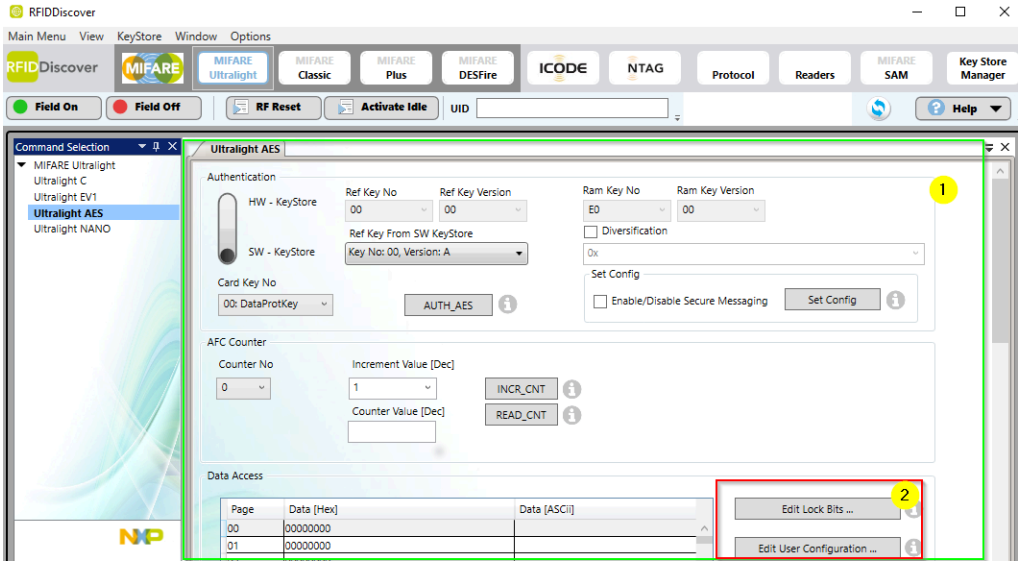


Figure 41. MIFARE Ultralight AES

4.2.5 Protocol button and ISO14443-4 tab

This tab provides all the functionality to work with ISO14443-4 and the command window is shown in Figure 42.

1. This part can be used to activate a card to Layer 4 and control the date exchange rate.
2. The textbox shows the state of the cards. Control which card is the active one.
3. Use the blue marked part to send commands to the card in a ISO14443-4 message frame format.

For more information on the provided commands of this window, refer to RFIDDiscover user manual.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

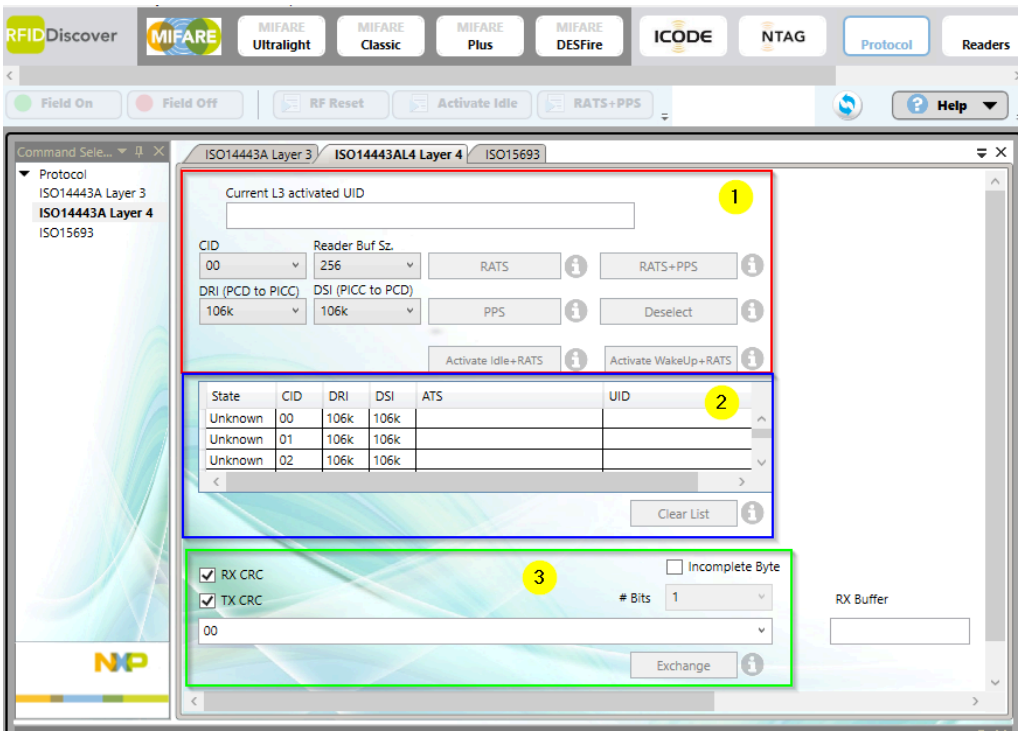


Figure 42. ISO14443A Layer 4

4.2.6 Key Store Manager

The Key Store Manager window as shown in Figure 43 allows you to define a number of Keys to be used for the authentication of e.g. memory sectors.

Each key block can have a nickname and a certain type. It is divided in 3 keys, A B, and C with individual Versions.

From more information on keys and how to be used with cards refer to the individual card IC data sheets.

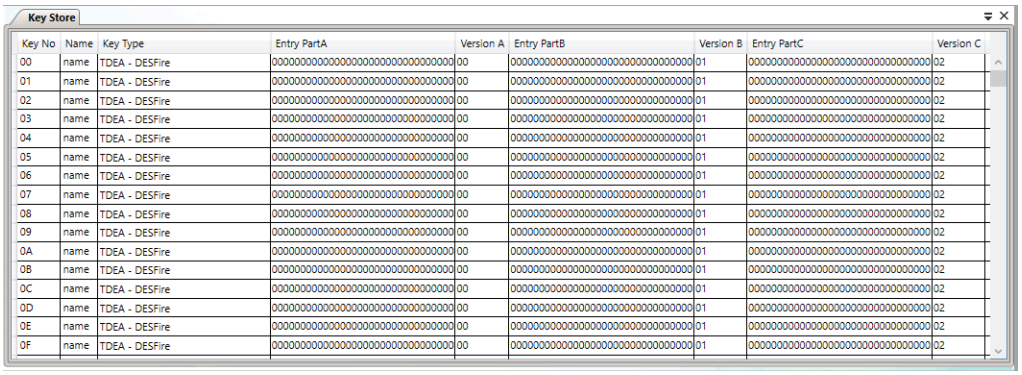


Figure 43. Key Store Manager

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

5 Electromagnetic compatibility

5.1 FCC Compliance Statement

NOTE:

This equipment has been tested and found to comply with the limits for a Class B digital device, according to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution!

The Federal Communications Commission warns the users that changes or modifications to the unit not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

The accessories associated with this equipment are as follows:

- Shielded communication cable

These accessories are required to be used in order to ensure compliance with FCC rules.

5.2 Compliance information according to 47 CFR Part 15, Subpart B

NXP declares that the product

CLRC730,

FCC ID: 2ADMJCLRD730

are in conformity with

- 47 CFR Part 15, Subpart B (Clause 15.107 and 15.109) in conjunction with ANSI C63.4:2014
- ICES-003, Issue 7 in conjunction with ANSI C63.4:2014

Operation of this product is subject to the following conditions:

1. this device may not cause harmful interference
2. this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

5.3 Compliance information according to Article 10.8 of the Radio Equipment Directive 2014/53/EU

The following information is provided per Article 10.8 of the Radio Equipment Directive 2014/53/EU:

(a) Frequency bands in which the equipment operates.

(b) The maximum RF power transmitted.

PN	RF Technology	Freq. Ranges	Max. Transmitted Power
CLRD730	RFID	13.553 – 13.567 MHz	30 dBm

EUROPEAN DECLARATION OF CONFORMITY (Simplified DoC per Article 10.9 of the Radio Equipment Directive 2014/53/EU).

This apparatus, namely CLRD730 Contactless Reader, conforms to the Radio Equipment Directive 2014/53/EU.

The full EU Declaration of Conformity for this apparatus can be delivered on request via https://www.nxp.com/mynxp/secure-files.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

6 References

[1] **Data sheet –** CLRD730, PEGODA contactless smart card reader based on open-controller NFC reader PN7642 with optional contact interface, available on https://www.nxp.com/products/:CLRD730

[2] **RFIDDiscover user manual** - UM10616 RFIDDiscover User Manual (available in My NXP Portal, Secure Files).

[3] **RFIDDiscover Lite**– NDA-free version, available on NXP website

[4] **NFC Cockpit Tool GUI** - NFC Cockpit configuration tools for NFC IC's

[5] **PN7642 data sheet** - Single chip solution with high performance NFC reader, customizable MCU and security toolbox

[6] **Card Test Framework GUI** – Installation, user manual and usage instructions, available in My NXP Portal, under Secure Files.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Legal information

Definitions

Draft — A draft status on a document indicates that 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 in a draft version of a document and shall have no liability for the consequences of use of such information.

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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

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 and its suppliers accept 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.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Licenses

Purchase of NXP ICs with NFC technology — Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Trademarks

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

NXP — wordmark and logo are trademarks of NXP B.V.

DESFire — is a trademark of NXP B.V.

EdgeVerse — is a trademark of NXP B.V.

ICODE and I-CODE — are trademarks of NXP B.V.

JCOP — is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

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

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

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

NTAG — is a trademark of NXP B.V.

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Figures

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© 2023 NXP B.V. **All rights reserved.**

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

Date of release: 6 November 2023
Document identifier: UG10039