EM MICROELECTRONIC - MARIN SA

SWATCH GROUP ELECTRONIC SYSTEMS

AN433

	Application Note AN433
Title:	**EMDB410 RFID Reader User Guide**
Product Family:	**RFID Solutions**
Part Number:	EMDB410 – EM4294 RFID Reader
Keywords:	ISO15693 - ISO14443 Type A,B
Date:	November 10, 2009

1. Introduction
The EMDB410 RFID Reader requires the minimum hardware and software resources;
Microsoft Windows XP, 10MB HDD space, 800x600 pixels video resolution.

1.1. Setup
At first, unpack the EMDB410 RFID Reader base station, installation CD, USB cable, and transponder samples from the EMDB410 RFID Reader box.

Following steps describe the first-time initialization of the EMDB410 Reader Application;

1. Log-in as administrator
2. Launch the Setup.exe executable located in the CD root directory, the EMDB410 RFID Reader SETUP window appears
3. Click on "Click here to start installation" label
4. Follow the application software installation wizard to install the application software. Beside this installation, the FTDI USB virtual COM port drivers are installed automatically
5. Connect the EMDB410 Reader to the USB port using USB cable
6. EMDB410 RFID Reader SETUP application detects the reader is connected automatically (label "Reader is connected" with appropriate COM port is displayed in the left-bottom corner)
7. Quit the EMDB410 RFID Reader SETUP window
8. In the Start->All programs menu, locate the EMDB410 Reader application software and launch it
9. Within EMDB410 Reader application software, select a menu Reader Connection -> Connect. The application finds every available virtual COM ports that are provided by FTDI USB drivers.
10. Choose the appropriate COM port in the Com Port List Box and click on Connect button to establish the connection.
11. The OK field inside the status bar and status window signalize a successful initialization while the reader connection modal window is closed automatically. Otherwise, status bar signalizes an error.

Possible problems caused by EMDB410 Application Software and their suggested solutions:

1. For the first time, the operating system asks for the **virtual COM port drivers** to be installed
2. No COM port is found – the operating system is not properly configured or the insufficient privileges are applied. Please inspect the hardware device list of your PC to check there is a USB<->COM converter device present while the EMDB410 Reader is connected via USB cable (and therefore powered on) and the drivers have been installed correctly.
3. To determine the virtual COM port (system way) - please inspect the hardware device list of your PC to check there is a USB<->COM converter device present while the EMDB410 Reader is connected via USB cable and the drivers have been installed correctly. On some systems, the virtual COM port number may collide with other virtual devices; in such case, please fix the COM port manually to another not-yet used port number.
4. To determine the virtual COM port (easy way) – run the EMDB410 Reader Application Software and select menu Reader Connection -> Connect. Remember the COM ports listed in the COM Port List Box. Then, connect the EMDB410 Reader via USB cable. After several seconds, the operating system creates a new virtual COM port, thus, click on Refresh button and check what a new port appears in the COM Port List Box.
5. The reader doesn't respond on startup – please determine the virtual COM port number and presence as described above.

1.2. User's guide
The user's guide chapter describes the functionality of EMDB410 Reader application software and shows how to communicate with the RFID transponders. The same information can be found in the EMDB410 Reader Application help available through pressing the key F1.

2. Starting EMDB410 Application Software
Following steps describe the standard initialization of the EMDB410 Reader Application Software when using USB cable assuming the drivers are already installed:

1. Connect the EMDB410 Reader to the USB port using USB cable
2. Run EMDB410 Reader Application Software
3. Select a menu Reader Connection -> Connect – the application finds every available COM port by trying to open it. Every available COM port is inserted into the Com Port List Box.
4. Choose the appropriate COM port in the Com Port List Box and click on Connect button to establish the connection
5. The OK field inside the status bar and status window signalizes a successful initialization while the reader connection modal window is closed automatically. Otherwise, status bar signalizes an error.

3. Graphics User Interface

The EMDB410 Application Software graphics user interface is split into two panels separated by a status bar. The upper panel displays a transponder specific frame (controls, commands, editable fields, etc). No transponder specific frame is displayed after the connection is established. The bottom panel contains a Message Window.
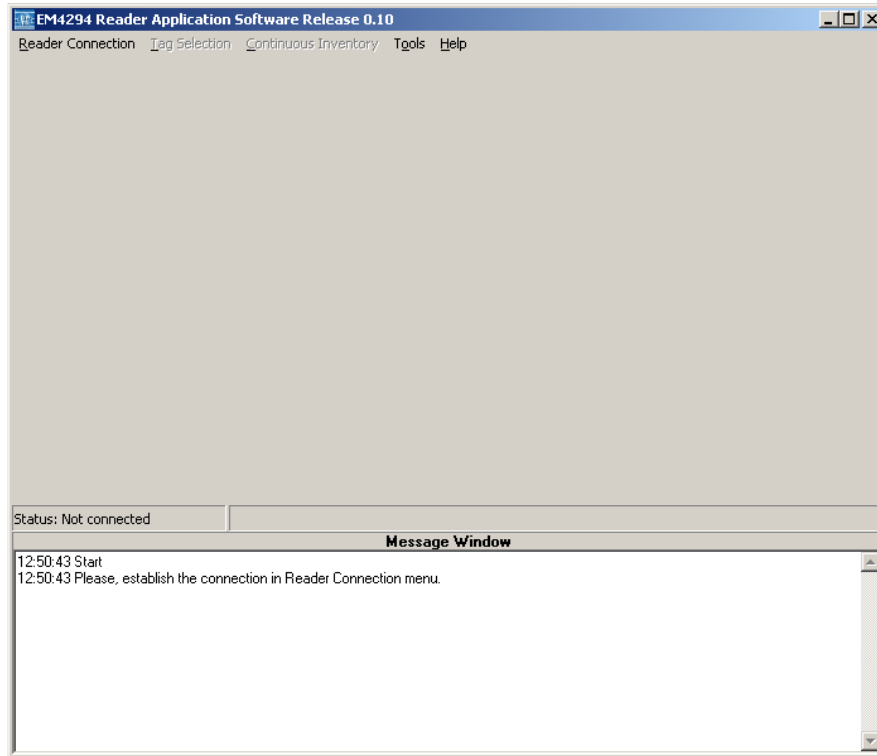

Figure 1 Graphics User Interface

Status Bar

For all the commands, the first field of status bar displays a Status (result) of the recent command execution;

- **O.K.**
- **ERROR**

Message Window

Message Window displays the commands and their responses actually processed by the application software. Although the message window can be hidden, it displays information about the results of the commands.

4. Operation Selector

Until the communication with the EMDB410 Reader is established, following menus are available;
- Reader Connection menu
  - o Connect - to establish the connection
  - o Exit - to exit the application software
- Tools menu
  - o Message Window - to clear or show/hide the message window
  - o Bootloader - to upload a new firmware to the EMDB410 Reader
- Help menu

As soon as the communication with the EMDB410 Reader is established, the current firmware family number is obtained. The firmware family number defines what communication menus are to be enabled for further usage.

Current firmware family numbers are two;
- Family 161 - the firmware (main_V15693.hex) implements ISO15693 EM tags and EM4006 tag command set only
- Family 162 - the firmware (main_V14443.hex) implements ISO14443 Type A and Type B tag command set only

To swap the firmware family in the EMDB410 reader, the opposite firmware family needs to be uploaded by the bootloader feature.

The communication menus comprise;
- Tag Selection menu (enabled for firmware family 161 only)
  - o EM4233 2k - to communicate with EM4233 ISO15693 Transponder in 2k version
  - o EM4233 SLIC - to communicate with EM4233 ISO15693 Transponder in SLIC version
- Tag Selection menu (enabled for firmware family 162 only)
  - o ISO14443 Type A - to get ISO14443 Type A Transponder UID
  - o ISO14443 Type B - to get ISO 14443 Type B Transponder UID
- Continuous Inventory menu (enabled for firmware family 161 only)
  - o ISO 15693 Inventory - to inventory the ISO15693 tags present in the RF field
- Tools menu
  - o EM4294 Advanced Configuration - to change current EM4294 configuration
  - o SIM Crypto Key Management - to update the user key for EM4035 secure communication (enabled for firmware family 161 only)
  - o Reader Version - to re-read firmware version
  - o Switch Off the RF Field - to switch the RF field off

When communicating with ISO15693 transponders, it is recommended to start in ISO 15693 Inventory menu.

4.1. EM4233 Transponder

Following notes describe typical usage of the EMDB410 Application Software graphics user interface for EM4233 ISO 15693 tags.

There are two versions of EM4233 chip; EM4233 2k version, and EM4233 SLIC version. EM4233 SLIC is reduced version of EM4233 2k version, it is equipped with 1Kb of FLASH memory and does not provide High Security mode and QuietStorage feature.

The reader is generally not aware which version is actually present in the RF field. Hence, for generic communication either Tag Selection menu item can be selected. Please, use the Continuous Inventory menu 1TS Continuous Inventory function to determine what actual version the tag is.

Further information on this page assumes the EM4233 2k version is used.

Setup

1. Select a Tag Selection -> EM4233 2k menu (see following figure)
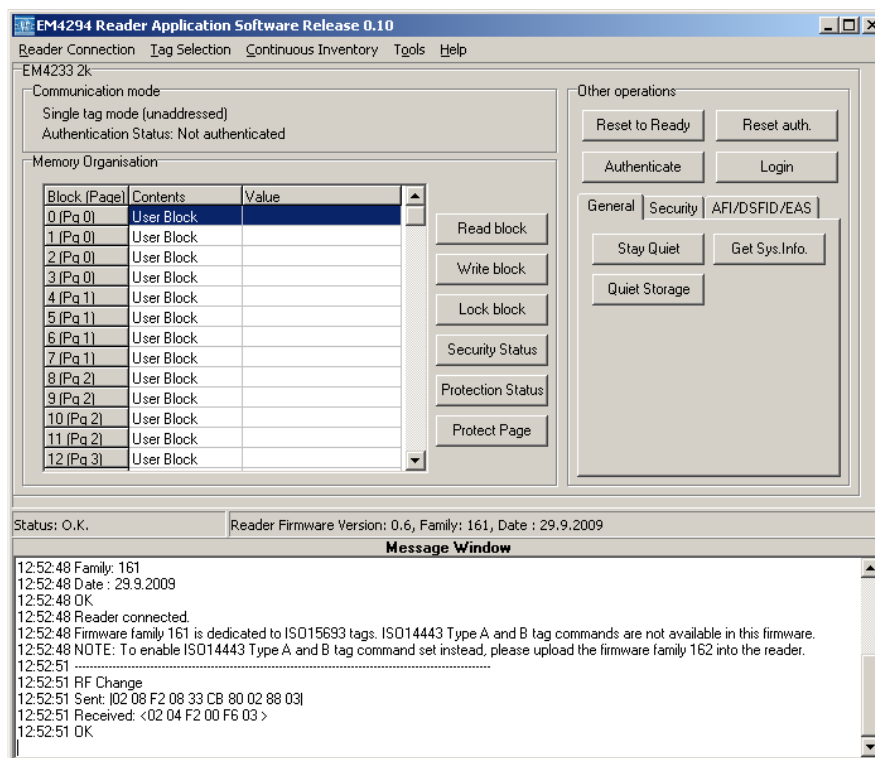2. Place a single EM4233 tag on the tag label on EMDB410 Reader

Figure 2 EM4233 communication frame

EMDB410 application software does not perform any antenna self-tuning. To communicate with small size tags (i.e. non ISO card size transponders) use the ISO 15693 Inventory menu first.

Read block

1. Click into the Memory Organization table to select a block to be read.
2. Click on Read block button

Up to 6 blocks can be read at once when selected as continuous block in the Memory Organization table.

Write block

1. Click into the Memory Organization table to select a block to be written to
2. Click on Write block button
3. Enter the new block value
4. Click on OK button

Security status

1. Click into the Memory Organization table to select a block which Security status is to be read.
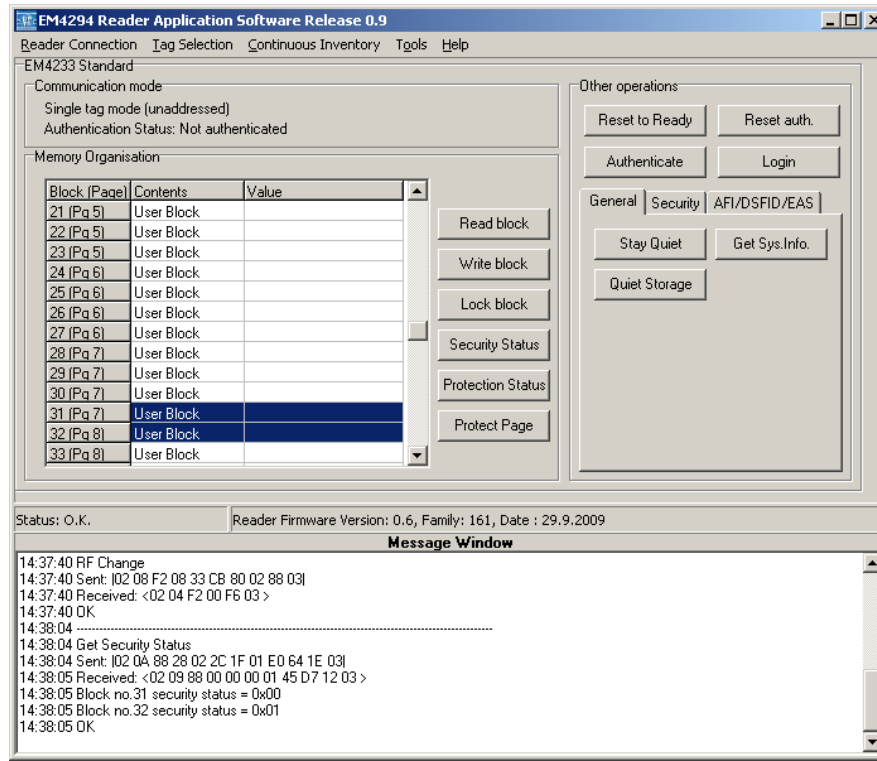2. Click on Security status

Figure 3 EM4233 Security status of 2 blocks

Security status is defined for each block specifying whether the block is locked against the writing forever. Security status of up to 16 blocks can be read at once.

Lock block

1. Click into the Memory Organization table to select a block to be locked against writing forever
2. Click on Lock block button

Protection and Security mode, Authentication/Login

Beside standard Lock block mechanism, EM4233 also provides a read/write protection of blocks. While the lock mechanism applies always according to ISO 15693 standard, protection applies only when the tag is not authenticated to/logged in (further noted as normal mode).
In other words, blocks protected against reading are returned as 0 values when read in normal mode, blocks protected against writing cannot be written in normal mode.
EM4233 is always configured to provide one of two security modes; High Security mode (mutual authentication process using reader's SIM crypto is required) and Low Security mode (Login command with a password is required). After the successful authentication (tag is configured in High Security mode) or login (tag is configured in Low Security mode), as appropriate, the protected blocks are accessible (this state is further noted as secure mode).
Protection status is defined for each page (4 blocks).

Note that SIM Crypto key no.2 is used as the EM4233 key for Authentication in High Security mode. Use Tools SIM Crypto Key Management menu item to upload the corresponding Key value into the SIM Crypto key no.2. See also SIM Crypto Key Management help page.
Note that asserted standard Lock block status overrides the Protection status against writing, such blocks cannot be written even when in secure mode.
Note that EM4233 SLIC version tag provides Low Security mode only.

Protection Status

1. Click into the Memory Organization table to select a block which Protection status is to be read.
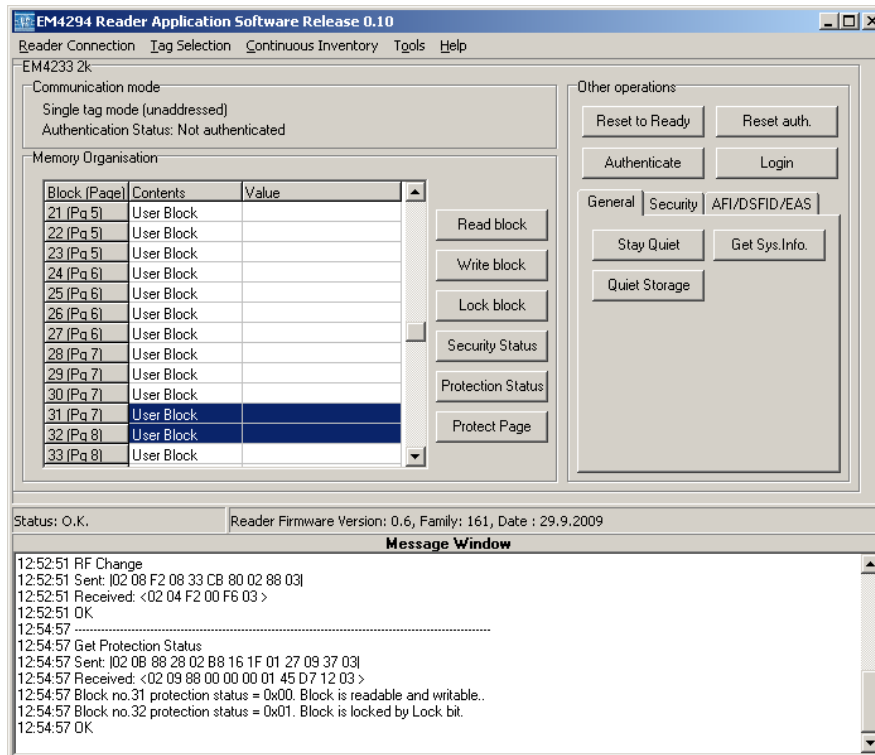
2. Click on Security status

Figure 4 EM4233 Protection status over 2 blocks (in 2 adjacent pages)

Protect Page

1. If not authenticated/logged, click on either Authenticate (tag is in High Security mode) or Login (tag is in Low Security mode) button in Other operations group.
2. Click into the Memory Organization table to select a block which Page Protection is to be updated.
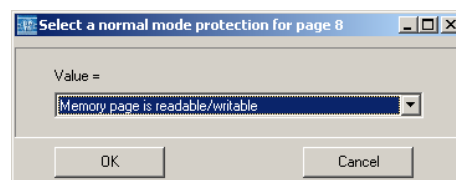3. Select a new page protection in the combo box.

Figure 5 Page Protection selection

4. Click on OK button
5. Verify the new protection by clicking on Protection Status button

Other operations - Security management

All the Security management functions that can be found in Security tab in Other operations group require the tag is in the secure mode.
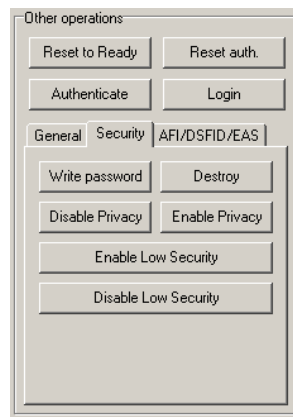
Figure 6 Other operations Security controls

Other operations - Security management - Key/Password update

Click on Write Password button to enter a new 96b key/password into the tag. The new password successfully written into the tag applies as soon as the tag is reset. In case of High Security mode, enter the Tools SIM Crypto Key Management menu to update the key value in the SIM Crypto too.

Note that the Low Security mode password occupies the 32 least significant bits of 96b key/password value.
Note: it is recommended to always save the new value in some notepad.

Other operations - Security management - Destroy

Click on the Destroy button to destroy the tag. This function requires the addressed mode.

Other operations - Security management - Privacy

Click on Enable Privacy button to set the Privacy mode. The Privacy mode updated in the tag applies after the tag is reset. When the tag's Privacy mode is enabled the tag responds only to Authentication/Login command (according to the tag's Security mode configuration). After successful authentication/login, the tag enters Secured mode and accepts all the command set.
The tags included in this kit have the Privacy usually disabled. Click on Disable Privacy button to disable the Privacy mode.

Other operations - Security management - Change the Security mode

When the tag is in High Security mode, use Enable Low Security button to switch the tag into Low Security mode.
When the tag is in Low Security mode, use Disable Low Security button to switch the tag into High Security mode.
Whenever the switch command is executed successfully the tag switches the Security mode configuration immediately and goes into the Normal mode.
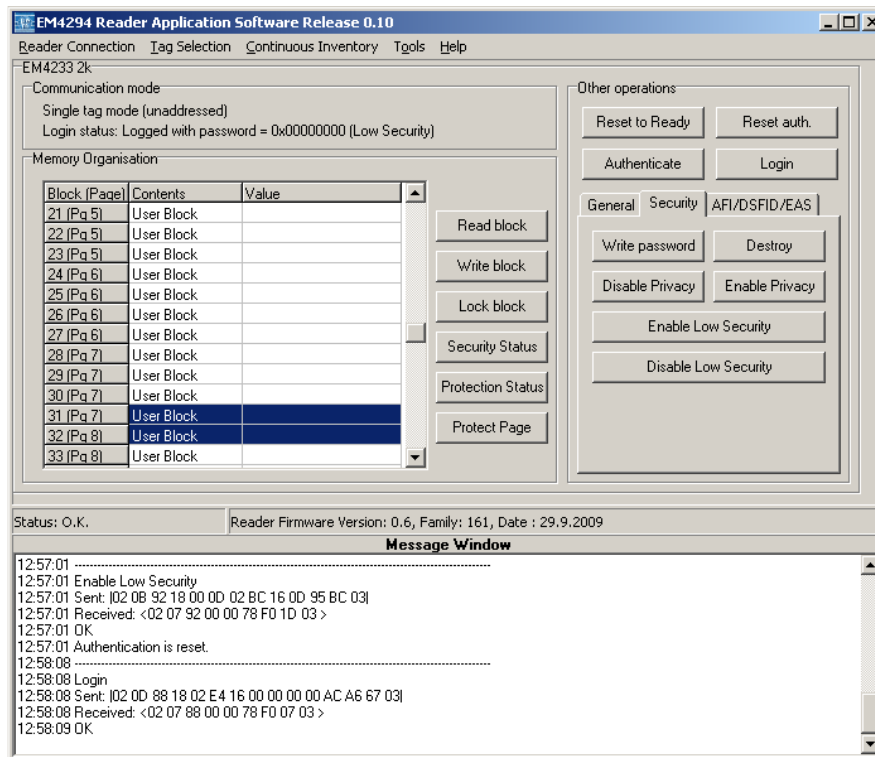
Figure 7 Low Security enabled

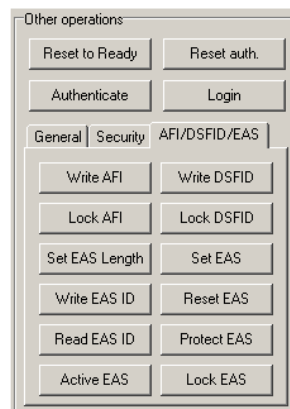**Other functions - AFI/DSFID/EAS**

Figure 8 Other operations AFI/DSFID/EAS controls

Tag AFI, DSFID, EAS, and EAS ID value can be modified and/or locked by means of the corresponding buttons.

Other functions - AFI/DSFID/EAS - EAS

EM4233 tag with enabled EAS feature returns the EAS memory contents of preprogrammed length upon ActiveEAS command reception. Furthermore, a sub-set of all the tags in the RF field that shall respond to this command can be further selected by specifying the EAS ID. By default, EAS feature is disabled.

Other functions - AFI/DSFID/EAS - Configuring EAS length and contents

EAS response can be 32b, 64b, 128b, or 256b long. For selected length, the EAS response contents shall be programmed into the end of the User memory. It is not the starting address but the ending address that all these EAS contents values have in common. Use Write Block and Read Block buttons to write the selected EAS response contents into the appropriate User memory locations;

- EM4233 2k version 32b EAS value is stored at address 51
- EM4233 2k version 64b EAS value is stored at addresses 50 and 51 (see example below)

- EM4233 2k version 128b EAS value is stored at addresses 48, 49, 50, and 51
- EM4233 2k version 256b EAS value is stored at addresses 44 to 51
- EM4233 SLIC version 32b EAS value is stored at address 31
- EM4233 SLIC version 64b EAS value is stored at addresses 30 and 31
- EM4233 SLIC version 128b EAS value is stored at addresses 28, 29, 30, and 31
- EM4233 SLIC version 256b EAS value is stored at addresses 24 to 31

Note: EMDB410 reader firmware currently does not support 256b EAS responses.
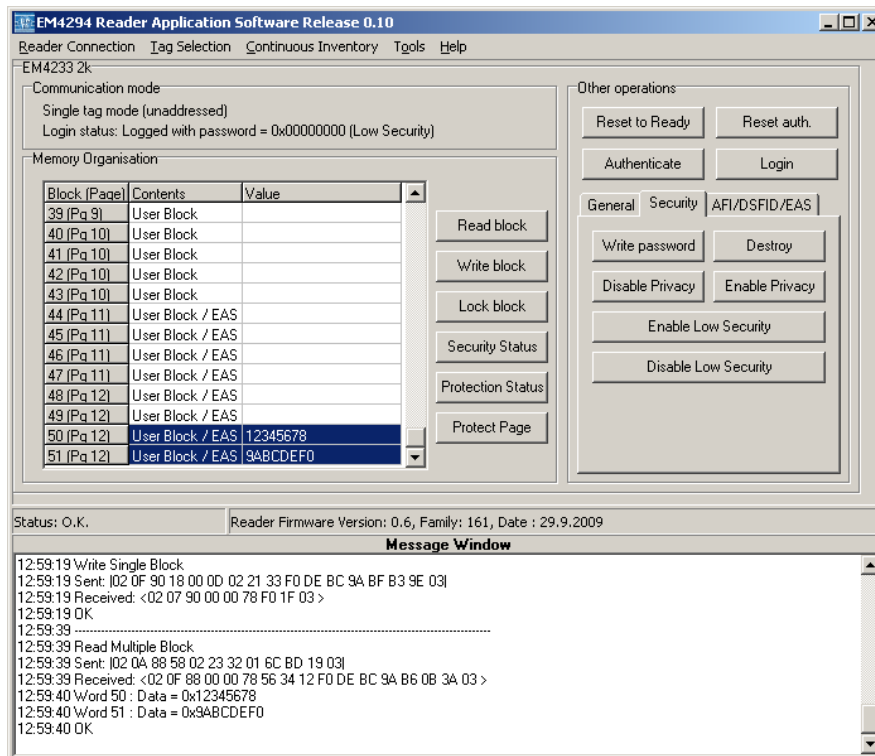
Figure 9 64b EAS value configuration example (EM4233 2k version)

1. Click on Set EAS Length button.
2. Select the EAS Length
3. Click on OK button
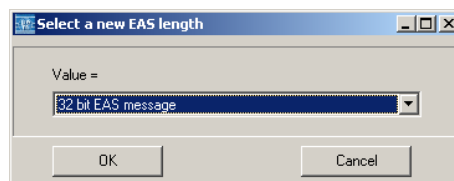
Figure 10 EAS length configuration selection

Note: Locked EAS configuration cannot be further modified.
Note: Protected EAS configuration can be modified only in Secured mode (i.e. Authentication/Login is required).

Other functions - AFI/DSFID/EAS - Configuring EAS ID

EAS ID is the 16b value that can be used to select a subset of the tags in the RF field – those with matching Least Significant Byte of EAS ID (8b EAS ID mask) or whole EAS ID value (16b EAS ID mask).
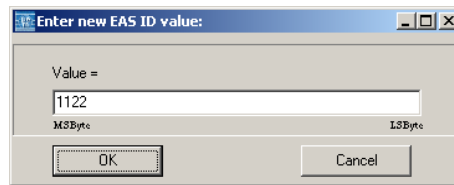
1. Click on Write EAS ID button.

Figure 11 New EAS ID value selection

2. Enter the new EAS ID value
3. Click on OK button

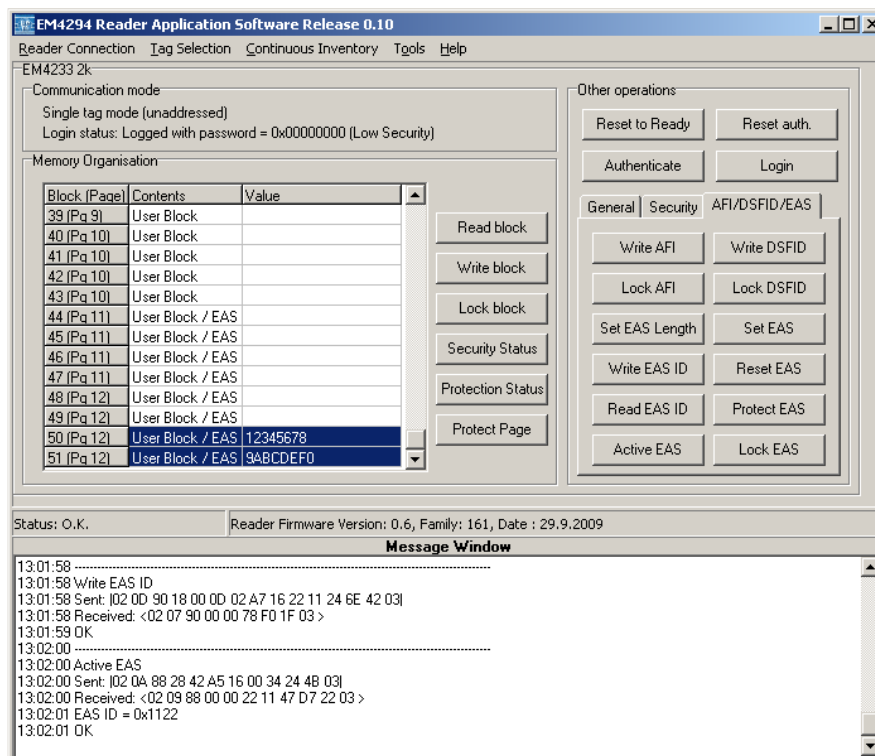To read or verify the EAS ID value, click on Read EAS ID button.

Figure 12 EAS ID Read example

Other functions - AFI/DSFID/EAS - Active EAS

The tags with enabled EAS feature can be queried to return their EAS code by means of ActiveEAS command.

1. Click on Active EAS button
2. Select the expected EAS response length and click on OK button. Note that the reader does not know how long the EAS response is hence the correct value needs to be supplied.
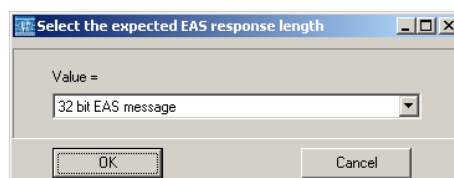

Figure 13 Active EAS expected EAS length selection

3. Select the EAS ID Mask to apply and click on OK. No EAS ID Mask means all the tags shall respond, 8b or 16b EAS ID Mask will select just a sub-set of tags with matching EAS ID Mask value programmed.
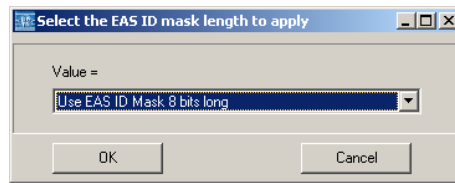
Figure 14 Active EAS ID Mask length selection

4. In case that 8b or 16b EAS ID Mask is to be applied, enter the corresponding EAS ID Mask value and click on OK button. Note that 8b EAD ID Mask is the least significant byte of the EAS ID value.
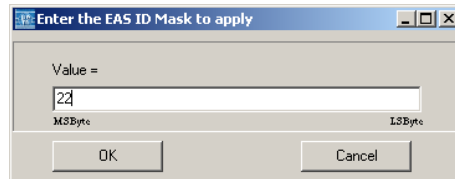

Figure 15 Active EAS 8bit ID Mask selection
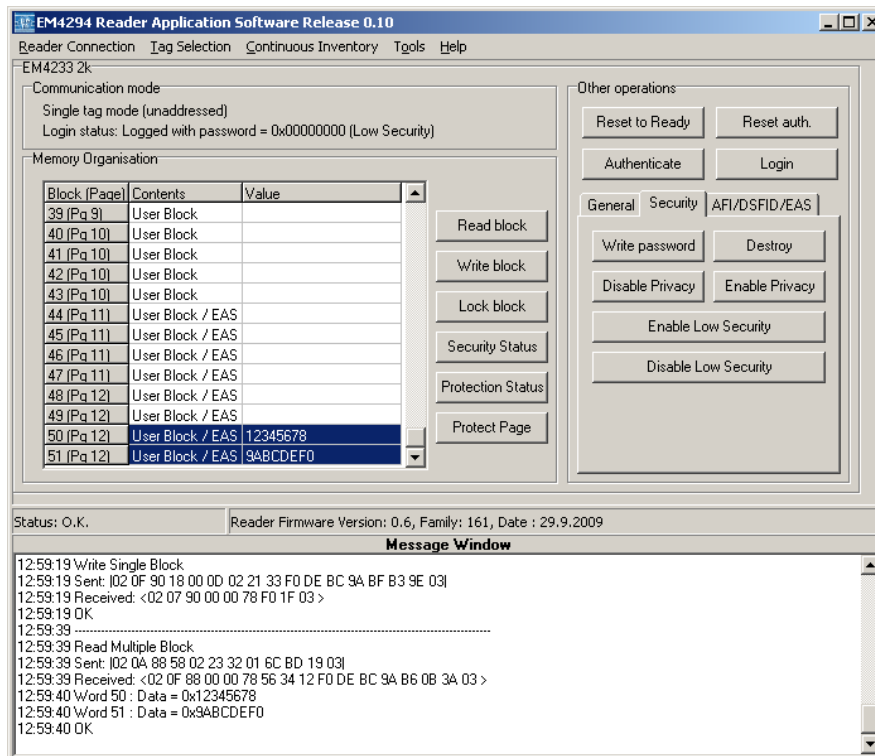
Finally, received EAS value is displayed.

Figure 16 Active EAS 64bit EAS response example

Note: Write Block command treats the block number in Little Endian format. However, EAS values are rather a stream of byte numbers, thus the EAS response byte ordering is reversed within the block boundary to Write Block command values entered.

4.2. ISO 14443 Type A Transponders

This chapter describes the usage of the EMDB410 Reader Application Software graphics user interface for single ISO 14443 Type A tags. This section assumes the ISO14443 firmware family 162 is uploaded into the EMDB410 reader by means of bootloader feature.

Setup
1. Tag Selection menu, select -> ISO14443 Type A menu (refer to Figure 17 ISO14443 Type A Communication Frame)
2. Place a single ISO14443 Type A tag on the tag label of the EMDB410 Reader

Get Type A UID

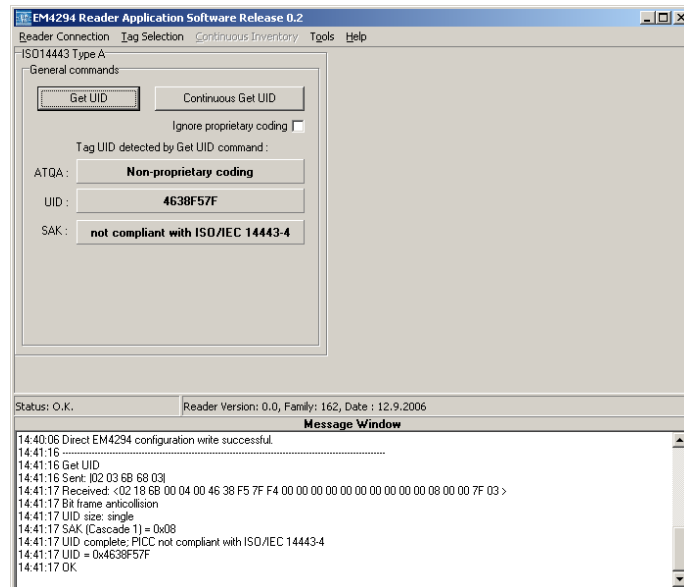1.   Click on Get UID button to identify the tag in the RF field

Figure 17 ISO14443 Type A Communication Frame

By invoking Get UID function, EMDB410 Reader performs a Type A Select sequence for single tag only. Also, EMDB410 Reader accepts tags with ATQA proprietary coding bits set to zero only. The Type A tags with proprietary coding are not identified (e.g.; refer to Figure 18 Proprietary coding of Type A Transponder).
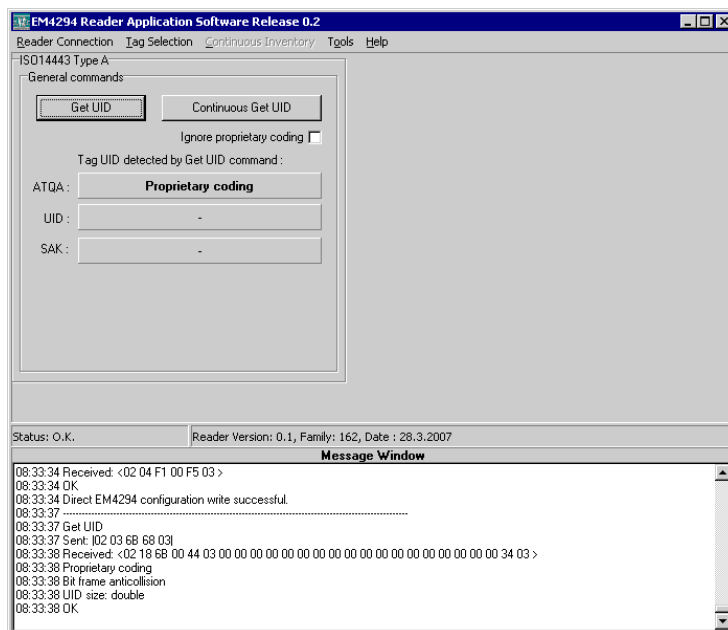

Figure 18 Proprietary coding of Type A Transponder

Some ISO14443 Type A tags may support standard Selection Flow even if the proprietary coding flags are set. To obtain the UID of such tag, check the Ignore proprietary coding box and run Get UID command again.

4.3. ISO14443 Type B Transponders

This chapter describes typical usage of the EMDB410 Application Software graphics user interface for single ISO 14443 Type B tag. This section assumes the ISO14443 firmware family 162 is uploaded into the EMDB410 reader by means of bootloader feature.

Setup

1. Tag Selection menu, select -> ISO14443 Type B menu
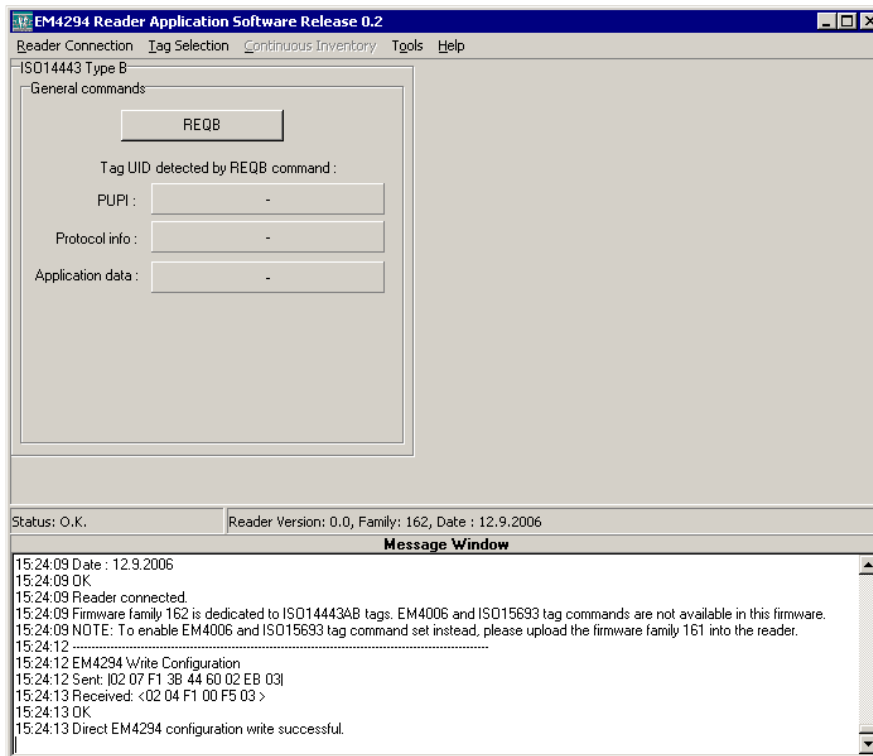2. Place a single ISO14443 Type B tag on the tag label on EMDB410 Reader

Figure 19 ISO14443 Type B Communication Frame

Get Type B UID

Click on REQB button to identify the tag in the RF field (refer to Figure 19 ISO14443 Type B Communication Frame)

4.4. ISO15693 Inventory

This chapter describes typical usage of the EMDB410 Application Software graphics user interface to inventory the ISO15693 tags placed inside the RF field.

Setup

1. Continuous Inventory -> ISO15693 Inventory menu
2. Place one or more ISO15693 tags on the tag label on EMDB410 Reader
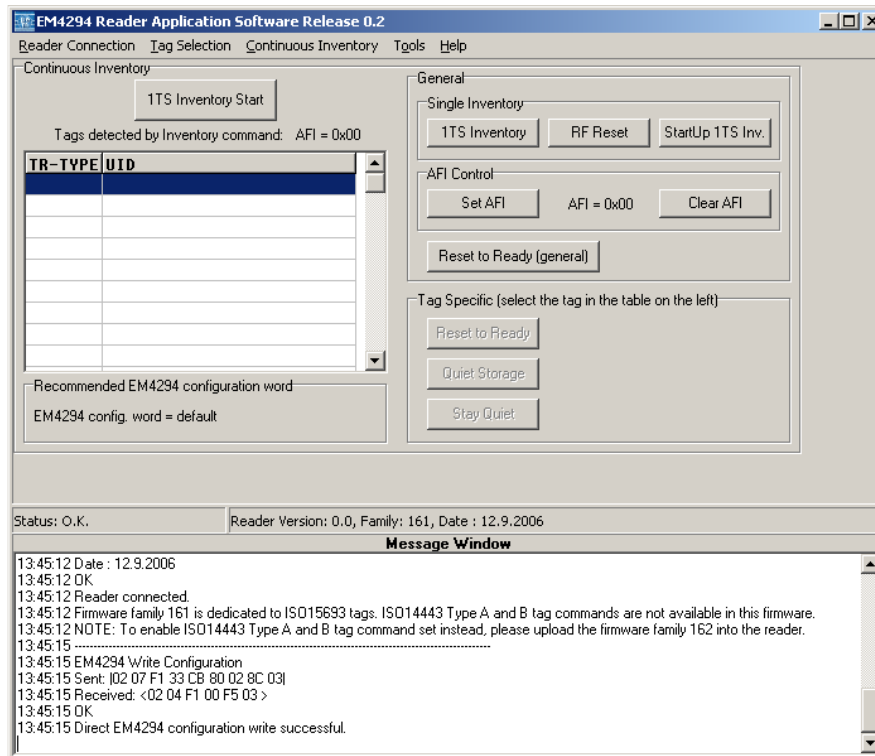

Figure 20 ISO15693 Continuous Inventory Communication Frame

Continuous Inventory

1. Click on 1TS Inventory Start button to identify the tags in the RF field. Found tags are displayed in the table of detected tags. Inventory process is repeated until stopped by clicking on the same button
2. Optionally, click on Set AFI button to change an AFI value of inventory process

AFI value allows the selection of an appropriate set of ISO15693 tags that have this AFI value set. Click on Clear AFI button to clear the AFI value to 00h, AFI value set to 00h means all the tags are to be identified by next inventory process. (Refer to the ISO15693 documentation about various AFI families and sub-families.)
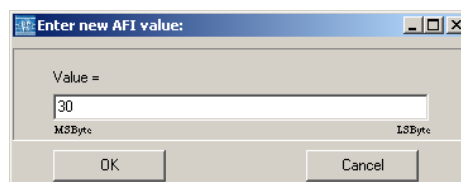

Figure 21 AFI Modal Window

Note: After Inventory process, the identified tags are switched to the Quiet state. Therefore, the RF field is reset automatically before each Inventory process so that the tags are identified continuously.

Single Inventory

1. Stop the Continuous Inventory process if it is running
2. Click on 1TS Inventory button to identify the tags in the RF field, such found tags are displayed in the table of detected tags

Identified tags are switched to the Quiet state (refer to EM4233, EM4034, or EM4035 datasheet), and any following invoking of 1TS Inventory will not detect them again (see following figure). To be found by next inventory process, the tags can be reset by clicking on RF reset button.
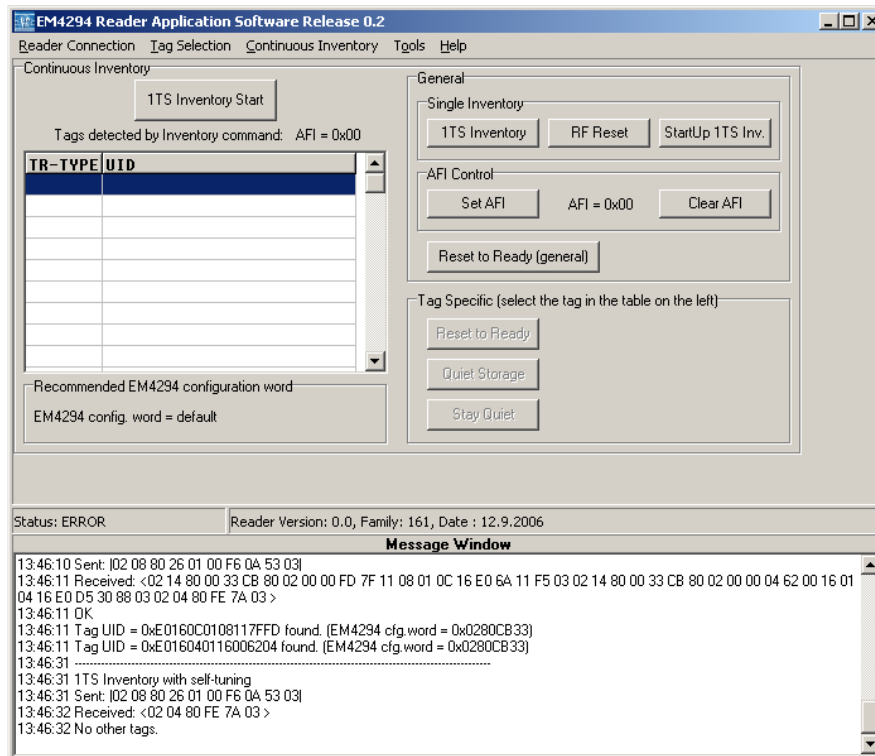

Figure 22 Single Inventory of tags in Quiet state

Small size transponders and recommended EM4294 configuration word

Current EMDB410 Reader firmware performs the ISO15693 Inventory process with antenna self-tuning. Whenever the low data reception level is detected during the inventory process, the EMDB410 Reader reconfigures the EM4294 AFE with alternative configuration word expecting the reception level becomes more sufficient. Such feature allows the detection of small size transponders (i.e. non ISO card size transponders) that need alternative antenna tuning to achieve sufficient data reception level.

Note: It is recommended to communicate with single small tag at once.

The configuration words obtained from Inventory process are examined resulting in the "Recommended EM4294 configuration word";

• EM4294 config. word = default – no alternative configuration is necessary. Any communication is possible without limitations.
• EM4294 config. word = 0xYYYYYYYY – single alternative EM4294 configuration word is to be used automatically during communication with particular tags (addressed mode, refer to next paragraph). To communicate with such single tag in unaddressed mode, retrieved EM4294 configuration word needs to be applied manually using   Tools -> EM4294 Advanced Configuration menu after entering appropriate communication frame.
• Message "Please, communicate with single tag." is displayed – more than one alternative EM4294 configuration has been found. In such case, generally, the tags influence themselves too much avoiding the sufficient reception level from all the tags when using single communication word. Encountering this message, please, remove the transponders from the EMDB410 Reader but one.

Communication with one particular tag

1. Stop the Continuous Inventory process if it is running
2. Choose one of the following
   a. Select a tag by clicking on its UID in the table of detected tags. If the tag is either EM4233 2k or EM4233 SLIC, EM4034, EM4035, or EM4135, Tag Specific panel is enabled (see figure below) and specific functions can be invoked (Reset to Ready, Quiet Storage, Stay Quiet)
   b. By double-clicking on one UID of the EM4233 2k and EM4233 SLIC in the table of detected tags, the tag respective communication frame is displayed and a communication to this tag is available in Addressed mode. There, to return to Continuous Inventory frame, simply select a Continuous Inventory -> ISO15693 Inventory menu again
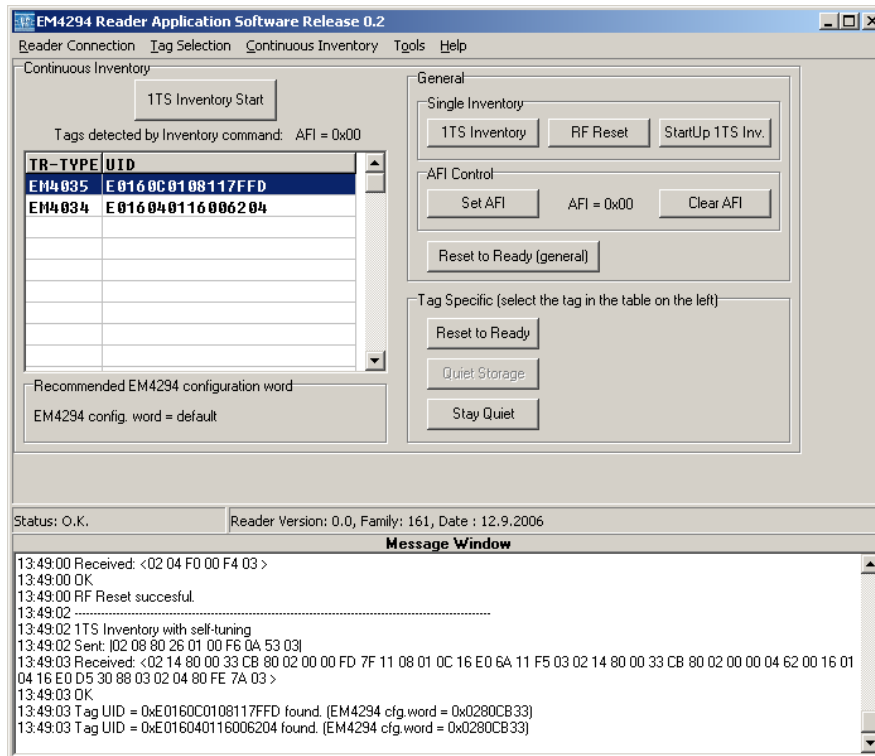

Figure 23 Enabled tag specific controls

4.5. EM4294 Advanced Configuration

EMDB410 Reader application software allows a change of current EM4294 configuration word. When entering a selected tag communication frame, default EM4294 configuration word is sent to the EMDB410 Reader automatically. Hence, it is not necessary to change the configuration word manually.

Setup
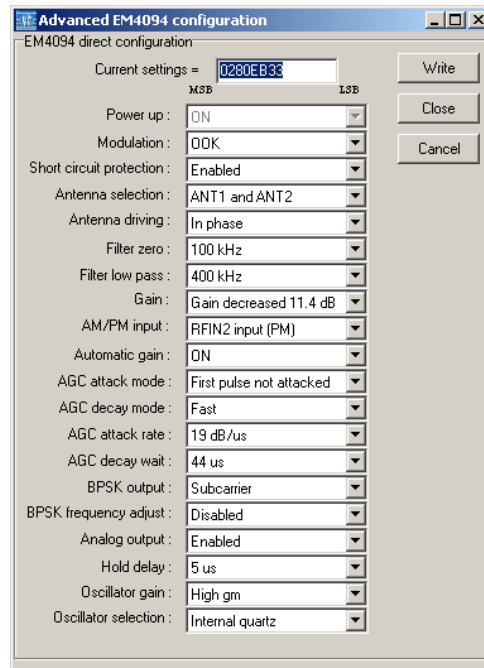1. Select a Tools -> EM4294 Advanced Configuration menu

Figure 24 EM4294 Advanced Configuration Modal Window

Click on Write button to apply the selected EM4294 settings.

4.6. EM4294 Crypto Engine Key Management

To authenticate successfully, the key value in the SIM crypto engine must match the key value stored in the EM4233/EM4035 transponder. In order to support both EM4233 and EM4035 transponders at the same time, EM4233 High Security mode key value shall be stored at SIM crypto Key no.2 position.

Setup
1. Select a Tools -> SIM Card Key Management menu - automatic SIM card detection is performed automatically
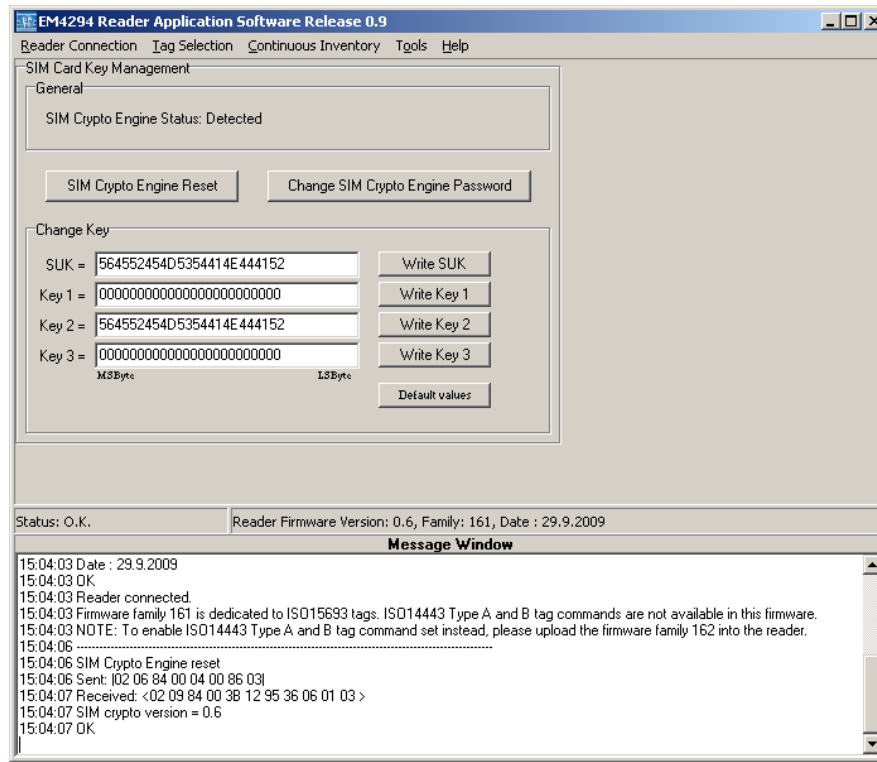

Figure 25 SIM Card Key Management Communication Frame

Key update
1. Enter a particular key new value into its edit box
2. Click on appropriate Write Key or Write SUK button
2. Enter the SIM card password that is required for changing the key content

After updating a key value, any further authentication with this new key is performed. To authenticate to the factory programmed EM4233/EM4035 transponder, update the Super User Key value in the SIM crypto obtained by clicking on Default values button.

Warning: No error message is asserted when applying incorrect password, the key change is simply not applied.

Change SIM card password
1. Click on Change SIM Card Password button
2. Enter the current and the new password

4.7.   EM4294 Crypto Engine Auxiliary Commands

Following auxiliary commands are available in the SIM Card Management -> Auxiliary Commands menu;
- ❑   Get Chip Supplier Serial Number – returns the unique serial number of EM4294 AFE
- ❑   Get Random Number – returns the random number generated by the EM4294 crypto engine feature
- ❑   Read/Write User Memory – provides the access to the free user memory within the EM4294 crypto engine
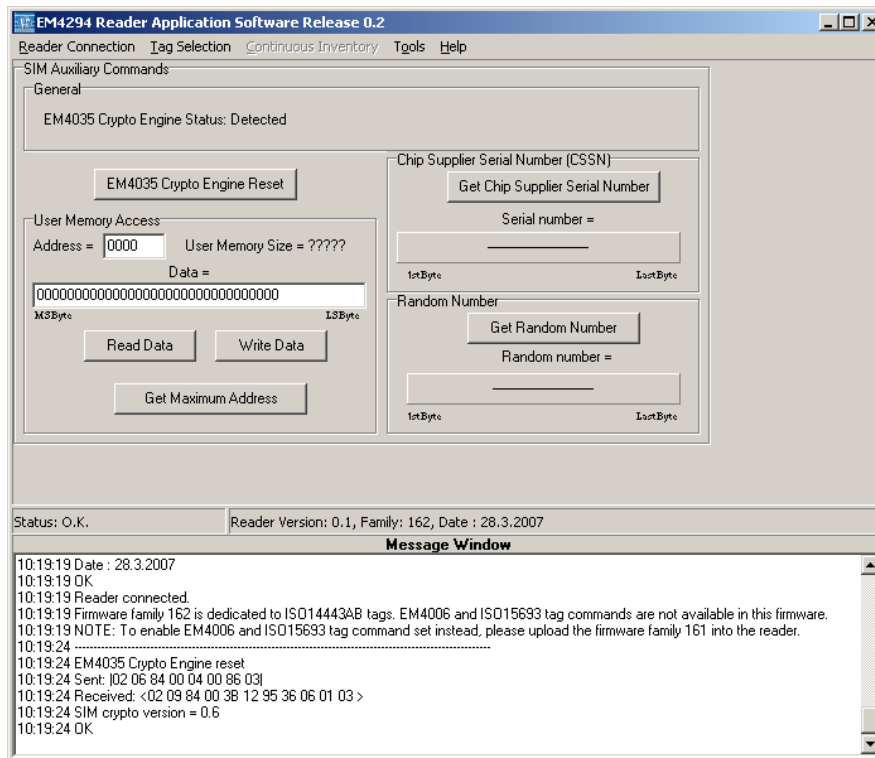

Figure 26 Crypto engine Auxiliary Command window

Note: User memory access into the EM4294 crypto engine user memory area is limited to the certain maximum address limit depending on the actual EM4294 crypto engine firmware version and sub version. Click on Get Maximum Address button to obtain the actual user memory size.

4.8. Bootloader

Following notes describe a process of uploading a new firmware into the EMDB410 Reader. It is possible to upload the firmware without performing an establishment of the connection.

<u>Setup</u>

1. Connect the USB cable to the EMDB410 Reader
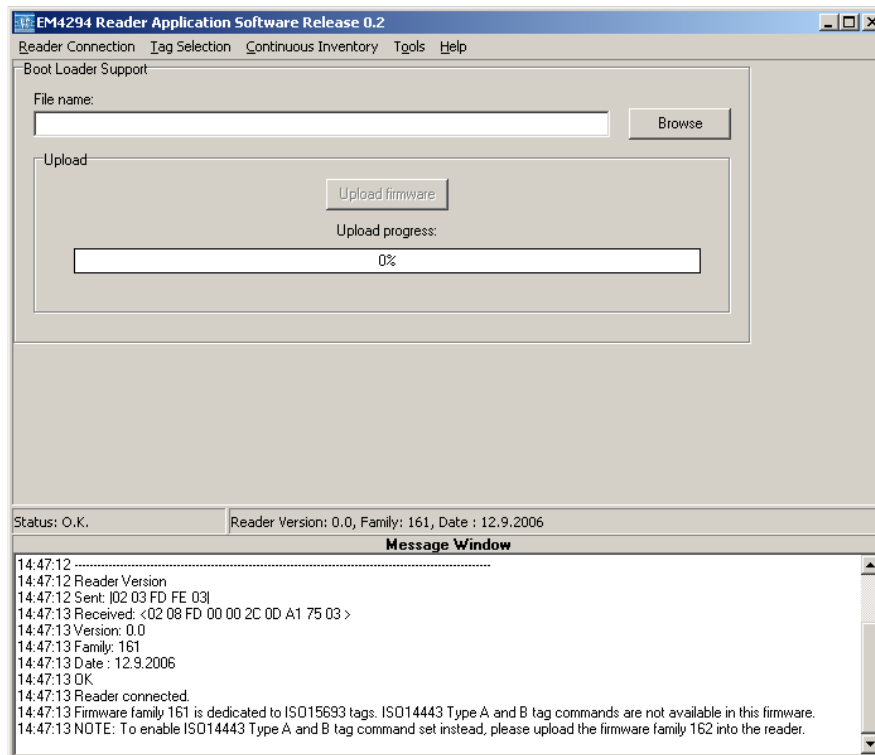2. Select a Tools -> Bootloader -> Import firmware menu

Figure 27 Bootloader Communication Frame

Click on Browse button to enter a complete path of the new firmware hex file. If the firmware hex file is imported to the PC memory successfully, Upload firmware button is enabled.

<u>Upload firmware</u>

1. Click on Upload firmware button
2. If the EMDB410 Reader connection is not yet established, the EMDB410 application software asks for the COM port – select the appropriate port the EMDB410 is connected to

Upload firmware process lasts about 1 minute. If the firmware is uploaded successfully, the connection is established automatically (see following figure). In the second item of the status bar, current firmware version, family, and date of creation is displayed.
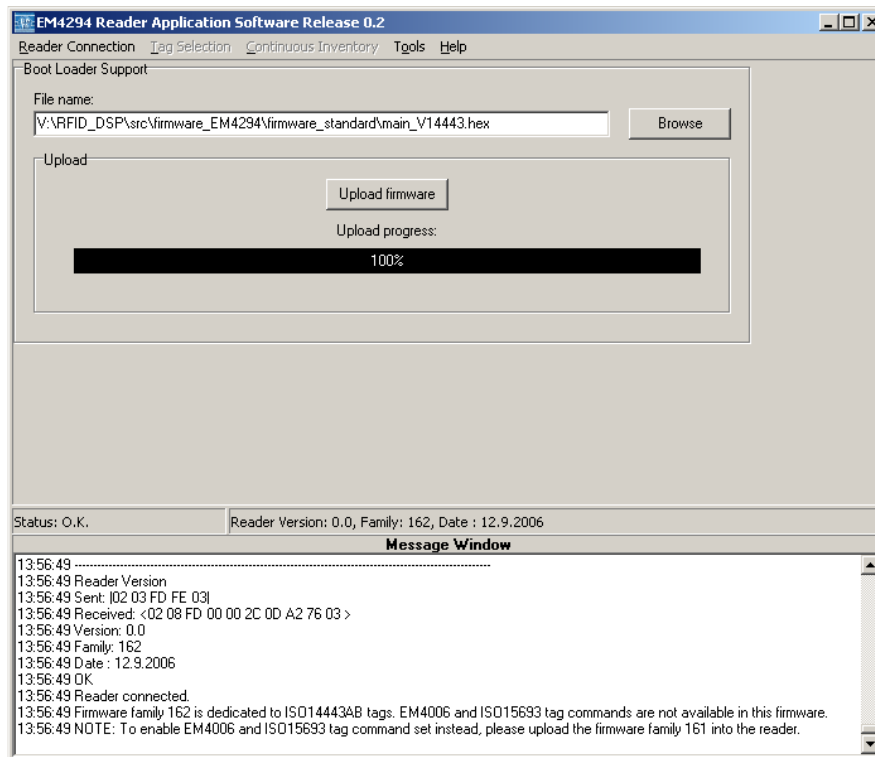
Figure 28 Firmware is uploaded successfully

Note: When the new firmware is being uploaded into the EMDB410 reader, it is the application part that is being modified only. The firmware bootloader part remains unchanged. In case the bootloader function is interrupted accidentally and the reader remains silent, i.e. no further communication is possible, please disconnect and connect back the USB cable. By means of such reconnection, the EMDB410 firmware is reset and switched into the bootloader mode. Then, click on Upload firmware button to repeat the upload again.

In other words, when the firmware application part is corrupted, always reconnect the USB cable and enter the Tools -> Bootloader -> Import firmware menu directly without entering the Reader Connection menu item.

5. Error handling

There are three kinds of errors;
- Reader Communication errors (e.g.; USB cable has been disconnected accidentaly and the EMDB410 reader does not answer at all) – check the USB cable is connected correctly, then the connection has to reestablished unconditionally (Reader Connection -> Connect menu)
- Tag Communication errors – insufficient RF energy (e.g.; tag response has CRC error) - try to change the position of the tag or mutual position among the tags in respect to the reader antenna
- Tag Communication errors – protocol issue (e.g.; no response from the tag) – try to determine whether the tag is the type it is considered to be or whether the tag is in some altered mode it is not exepected to respond