STid
Electronic Identification

SECARD

USER MANUAL

Designed in France
Made in France

www.stid-security.com

Acknowledgment

Welcome to the world of high security!

You have purchased SECard software; it will allow you to program configuration and user cards.

We thank you for the confidence you place in us and hope that this solution developed by STid will satisfy you.

We remain at your disposal for any questions about using this software on range of products.

We look forward to seeing you for more information on our website www.stid-security.com.

STid Team

Introduction

This manual is composed of two parts:

Part 1: Detailed description of all the functionalities

Part 2: Technical

Summary

SECARD

USER MANUAL

Part 1: Detailed description of all the functionalities

Designed in France
Made in France

www.stid-security.com

I. Informations

I. 1 - PC requirements

- A PC with operating system: Windows 7, 8 or 10 or Windows server 2012r2.
- USB available communication port.
- 50 MB min of free disk space.

I. 2 - USB Key Content

- FTDI USB Driver for Windows 7, 8.x and 10.
- SECard Version 3.x.x.
- MorphoCBM Driver.

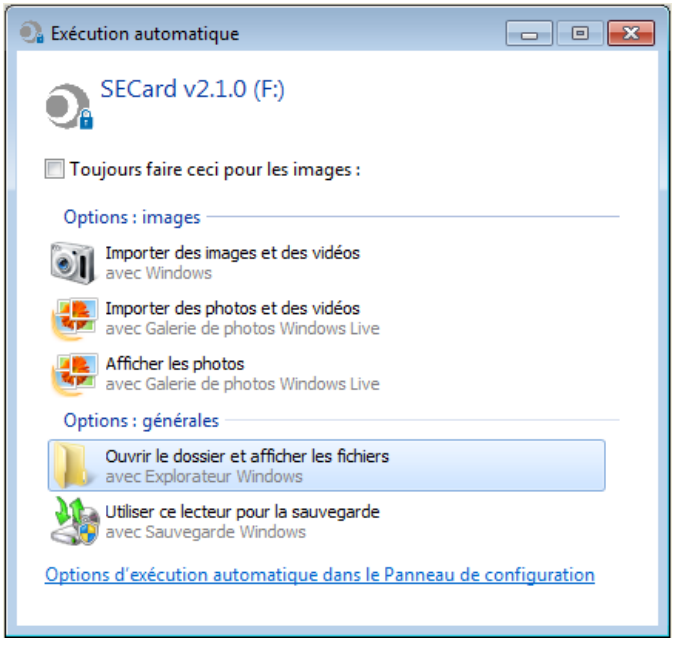
I. 3 - Hardware required *Modification v3.6*

USB 13.56 MHz & Bluetooth® STid encoder Ref. ARCS-W35-E-BT1-5AA-1.
Z10 firmware version required (Identification on the back of the encoder).

To create SCB/OCB: MIFARE® DESFire® EV2/EV3 8ko not locked in EV2 mode

I. 4 - Windows Installation

- Insert the SECard USB Key on an USB port of your PC.
- Wait for the automatic opening of the browser window.



- Launch SECard V3.x.x_setup.exe.
  - Follow the instructions on the screen.

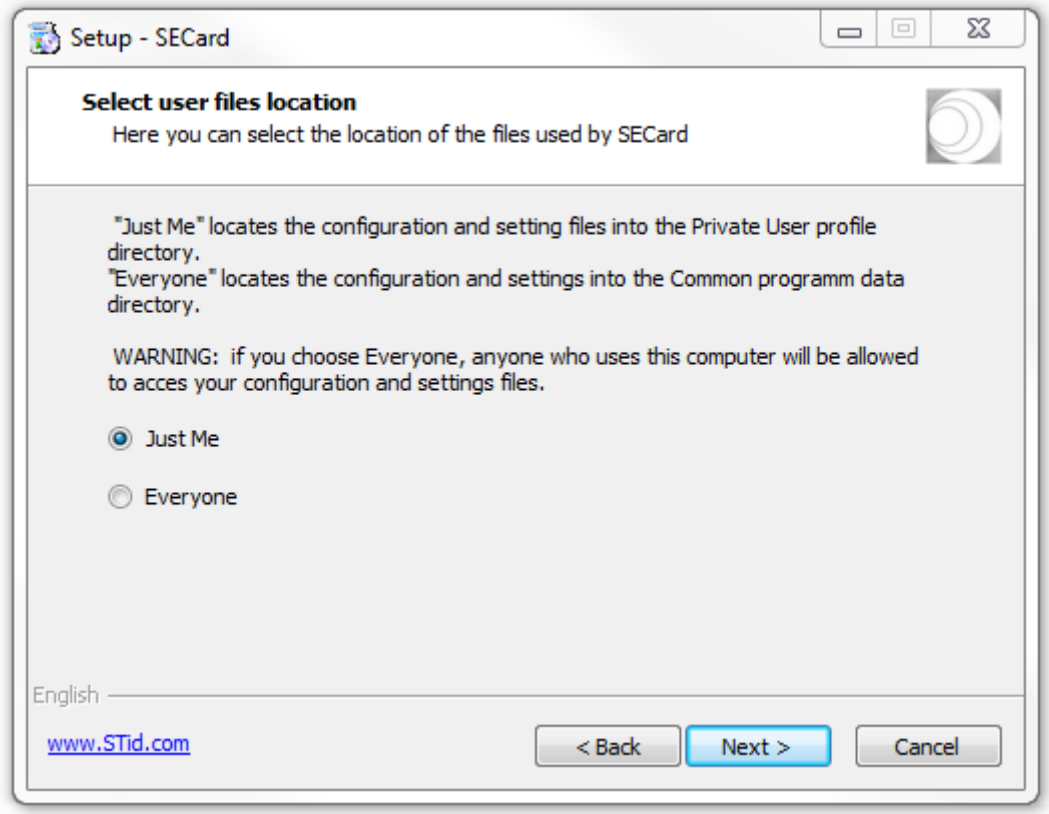
Notes:

If FTDI driver has already been installed on the PC during a previous installation of SECard uncheck FTDI driver in installation wizard

If biometry has already been installed on the PC during a previous installation of SECard uncheck biometry in installation wizard

- Location of user files.

With SECard V3.x.x the settings files will be installed in the directory containing the executable (as previous SECard version) **and** in the following directories depending on user choice.



✓ « Just me » : user files are saved in:

../Users/userXX/STid/SECard v3.x.x.x/

In this case files are only accessible to the userXX or to the Administrator.

✓ « Everyone » : user files are saved in :

../ProgramData/STid/SECard v.x.x.x/

In this case files are accessible to everybody.

Note: To change the location of user files, open the .gcf file located in the same directory as SECard.exe and change the value of the [File]

Location=X ;X=0 for « Just me », X=1 for « Everyone »

```
[File]
Settings=.\SECard.pse
Location=0
```

I. 5 - Compatibility *Modification v3.6*

❖ Firmware / SECard version

This SECard version (3.6.x) provides compatibilities tables between SECard versions and firmware versions of readers.

The objective is to configure with a unique tool SECard WAL* and Architect® readers.

SECard version	SCB version	Firmware version
V2.0.x	V7	Z01
V2.1.x	V8	≥ Z02
V2.2.x	V9	≥ Z04
V3.0.x	V10	≥ Z05
V3.1.x	V11	≥ Z07
V3.1.x	V12	≥ Z08
V3.3.x	V13	≥ Z11
V3.4.x	V14	≥ Z14
V3.5.x	V15	≥ Z16
V3.6.x	V16	≥ Z17

SECard version	OCB version	Firmware version
V3.3.x	OCBv3	≥ Z05
V3.4.x	OCBv4	≥ Z08
V3.5.x	OCBv5	≥ Z09
V3.6.x	OCBv6	≥ Z10

* To configure standard readers and WAL with firmware SZ188F21, use a SECard version < v3.3.x and refer to SECard User Manuel v6.4.

(1): When an SCB (Standard, WAL, ARC, ARCs) without Bluetooth® configuration and with DESFire configuration* is presented to an ARCS Bluetooth®, a Bluetooth® configuration, named “DESFireAuto”, is activated for the Bluetooth®. All parameters (size, number of key, site code…) are the same as DESFire parameters.

Important note for Architect® readers

With SECard it is possible to configure all the features of the Architect® (RFID, keypad, touch screen, biometric, Bluetooth®, Matrix / QR code module) on a same SCB. The reader will recover in SCB only the parameters that are necessary. To disable a feature, disconnect the subassembly and represent the SCB

* DESFire configuration: private ID with one file, data type: Raw and without biometry.

❖ Configuration file / SECard version

	SECard V1.x	SECard V2.x	SECard V3.x
.ese	✓	File converter	File converter
.pse generated with version < 3	x	✓	✓*
.pse generated with version ≥ 3	x	x	✓

Warning*

When a .pse file created with SECard V2.x is loaded and saved in SECard V3.x with a password, it will not be possible to load it again in SECard V2.x.

❖ Configuration card New 3.6

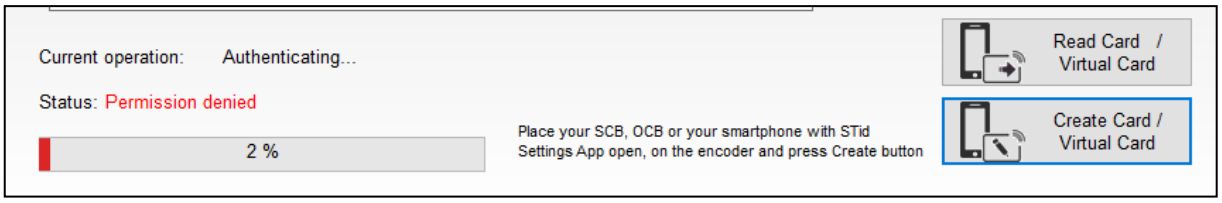
From SECard v3.6, the encoding of configuration cards has been modified.

Result:

SCB V16 badge: re-encoding in an earlier version of SCB IMPOSSIBLE

OCB V06 badge: re-encoding in an earlier version of OCB IMPOSSIBLE

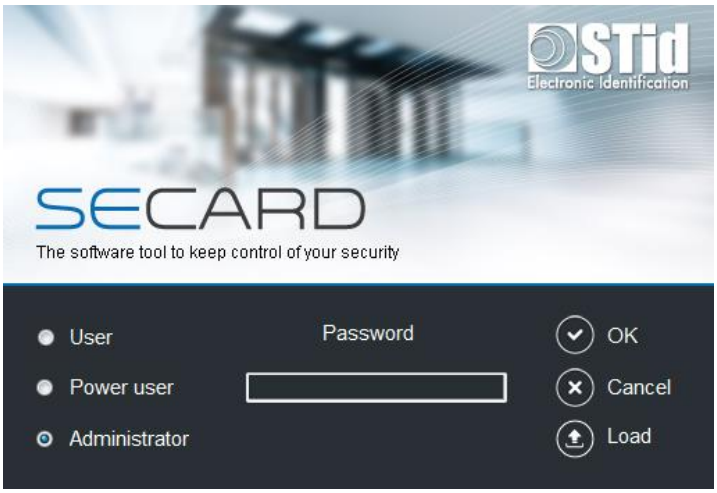
Error message when encoding an SCB v16 to SCB v15 or lower:



I. 6 - Starting SECard software

At first use, the software opens a window to enter the serial number of 32 characters located at the back of the encoder. After recording the number, the software doesn't reiterate this request.

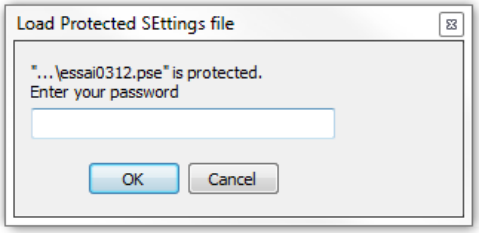
It is possible to install the software on an unlimited number of workstations, but it is only possible to use it with the dedicated encoder (corresponding to the serial number). This number allows SECard to authenticate with the encoder provided in the kit. If you want to order an additional encoder contact the sales department.



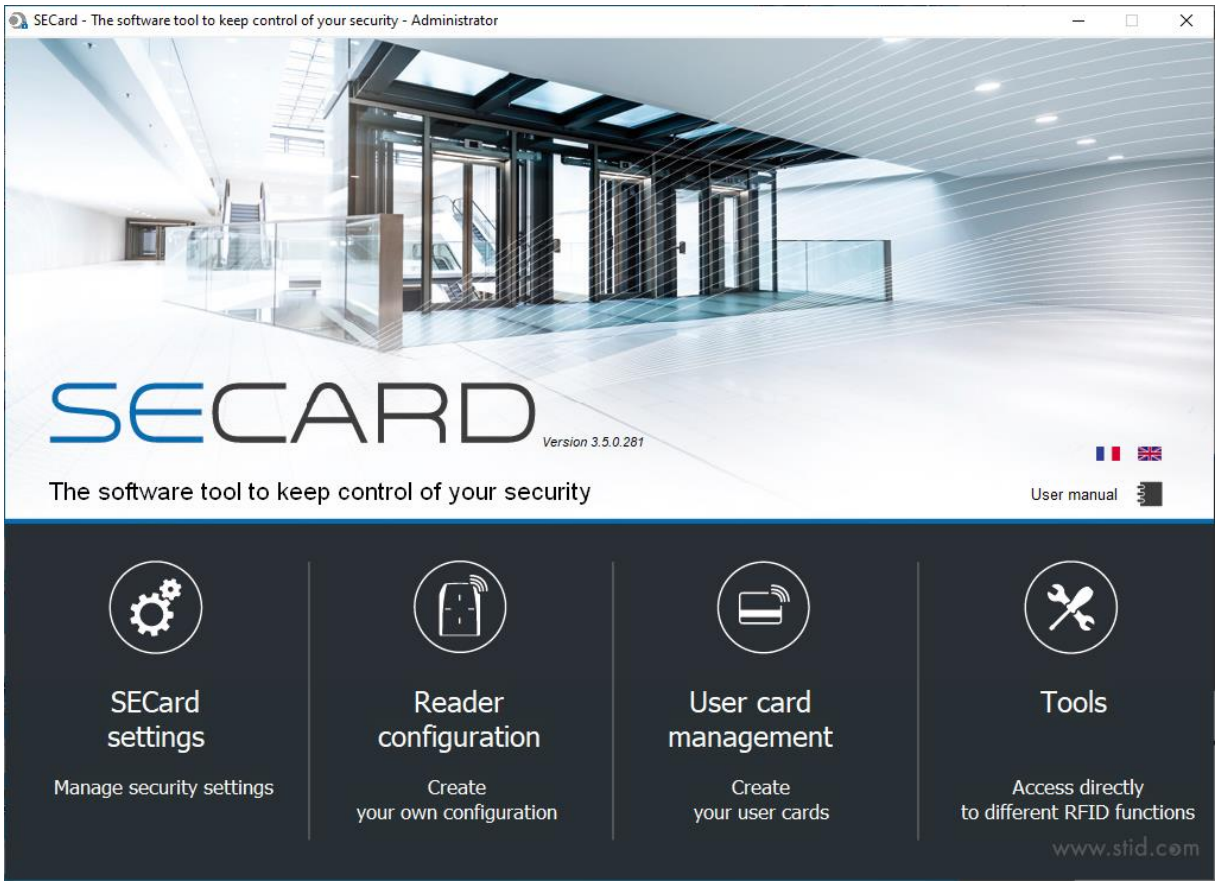
When starting the software, a window appears to enter the login information or to load a specific configuration file.
There are three Access level, managing different permissions within the software. These passwords are saved in the configuration file.

Access level	Default password	Associated rights
Administrator	STidA	Software configuration and use without restriction
Power User	STidP	Configurable by the Administrator
User	STidU	Create user cards

Note: if the following window appears and the password required is not known, press cancel and then use the "Load" button to load another file. The default file is in installation directory.



I. 7 - Overview



❖ The software is divided into four distinct parts:

SECard and encoder settings

Create configuration card

Create user cards

Tools

❖ On the Home page you have the choice of language and the link for user manual.
User manual is available anytime with the F1 key.

❖ The encryption/signature user keys can be filled:

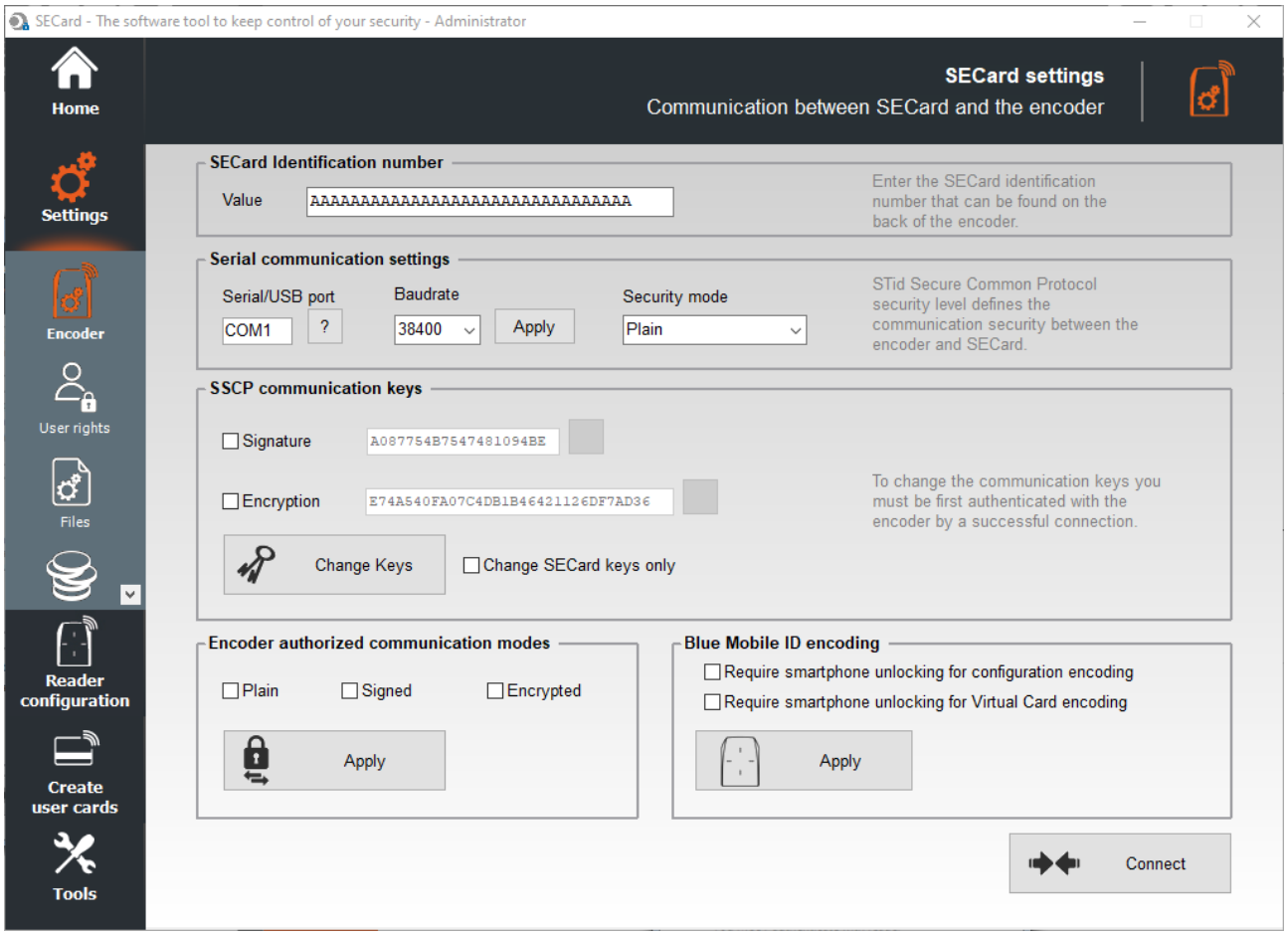
- with a random value by a right click into the field and by choosing “Fill with random value” or by pressing on the keys CTRL+R. The random values have cryptographic level and are generated by ISAAC generator.
- with FF by pressing on the keys CTRL+F or with right click.
- with 00 by pressing on the keys CTRL+O or with right click.

❖ It is possible to Copy / Paste:

- by a right click into the field and by choosing “Copy / Paste”.
- by pressing on the keys CTRL+C / CTRL+V.

II. SECard Settings

II. 1 - Encoder



SECard Identification number

Register the new encoder or check value.

Serial communication settings

Set the communication between encoder and SECard.

- The default baudrate of the encoder is 38400 bauds.
  Caution, this baudrate must be exactly the same as that defined in the software.

  To change the serial communication speed, it is possible to change the value of baudrate. To do this, ensure that communication encoder / SECard is correct, select a baudrate from the drop down "Baud rate" (115200 baud is the maximum baudrate) and click on "apply".

Note:

- If you don't know the correct communication port connected to the reader, it is possible to find it by clicking on the button ?.
  It is necessary to install the USB driver, and it is necessary to connect the reader.

- By pressing the left CTRL key and by using the ? button SECard will search for a connected reader on all serial com. ports and all speed rates. It can take some time.

❖ The communication between SECard software and encoder is done by serial link or USB, it is based on the communication protocol SSCP® (Secure & Smart Communication Protocol).
Encoders integrate public signature algorithms (HMAC-SHA1) and encryption (AES), which can be used to secure data in serial communication between the encoder and SECard.

Communication can be done in four different ways:

- ✓ Plain : Plain communication encoder / SECard
- ✓ Sign : Signed communication encoder / SECard
- ✓ Encipher : Enciphered communication encoder / SECard
- ✓ Sign and Encipher : Signed and Enciphered communication encoder / SECard

Note:
Communication encoder / SECard is more secured when it is used signed and enciphered (Security mode to “Sign and Encipher”). Plain communication (Security Mode to "Plain") is not secured.

SSCP® communication keys

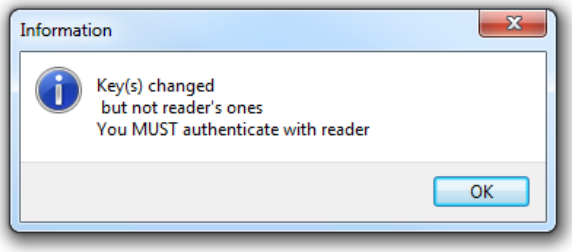
When the communication is Signed and / or Enciphered, the software SECard and encoder use the user default keys:

Signature key: *A087754B7547481094BE*
Encipherment key: *E74A540FA07C4DB1B46421126DF7AD36*

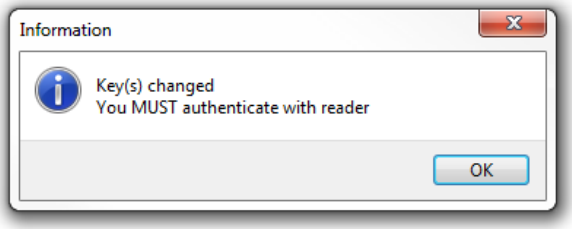
To change the value of these keys, simply check the box "Signature and / or Encipherment" and write the value. Then click-on the button “Change keys”.

Note:

- ✓ The button allows you to restore default value.
- ✓ Software **and** encoder key must be the same so that the two parts can communicate.
- ✓ If the box "Change SECard key only" is checked, only the keys of the software will be changed.



- ✓ When changing user keys and software encoder, a window will appear requesting authentication.



Warning

It is important to know the current user keys.

If lost, it would not be possible to communicate securely with the reader.

Only "Plain" mode would remain usable if it is still authorized.

Encoder authorized communication modes

Authorized / unauthorized communication mode between encoder and SECard.

To authorize a mode, simply click on the button "Set Modes" while checking desired modes. Those that are not checked will be unauthorized.

In order to authorize them again, simply restart the command in the right mode of communication while taking care to validate the desired mode.

Warning

If the plain mode is unauthorized **and** the user keys are lost, it will not be possible to communicate with the encoder.

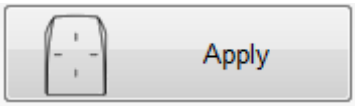
It will be necessary to return the equipment for a factory reset.

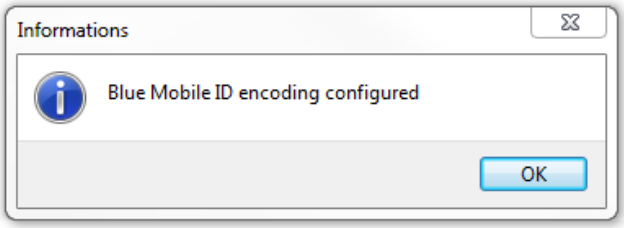
Blue Mobile ID encoding

Configure the Bluetooth® encoder (ARCS-W35-G-BT1-5AA) to authorize or not the encoding of smartphone in standby.

- Require smartphone unlocking for configuration encoding
  If checked, requires that the phone is unlocked to encode configuration.

- Require Smartphone unlocking for Virtual Card encoding
  If checked, requires that the phone is unlocked to encode virtual card.

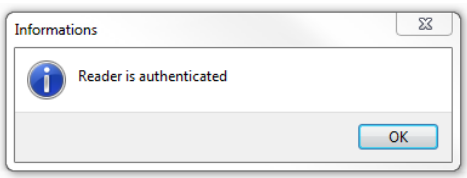
Confirm your selection by clicking on this button: 



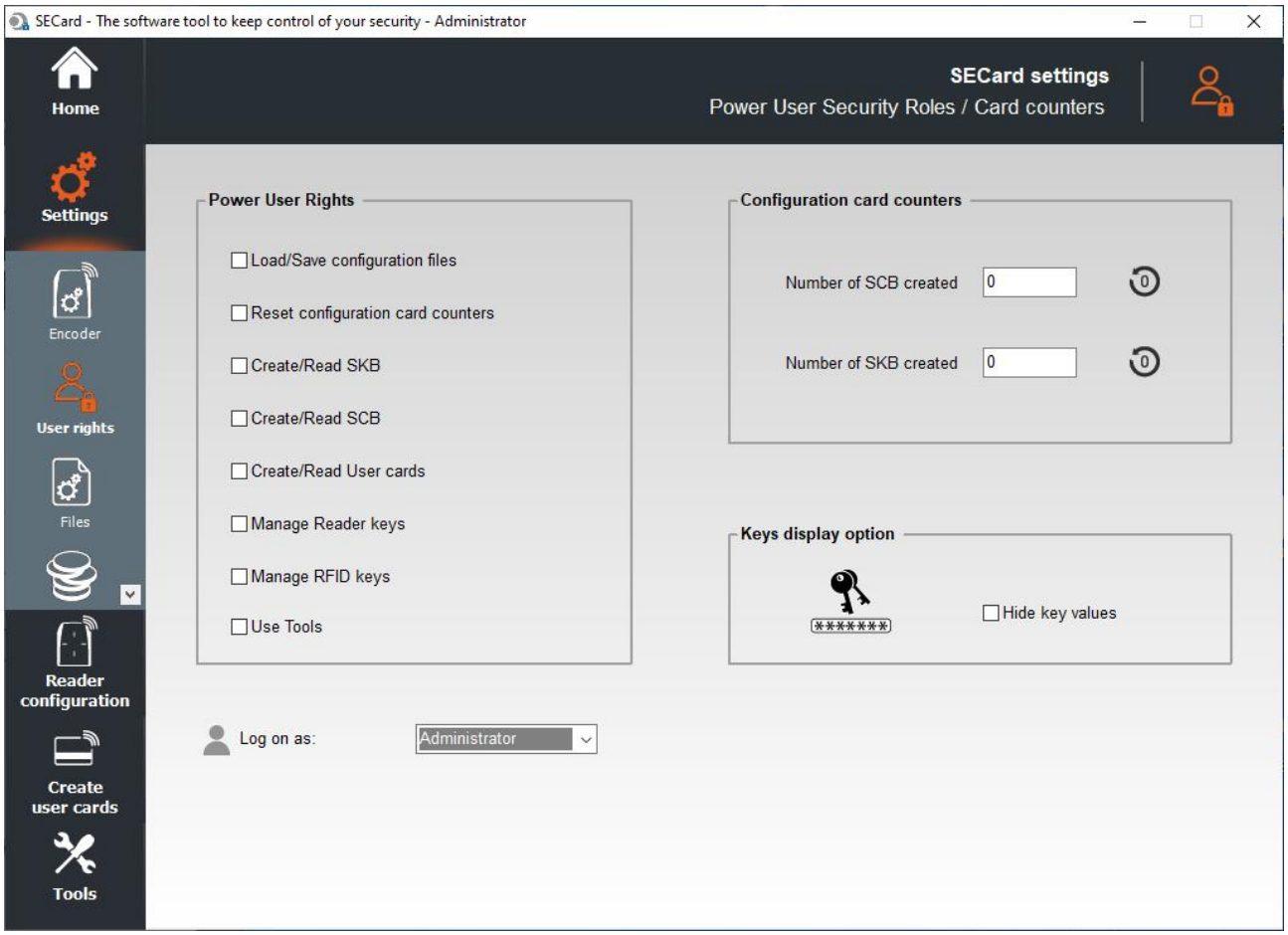
Connect

When powered on the encoder will light the white Led and emit a beep.

To verify the communication parameters with the encoder, use the button “Connect”. If the communication configuration is ok, the encoder will respond with light and sound signals and an acknowledgment window will appear.



II. 2 - User rights



Power User Rights

"Power User" mode is the transition between "*Administrator*" and "User" modes.
The administrator allocates the rights to the power user.

Configuration card counters

Counters display the number of SCB configuration card programmed and the number of SKB card programmed.

These values can be reset through the reset button only by Administrator or Power User if authorized.
Note: these values are saved into the .pse file.

Keys display option

It is possible to hide the values of the keys in their fields.

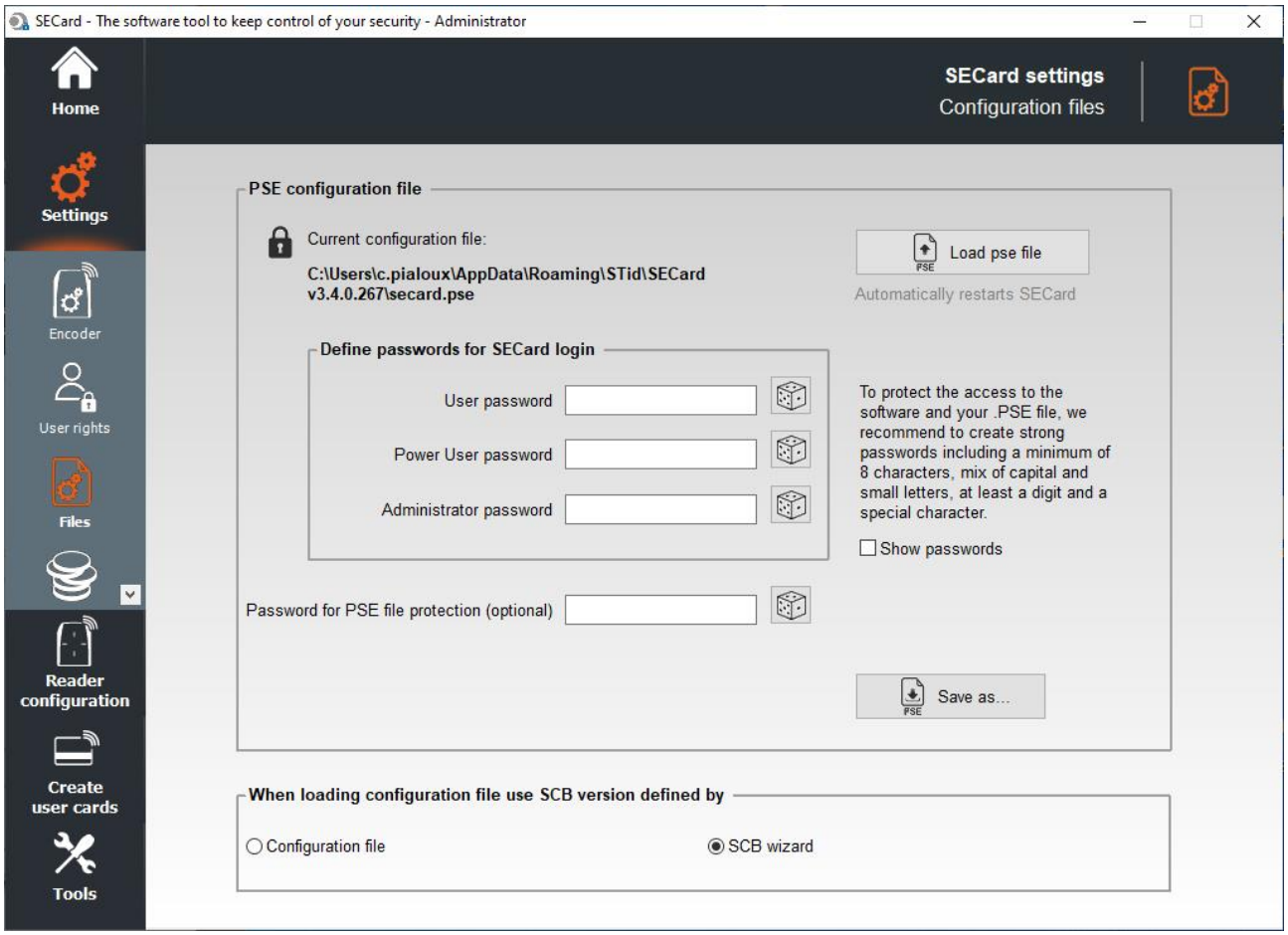
It can be activated by Administrator and remains activated when logged as Power *User* or *User*.

Log on as:

Change the access level.
It is necessary to know the password of the selected level.
Authorized changes:

- Administrator to Power User and to User.
- Power User to User and to Administrator.

II. 3 - Files



When loading configuration file use SCB version defined by

SCB version is contained in the configuration .pse file.
It is possible to:

- Keep the version of SCB by checking Configuration file.
  SECard automatically retrieves the firmware version in the .pse file that was loaded and selected compatible SECard version.

- Choose the SCB version compatible with reader firmware.
  This choice will be made in the SCB Wizard.

PSE configuration file

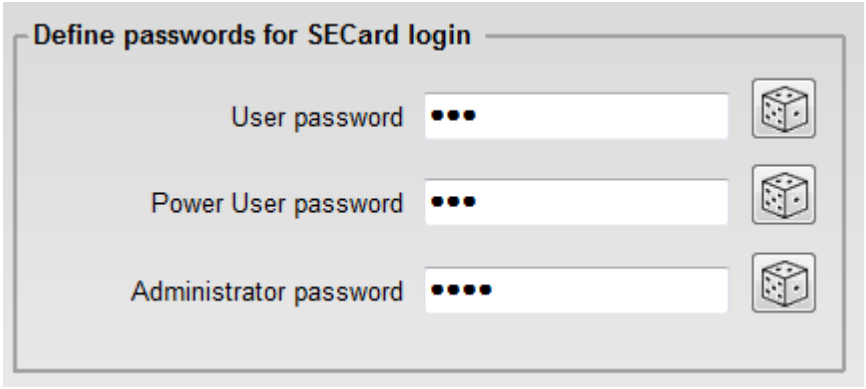
Passwords for SECard login are contained in the configuration file.
This page allows you to save the configuration file containing all the current configuration settings (keys, formats, reader...). You can select a location and password to protect the file.

When loading a configuration file (.pse), SECard automatically restarts.

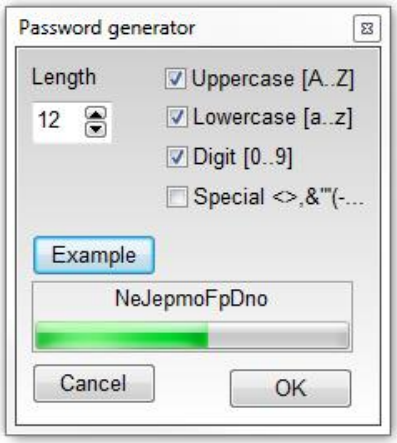
Refer to *T14 - Recommendation to save the configuration files PSE.*

Save as…

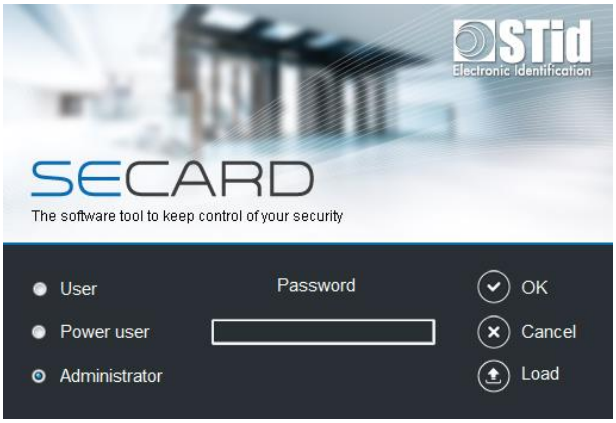
- **Passwords for SECard login**

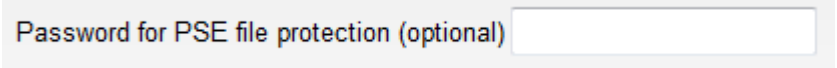


 Random Password Generator Generates Logins:



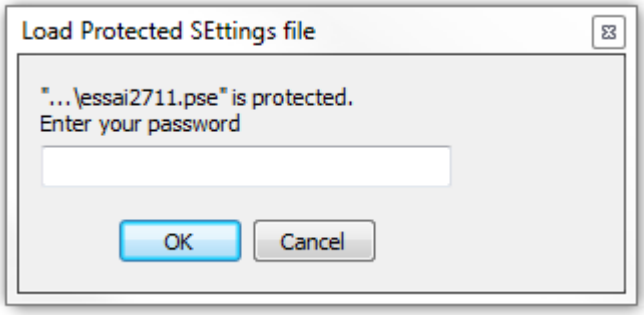
These passwords are needed to open SECard with the corresponding configuration.



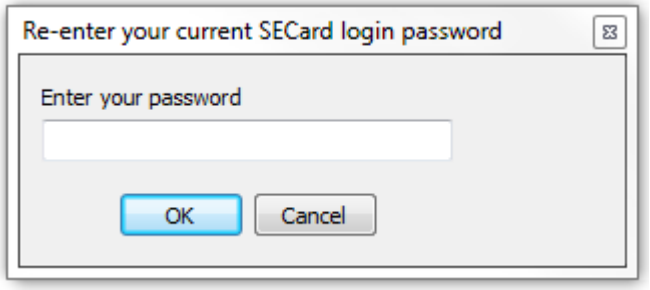
- 

This password is used to protect .pse file. It is optional.

Note: when a .pse protected file is loaded, the window below appears:



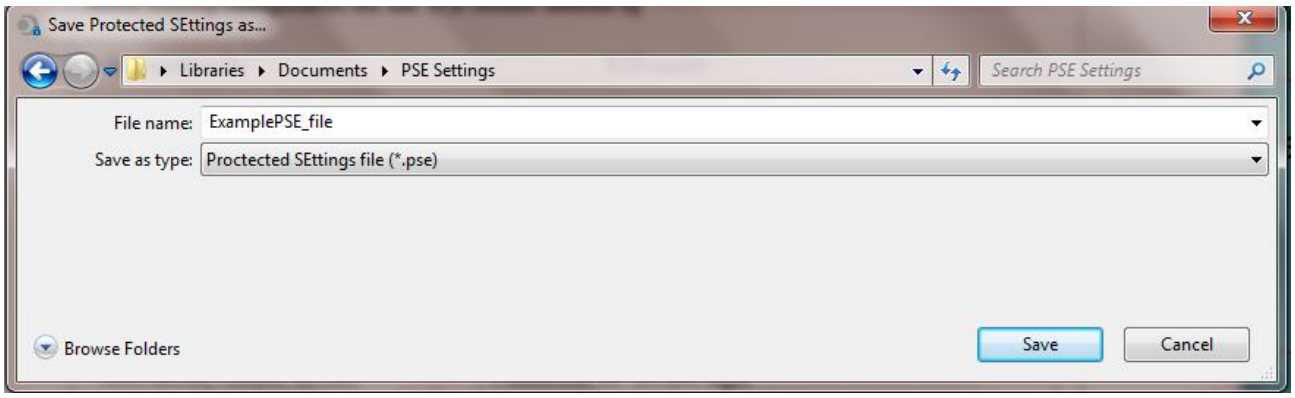
- When you click on Save As…a window asks to re-enter the current **Administrator SECard** login password.



Note: with pse default file, enter STidA.

Note: a Power User with “Load/Save configuration files” rights cannot change the Login Password.

A second window will open allowing you to select the file save location:

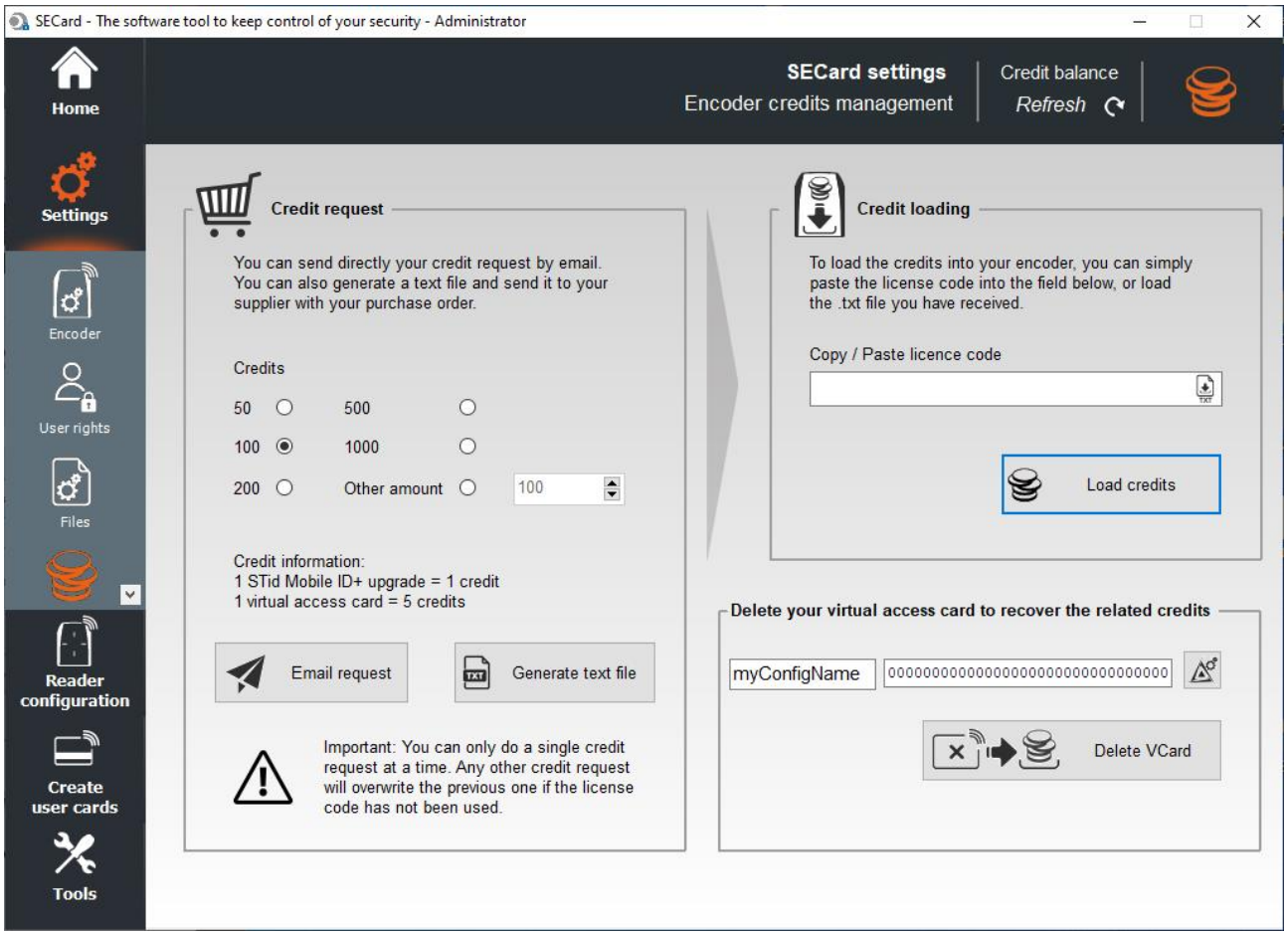


Once name and location entered, click Save.

- 

: To load a configuration file (.pse) into SECard without closed the software.

II. 4 - Credits



To encode virtual user cards in the phone, you have to buy credits that will be loaded into the encoder.

Credits

Links to download the application for your mobile device:

ANDROID Google play

iOS Available on the App Store

STid Mobile ID® can store 3 types of cards:

Credit Request

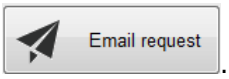
This part of the software lets you make a credit request to your supplier.

Two methods are proposed:

- "Email request" if the station has an internet connection and an e-mail messaging software available.

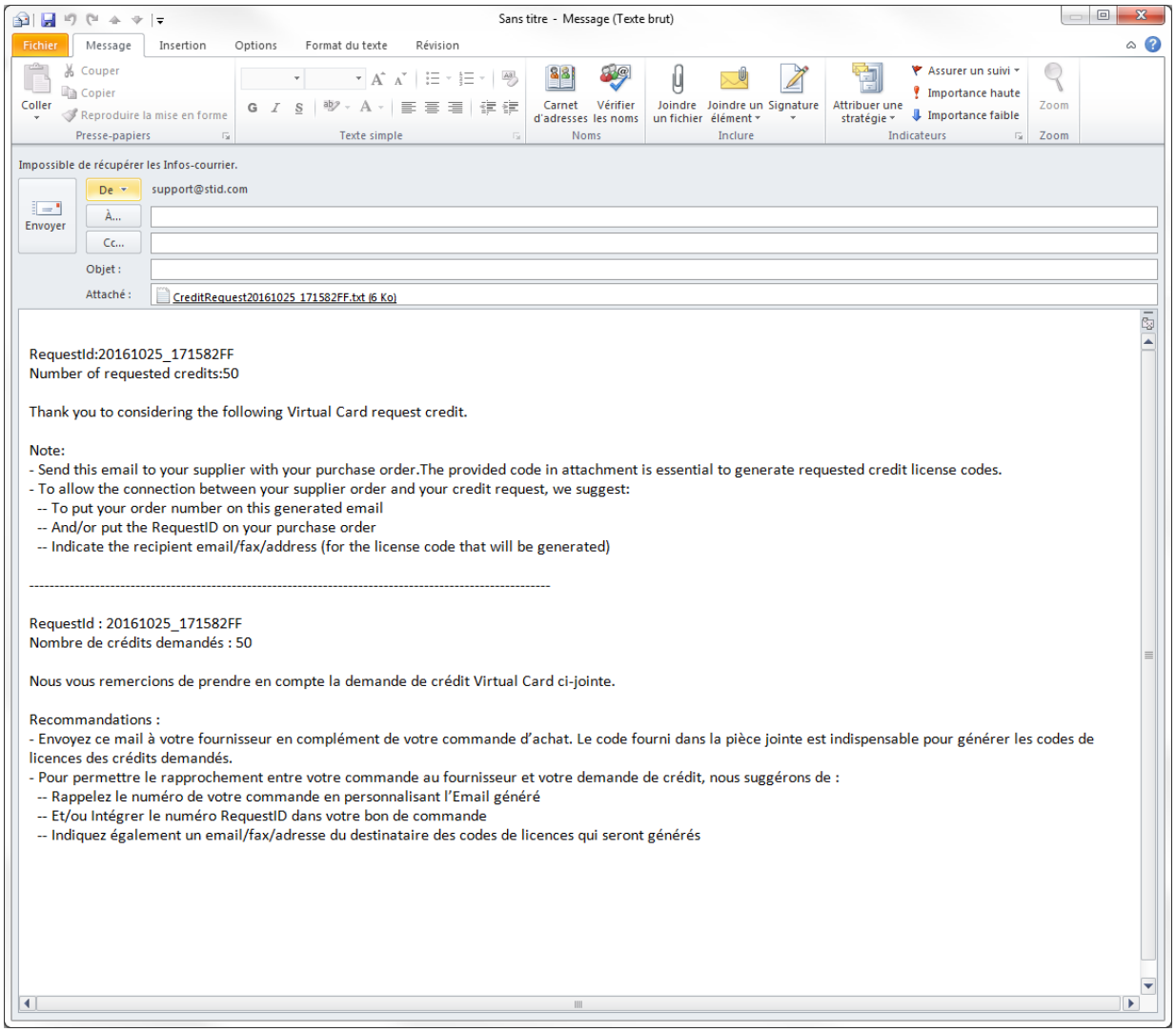
- "Generate text file": request file that can be sent by e-mail or any other mean.

Email Request

Select the credit required and click on 

.

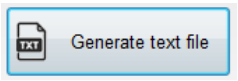
A window will open with your e-mail messaging software:



Follow the instructions in the e-mail.

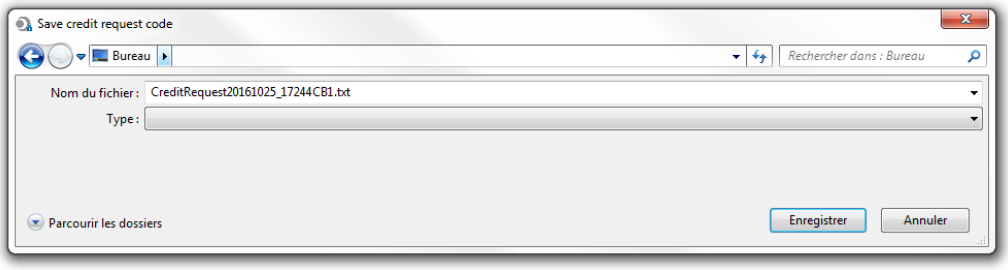
Warning: you can only make a single credit request at a time. Any other credit request will replace the previous if the license code generated by the first request has not been used.

Generate text file

Select the credit required and click on 

.

A window will open allowing you to select the location where to save the file:

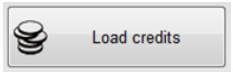


Send an email to your supplier with your purchase order and attach the document. The code provided in the attachment is essential to generate the credit license codes.

To allow the connection between your supplier order and your credit request, we suggest:

- To put your order number in your email
- And/or put the RequestID on your purchase order
- Indicate the recipient email/fax/address (for the licence code that will be generated)

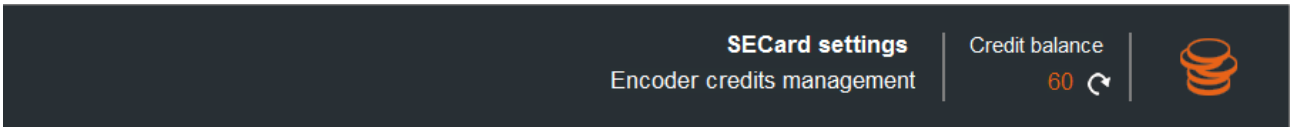
Credits Load

1- Connect the encoder that generated the request.
2- Enter the license code provided.
3- Click on 

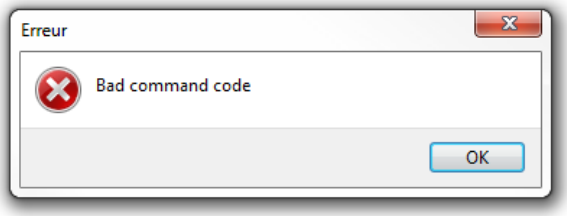
.

Credit balance

To check the credit balance available in the encoder, connect the Bluetooth® encoder and click on Check. The credit balance is displayed as follows:

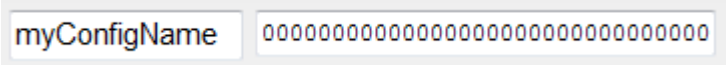


If the encoder connected is not a Bluetooth® model and you try to generate a Request Credit the following error appear:



Delete your virtual access card to recover the related credits

In Administrator profile:

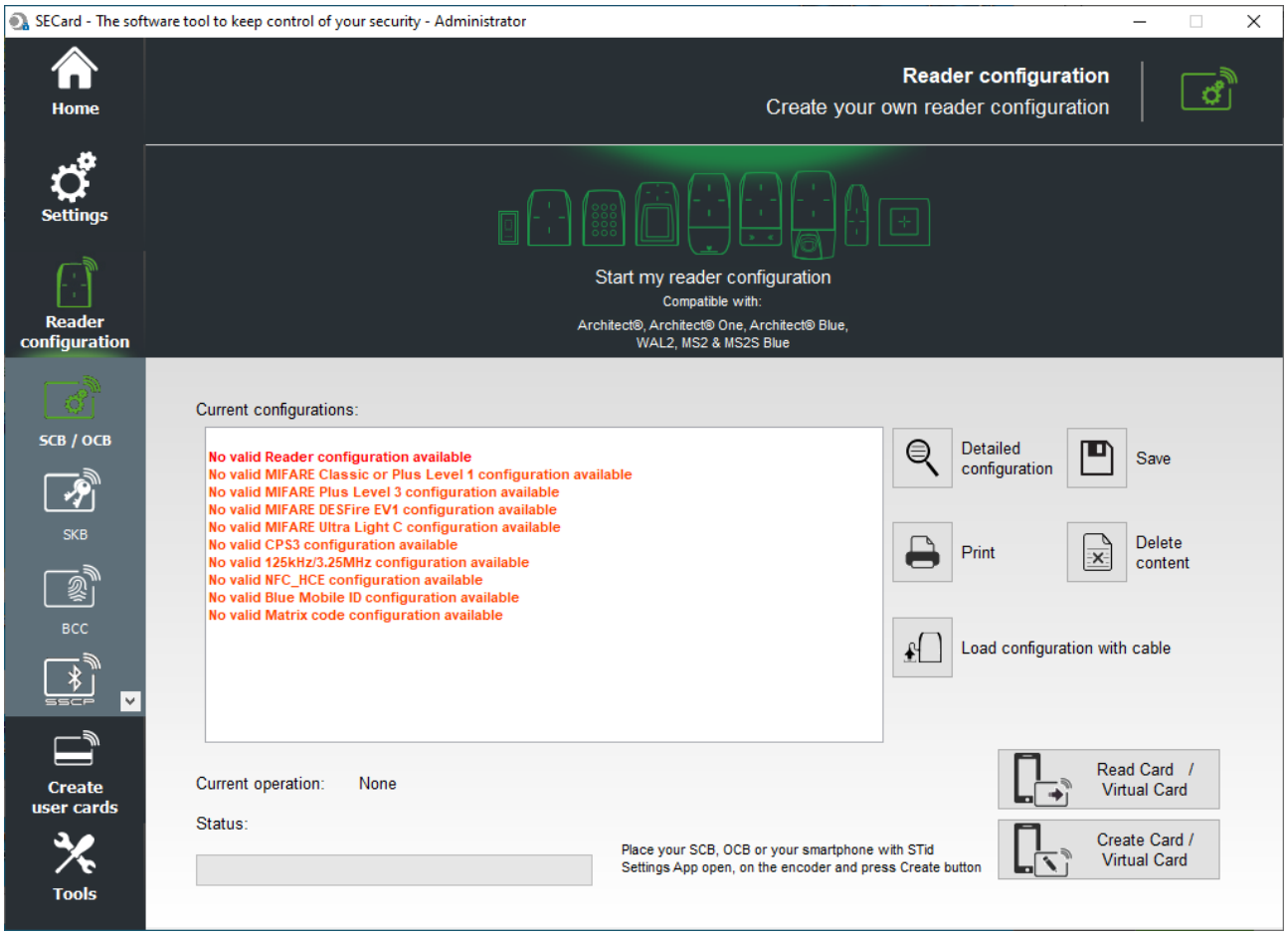


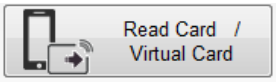
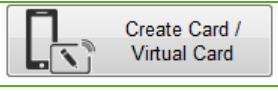
Enter the configuration name and the write key used to create the virtual card and click Delete VCard.
Credits are automatically reloaded into the encoder.

 Load the current configuration settings into the field.

In Power User and User:
It's only possible to delete the VCard corresponding to the current settings.

III. Reader Configuration – SCB / OCB

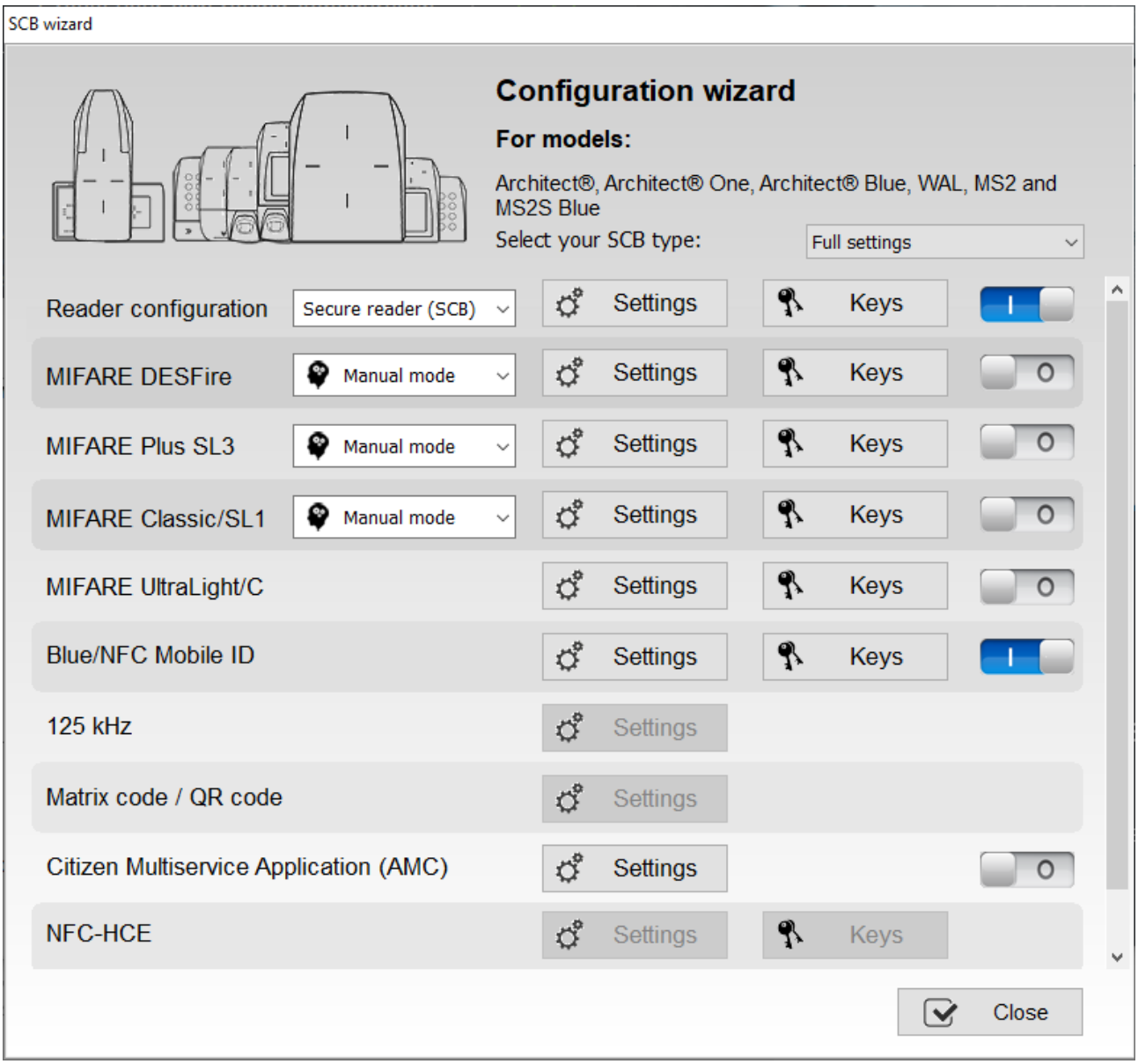


	Open the configuration wizard for readers
	Print the configuration list displayed.
	Save in .rtf file the configuration list displayed.
	Clear the configuration list displayed.
	Display details information of current configuration.
 Wizard SCB	Load the configuration to the reader by serial link.
 Wizard OCB New 3.6	Load the configuration to the reader by serial link or create configuration file.
	Read a SCB/OCB RFID configuration card. **Use SCB/OCB Company Key defined in the configuration wizard.**
	Create a SCB/OCB RFID/virtual configuration card with parameters defined in the configuration wizard.

This version of SECard allows you to create the configuration for WAL range, Architect® range (ARC, ARC One, ARCS and ARCS Blue) and OEM module MS2, MS2S.

When the configurations settings are validated, the button turn on “1”  .

These buttons are useful to enable or disable configurations.



SCB-Load configuration with cable

From v3.1.0 version, the SCB configuration can be load into the reader via serial link.

When all the settings are filled in the SCB configuration wizard:

1- In “Serial communication settings” select the port number.

2- Connect the reader ARC-R3x to configure via converter cable to the PC.

3- Click on “Load configuration with cable” while the LED blinks orange for serial readers or at any time for TTL readers

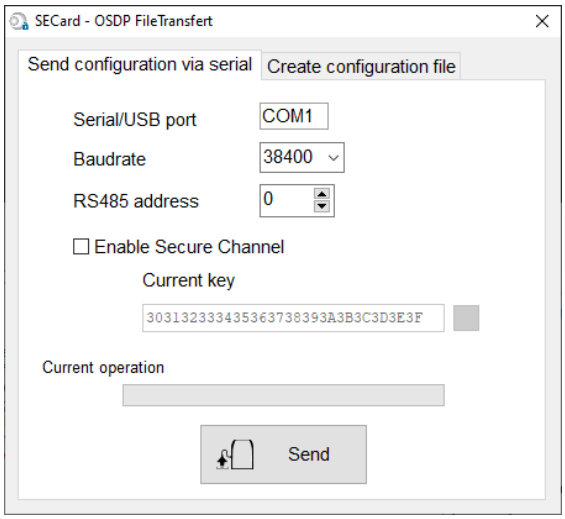
OCB-Load configuration with cable or Create configuration file *New 3.6*

From v3.6.0 version, the OCB configuration can be load into the reader:

- via serial link directly in SECard
- using *osdp_FileTransfer* command with configuration file created with SECard.

❖ Send configuration via serial:

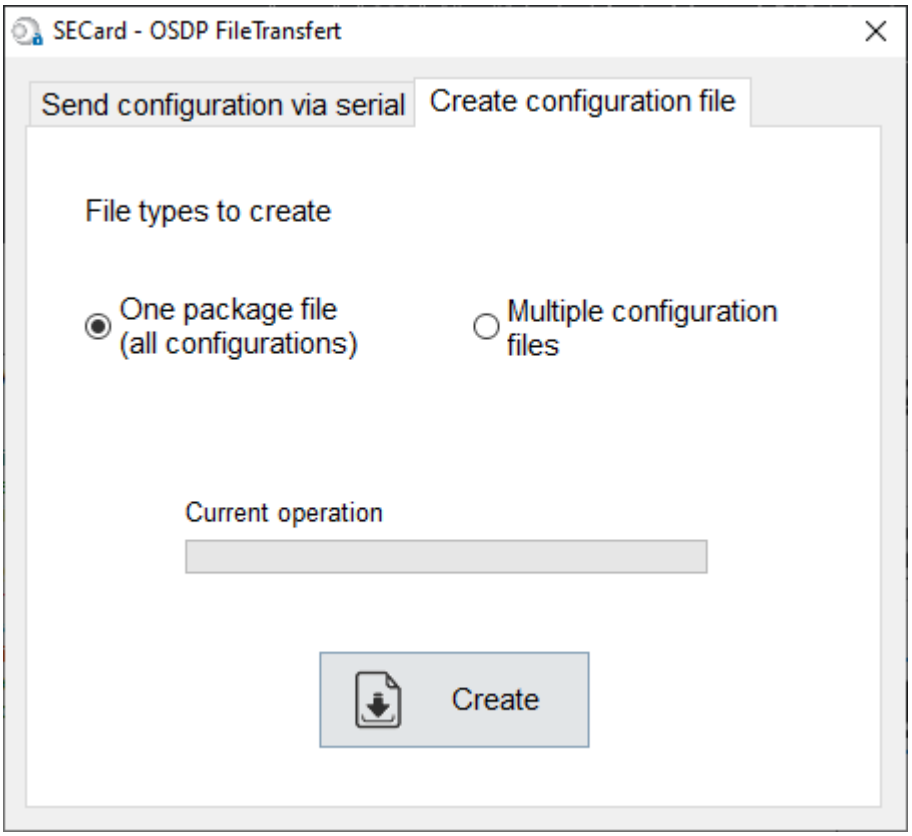
1- When all the settings are filled in the OCB configuration wizard click on



2- Connect the reader W33-XX-7OS to configure via converter cable to the PC.
3- Select the port number / Baudrate (default is 9600) / RS485 address (default is 0) of the reader.
4- If the reader has a Secure channel: select Enable Secure Channel and enter your key value.
5- Click on “Send”.

❖ **Send configuration via serial:**

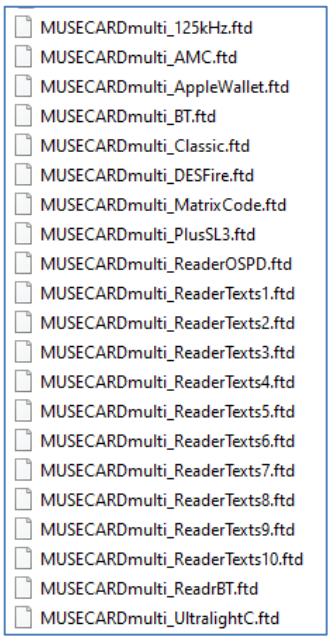
1- When all the settings are filled in the OCB configuration wizard click on 



2- File types to create:

One package file: all configurations are saved in a single file

Multiple configuration files: each configuration is saved in its own file:



3- Select a name and a directory to save file(s).

Creating SCB/OCB RFID cards

From version V3.6.x of SECard, SCB/OCB configuration card must be created with the types of cards below:

Chip to be used
MIFARE® DESFire® EV2/ EV3 not locked 8ko

It's possible to reuse an SCB/OCB card when we know his master key.(I. 5 - Compatibility *Modification v3.6*)

Warning

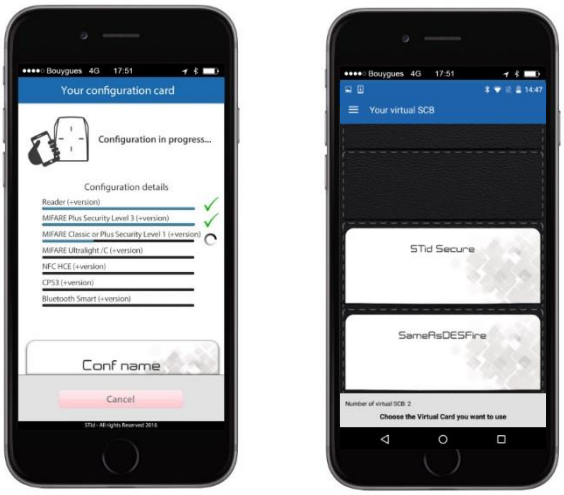
Changing a reader reference is not possible through a *SCB/OCB* card.

Example: ARC-R31-E-**103**-xx reader cannot be configured as an ARC-R31-E-**PH5**-xx reader.

It is necessary to return the product at the factory to change a reference.

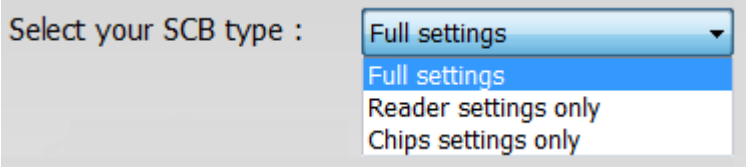
Creating virtual SCB/OCB card (only for Bluetooth® reader and STid Mobile ID® app) *Adding functionality 3.6*

From the V3.6.x SECard version, the configuration cards can be loaded into a smartphone. **STid Settings application is required**.
A smartphone can contain multiple virtual configuration cards.



III. 1 - SCB Wizard: Reader configuration settings

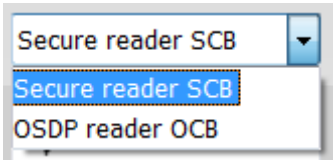
SCB level



Choose the settings, to be encoded in the SCB:

- Full settings: reader **and** chip settings will be encoded in SCB card.
- Reader settings only: only the reader settings and reader keys will be encoded (not available for reader Bluetooth® configuration).
- Chips settings only: only the chip settings and chip keys will be encoded, reader's settings have been configured via the UHF or via another SCB card.

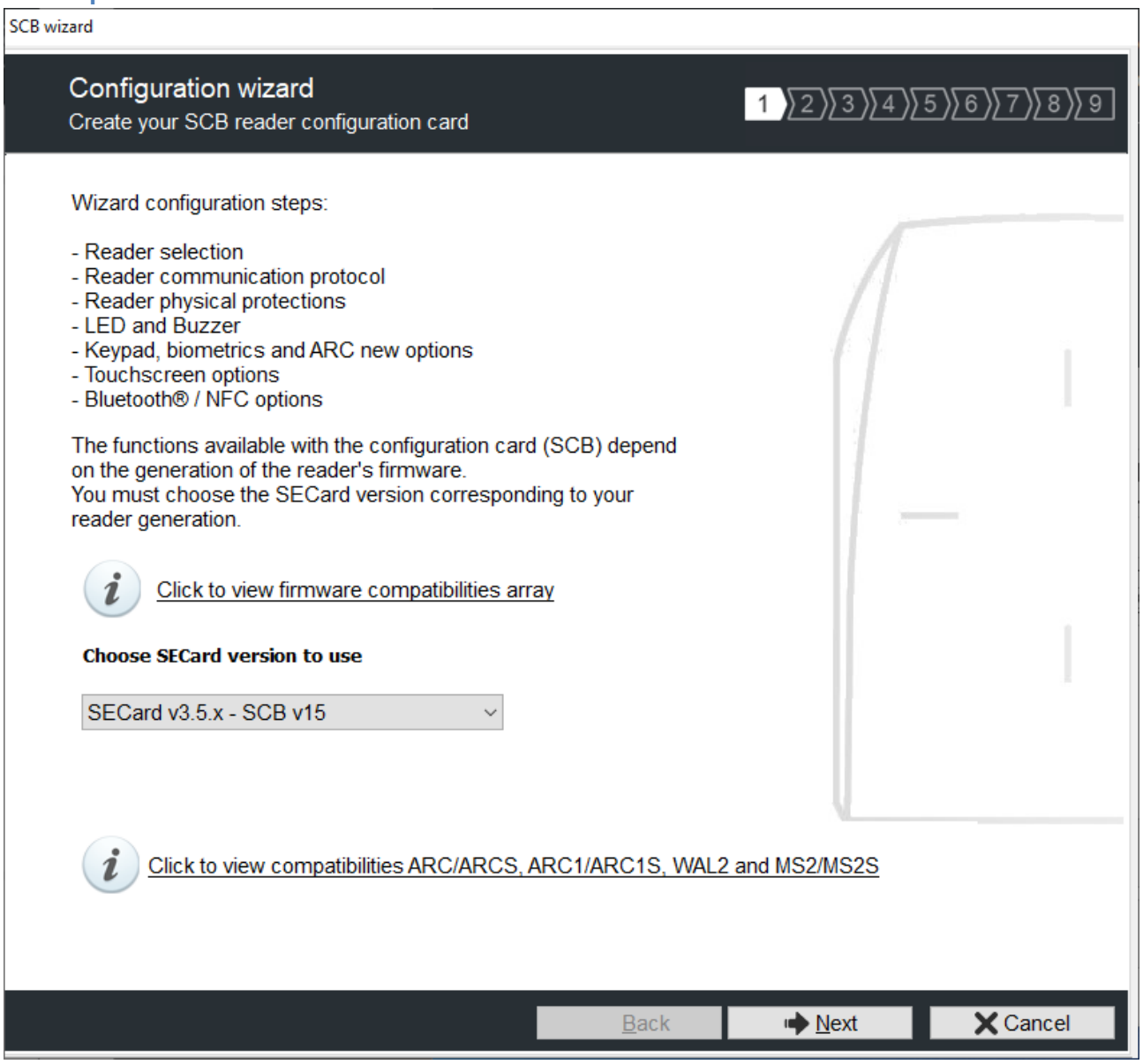
Reader configuration: In the list select Secure reader SCB



Reader "settings": The reader configuration is done in eight steps. To move from one stage to another, you must click on "Next".

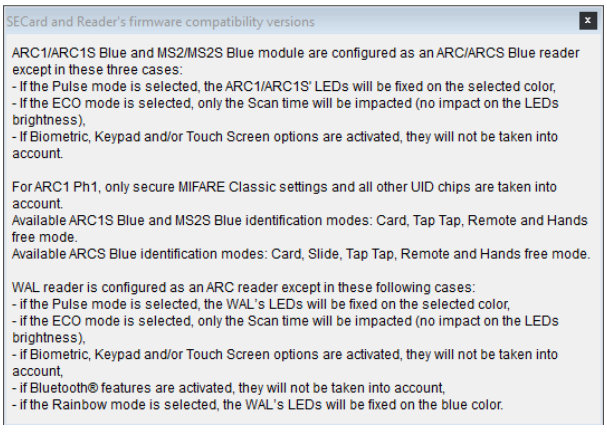
 Click here	Configuration wizard / Choose SECard version to use
 Click here	Reader reference selection
 Clich here	Reader communication protocol
 Click here	Reader physical protections
 Click here	LED and Buzzer
 Click here	Keypad, biometric and ARC new options
 Click here	Touchscreen options
 Click here	Blue/NFC Mobile ID options
 Click here	Matrix / QR Code options

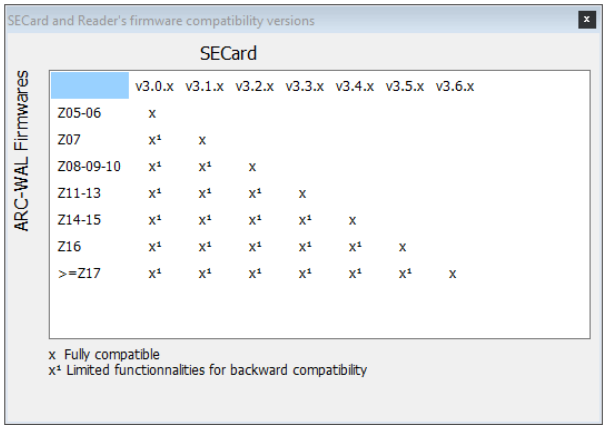
SCB - Step 1



The available functionalities and the compatibility of SCB depend on reader firmware generation.

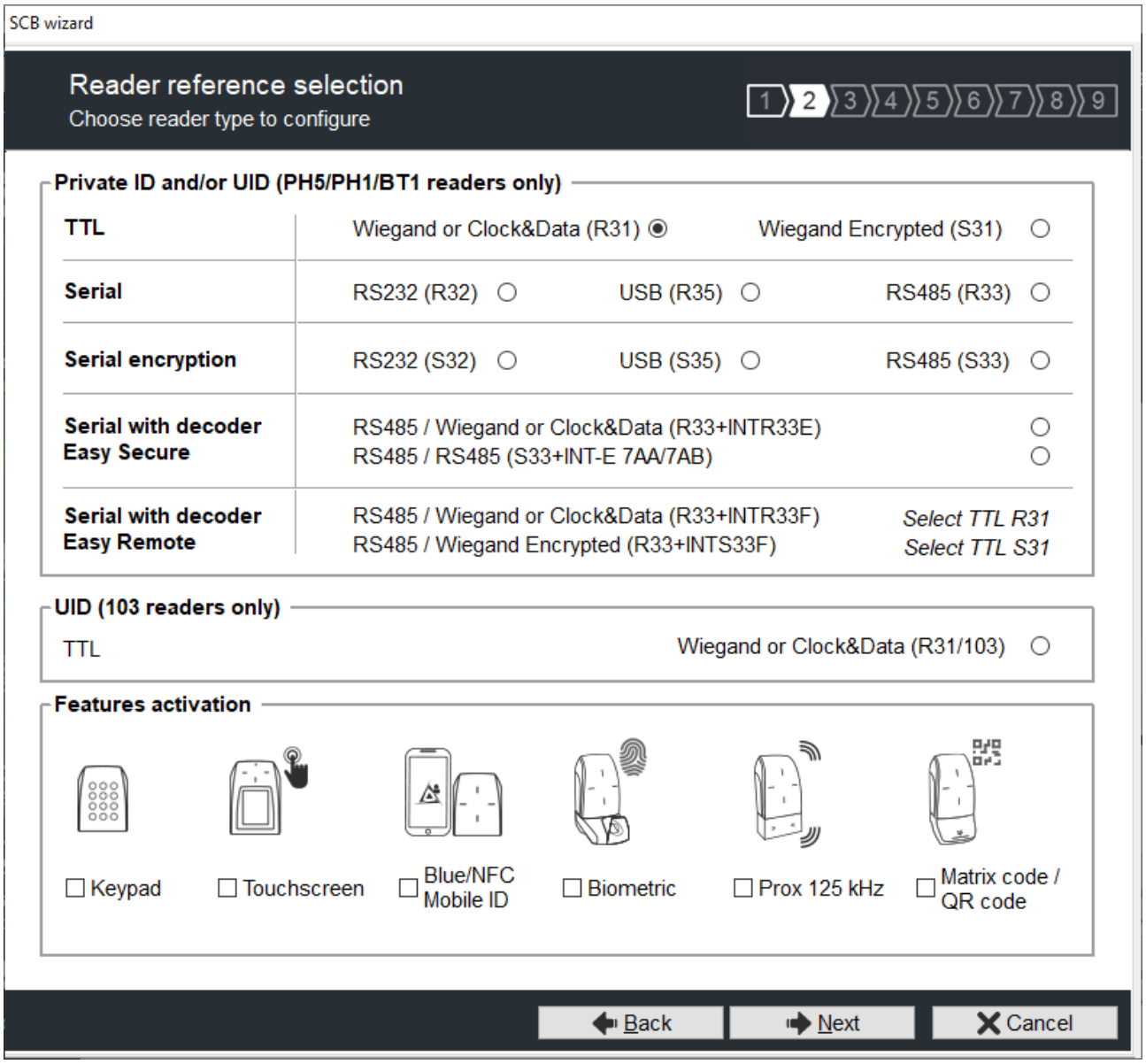
To provide compatibility between SECard and firmware versions, SECard proposes the choice about SECard version to use if the option is validated in “Files” cf. *II. 3* - Files.





To determine the version of firmware, refer to paragraph.*T2.1 - Powering up*

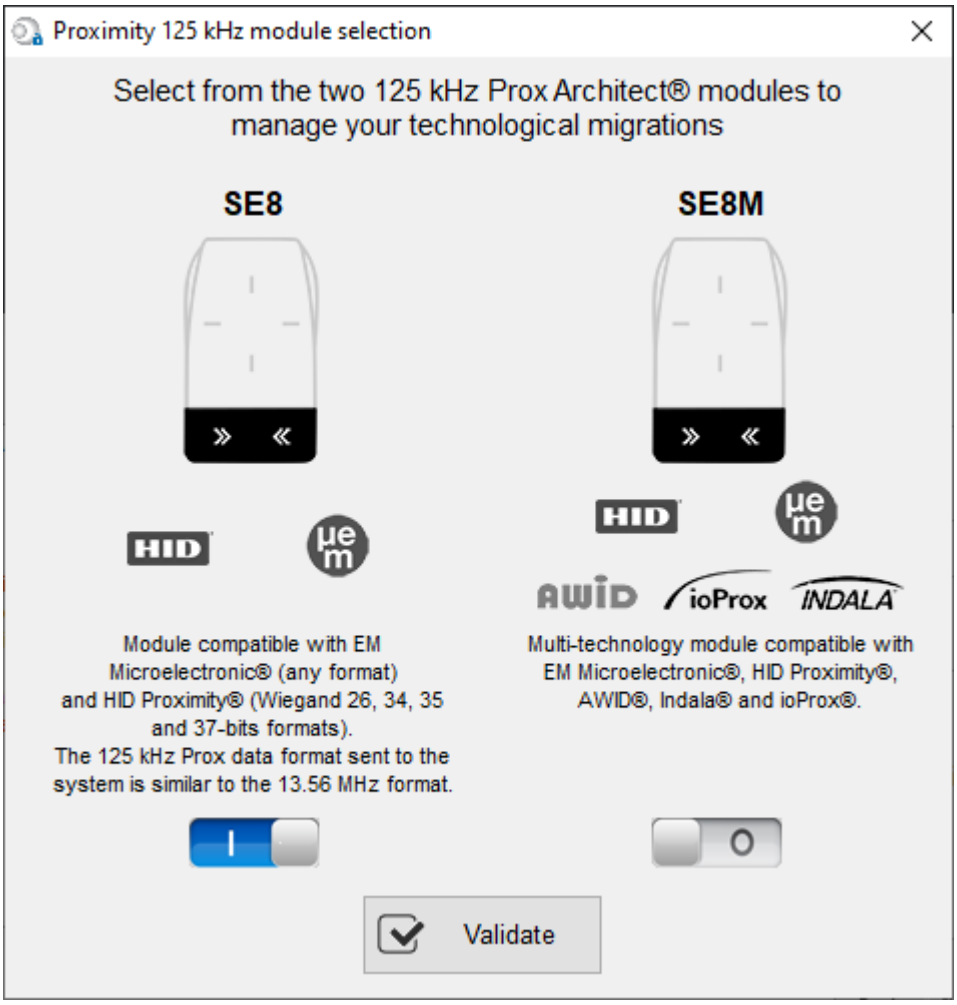
SCB - Step 2



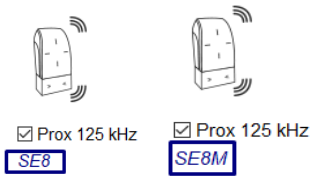
This step allows you:

- To choose the type of reader to configure.
- To activate keypad configuration.
- To activate touchscreen configuration.
- To activate Blue/NFC Mobile ID configuration.
- To activate the biometric configuration.

❖ To select 125 kHz module (SE8 or SE8M) and activate configuration.



The current model appears on the screen



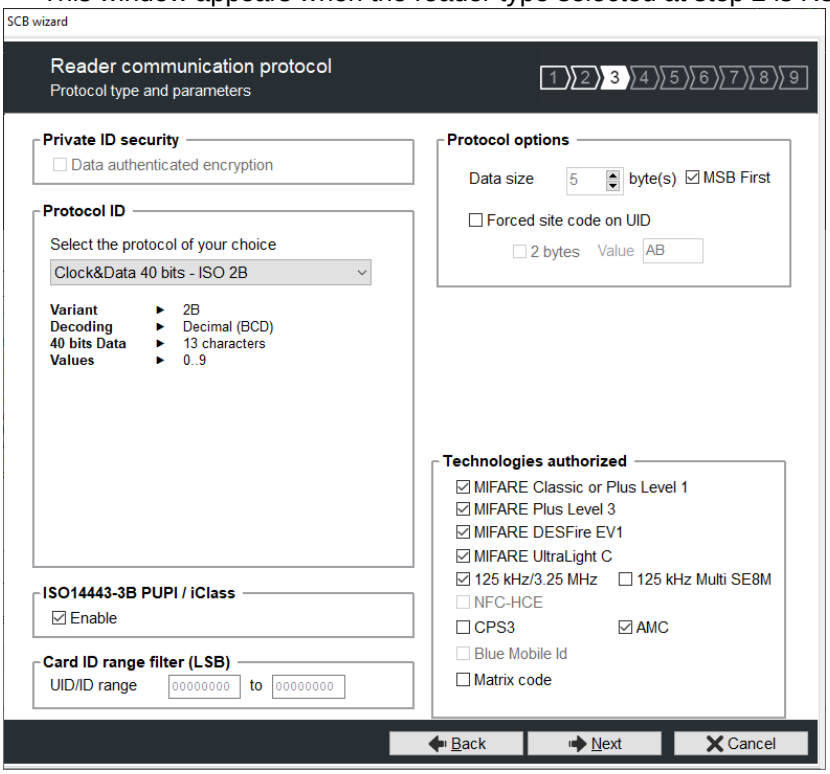
The SE8M module is only available for TTL R31/S31 and R31/103 readers in Wiegand output protocol (Wiegand 26 bits-3i default).

This choice impacts on 125kHz settings.

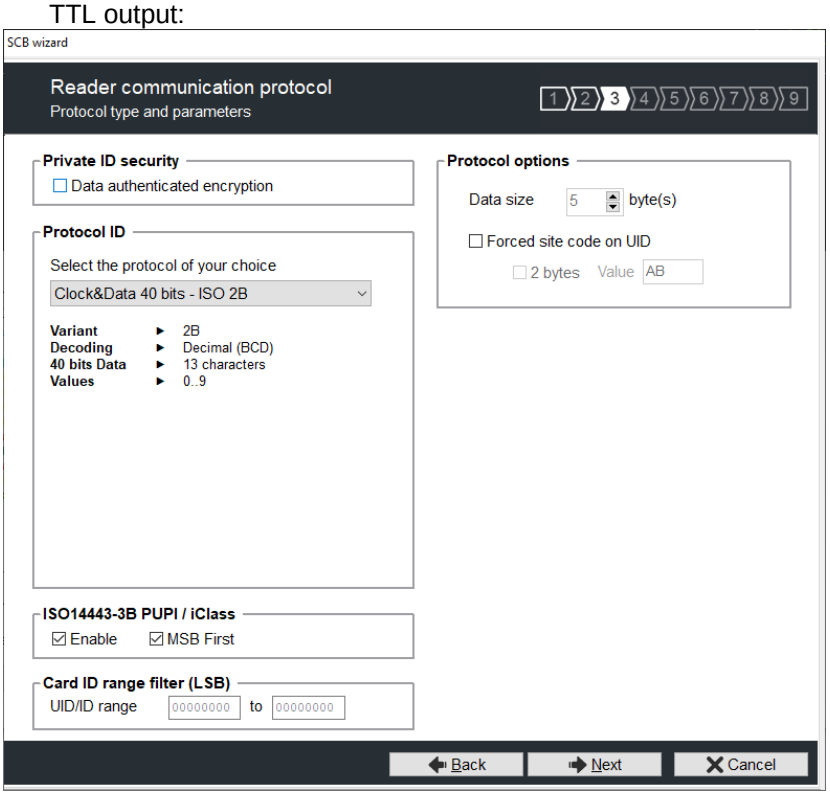
❖ To activate Matrix / QR code configuration.

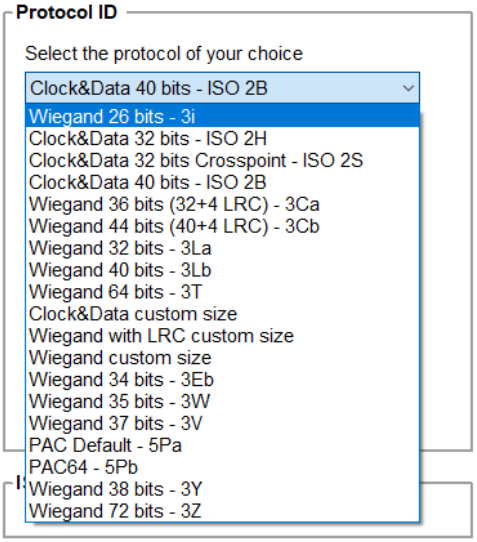
SCB - Step 3 *Adding functionality 3.6*

This window appears when the reader type selected at step 2 is R31/103:



This window appears when the reader type selected at step 2 is TTL output:





Protocol

It contains the different TTL communication protocols supported by the reader.

For more information about the protocols refer to *T4 - About TTL communication protocols*.

Note: When encoding, the ID format is formed according to the format of the current protocol (example: Decimal 13 characters for the protocol 2B - 10 hexadecimal characters for 3CB protocol).

Protocol options

- *"Data size":* adjust the size for custom protocol.

  Maximum size in Wiegand: 48 bytes
  Maximum size in Data/Clock: 10 bytes

- "Forced site *code on UID":* force a site code whatever the communication protocol.
  The value of the code will be transmitted most significant on one or two bytes.
  UID can be truncated according to the protocol used.
  This option is only available in UID mode (not available on Wiegand 64 bits - 3T Protocol).

ISO 14443-3B PUPI / iCLASS™*

It is possible to manage differently the PUPI ISO14443-3B and the ISO 14443-2B by calculating an authentication code using a cryptographic hash function (SHA1) and a secret key. Other norms (ISO14443-A) and frequencies (125 kHz & 3.25 MHz) are not concerned by this option.

If the protocol size is less than 20 bytes, the 20 bytes obtained signature will be LSB truncated.
If the protocol size is more than 20 bytes, a zero padding will be made.

*Our readers only read the UID/Chip Serial Number. They do not read secure HID Global's iCLASS™ cryptographic protections.

Card ID range filter (LSB)

It is possible to return an UID / ID only if it is within a specified 4 bytes bounded range.

If the size of the UID / ID is more than 4 bytes, the range will be made on the 4 bytes LSB (taking into account the MSB First option first). The limits are included, lower limit ≤ UID / ID ≤ upper limit.

If the UID / ID is in the range, the reader will return the code for the current protocol and perform an action card LED + Buzzer (SCB). Otherwise, the reader light up (not configurable and not disabled) red LED + Buzzer for 400ms.

The UID / ID is compared to the hexadecimal value after taking into account the MSB First parameter and before entry into protocol shape.
For example, for a protocol 2S, the code to compare will be the code on 4 bytes before coding to 2S format.

Technologies authorized

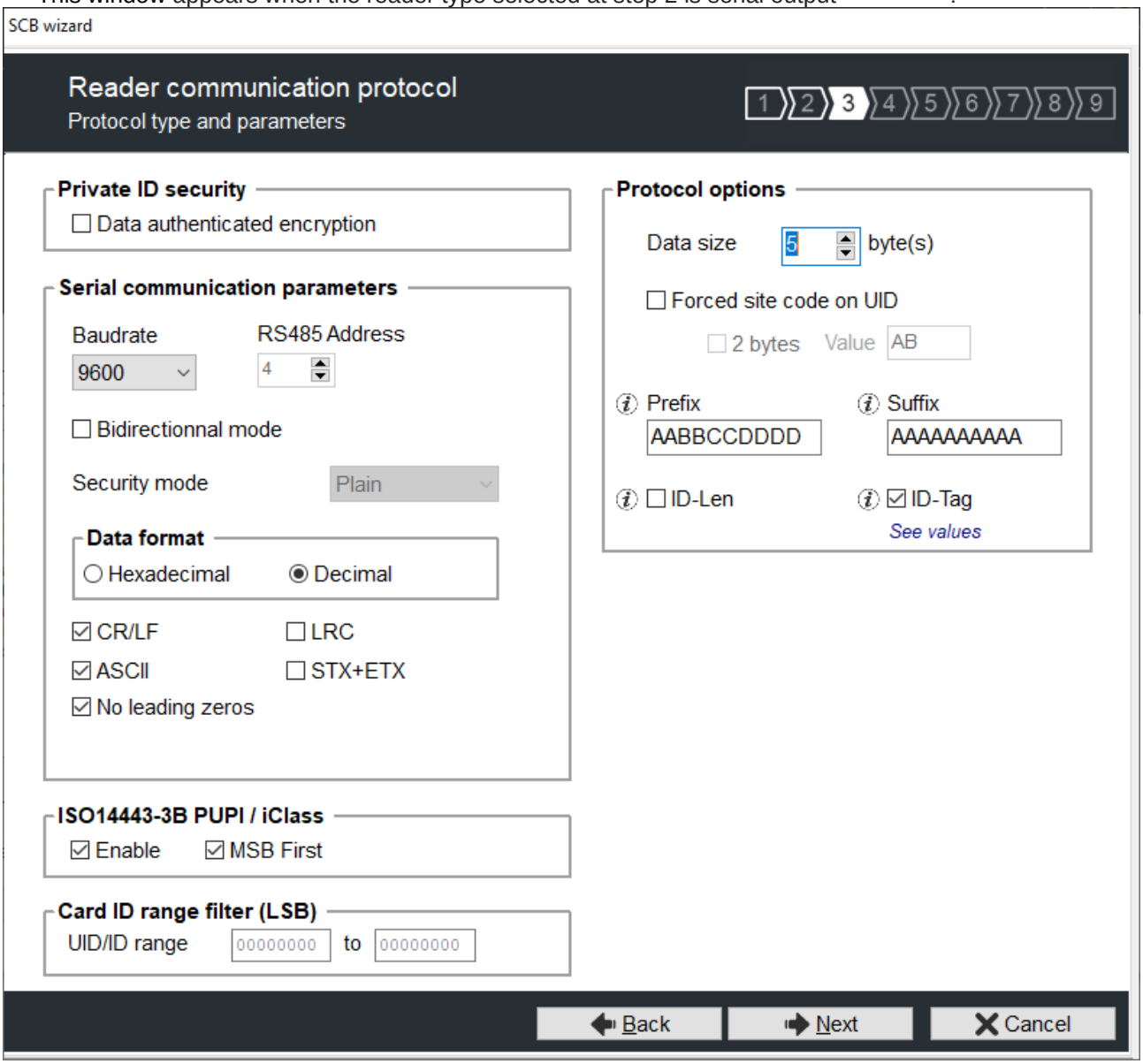
When the selected reader type is "UID only", you can select the type of chip technologies that can be read by the reader.

Private ID security

Private ID can be encrypted AND signed before being written in the card.
The reader will decrypt and authenticate the private ID before sending it on its output media.
Only an ID correctly decrypted and authenticated will produce an output data, otherwise the reader will remain mute.
The Authenticated Encryption uses the MtE mode (Maced then Encrypt).

Note: The size of private identifier is limited to 12 bytes.

This window appears when the reader type selected at step 2 is serial output *Modification 3.6*:



Serial communication protocol

It contains the different serial communication parameters.

For more information about the protocol, refer to *T5 - Serial communication protocol.*

Protocole Options

- *"Data size":* adjust the size for custom protocol.

  Maximum size in Hexadecimal: 48 bytes
  Maximum size in decimal: 10 bytes

Note:
It is possible to increase the size of the field beyond the maximum size for this, hold the button CTRL and click in the "Data Size", and then the value appears underlined. This manipulation does not work for encoding but only for reading an identifier. Only available on series readers.

- Forced site c*ode on UID:* force a site code whatever the communication protocol.
  The value of the code will be transmitted most significant on one or two bytes.
  UID can be truncated according to the protocol used.
  This option is only available in UID mode.

New 3.6

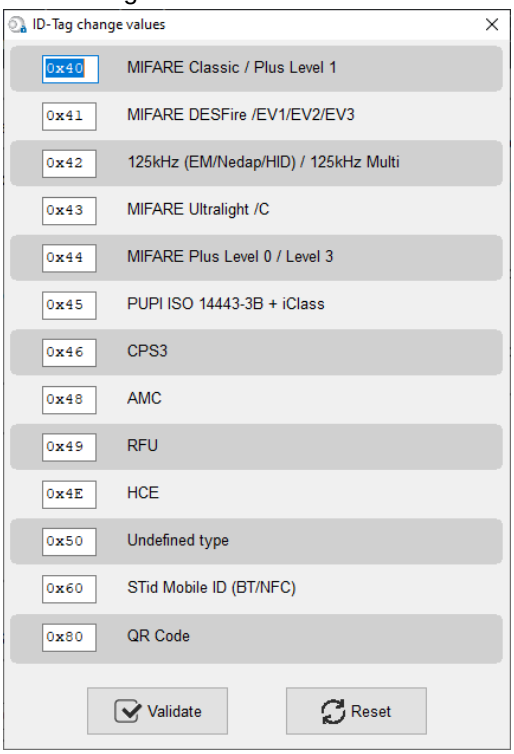
In Serial mode, it is possible to customize the data before transmission with the following information:

<Prefix><ID-Tag><ID-Len><ID-Number><Suffix>

- *Prefix*: add a prefix before sending the frame. Hexadecimal value on maximum 5 bytes.
- *Suffix:* add a suffix before sending the frame. Hexadecimal value on maximum 5 bytes.

- *ID-Tag:*

  One byte which identifies the type of "tag" read and will be added to the frame.
  The ID-Tag will be added to a UID or to a private ID.
  The ID-Tag values can be modified in the table below:

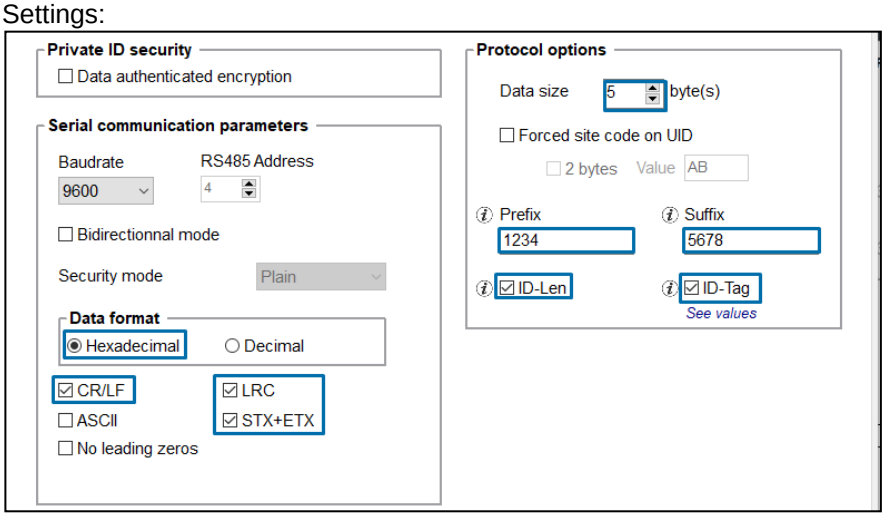


The Reset button restores the default STid values.

- *ID-Len:* 2 bytes indicating the length of the ID-Number
  - For data in Hexadecimal: ID-Len = number of bytes of ID-Number
  - For data in decimal: ID-Len = number of characters of ID-Number

Example 1:

Settings:



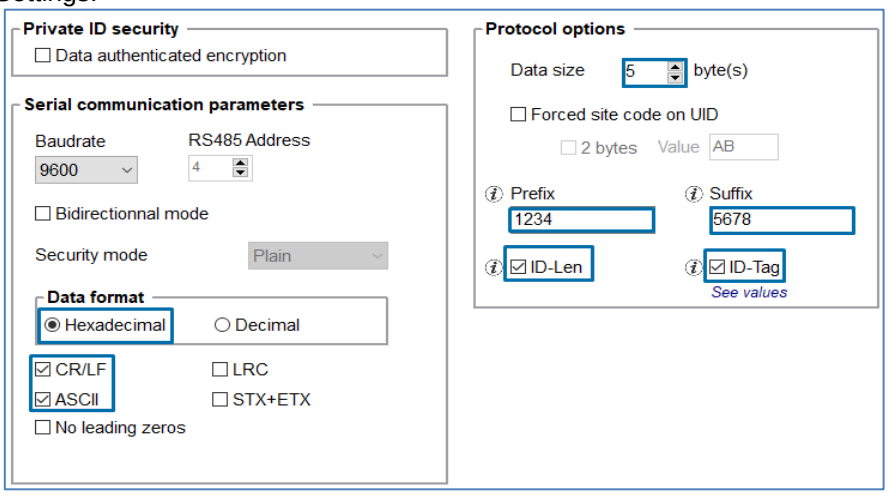
Tag: DESFire
ID-Number = 0000ABCDEF
ID-Len = 5

Frame:

STX	Prefix	ID-Tag	ID-Len	ID-Number	Suffix	LRC	0x0D	0x0A	ETX
02	1234	41	0005	0000ABCDEF	5678	LRC calculé sur les données 12344100050000ABCDEF5678	0D	0A	03

Example 2:

Settings:



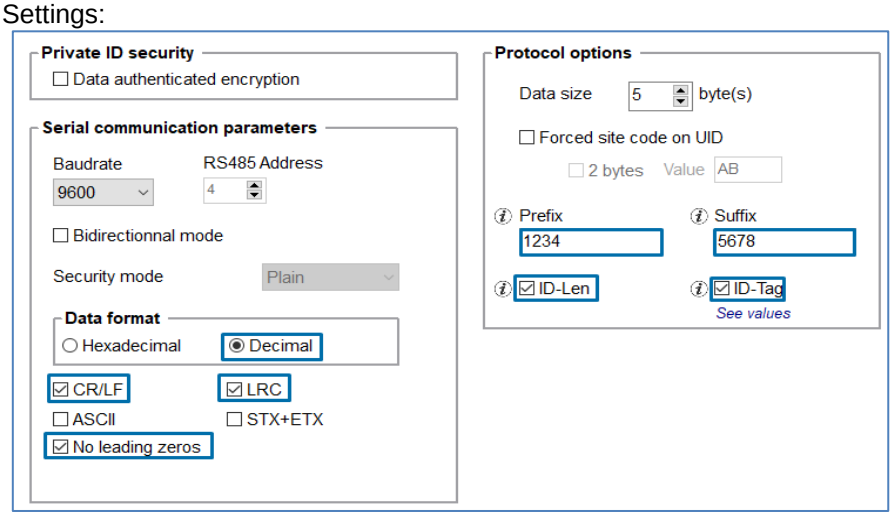
Tag: DESFire
ID-Number = 0000ABCDEF
ID-Len = 5

Frame:

Prefix	ID-Tag	ID-Len	ID-Number	Suffix	0x0D	0x0A
31323334	3431	30303035	30303030414243444546	35363738	0D	0A

Example 3:

Settings:



Tag: DESFire
ID-Number = 0000ABCDEF

ID-Number in decimal = 0000011259375

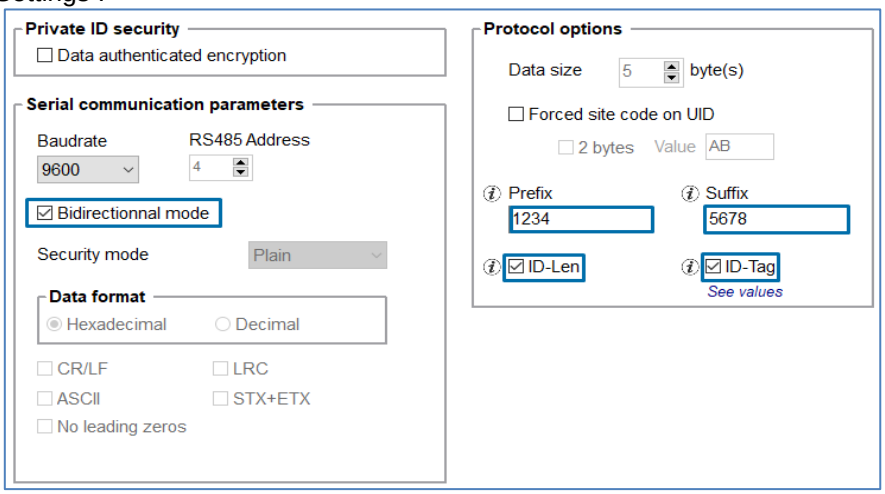
With No Leading zeros option: ID-Number=11259375 = 8 characters.

Frame:

Prefix	*ID-Tag*	*ID-Len*	*ID-Number*	*Suffix*	*LRC*	*0x0D*	*0x0A*
1234	*41*	*0008*	*11259375*	*5678*	*LRC*	*0D*	*0A*

Example 4: Bidirectionnal mode

Settings :

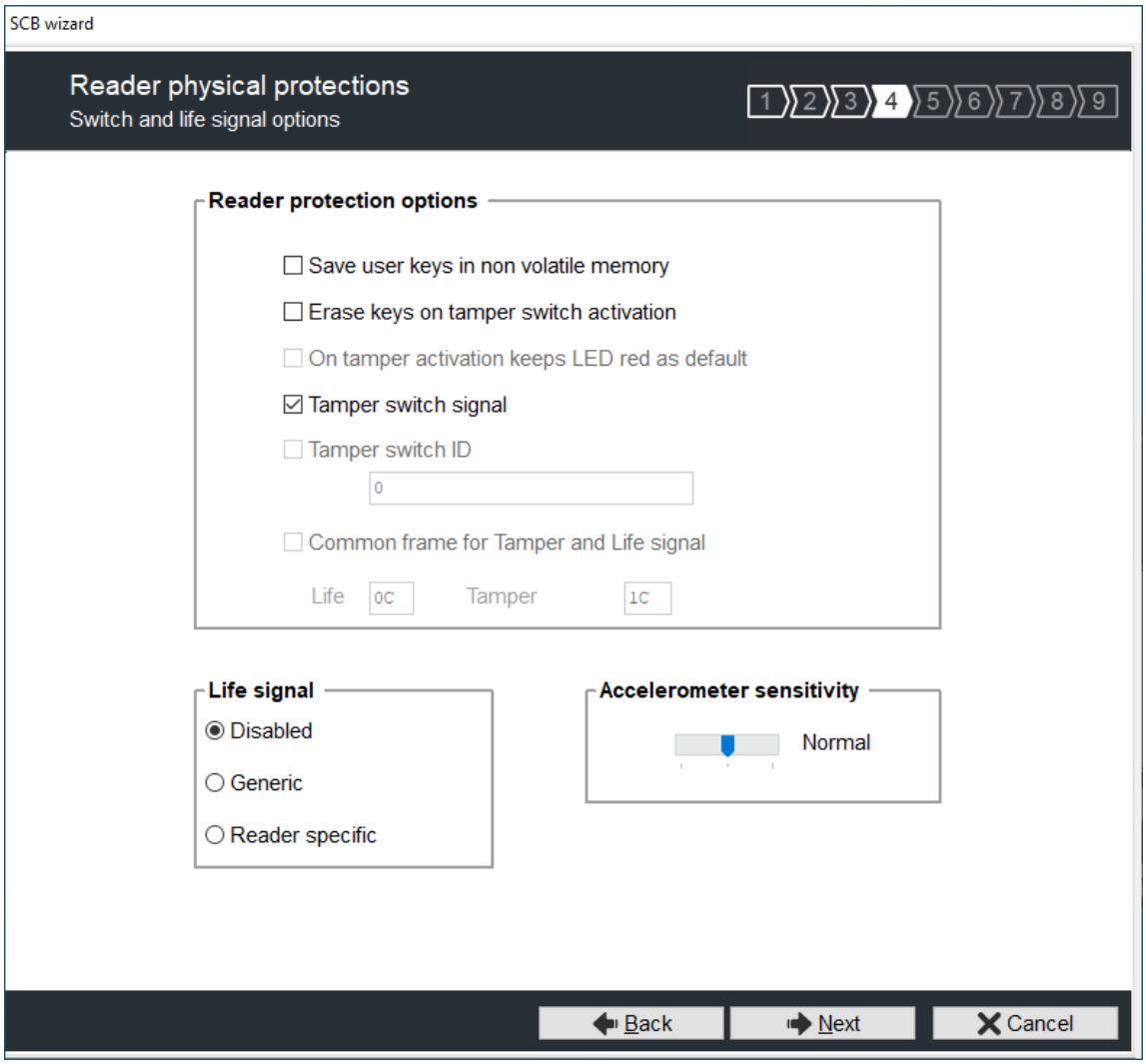


Tag: DESFire
ID-Number = 0000ABCDEF

Frame:

Len	*Prefix*	*ID-Tag*	*ID-Len*	*ID-Number*	*Suffix*
000C	*1234*	*41*	*0005*	*0000ABCDEF*	*5678*

SCB - Step 4



Reader protection option

- Save user keys in non-volatile memory: enables the keys to be saved, in encrypted form, in EEPROM non- volatile memory, in case of power failure.
- Erase keys on tamper switch activation: enables all the reader keys to be erased, if the status or accelerometer is changed.
- On tamper activation keeps red as default: requires activation of tearing.
  If the status of accelerometer is changed, LED is on the red indicating that the keys have been erased.
- Tamper switch signal: enables the tamper switch signal to be activated. Refer to *T10 - Tamper switch*.
- Tamper switch ID: enables the tamper switch ID to be activated. Refer to *T11 - Tamper switch ID*.
- Common frame for Tamper switch and Life signal: allows you to enable sending in a frame of a tamper signal and life, available only for R31, S31 and R33+INTR33E readers. Refer to *T12 - Mutual Life / Tamper switch Signal*.

Note: There is no tearing management on USB readers.

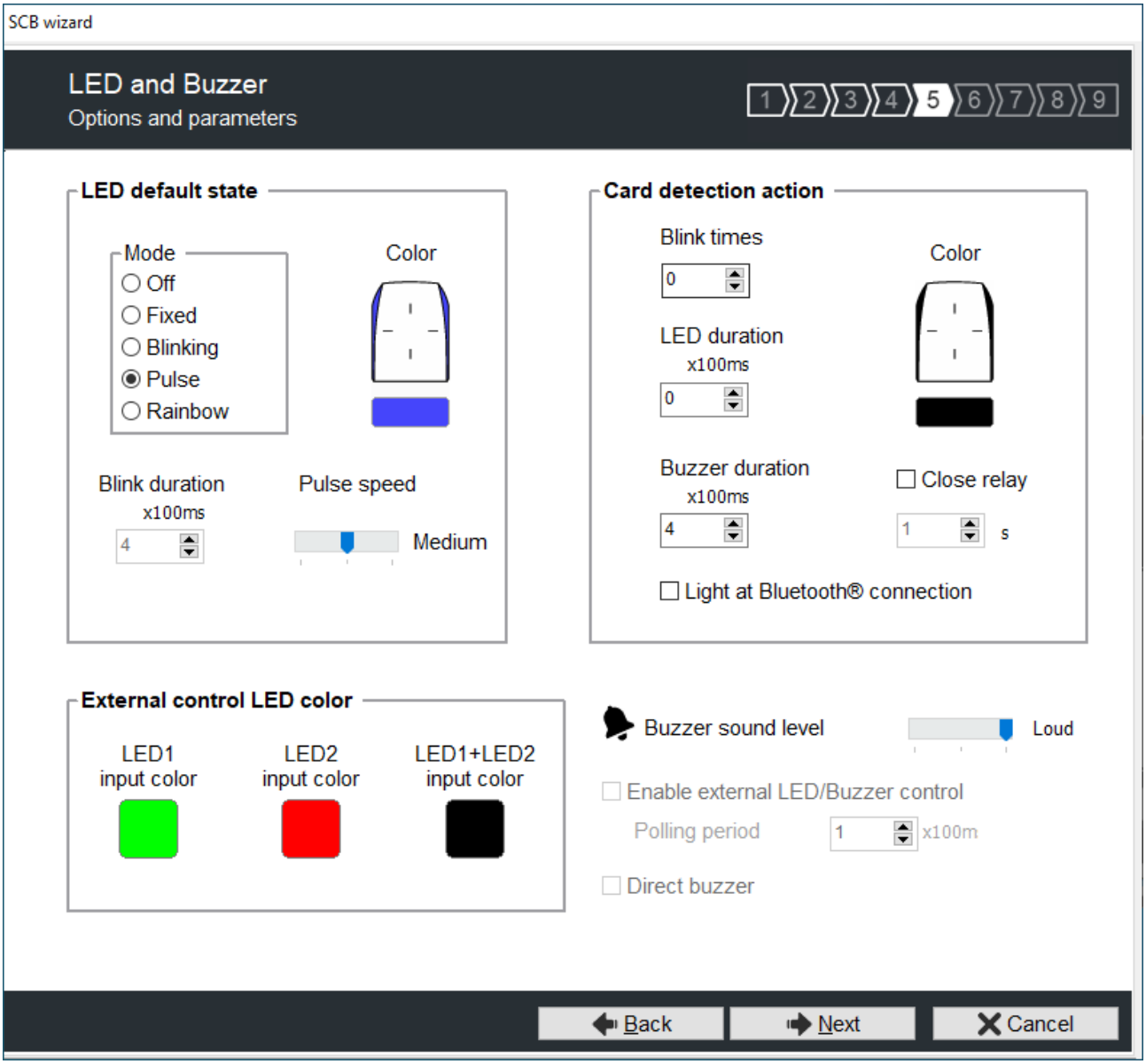
Life signal

Enable / disable the life signal and choose the type of signal "Generic" or "specific". Refer to *T9 - Life signal function*.

Accelerometer sensitivity

The ARC reader range includes an accelerometer to detect the reader tearing.
Depending on the support / installation location of the reader, it may be necessary to adjust the sensitivity of the sensor so that only an effective tear is detected.

SCB - Step 5



LED default state

Define the default LED state (color and blink mode).

Availables modes for ARC readers:

- OFF
- Fixed
- Classic blinking
- Pulse
- Rainbow

Availables modes for WAL readers:

- Fixed
- Classic blinking

The image on the right allows you to view the selected effect: blinking and color.

Card detection action

- Define the LED and buzzer state (color and blink) when a card is detected.
  This information is independent of the acceptance of the identifier.

- Light at Bluetooth® connection
  Flash LED when smartphone start connection on the reader. The color can be selected by clicking on the right square.
  This action, independent of the detection of the virtual badge, informs the user that the communication between the smartphone and the reader is in progress.

- Close relay:
  On ARC/ARCS close the relay during time selected if the card has been well read (UID or PrivateID). If this function is enabled, the relay is no longer used for tamper or ring functionalities.

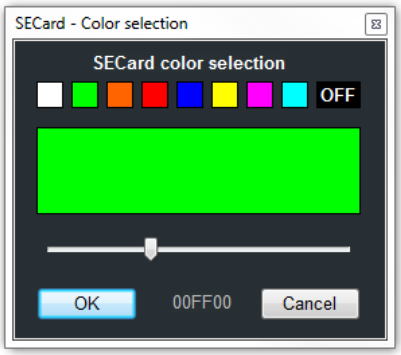
Note: Blinks times or LED duration defines, for the ARC Screen, the display time of the “image and text badge detection” state.

Buzzer sound level

Define the sound level for the buzzer **only available for ARCS, ARC1 and ARC1S**.

External control LED color

Define the color of LED1 input, LED2 input and both LED if they are controlled simultaneously.
To modify and select a color, click on the symbol ARC or color buttons, the following window opens:



To select a predefined color, click on one of the colored squares color.

For ARC readers only, it is possible to choose a different color. Move the cursor to the desired color, the value displayed corresponds to the RGB hexadecimal code of the selected color. It is possible to copy the value by double clicking.

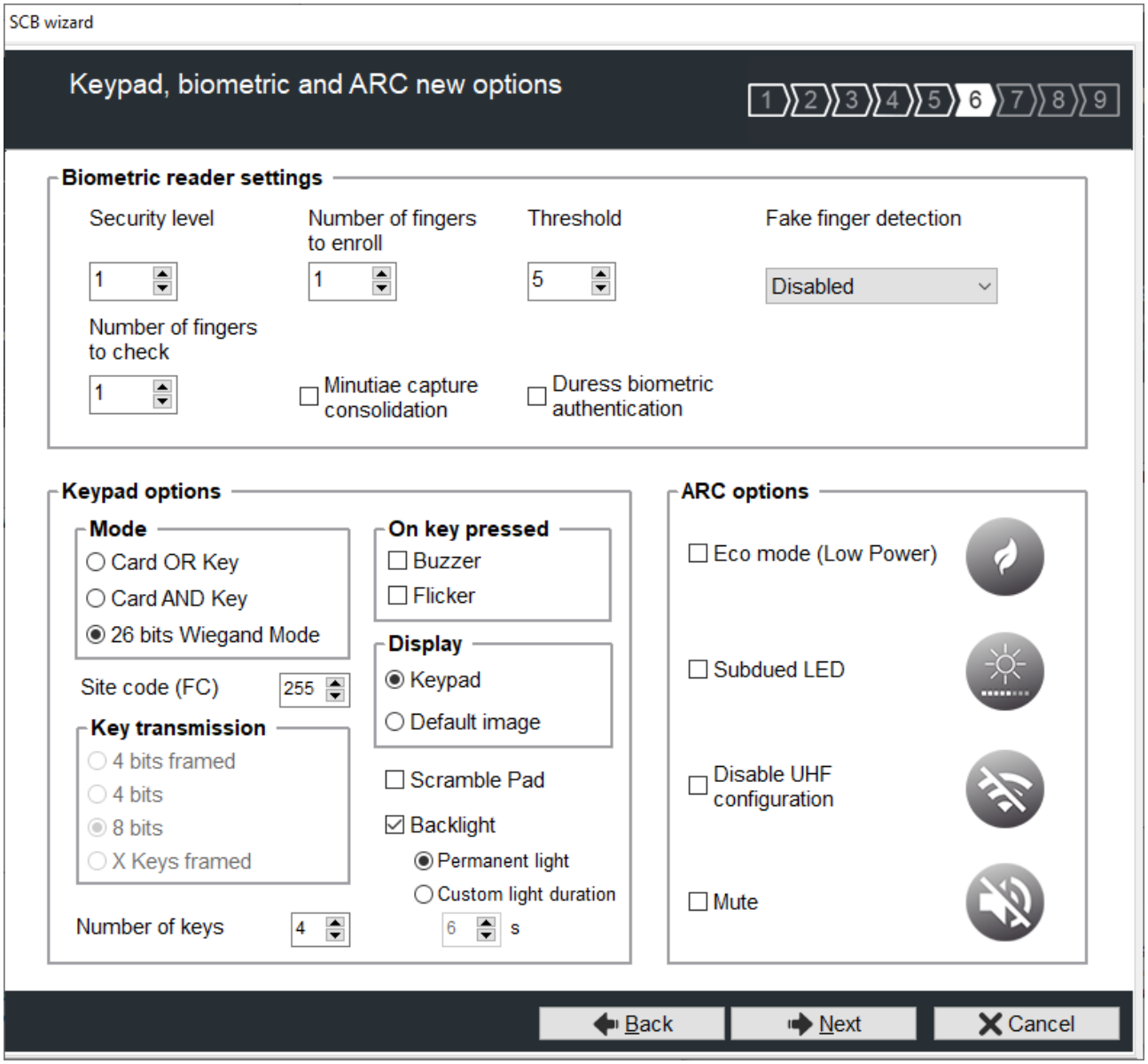
Enable external LED / Buzzer control

Control LED and buzzer externally. The polling period is adjustable in increments of 100ms.
Only available for serial readers (R/S-32 and R/S-33) in bidirectional mode.

Direct buzzer

Activate the buzzer as soon as a card is detected without waiting for an external command.
Only available for serial readers (R/S-32 and R/S-33) in bidirectional mode.

SCB - Step 6 *Adding functionality 3.6*



Reader biometric settings

- Security level: represents the reliability rate between the encoded and read fingerprints.
  - Security level = 1: low false finger security level (Morpho Sagem recommendation).
  - Security level = 2: medium false finger security level.
  - Security level = 3: high false finger security level.
- Threshold: represents the quality level of the fingerprints to encode in the chip (0 up to 10). Lower threshold = less false rejection. Morpho Sagem recommendation: 5.
- Number of fingers to enroll: represents the number of fingerprints to encode.
- Number of fingers to check: represents the number of finger to check.
- Minutiae capture consolidation: allows to capture the same finger three times. The biometric sensor will choose the best one during the encoding.

- Duress biometric authentication: The UID or private ID returned by the reader will be modified to include the finger number with which the user authenticated.
  This feature takes precedence over the site code if used.

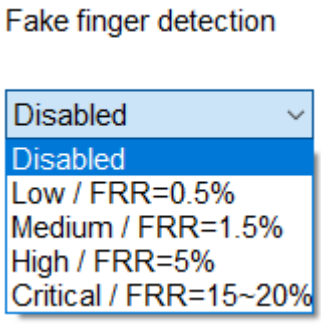
  Example: ID 0x1122334455 / 73 588 229 205 (decimal)

  Detection of finger number 2: ID sent by the reader is 0x**02**22334455 / 9 163 719 765.

  Note: not available in Wiegand 3T protocol, le 1st byte being used for the chip type.

Note: A new user card encoding with different number of fingers requires to format the chip.

- Fake finger detection: Enable / Disabled the Fake finger detection with specific detection level.

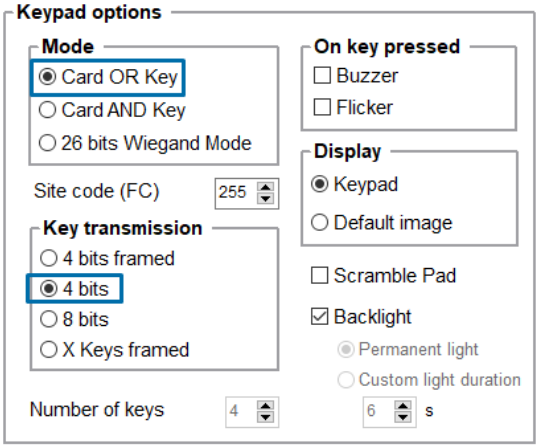


Keypad options

For more information on the functioning and format, refer to paragraph *T6 - About keypad readers*

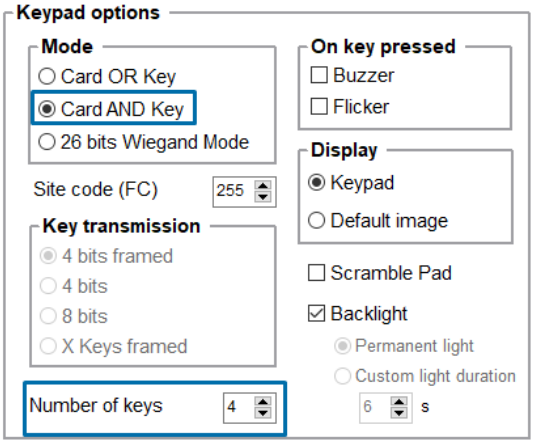
Choose between the modes “Card OR Key”, “Key AND Card” or “26-bits Wiegand Mode”:

- Card OR Key + format choice:



Once the reader detects a card, its ID number is sent according the selected protocol followed by an acknowledgement sound.
Each time a key is pressed, its number is sent to the host according the selected protocol and encoding mode followed by an acknowledgement sound.

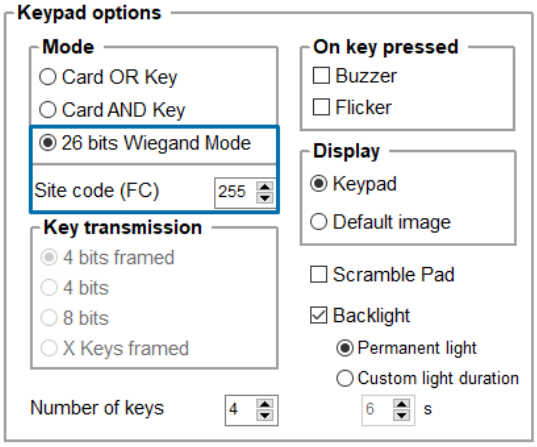
- Card AND Key + keys number:



When the key sequence is finished, the reader expects an identifier for a period of 6 seconds (a beep sound to indicate pending identifier).
The "key + card " sequence is sent according to the current protocol (except W3i, W3EB, W3V, W3W, W3y, W3z).

.

❖ Mode 26 bits Wiegand *New 3.6* :

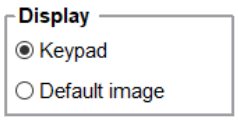


This mode activates the 26-bit Wiegand format only for keypad data.
The other identifiers (MIFARE® DESFire®, Bluetooth®, 125, etc.) will be transmitted according to the protocol defined in step 3.

In this mode, the keypad code is sent to the system in the form of a badge identifier attached to a site code defined in the "Site code (FC)" field.
#: validate the entry of the PIN code.
*: cancels the entry of the PIN code entered previously, the reader emits 4 beeps to indicate that it has been taken into account.

bit 1	bit 2 ... bit 9	bit 10 ... bit 25	bit 26
Even parity from bit 2 to bit 13	*Site code FC (0 à 255) configure in SECard bit 2 = MSB*	*PIN code (0 to 65 535) bit 10 = MSB*	*Odd parity from bit 14 to bit 25*

❖ Display:



Choose de default display for touchscreen if keyboard is active.

- Keypad:
  Display the keyboard.

- Default image:
  Display the default text and image (see step 7).

  To display the keyboard, touch a first time the screen.

  The display reverts to the default image after a timeout of 10s.

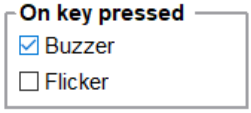
❖ Scramble Pad (Only available for screen touch ARC): Activate the scramble on keypad.
The scramble is performed:

- Card AND Key:
  - After each sequence: enter the number of configured keys and reading a valid card.
  - After a time out of 6s after the seizure of configured keys without presentation of a valid card.
  - Following the annulment by the * or # key.

- Card OR Key:
  - After reading a valid card.
  - Every 30s. Pressing a key or reading a card resets the timer.

- 26 bits Wiegand mode:
  - After reading a valid card
  - Every 30s.
  - Following key #

❖ On Key Pressed



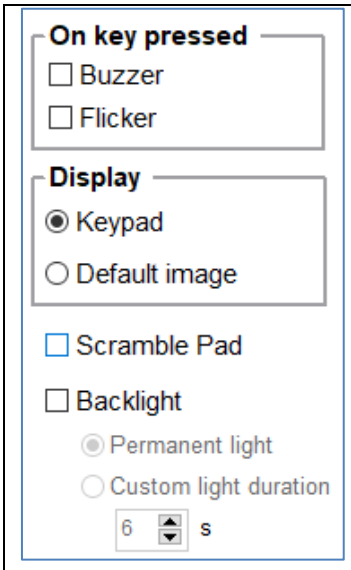
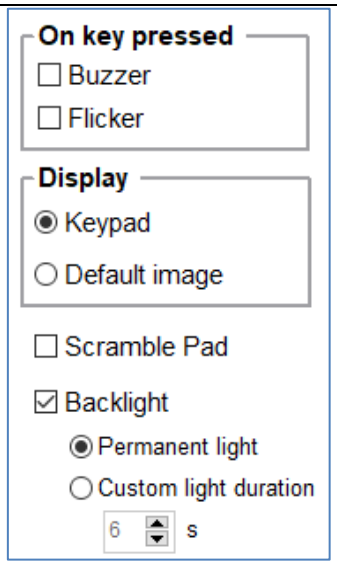
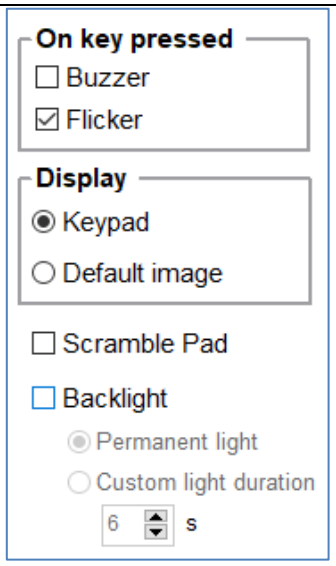
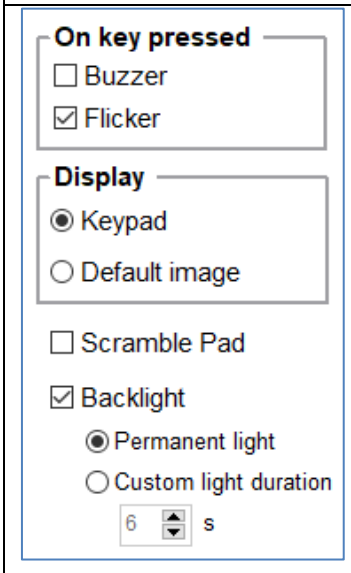
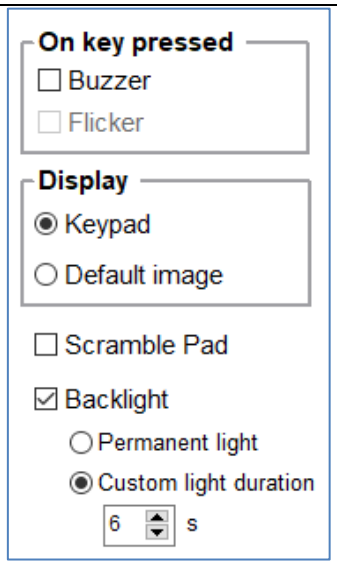
Buzzer: Allow to activate / deactivate Buzzer when user press one touch of the keyboard.

❖ Backlight: Allow to activate / deactivate the keypad backlight. Options available:

Permanent light: backlight is permanently activated.

Custom light duration: Keyboard backlighting when pressing a key and for a configurable time.

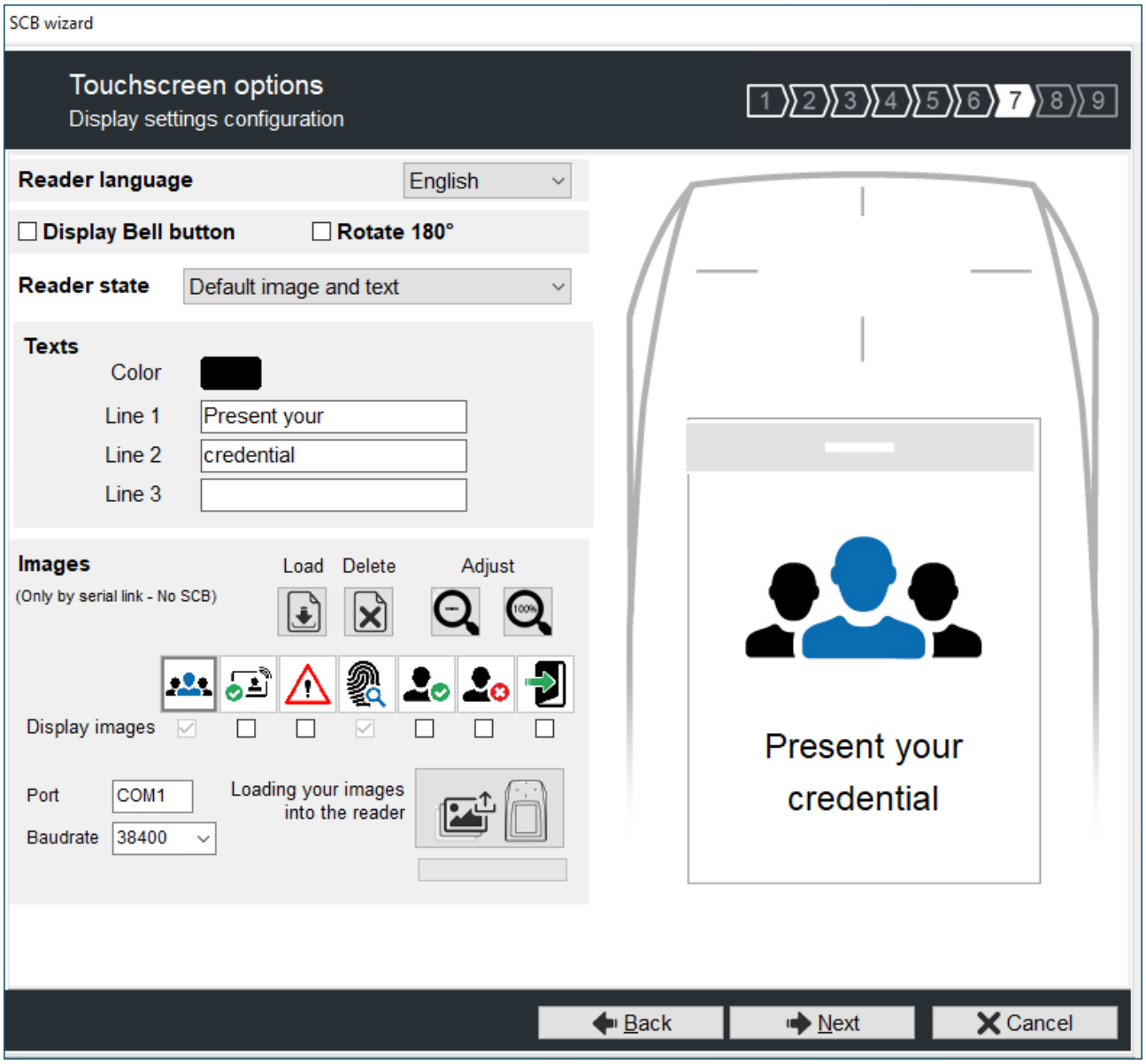
Flicker: depending on the backlight mode chosen, allows the keypad backlight LEDs to flash ON or OFF when a user presses a key on the keypad.

		
No backlight No backlight flash on key press	Backlight on No backlight flash on press	No backlight Backlight short flash ON when pressed
		
Backlight on Short flash OFF of the backlight on press	Backlight OFF and turns ON by pressing the key for a configurable time then returns OFF	

ARC options

	Eco mode (Low Power) In this mode, light is less intense, and the scan cycles reduced, the consumption of the reader is reduced of about 25%.
	Subdued (LED) Reduce drastically the led intensity
	Disable UHF configuration Deactivate the UHF chip. For more details about UHF configuration, refer to *VII. 10* - UHF config
	Disable all sounds emitted by the reader

SCB - Step 7



Display Bell button

Display or not the bell button on screen.
When you press the bell, it will be activated during 1s.

	Headband appearance
Keypad inactive and ring inactive	
Keypad active in Card AND Key mode and ring inactive	_ _ _ _ _
Keypad active in Card AND Key mode and ring active	_ _ _ _ _
Keypad inactive and ring active	

Warning

When the ring is active and if the reader has a screen then the tearing will not be effective on static relay (used for the ring).

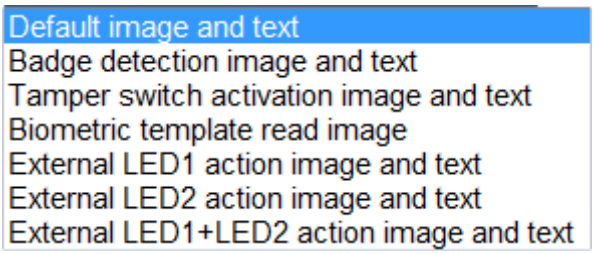
Rotate 180°: Used to rotate the image at 180°.

Reader Language

Choose the language used to display the text on the screen: English (default) or French.

Reader State

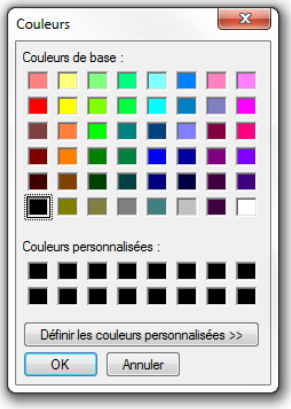
Select the state to change, either from the drop-down menu, or by clicking on the corresponding icon.



For each state, it's possible to change the image, the text and the text color.
Note: for the biometric, the text is not modifiable because it takes into account the number of fingers defined in the configuration wizard.

Texts

To change the text color, click on the color button.



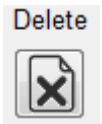
(the language of this windows depends on your Windows language)

The color applies to the three lines of text.

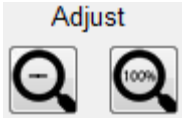
Image

Load an image file in SECard and adjust with the three button:

Load an image file for the selected state.



Delete the image file to the selected state.



Reduces the image on the screen.

Note: The classic image formats are supported (bmp, png, jpeg, ...). By against the screen reader does not support transparency, the background color is white.

Loading image into the reader

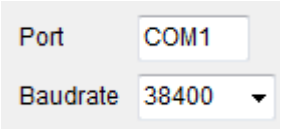
After loading the images into SECard for the seven states, they must be loaded into the reader.

The check boxes allow you to select the states will be activated by the SCB and validate the image on the screen. “Default” and “biometric” states are automatically activate.

Warning

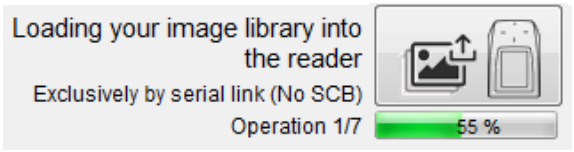
Loading images into the reader is possible only through the reader serial communication, not with the SCB.

1 - Connect the screen touch reader to your computer with the reader serial link and set the communication:

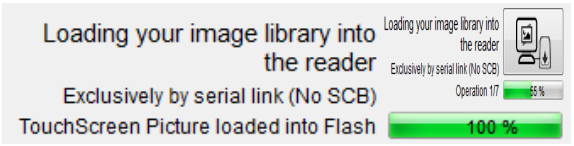


2 - Power on the reader and click on  while the **LED blinks orange for serial readers** or at any time for TTL readers.

3 - The loading progress is indicated by the progress bar:
The operation is repeated seven times, once for each image.

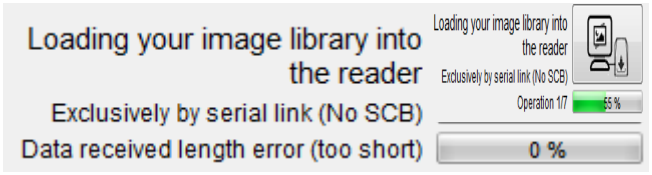


At the end you must have the message below:



Note:

* Each image has an index, a new load erases the image loaded before.
* If you get the message below, your communication settings are not correct, return to the step 1.



* If the image has been loaded into SECard was moved, the preview will not be available and the next image will be displayed in the IHM SECard.

* The display time of the state “Badge detection image and text” is defined in step 5 “LED and Buzzer” with “Blinks times” if the blink is activated or “LED duration”.

Default Image and text

	Visuel
Default Image and text	 Present your credential
Badge detection image and text*	 Detected card
Tamper switch activation image and text	 Alert Attempted tampering
Biometric template read image (none editable text)	 Place your finger on the sensor
External LED1 action image and text	 Authorized access
External LED2 action image and text	 Access denied
External LED1 + LED2 action image and text	 Free access

Important note

A configuration card created with a version of SECard <V2.1 (SCB < V8) for a standard reader will automatically activate the screen if it is presented to a reader ARC screen with only the image “default image and text” and images related to the states LED1 and LED2.

A configuration card created with a version of SECard <V2.1 (SCB < V8) for a standard keypad reader will automatically activate the screen in keypad mode if it is presented to a reader ARC screen with only the image “default image and text” and images related to the states LED1 and LED2. The default image is the keypad.

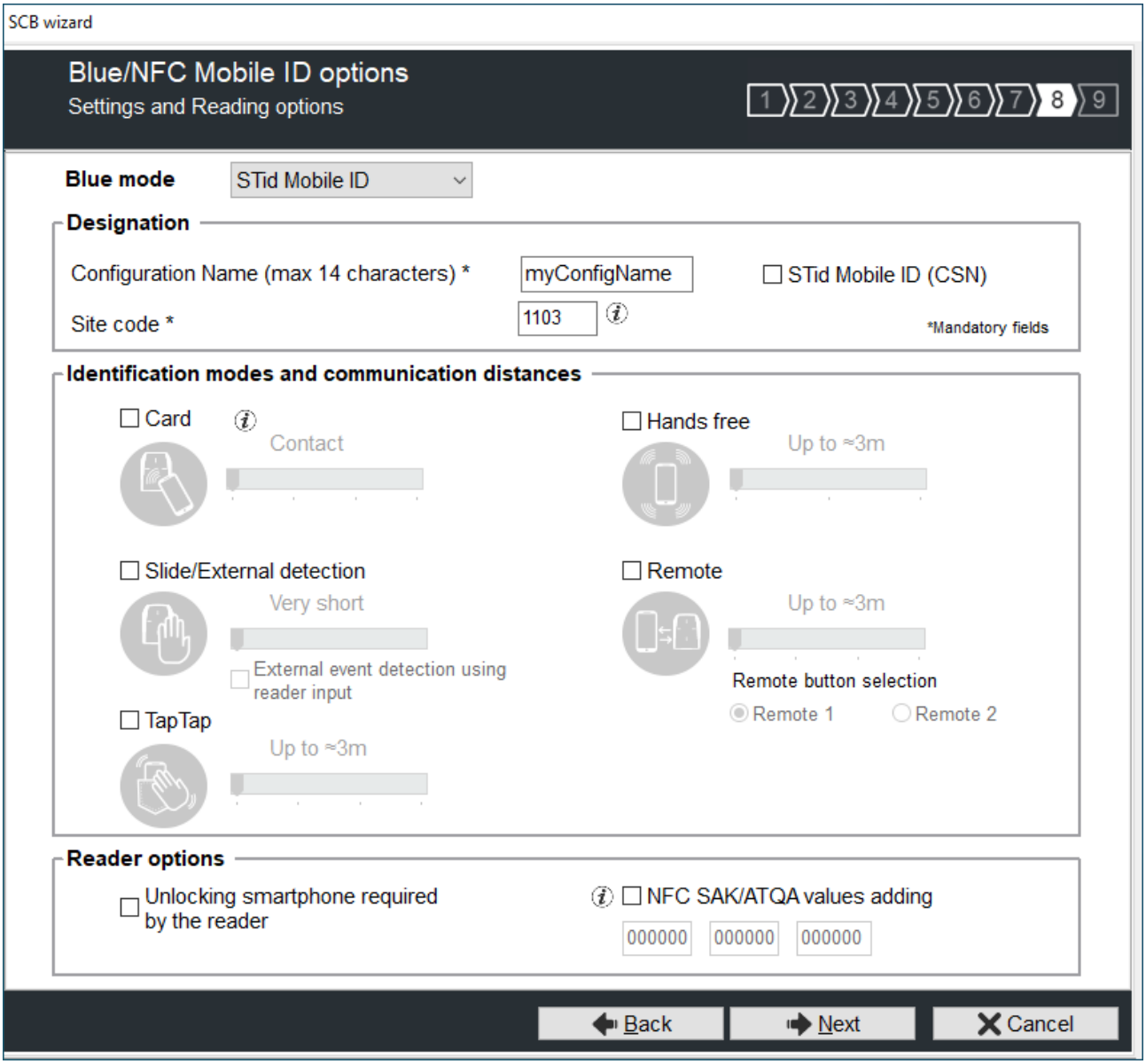
Compatible characters

'SPACE'	0x20
'!'	0x21
' " '	0x22
'#'	0x23
'$'	0x24
'%'	0x25
'&’	0x26
' ' '	0x27
'('	0x28
')'	0x29
'•'	0x2A
'+'	0x2B
','	0x2C
'-'	0x2D
'.'	0x2E
'/'	0x2F
'0'	0x30
'1'	0x31
'2'	0x32
'3'	0x33
'4'	0x34
'5'	0x35
'6'	0x36
'7'	0x37
'8'	0x38
'9'	0x39
':'	0x3A
';'	0x3B
'<'	0x3C
'='	0x3D
'>'	0x3E
'?'	0x3F
'@'	0x40
'A'	0x41
'B'	0x42
'C'	0x43
'D'	0x44
'E'	0x45
'F'	0x46
'G'	0x47
'H'	0x48
'I'	0x49

'J'	0x4A
'K'	0x4B
'L'	0x4C
'M'	0x4D
'N'	0x4E
'O'	0x4F
'P'	0x50
'Q'	0x51
'R'	0x52
'S'	0x53
'T'	0x54
'U'	0x55
'V'	0x56
'W'	0x57
'X'	0x58
'Y'	0x59
'Z'	0x5A
'['	0x5B
'\'	0x5C
']'	0x5D
'^'	0x5E
'_'	0x5F
'`'	0x60
'a'	0x61
'b'	0x62
'c'	0x63
'd'	0x64
'e'	0x65
'f'	0x66
'g'	0x67
'h'	0x68
'i'	0x69
'j'	0x6A
'k'	0x6B
'l'	0x6C
'm'	0x6D
'n'	0x6E
'o'	0x6F
'p'	0x70
'q'	0x71
'r'	0x72
's'	0x73

't'	0x74
'u'	0x75
'v'	0x76
'w'	0x77
'x'	0x78
'y'	0x79
'z'	0x7A
'{'	0x7B
'|'	0x7C
'}'	0x7D
'~'	0x7E
'*'	0x7F
'§'	0xA7
'°'	0xB0
'Ä'	0xC4
'Å'	0xC5
'Æ'	0xC6
'Ð'	0xD0
'Ö'	0xD6
'Ø'	0xD8
'Þ'	0xDE
'Ü'	0xDC
'ß'	0xDF
'à'	0xE0
'â'	0xE2
'ä'	0xE4
'å'	0xE5
'æ'	0xE6
'ç'	0xE7
'è'	0xE8
'é'	0xE9
'ê'	0xEA
'ë'	0xEB
'î'	0xEE
'ï'	0xEF
' ð '	0xF0
'ô'	0xF4
'ö'	0xF6
'ø'	0xF8
'û'	0xFB
'ü'	0xFC
'þ'	0xFE

SCB - Step 8



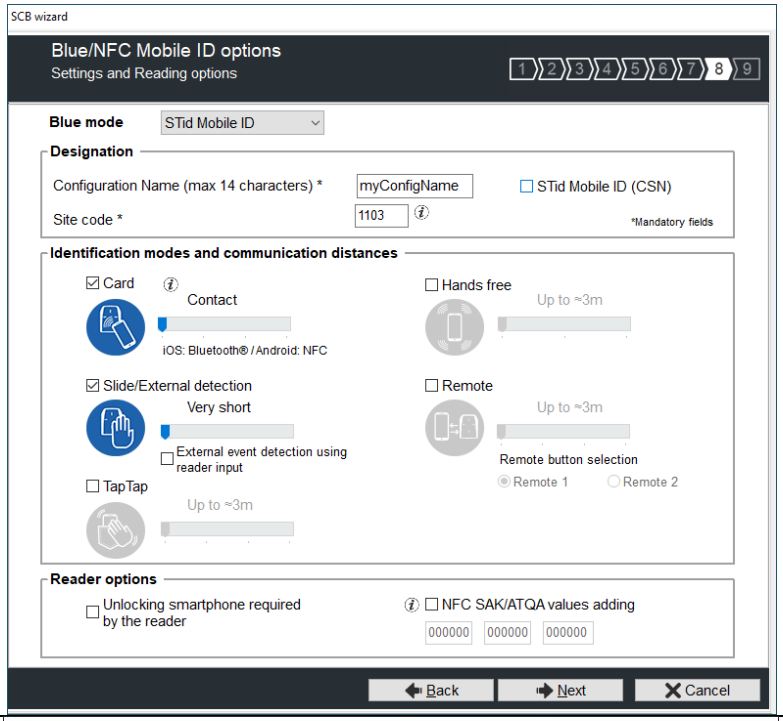
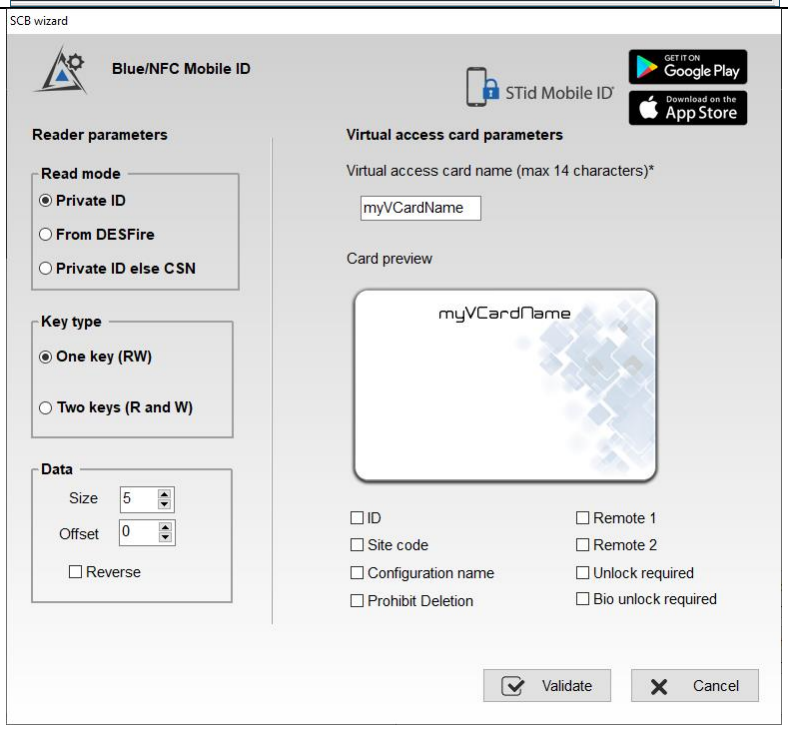
Four configurations are available for Bluetooth® authentication:

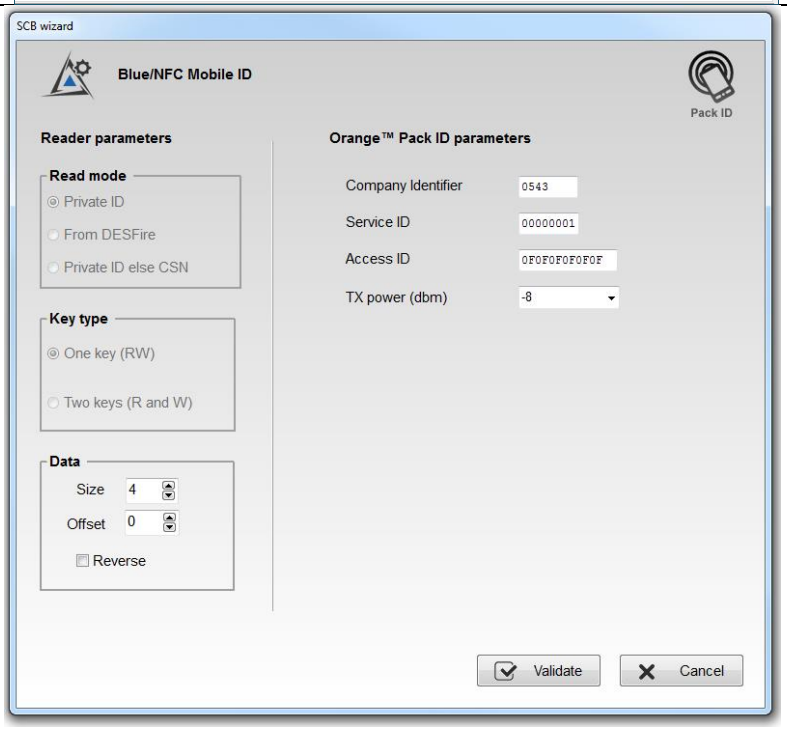
Configuration Name / Characteristics	ConfMobileID	ConfMobileID	SameAsDESFire	Custom
VirtualAccesCardName	STid Mobile ID	STid Mobile ID+	STid Secure ID	Custom
Identification modes	Only Card	All available except Remote	Only Card up to 0.5m	All available
Requires smartphone unlocking to authenticate	Select by customer	Select by customer	No	Custom
Site code	51BC	51BC	CRC16 CCITT AID DESFire	Custom

Blue/NFC mode

Configure the reader to read STid Mobile ID® or Orange™ Pack ID or Open Mobile Protocol.

This choice impacts the screen wizard Step 8 and Blue/NFC Mobile ID Settings:

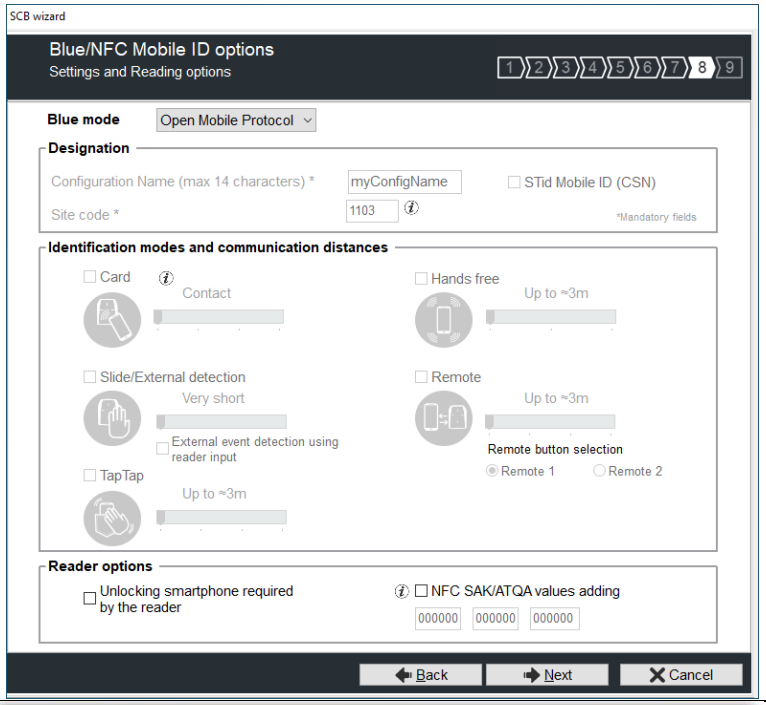
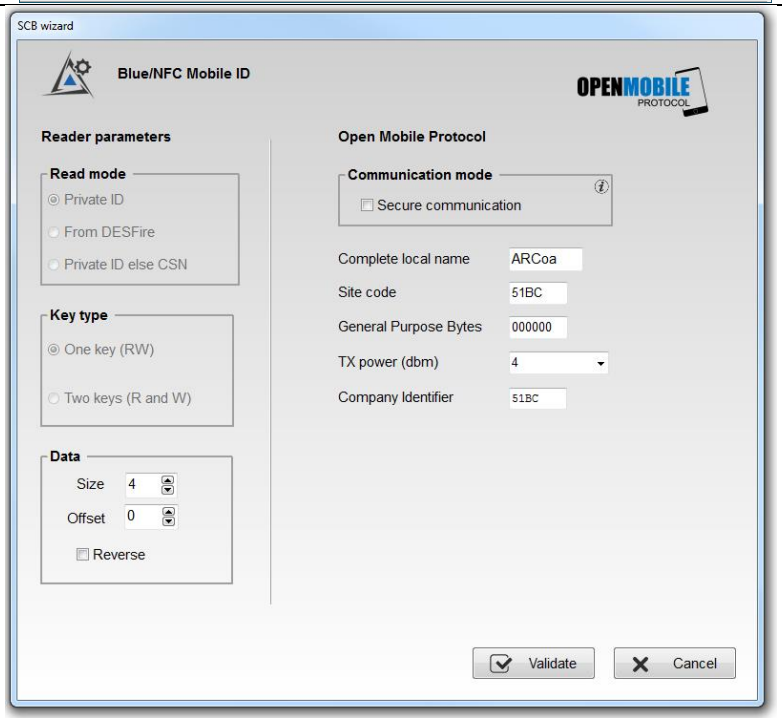
	STid Mobile ID®
Wizard Step 8	
Wizard Blue/NFC Mobile ID settings	

	Orange™ Pack ID
Wizard Step 8	
Wizard Blue/NFC Mobile ID settings	

Blue Mode Orange™ Pack ID

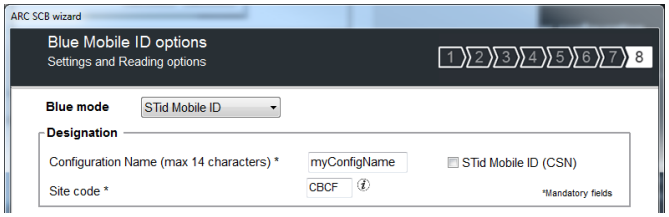
The detection mode for this application is fixed to Contact.

Warning: To configure the reader for this application, you must create a physical SCB and not a virtual SCB.

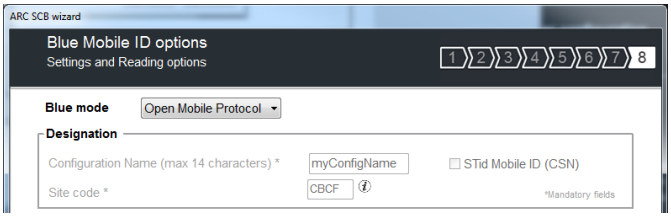
	Open Mobile Protocol
Wizard Step 8	
Wizard Blue/NFC Mobile ID settings	

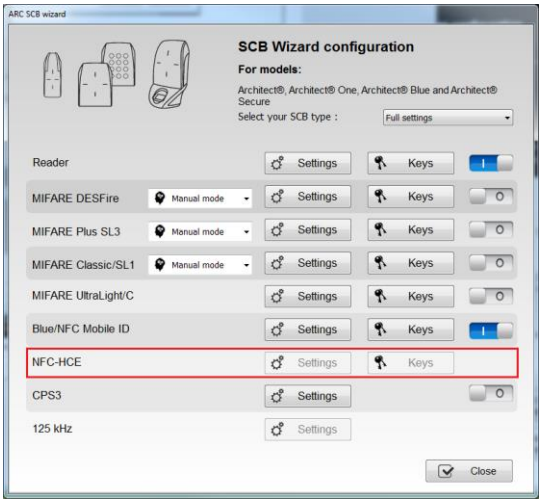
Blue/NFC Mobile ID and NFC-HCE compatibility

If “STid Mobile ID® “or “Open Mobile Protocol “ is activated, then it is not possible to activate “NFC-HCE“, the parameters and keys are greyed. The NFC Mobile ID is automatically activated.

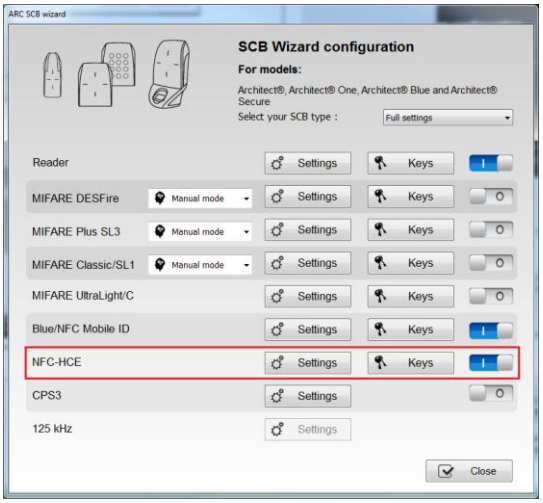


or



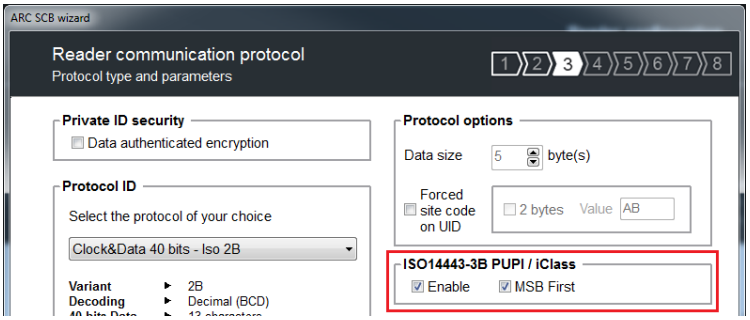


If “Orange™ Pack ID“ is activated it is possible to activate “NFC-HCE“, the parameters and keys are not greyed.



NFC Mobile ID and « ISO14443-3B PUPI / iClass » compatibility

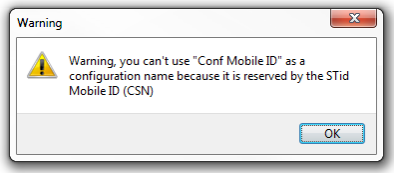
“NFC Mobile ID” and “ISO14443-3B PUPI“ can be activated at the same time as “NFC Mobile ID“ is compliant with ISO14443-A.



Blue Mode STid Mobile ID®

Designation

- Configuration Name: enter the name of the configuration Mobile ID Secure Plus: 14 characters max.
  Note: configuration name “Conf Mobile ID” is reserved to STid Mobile ID®.



- Site Code: 2-bytes data used for the site code of the configuration.
  Note: site code 51BC is reserved for STid Mobile ID®.

- STid Mobile ID® (CSN): configure the Blue reader to read only a CSN on the smartphone.

Identification modes and communication distances

For each identification mode the communication distance is adjustable.

❖ **Card:**

By placing the smartphone in front of the reader.

- Contact: smartphone must be in contact with the reader.
- Up to 0.2m: smartphone must be in an area of 0.2m around the reader
- Up to 0.3m: smartphone must be in an area of 0.3m around the reader.
- Up to 0.5m: smartphone must be in an area of 0.5m around the reader.

❖ **Slide/External detection:**

Slide: By placing your hand close to the reader without taking out your smartphone.

External detection: Works by changing the potential applied to the LED2 input (see details below).

The distance between the smartphone and the reader can be:

- Very short
- Short
- Medium
- Long
- Very long

Not available for ARC1S neither ARCS keypad in Card or Key mode.

❖ **Tap Tap:**

By tapping your smartphone twice in your pocket for near or remote opening.
The communication distance can be:

- Up to 3m
- Up to 5m
- Up to 10m
- Up to 15m.

❖ **Hands free:**

By simply passing in front of the reader.
Communication distance around the reader:

- Up to 3m
- Up to 5m
- Up to 10m

❖ **Remote:**

By controlling your access points remotely.
Communication distance around the reader:

- Up to 3m
- Up to 10m
- Up to 15m
- Up to 20m

❖ **Remote button selection**

If the identification mode "Remote" has been activated, it allows to associate the current configuration to the Remote button 1 or Remote button 2.

Notes:

The notion of distance in Bluetooth® corresponds to an area around the reader, not just in the front.
Reading distances depend on the environment, on the position smartphone // reader ...

It is recommended to do on-site testing to evaluate the settings.

Warning

When Architect® Blue readers are installed close to each other, detection distances must be defined to accommodate the distance between the readers to avoid cross readings.

❖ **External event detection using reader input:**

Hand (slide mode) information is given by capacitive sensor or input LED2 level on ARCS reader.

If enabled: information is given by LED2 level.

- LED2 no connected or connected to high level = Hand not present
- LED2 connected to the GND = Hand present.

For example: connect a detection system to the LED2. When people are detected, the smartphone reading is activated.

❖ **Unlocking smartphone required by the reader: security option**

- If checked: the smartphone must be unlocked (with PIN code or other unlocking option depending on the smartphone) to authenticate with the reader.
- If unchecked: unlocking the smartphone is not required to authenticate with the reader.

❖ NFC SAK/ATQA values adding

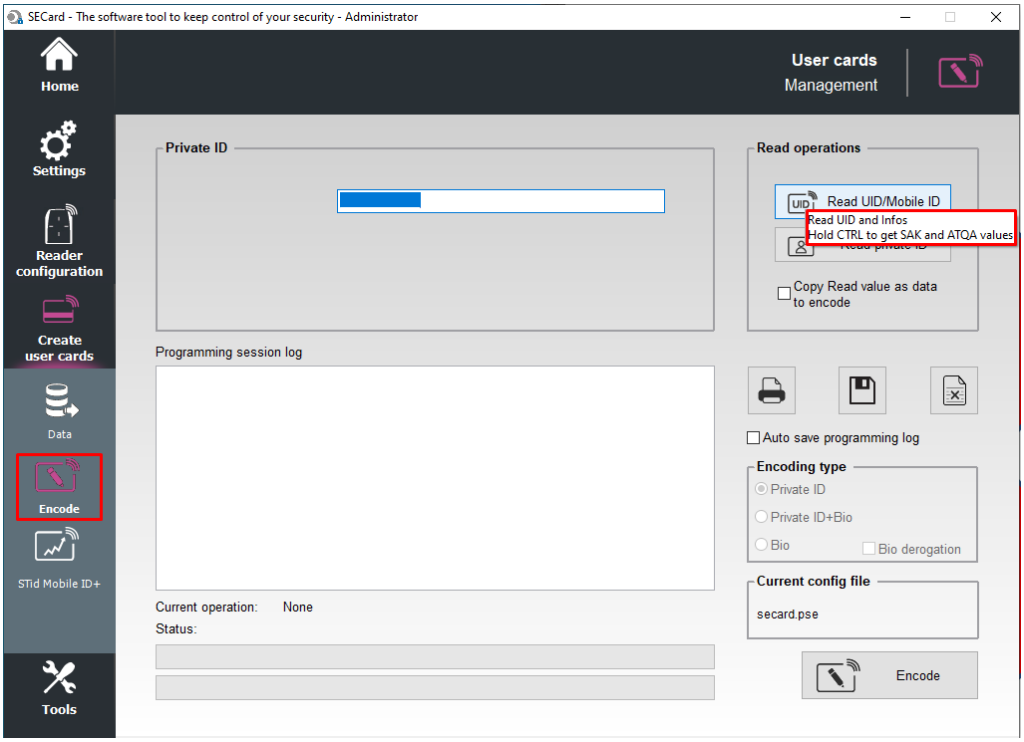
In RFID a chip is identified by two parameters ATQA and SAK. These parameters must be known to the readers for read the identifiers.

Smartphones in NFC mode meet this same rule. Some ATKA + SAK are already implemented in STid readers.

To ensure the compatibility of the readers with the reading of new smartphones in NFC mode, these fields make it possible to set up three values of ATQA and SAK**.**

How to know these values for your smartphone:

- ❖ Enabled the NFC on the smartphone
- ❖ Go to Create user cards

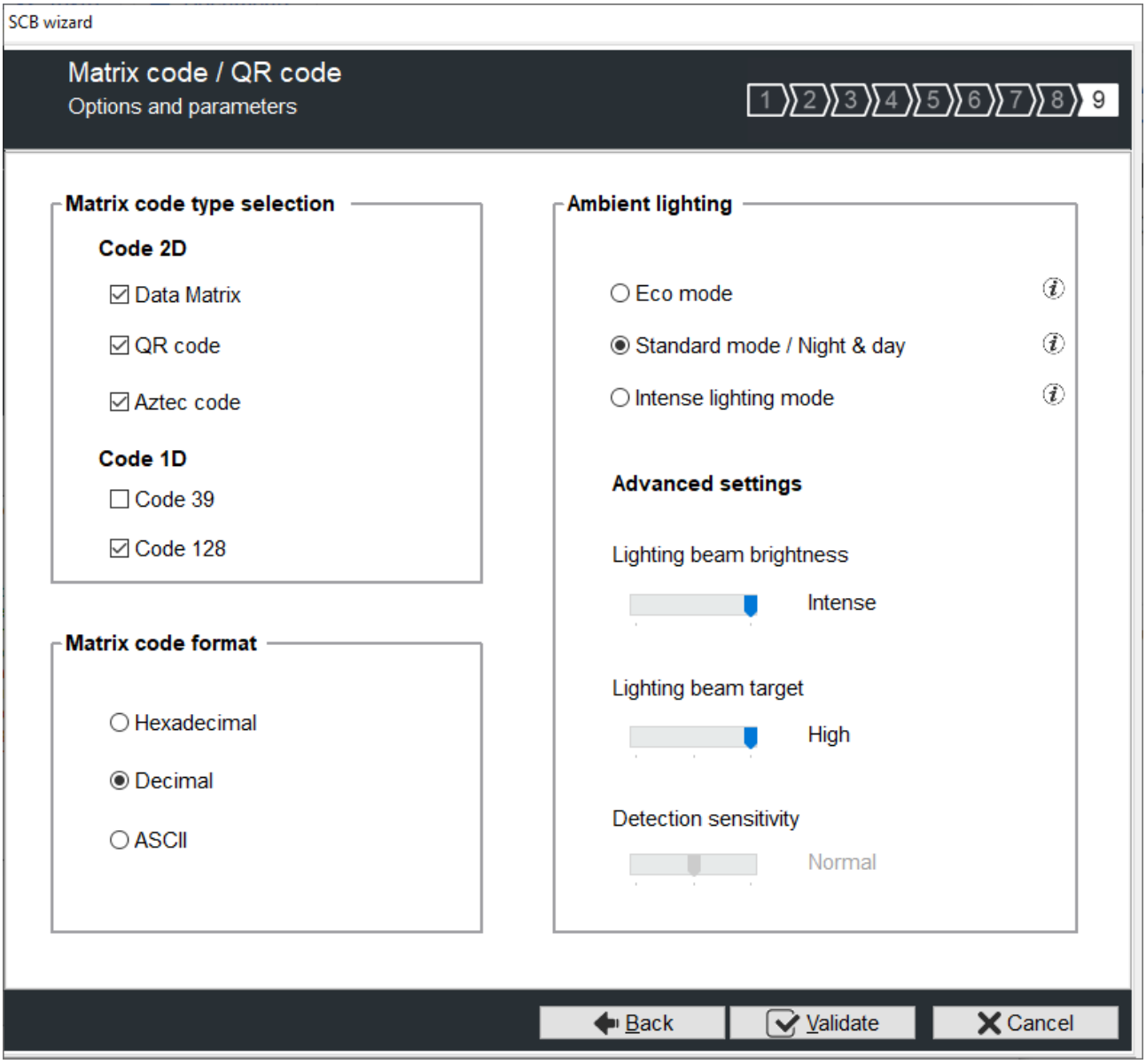


- ❖ Present the smartphone to SECard encoder and hold CTRL + click on Read UID button
- ❖ Result Current operation: SAK=20, ATQA=0004
- ❖ Enter this value in the field: ☑ NFC SAK/ATQA values adding 200400 000000 000000

Notes:

- The NFC-HCE option for “NFC Mobile ID” is not a SECard option. It has to be activated in STid Mobile ID® app (activated by default).
  This feature is only available for Android phones.
- “NFC Mobile ID” is not compatible with STid Settings app.

SCB - Step 9 *Adding functionality 3.6*



❖ **MATRIX / QR code type selection**
Select the code type to be read:

Data Matrix	QR Code	Aztec code	Code 128	Code 39
			 123456	 123456
123456	123456	123456		

❖ **MATRIX / QR code format**

Select the format of the matrix / QR code to be read.

The maximum size of the code depends on the format chosen:

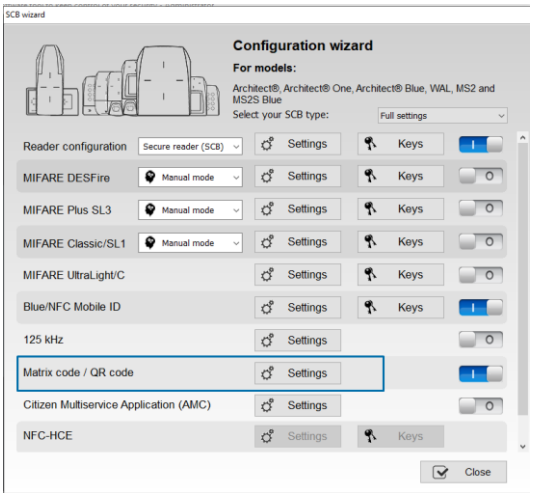
Format	Size in characters	Size in bytes	
Hexadecimal	96	48	
Decimal	25	10	De 0 à 120892581961462917470617 5 0x0 à 0xFFFFFFFFFFFFFFFFFFFF
ASCII	192	48	

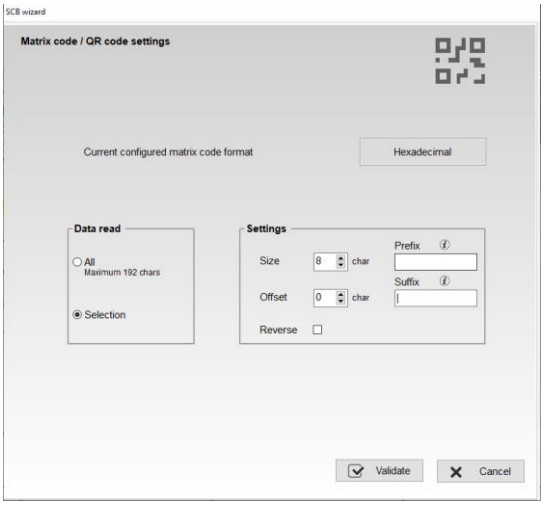
Note: only the characters list below are authorized in ASCII:

Value	ASCII character	Value	ASCII character	Value	ASCII character
30	0	38	8	61	a
31	1	39	9	62	b
32	2	41	A	63	c
33	3	42	B	64	d
34	4	43	C	65	e
35	5	44	D	66	f
36	6	45	E		
37	7	46	F		

Note: if the code to read is not in the code type set in the wizard, the code is not read. For example, if decimal type is set and the code to read contain letter the code will not read.

To read a specific part of the data code go to the settings Matrix / QR code:



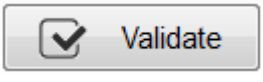


❖ **Ambient lighting**

- Eco mode
- Standard mode / Night day
- Intense lighting mode

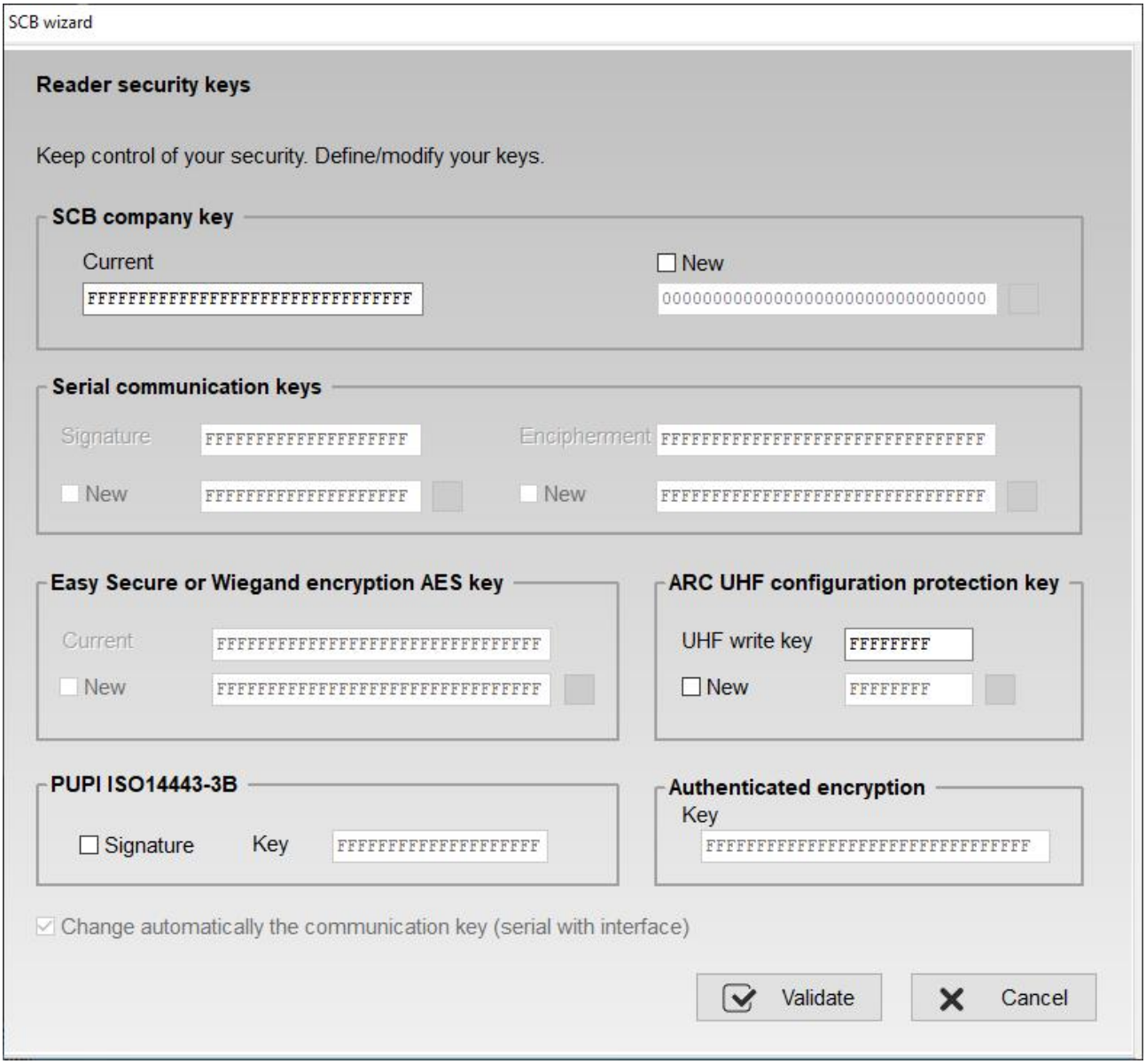
❖ **Advanced settings**

Lighting beam brightness	Control the power of the spot which illuminates the code	Normal		Intense
Lighting beam target	Control the power of the laser which targets the code	Low	Normal	High
Detection sensitivity	Control the sensitivity of the trigger to start scanning the code	Low	Normal	Max

Click the button 

to complete the reader configuration settings.

III. 2 - SCB Wizard: reader security keys



SCB company key

Configurable readers with « *SCB* » card are initially supplied with default configuration (factory key 0XFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF).
These can be configured by a "SCB" with 0xFF…FF in current key to a new company key.
It can be entered manually or automatically by pressing CTRL + R or by right click "Fill with a random value."

After the initial configuration and in order to reconfigure the reader, it will be necessary to present to the reader "SCB" with a company key similar to that recorded by the reader.

Warning

This key is important and should definitely be known by the administrator. It protects the data from the "SCB" and allows changes to the configuration of readers.

If you lose this key, the reader cannot be reconfigured for another "SCB" and will must be reset at the factory.

Serial communication keys

Modify the signature and encipherment keys for serial secured reader (S32 / S35 / S33).
For more information about the protocol, refer to
T5.2 - Bidirectional communication mode

Easy Secure or Wiegand encryption AES key

Modify the enciphered AES key used to secure the connection between the reader R33 and INTR33E and the output reader S31.
Note:
The default value (factory settings) is «*FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF*».
It is mandatory to change the value of this key so that the output is encrypted.

PUPI ISO 14443-3B

Enter the key used for the signature calculation, called “secret key” (10 bytes).

ARC UHF configuration protection key

Change the write UHF configuration key, if enabled. It recommends to change it, to protect the configuration in the chip in against further write operations.

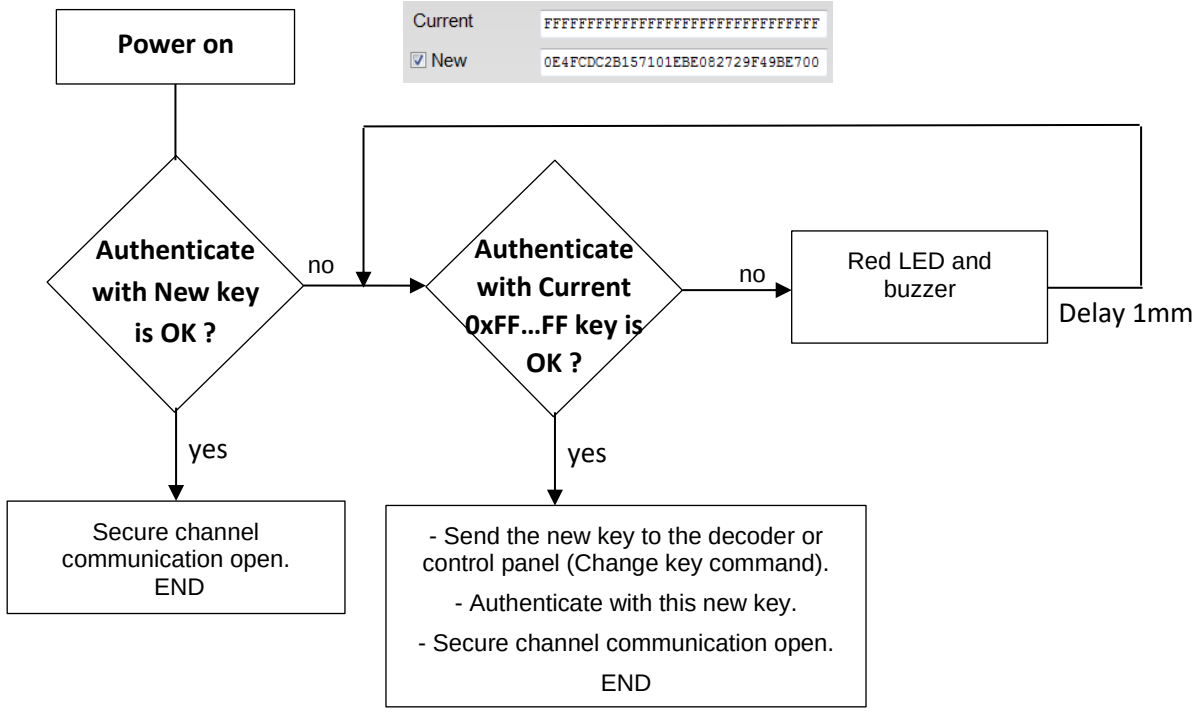
Authenticated encryption:

Enter the authenticated encryption key.

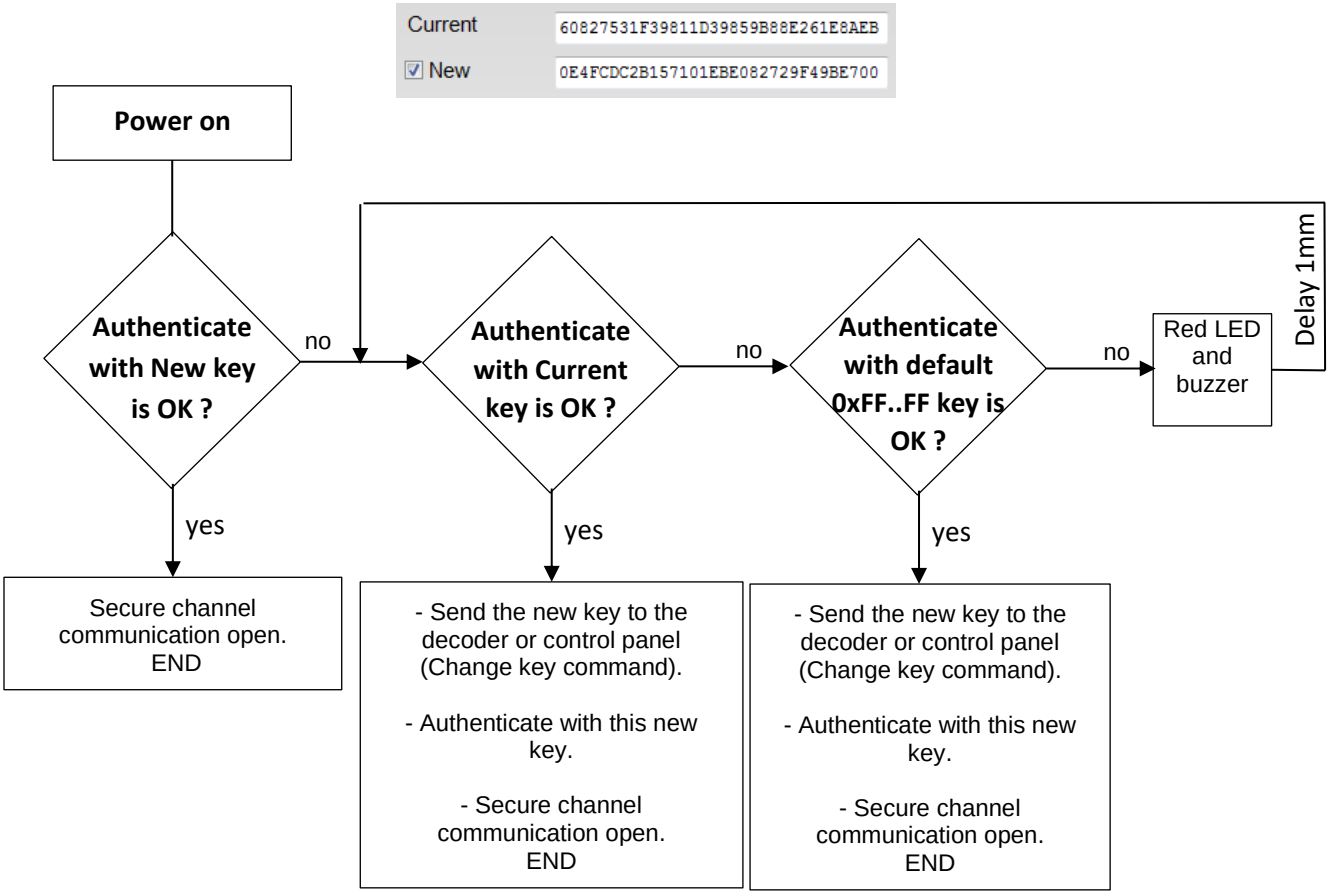
Change automatically the communication key: by default, select this option.

- **Activate:**
  In SECard <v3.3.x this option is automatically activate. The authentication sequence at the power on of the reader are:

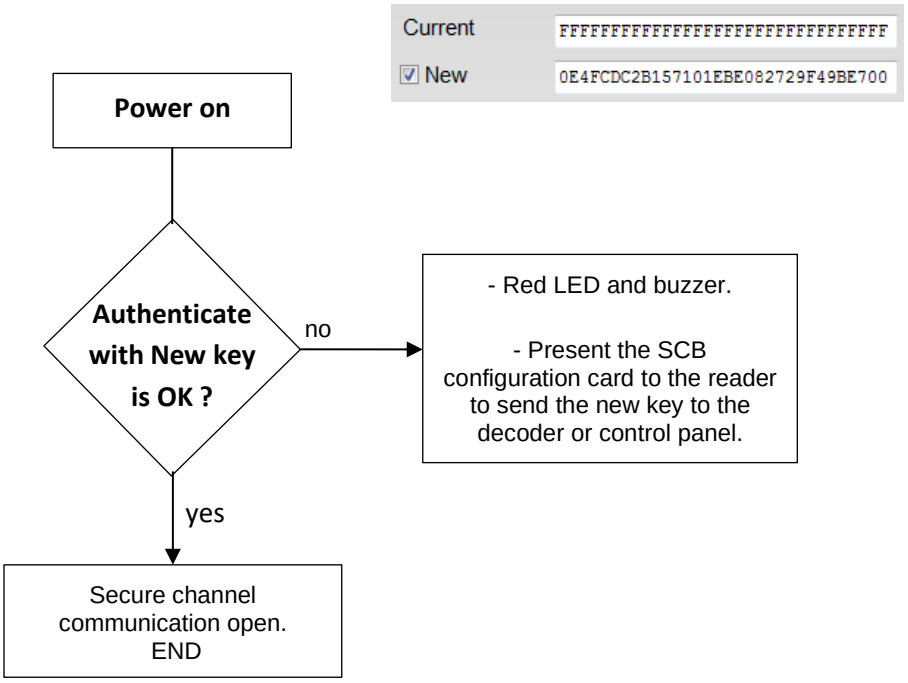
- 1st case: The current decoder or control panel key is the default key 0xFF…FF.



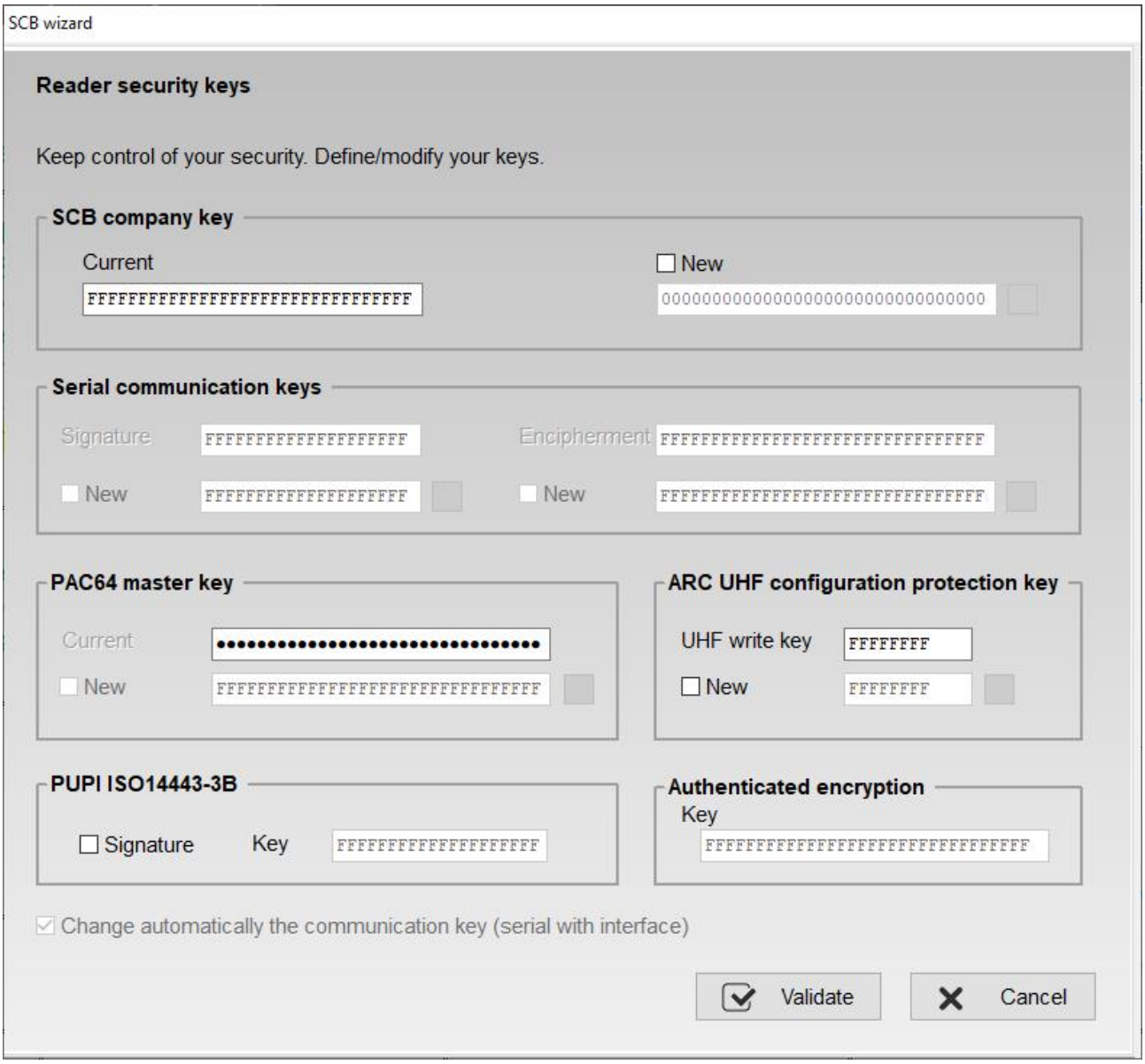
- 2nd case: The current decoder or control panel key is different to default key.



❖ **Not Activate:** the authenticate sequence is:



If PAC 64 protocol selected at step 3



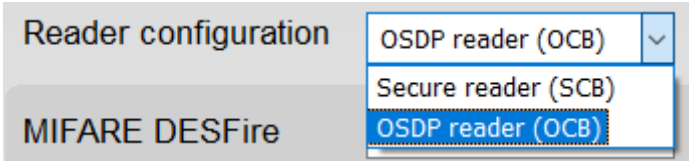
PAC64 master key: Enter the authenticated PAC64 encryption key.

Click the button 

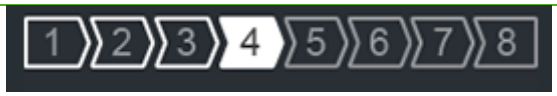
to complete the key settings.

III. 3 - OCB Wizard: Reader configuration settings

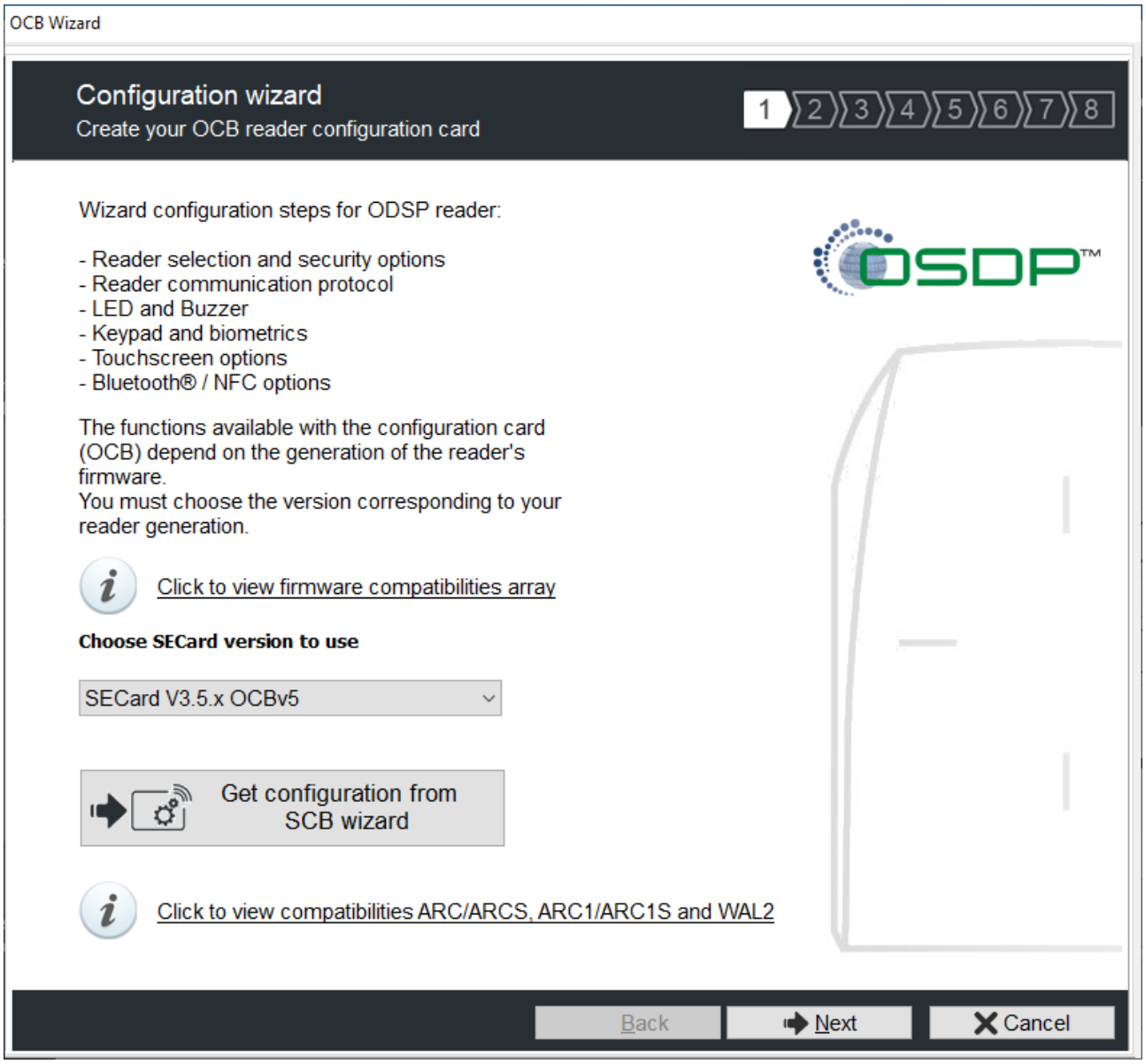
Reader configuration: In the list select OSDP reader OCB



Reader "settings": The reader configuration is done in five steps. To move from one stage to another, you must click on "Next".

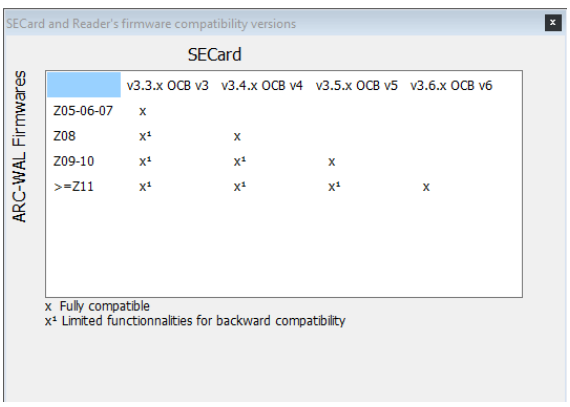
 Click here	Configuration wizard
 Click here	Reader type and options
 Click here	Protocol and options
 Click here	LED and Buzzer
 Click here	Keypad and biometrics options
 Click here	Touchscreen options
 Click here	Blue/NFC Mobile ID options
 Click here	Matrix / QR code

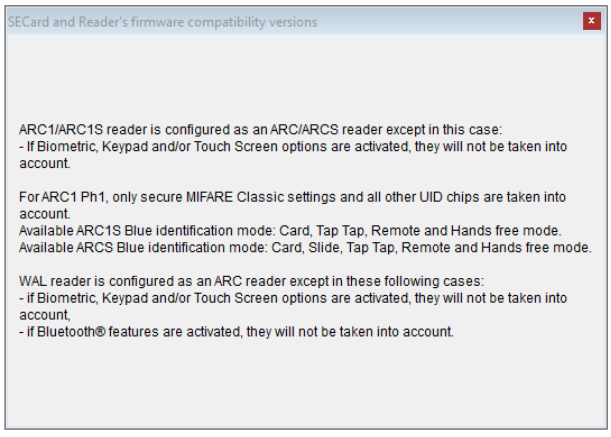
OCB - Step 1

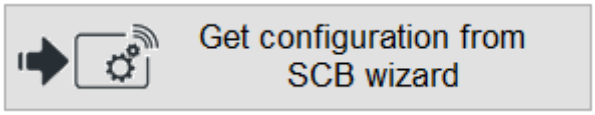


The available functionalities and the compatibility of OCB depend on reader firmware generation.

To provide compatibility between SECard and firmware versions, SECard proposes the choice about SECard version to use if the option is validated in “Files” cf. *II. 3* - Files.

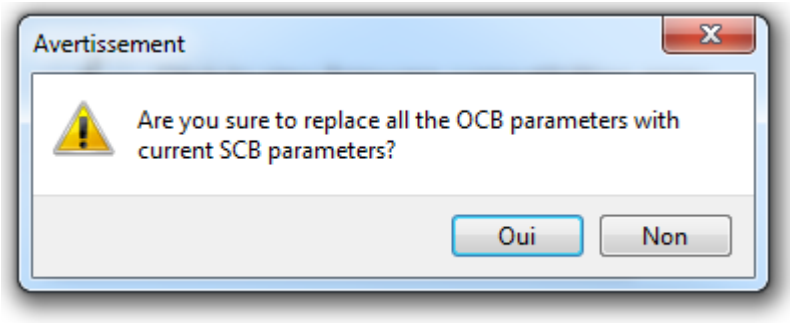


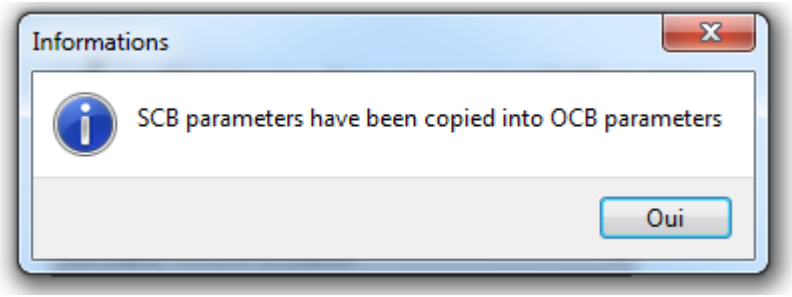




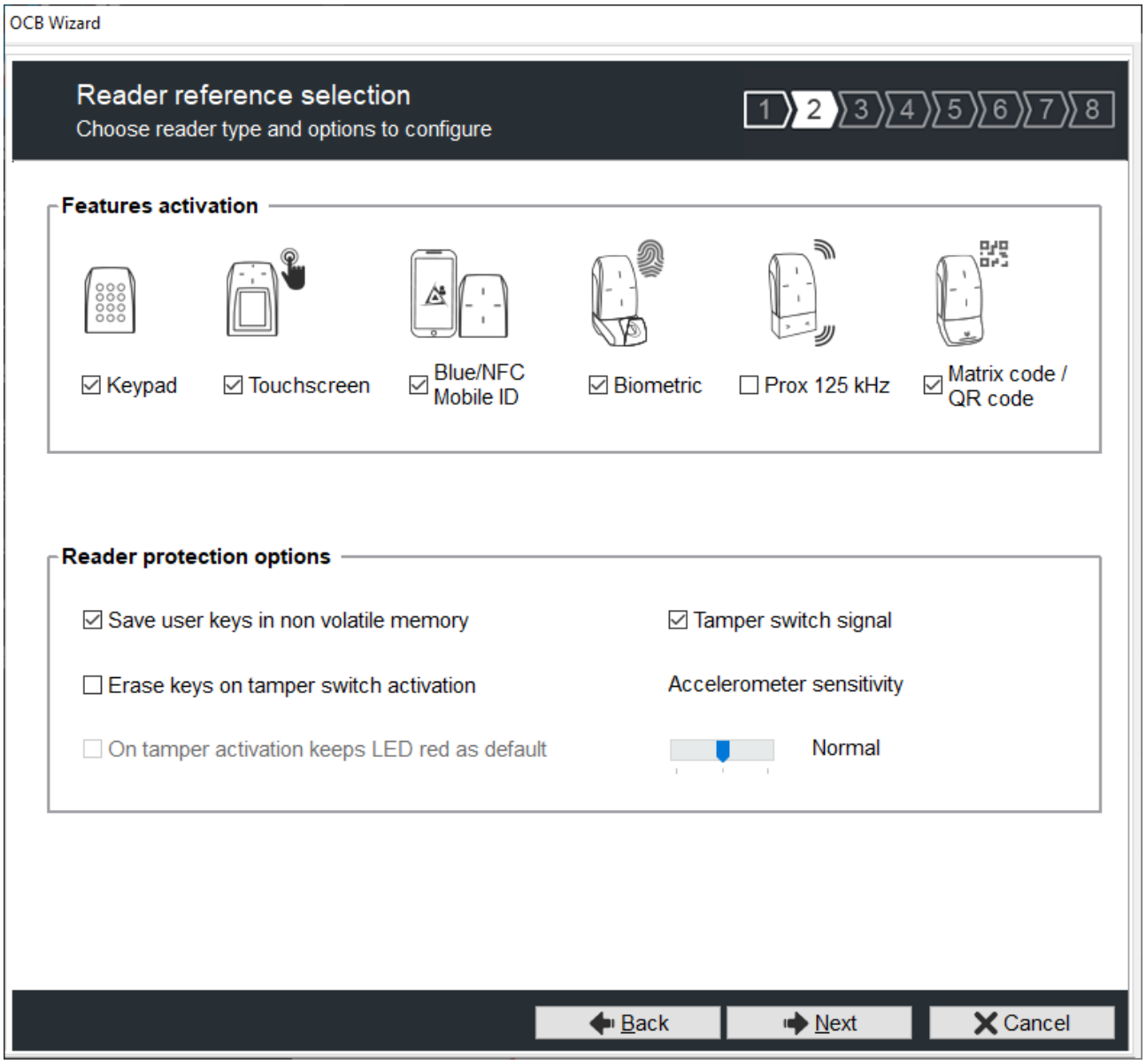
❖

When you click on Get configuration from SCB wizard all parameters defined in OCB wizard are set in wizard will be replace by the parameters presents on the SCB.





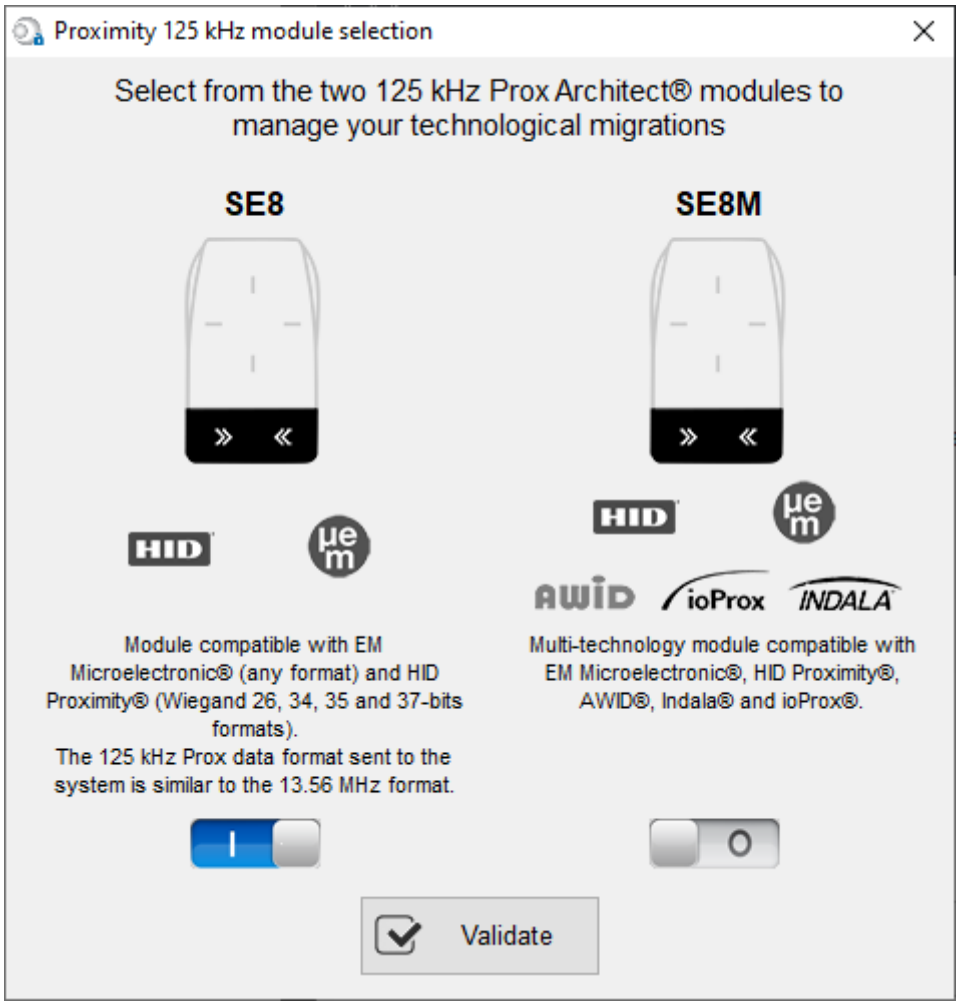
OCB - Step 2



Features activation:

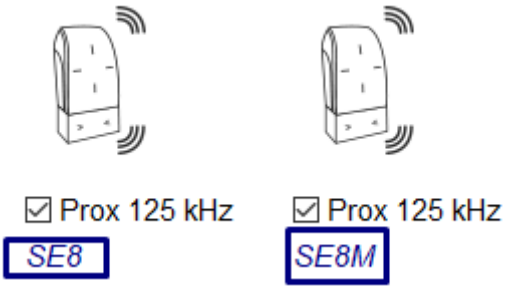
- To activate keypad configuration.
- To activate touchscreen configuration.
- To activate Blue/NFC Mobile ID configuration.
- To activate the biometric configuration.

❖ To select 125 kHz module (SE8 or SE8M) and activate configuration.



This choice impacts on 125kHz settings.

You can see the current model on the screen



❖ To activate Matrix / QR code configuration.

Reader protection option

- Save user keys in non-volatile memory: enables the keys to be saved, in encrypted form, in EEPROM non- volatile memory, in case of power failure.

- Erase keys on tamper switch activation: enables all the reader keys to be erased, if the status or accelerometer is changed.

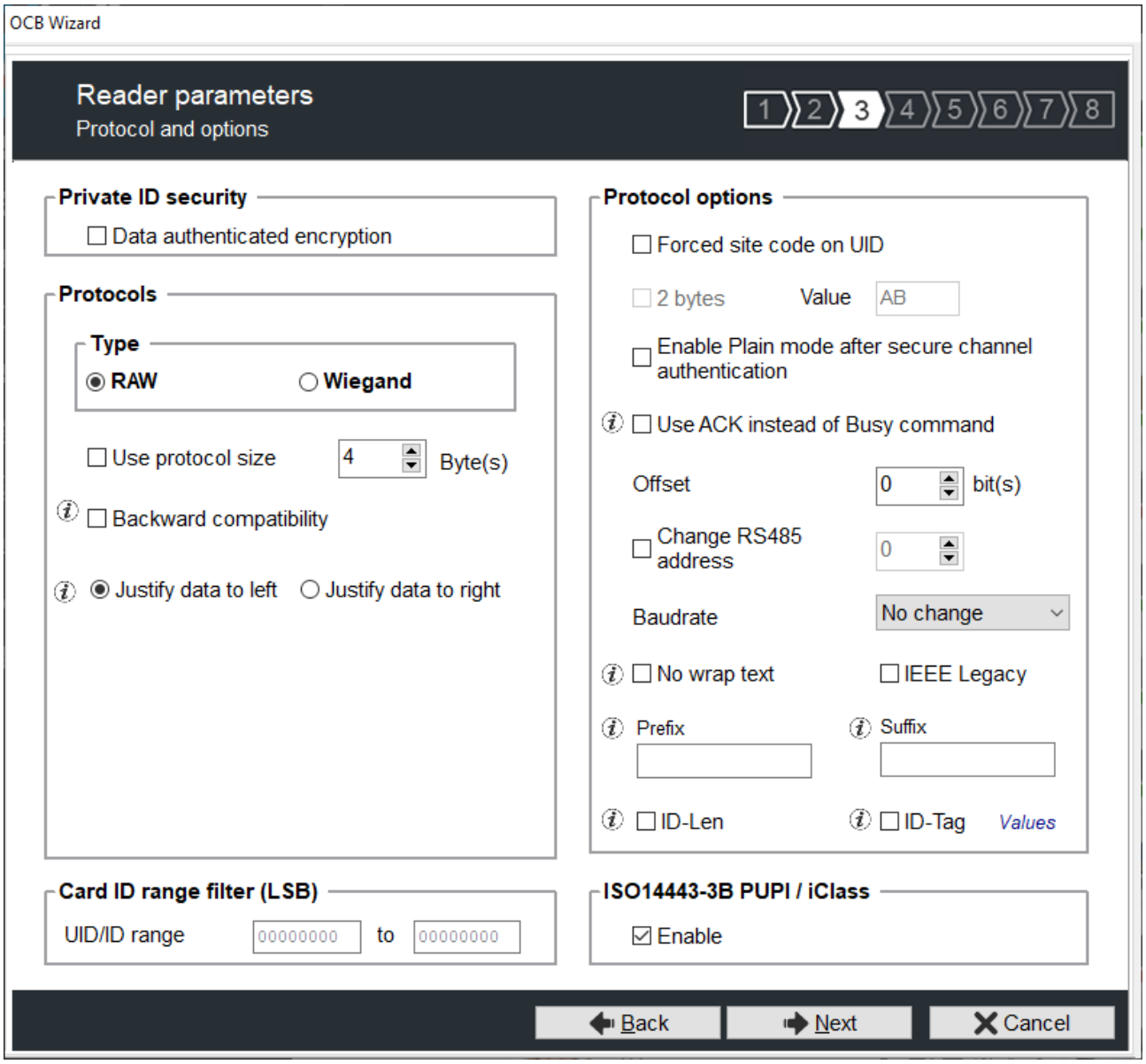
- On tamper activation keeps red as default: requires activation of tearing.
  If the status of accelerometer is changed, LED is on the red indicating that the keys have been erased.

- Tamper switch signal: enables the tamper switch signal to be activated.

- Accelerometer sensitivity

  The ARC reader range includes an accelerometer to detect the reader tearing. Depending on the support / installation location of the reader, it may be necessary to adjust the sensitivity of the sensor so that only an effective tear is detected.

OCB - Step 3 *Adding functionality 3.6*



❖ Private ID security

Private ID can be encrypted AND signed before being written in the card.
The reader will decrypt and authenticate the private ID before sending it on its output media.
Only an ID correctly decrypted and authenticated will produce an output data, otherwise the reader will remain mute.
The Authenticated Encryption uses the MtE mode (Maced then Encrypt).

Note: The size of private identifier is limited to 12 bytes.

❖ Protocols

[REPLY]: osdp_RAW – 50h

SOM	ADDR	LEN	CTRL	REPLY	DATA				CRC / CKSUM
							Count		
					Reader number	Format code	LSB	MSB	Data	
53h	Physical Reader Address [80h...FEh]	XXh XXh: CKSUM XXh XXh: CRC	XXh	50h: osdp_RAW						XXh / XXh XXh

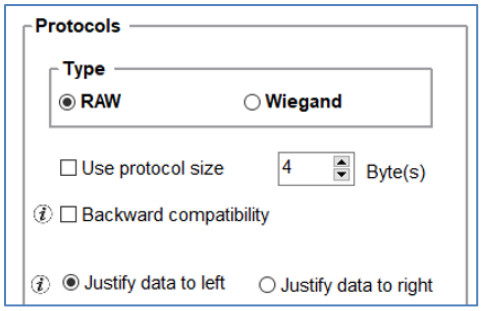
Reader number: 00h First reader
1 byte 01h Second reader….

Format code: 00h not specified, raw bit array
1 byte 01h P/data/P (Wiegand)

Count: 2-byte size (in bits) of the data at the end of the record
2 bytes

Data: MSB to LSB (left justified)
n bytes

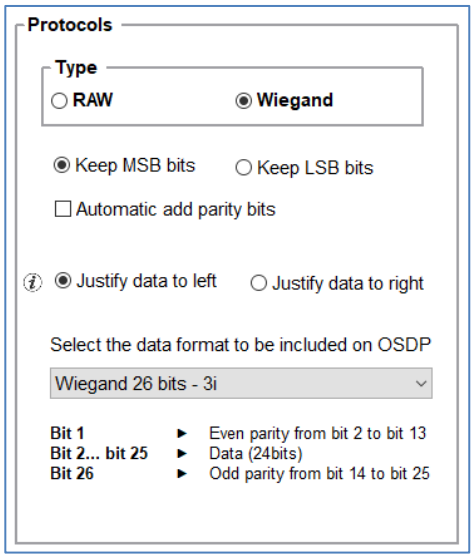
Type RAW



- Type Raw + Backward compatibility: Format code is fixed to 01h.
- Type Raw: Format code is fixed to 00h.

Use protocol size: Allow to fix the data size send by the reader to the OSDP_RAW command (UID and Private ID).

Type Wiegand



- Format code is fixed to **01h**.
- 3 different Wiegand are available: Wiegand 26bits, 35 bits and 37 bits.

For 13.56MHz, BLE/NFC and Private ID 125kHz possibility to format the data send in osdp_RAW with Keep MSB or LSB bits data, add a zero padding on left or right (Left justified or Right justified) and add parity bits on the data read.

For UID 125kHz, the reader calculates and adds the parity bits obligatorily with the configuration Keep LSB / Add parity bit / Left justified. The options defined in SECard are not take into account.

Protocol options

- "Forced site c*ode on UID":* force a site code whatever the communication protocol.
  The value of the code will be transmitted most significant on one or two bytes.
  UID can be truncated according to the protocol used.

- Enable Plain mode after secure channel authentication:

  - disable: after osdp_keyset command with a key different from default key SCBKD, it is mandatory to communicate over the secure channel.

  - enable: after odsp_keyset command with key different from default key SCBKD, it is possible to communicate in plain mode even after successful authentication.

- Use ACK instead of Busy

  Tick this option if the system does not take into account "osdp_Busy" reply.

  - disable: reply is osdp_busy.

  - enable: reply is osdp_ACK.

  Corresponds to the Manufacturer command:

IX.5- MFG_BUSY_ACK_SWITCHING

The command MFG_ BUSY_ACK_SWITCHING allows to send osdp_ACK reply instead of osdp_BUSY.

Allows compatibility of STid osdp readers with control panels that do not support osdp_BUSY replies. This command is only available in plain mode.

SOM	ADDR	LEN	CTRL	CMD	DATA			CKSUM / CRC
53h	Physical Reader Address [00h...7Eh]	0Dh 00h: CKSUM 0Ch 00h: CRC	XXh	80h: osdp_ MFG	F5h1Bh C0h	05h	DATA	XXh / XXh XXh

DATA: *1 byte*
00h reply is osdp_BUSY
01h reply is osdp_ACK

- Offset in bit

  Allow to fix the first bit of ID send by the reader to the OSDP_RAW command (UID and Private ID).
  Adjustable from 0 to 255 bits.

  example: if the offset is 6 and the data is 0x123456 (hexa), 0b0001 0010 0011 0100 0101 0110 (binary)
  The data with the offset will be 0b10 0011 0100 0101 0110 (binary), 0x023456 (hexa)

- Change RS485 address / Baudrate:

  Allow to fix the RS485 address and the Braudate with OCB configuration badge, without use the osdp_COMSET command.

- No wrap text: Link to OSDP_TEXT command (default disable)

  - Disable: if the OSDP_TEXT command is used to display more than 1 text line or 1 text line that not fitted on only 1 text line, then the reader will clear all the screen and will display the corresponding text.

  - Enable: the reader will cut the text beyond the first line; the reader will display only the first line and will not clear all the screen.

New 3.6

- IEEE Legacy:

For readers with firmware version < Z11: IEEE= 0xF51BC0
For readers with firmware version ≥ Z11: IEEE= 0x2C17E0

☐ IEEE Legacy IEEE= 0xF51BC0

☑ IEEE Legacy IEEE= 0x2C17E0

Note: Following an update with firmware ≥ Z11, it automatically switches with the new IEEE number (0x2C17E0).

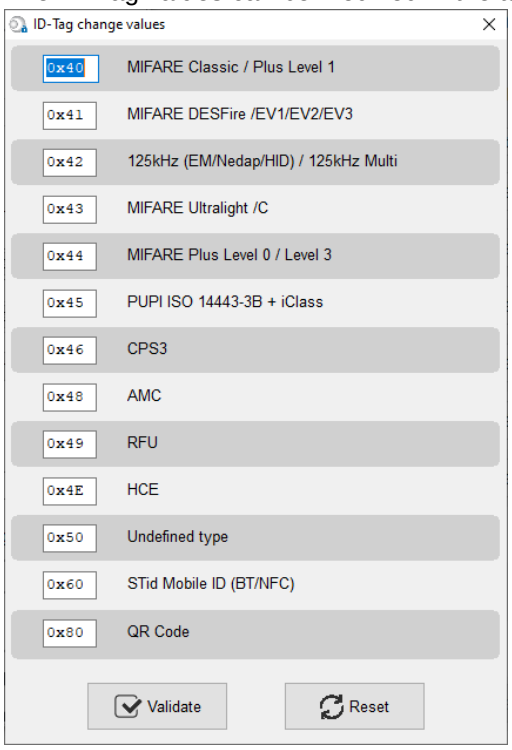
In Raw mode, it is possible to customize the data before transmission with the following information:

<Prefix><ID-Tag><ID-Len><ID-Number><Suffix>

- *Prefix*: add a prefix before sending the frame. Hexadecimal value on maximum 5 bytes.
- *Suffix:* add a suffix before sending the frame. Hexadecimal value on maximum 5 bytes.

- *ID-Tag:*

One byte which identifies the type of "tag" read and will be added to the frame.
The ID-Tag will be added to a UID or to a private ID.
The ID-Tag values can be modified in the table below:

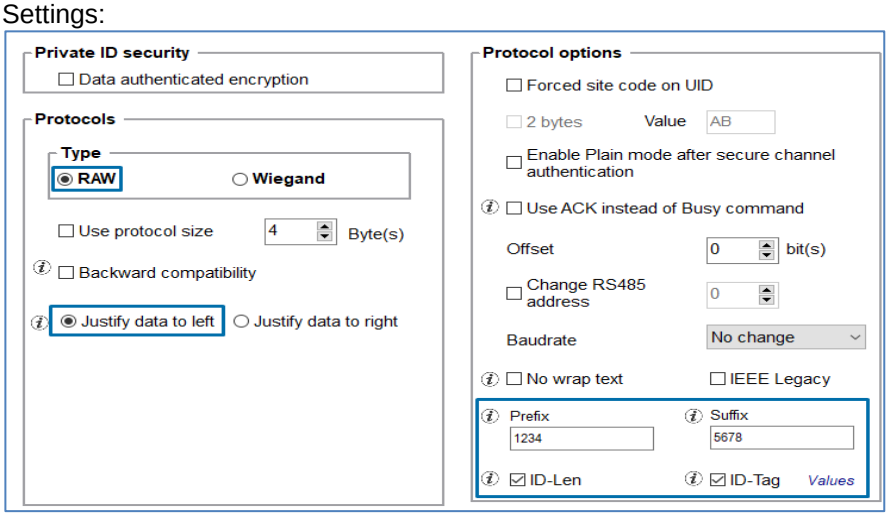


The Reset button restores the default STid values.

- *ID-Len:* 2 bytes indicating the length of the ID-Number
  - For data in Hexadecimal: ID-Len = number of bytes of ID-Number
  - For data in decimal: ID-Len = number of characters of ID-Number

Example 1:

Settings:



Tag: DESFire
ID-Number = 0000ABCDEF
ID-Len = 5

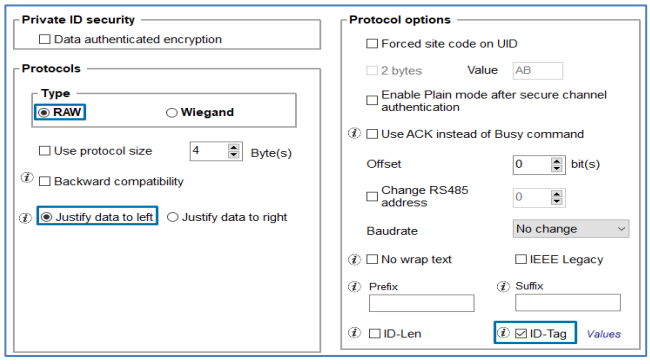
OSDP Data:1234541000500000ABCDEF5678

Prefix	ID-Tag	ID-Len	ID-Number	Suffix
1234	41	0005	0000ABCDEF	5678

OSDP bit count = 96 ($16_{prefix} + 8_{tag} + 16_{len} + 40_{id} + 16_{suffix}$)

Example 2:

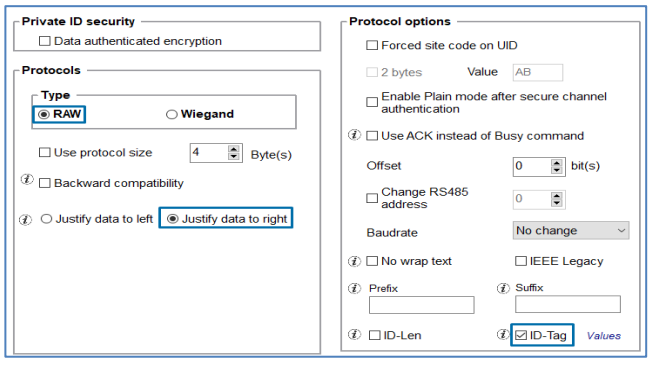
Tag: ioPROX
ID-binary = 100 1110 0000 0101 0001 0101 1001 1011 1011 1100
ID-Len = 39 bits



ID Justify to left: 100 1110 0000 0101 0001 0101 1001 1011 1011 1100 **0** = 0x 9C0A2B3778

OSDP Data: 0x 42 9C0A2B3778

OSDP bit count = 47 ($8_{tag} + 39_{len}$)



ID Justify to right: **0** 100 1110 0000 0101 0001 0101 1001 1011 1011 1100 = 0x 4E05159BBC

OSDP Data: 0x42 4E05159BBC

OSDP bit count = 47 ($8_{tag} + 39_{len}$)

❖ ISO 14443-3B PUPI / iCLASS™*

It is possible to manage differently the PUPI ISO14443-3B and the ISO 14443-2B by calculating an authentication code using a cryptographic hash function (SHA1) and a secret key. Other norms (ISO14443-A) and frequencies (125 kHz & 3.25 MHz) are not concerned by this option.

If the protocol size is less than 20 bytes, the 20 bytes obtained signature will be LSB truncated.
If the protocol size is more than 20 bytes, a zero padding will be made.

*Our readers only read the UID/Chip Serial Number. They do not read secure HID Global's iCLASS™ cryptographic protections.

❖ Card ID range filter (LSB)

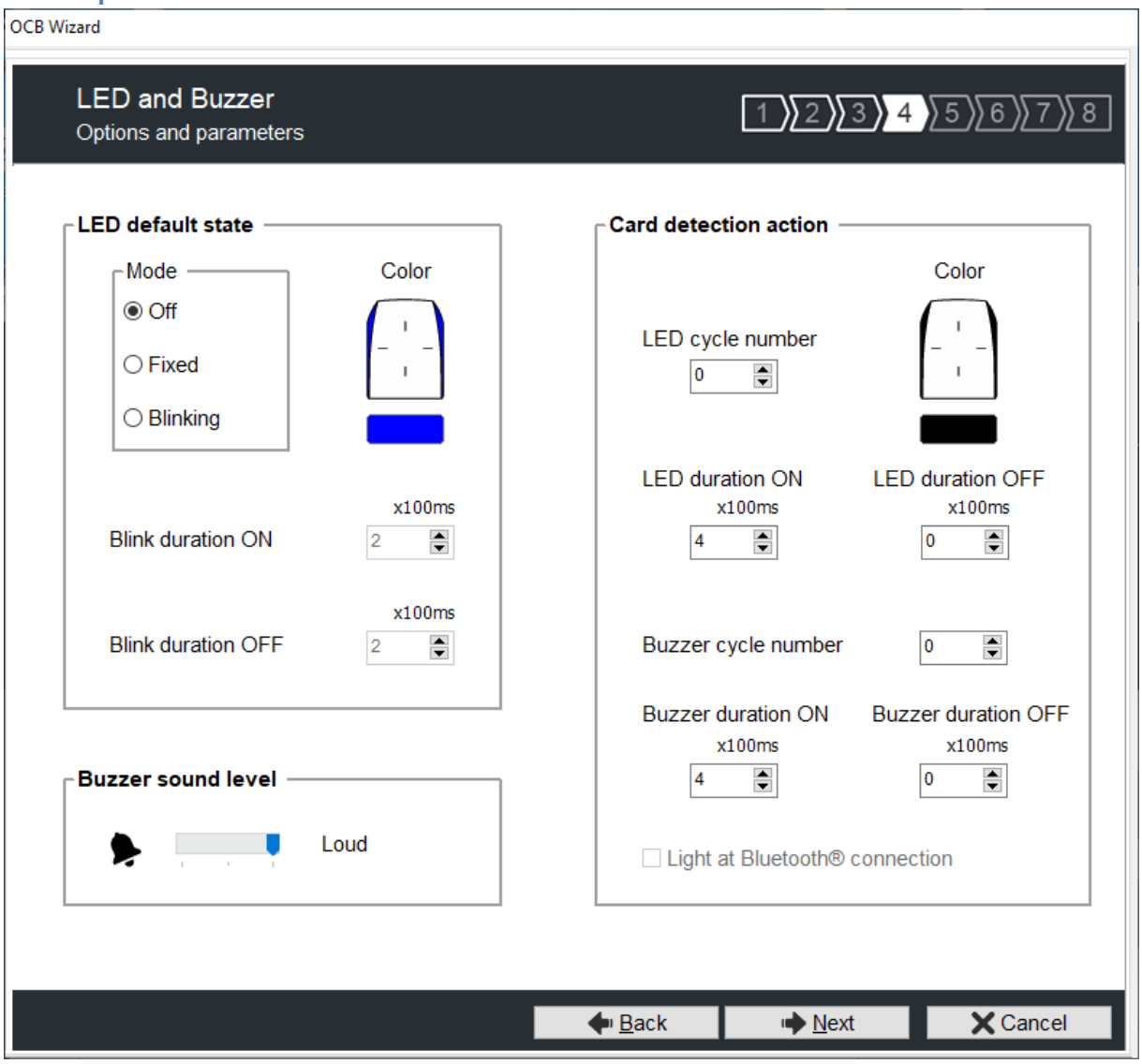
It is possible to return an UID / ID only if it is within a specified 4 bytes bounded range.

If the size of the UID / ID is more than 4 bytes, the range will be made on the 4 bytes LSB (taking into account the MSB First option first). The limits are included, lower limit ≤ UID / ID ≤ upper limit.

If the UID / ID is in the range, the reader will return the code for the current protocol and perform an action card LED + Buzzer (SCB). Otherwise, the reader light up (not configurable and not disabled) red LED + Buzzer for 400ms.

The UID / ID is compared to the hexadecimal value after taking into account the MSB First parameter and before entry into protocol shape.

OCB - Step 4



LED default state

Define the default LED state (color and blink duration).

- OFF
- Fixed
- Blinking with Duration ON and OFF

The image on the right allows you to view the selected effect: blinking and color.
You can always change this state with the command osdp_LED and permanent settings.

Card detection action

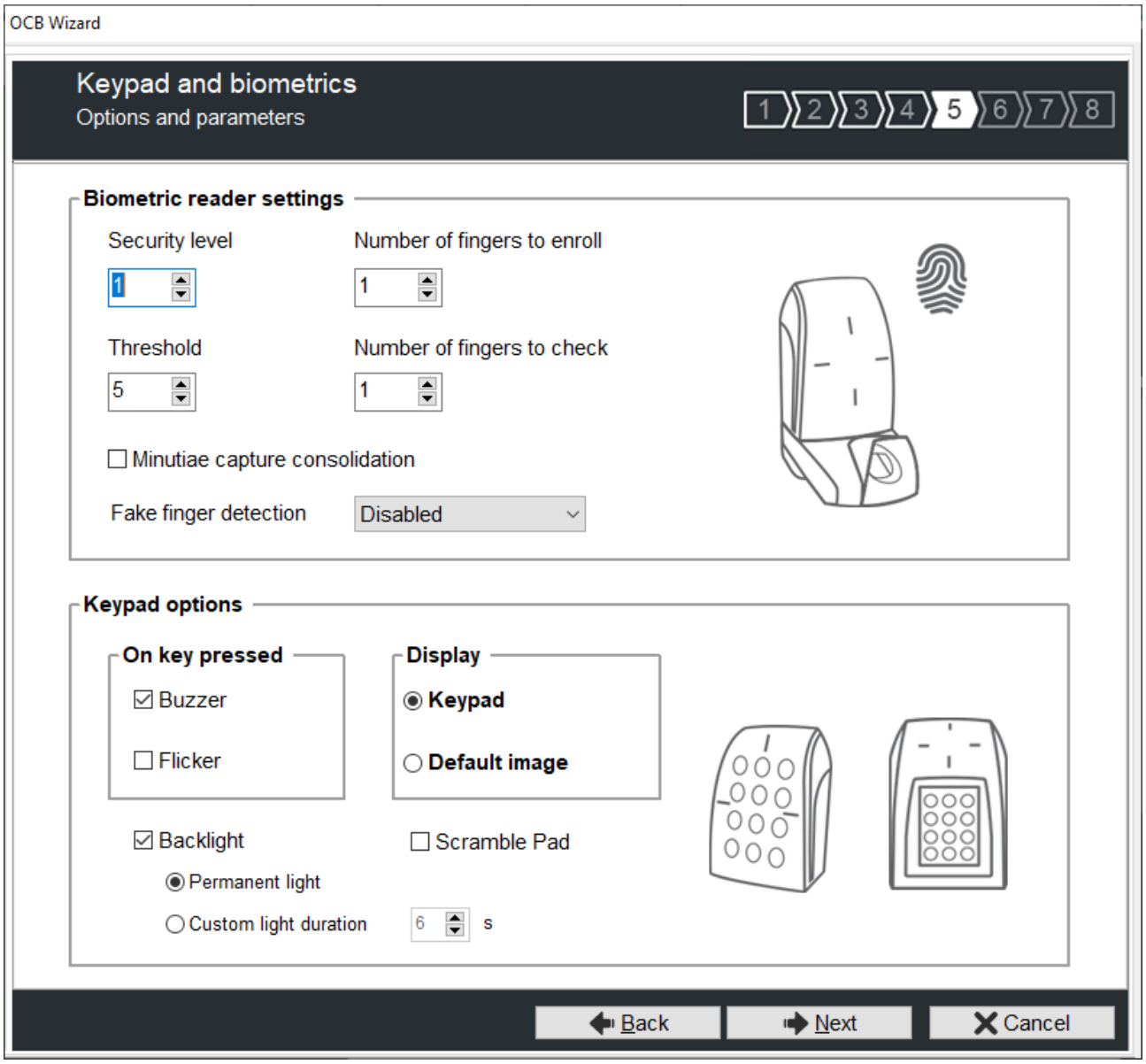
- Define the LED and buzzer action (color and blink) when a valid identifier is detected.
  This information is independent of the acceptance of the identifier.

- Light at Bluetooth® connection
  Flash LED when smartphone start connection on the reader. The color can be selected by clicking on the right square.
  This action, independent of the detection of the virtual badge, informs the user that the communication between the smartphone and the reader is in progress.

Buzzer sound level

Define the sound level for the buzzer **only available for ARCS, ARC1 and ARC1S**.

OCB - Step 5 *Adding functionality 3.6*



Biometric reader settings

- Security level: represents the reliability rate between the encoded and read fingerprints.
  - Security level = 1: low false finger security level (Morpho Sagem recommendation).
  - Security level = 2: medium false finger security level.
  - Security level = 3: high false finger security level.

- Threshold: represents the quality level of the fingerprints to encode in the chip (0 up to 10). Lower threshold = less false rejection. Morpho Sagem recommendation: 5.

- Number of finger to enroll: represents the number of fingerprints to encode.

- Number of finger to check: represents the number of finger to check.

- Minutiae capture consolidation: allows to capture the same finger three times. The biometric sensor will choose the best one during the encoding.

- Fake finger detection: Enable / Disabled the Fake finger detection with specific detection level.

Keypad options

- On Key Pressed:
  Allow to activate / deactivate Buzzer when user press one touch of the keyboard.

- Display: Choose de default display for touchscreen if keyboard is active.

  - Keypad: Display the keyboard.

  - Default image: Display the default text and image (see step 7).
    To display the keyboard, touch a first time the screen.
    The display reverts to the default image after a timeout of 10s.

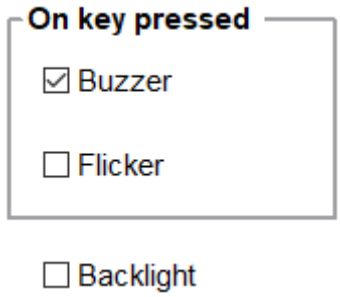
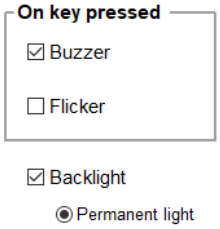
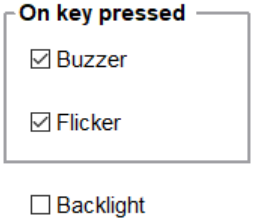
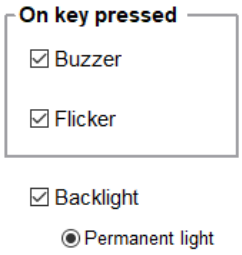
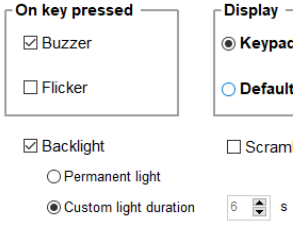
- Scramble Pad (only available for screen touch ARC): Activate the scramble on keypad.
  The scramble is performed:
  - After reading a valid card.
  - Every 30s. Pressing a key or reading a card resets the timer.

- Backlight : Allow to activate / deactivate the keypad backlight. Two options are available:

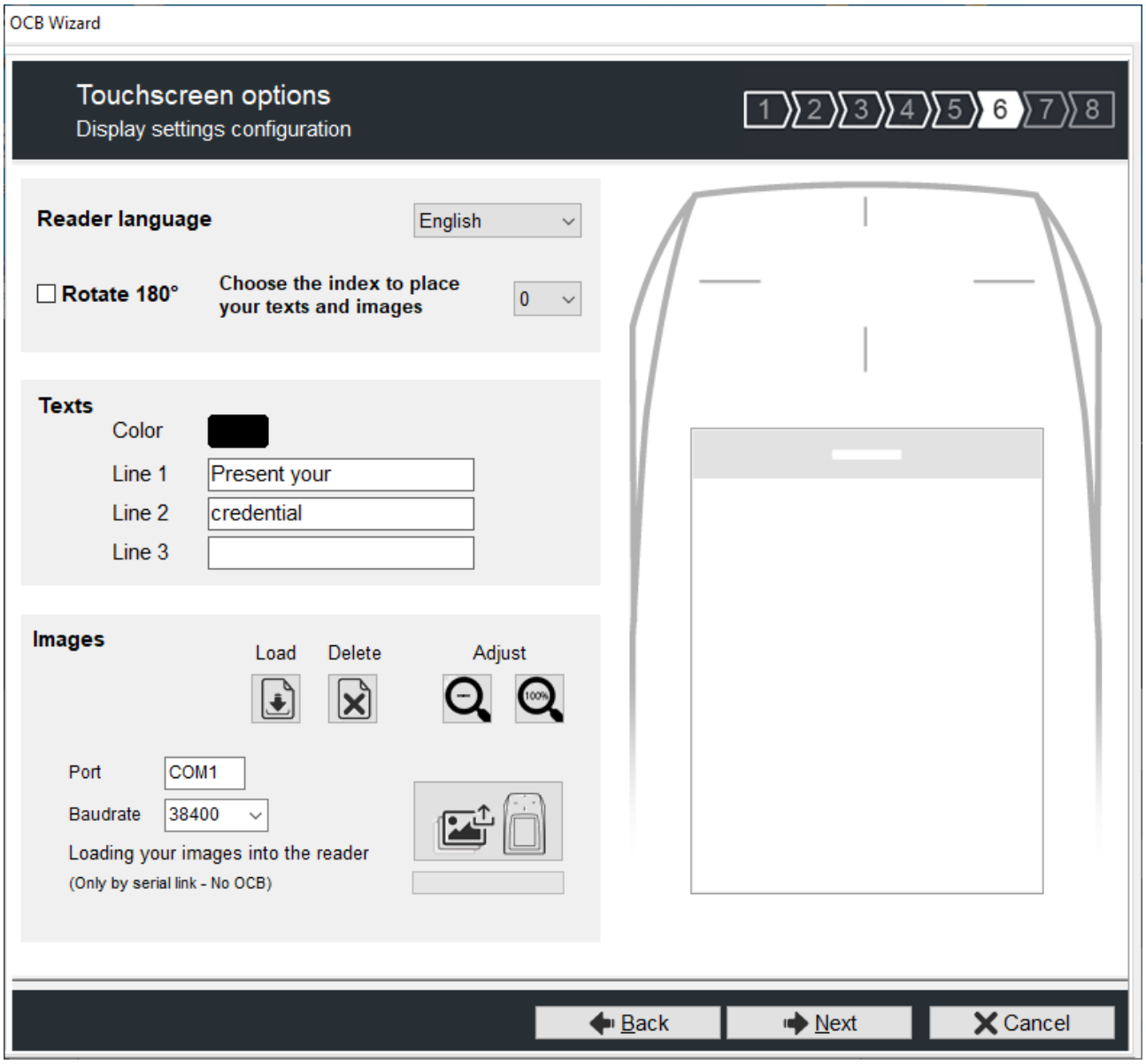
Permanent light : backlight is permanently activated.

Custom light duration: Keyboard backlighting when pressing a key and for a configurable time.

Flicker: depending on the backlight mode chosen, allows the keypad backlight LEDs to flash ON or OFF when a user presses a key on the keypad

 No backlight No backlight flash on key press	 Backlight on No backlight flash on press	 No backlight Backlight short flash ON when pressed
 Backlight on Short flash OFF of the backlight on press	 Backlight OFF and turns ON by pressing the key for a configurable time then returns OFF	

OCB - Step 6

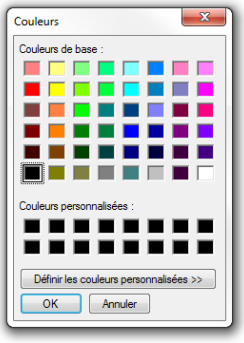


Reader Language: Choose the language used to display the text on the screen: English (default) or French.

Rotate 180°: Used to rotate the image at 180°.

Index: select the Index number [0 ; 9] to load the selected image and text**.**

Texts: To change the text color, click on the color button.

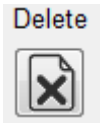


(the language of this windows depends on your Windows language)

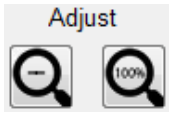
The color applies to the three lines of text.

Load your images:

Load an image file for the selected state.



Delete the image file to the selected state.



Reduces the image on the screen.

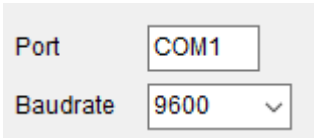
Note: The classic image formats are supported (bmp, png, jpeg, ...). By against the screen reader does not support transparency, the background color is white.

Loading your image into the reader

Warning

Loading images into the reader is possible only through the reader serial communication, not with the OCB.

1 - Connect the screen reader to your computer with the reader serial link and set the communication parameters:



2 - Power on the reader and click on 

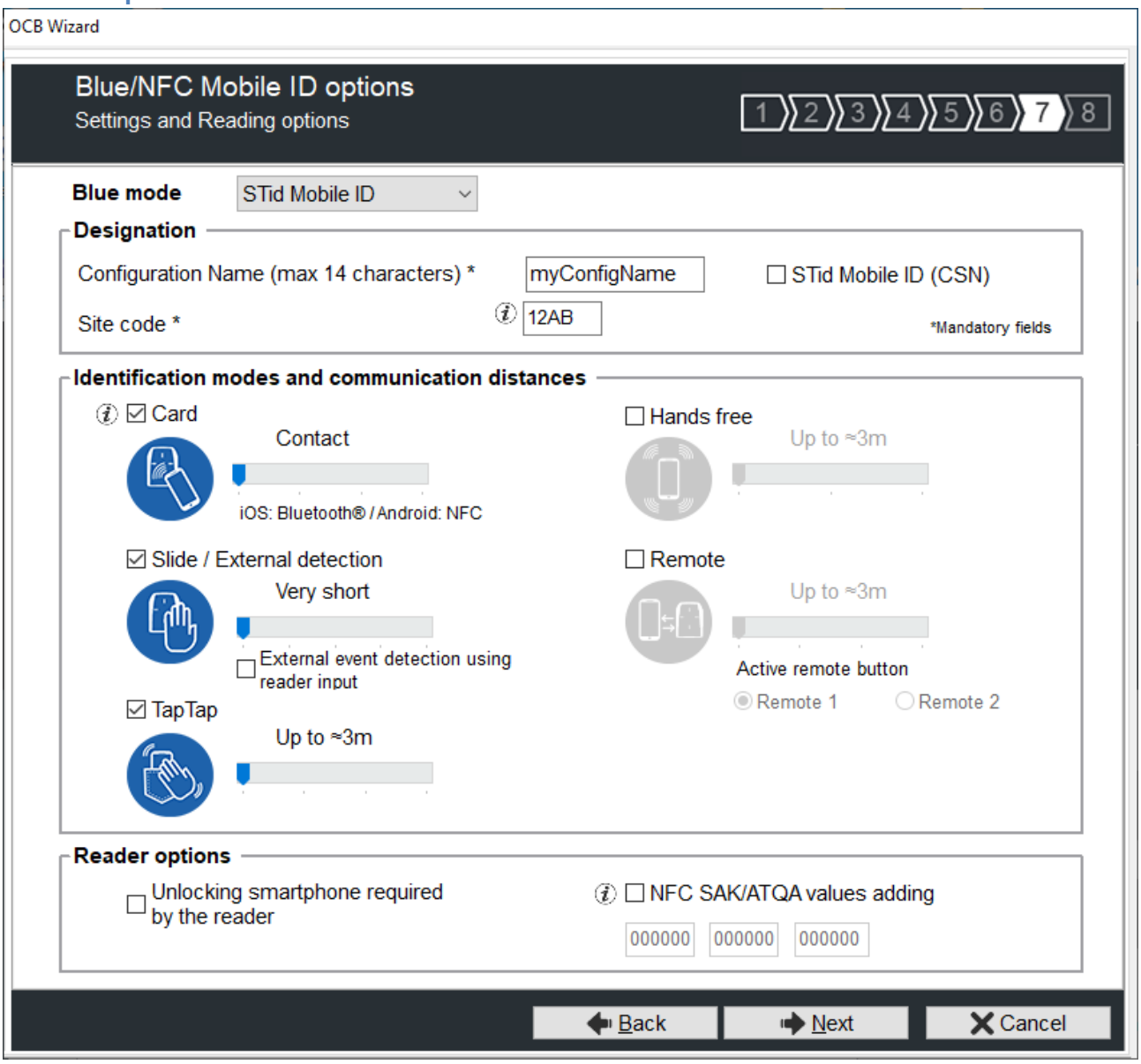
3 - The loading progress is indicated by the progress bar

Note:

* Image/text has an index; a new load erases the image/text loaded before.
* If you get the message below, your communication settings are not correct, return to the step 1.

* If the image has been loaded into SECard was moved, the preview will not be available, and the next image will be displayed in the IHM SECard.

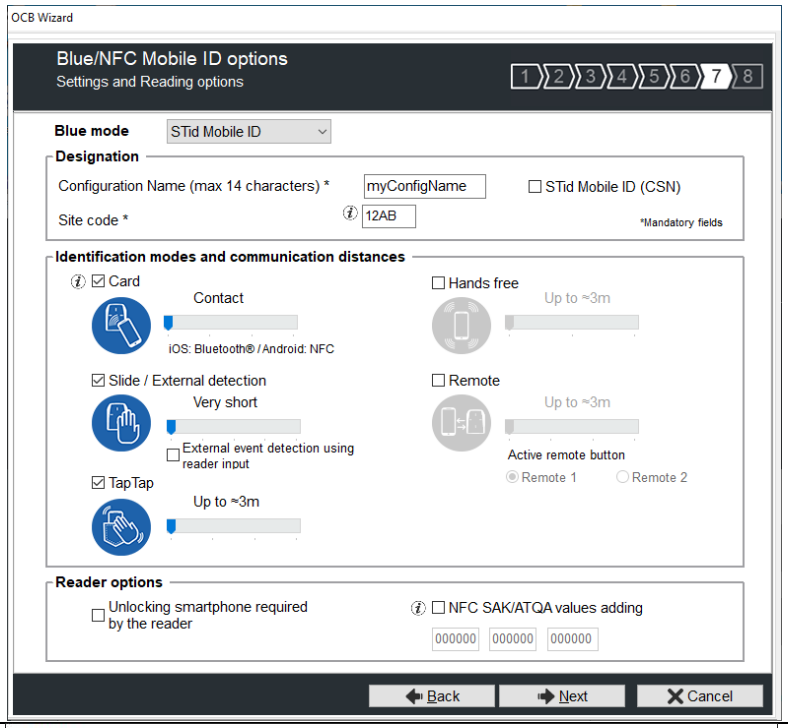
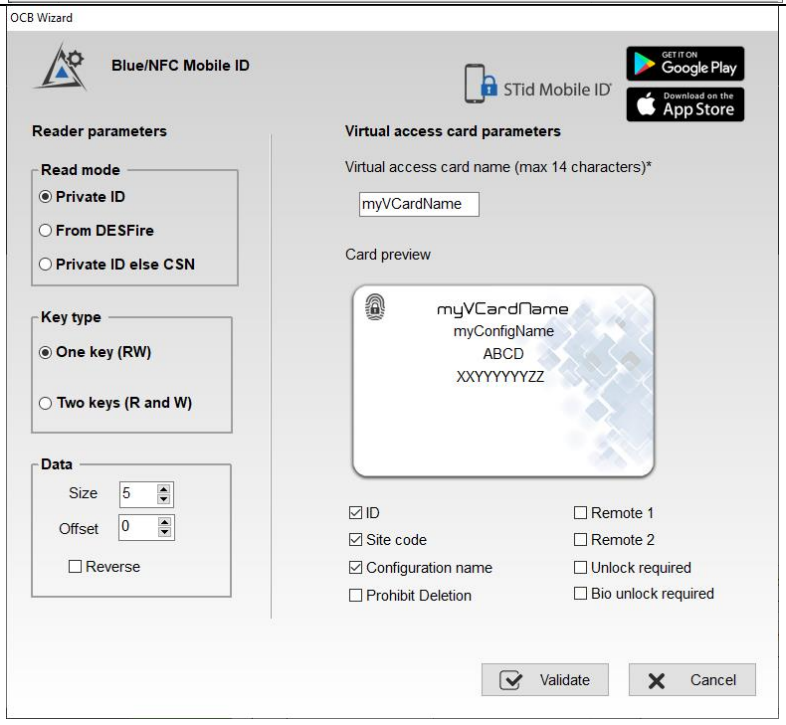
OCB - Step 7

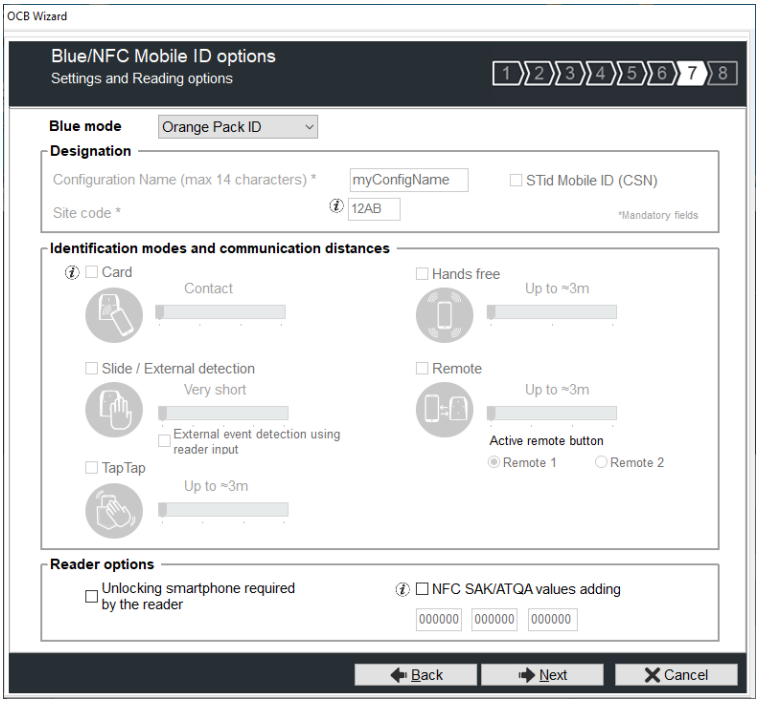
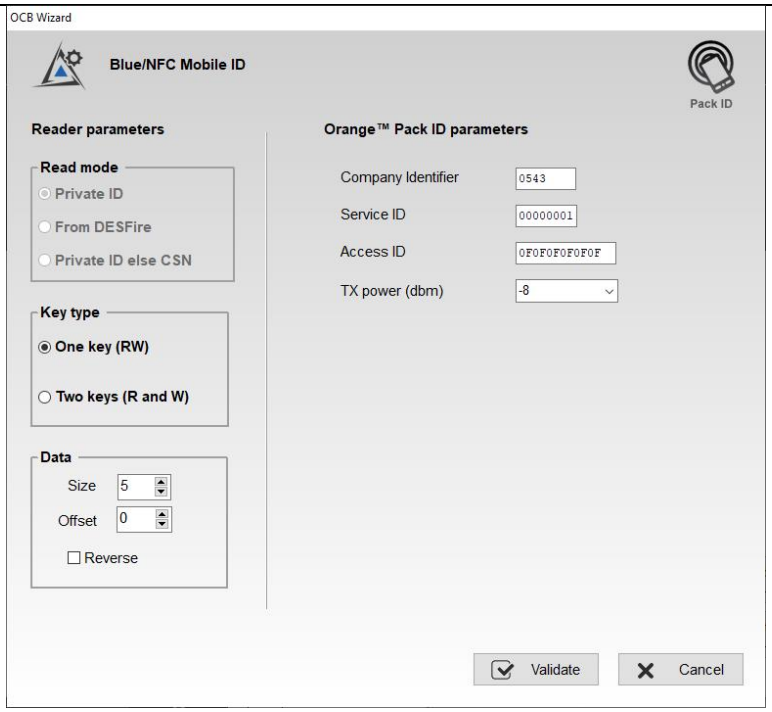


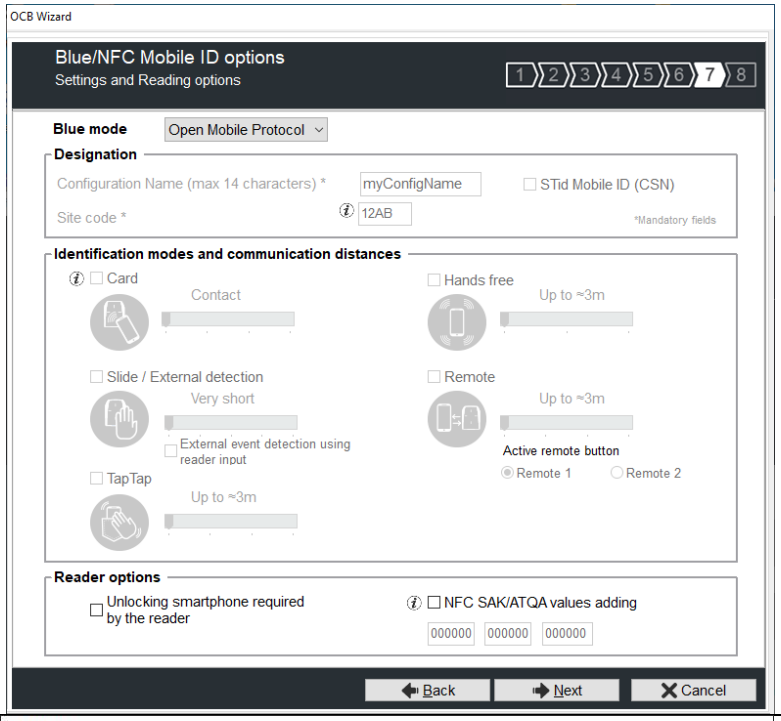
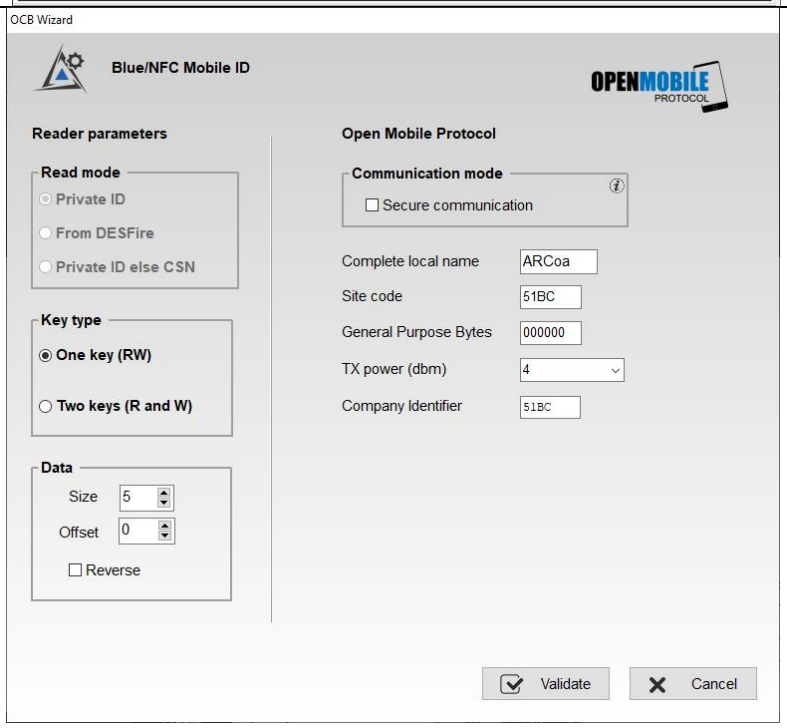
Blue/NFC mode

Configure the reader to read STid Mobile ID® or Orange™ PackID or Open Mobile Protocol.

This choice impacts the screen wizard Step 7 and Blue/NFC Mobile ID Settings.

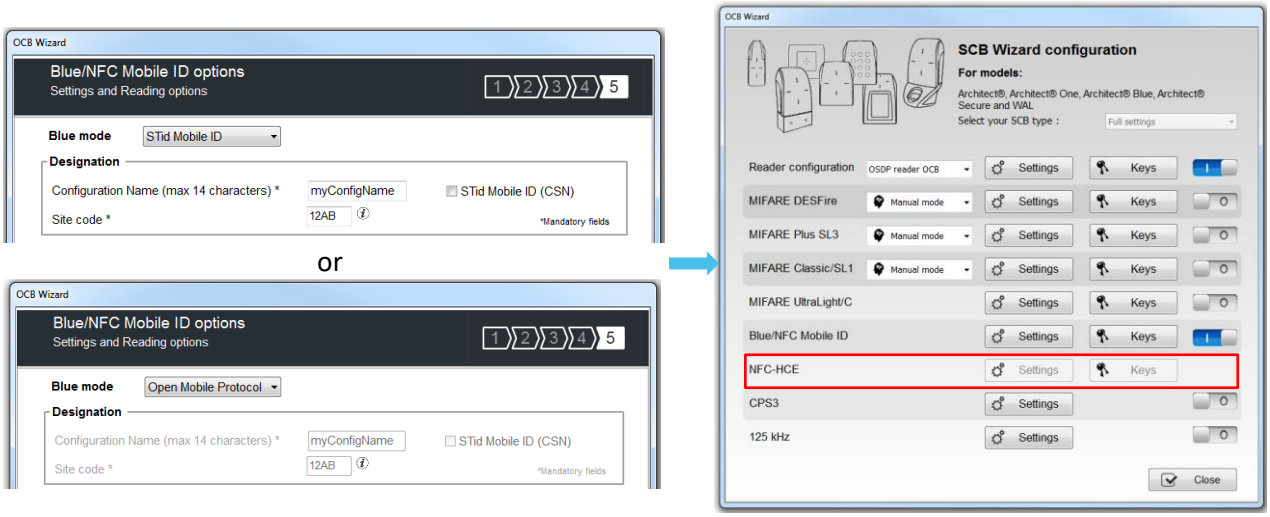
	STid Mobile ID®
Wizard Step 7	
Wizard Blue/NFC Mobile ID settings	

	Orange™ Pack ID
Wizard Step 7	 The detection mode for this application is fixed to Contact.
Wizard Blue/NFC Mobile ID settings	

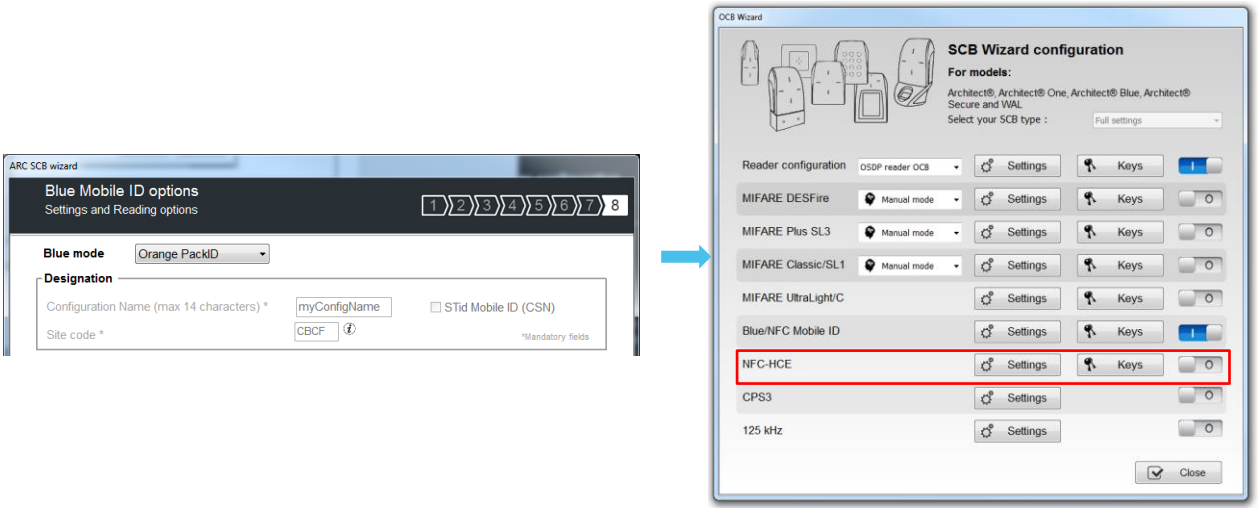
	Open Mobile Protocol
Wizard Step 5	
Wizard Blue/NFC Mobile ID settings	

Blue/NFC Mobile ID and NFC-HCE compatibility

If “STid Mobile ID® “or “Open Mobile Protocol “is activated, then it is not possible to activate “NFC-HCE“, the parameters and keys are greyed. The NFC Mobile ID is automatically activated.

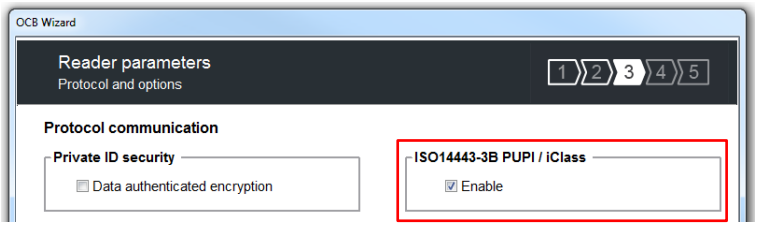


If “Orange™ Pack ID “ is activated it is possible to activate “NFC-HCE“, the parameters and keys are not greyed.



NFC Mobile ID and « ISO14443-3B PUPI / iClass » compatibility

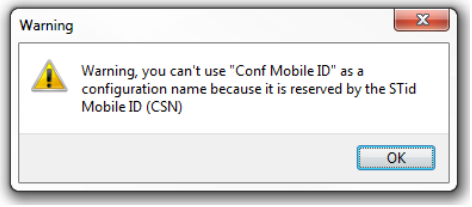
“NFC Mobile ID” and “ISO14443-3B PUPI“ can be activated at the same time as “NFC Mobile ID“ is compliant with ISO14443-A.



Blue Mode STid Mobile ID®

Designation

- Configuration Name: enter the name of the configuration Mobile ID Secure Plus: 14 characters max.
  Note: configuration name “Conf Mobile ID” is reserved to STid Mobile ID.



- Site Code: 2-bytes data used for the site code of the configuration.
  Note: site code 51BC is reserved for STid Mobile ID®.

- STid Mobile ID® (CSN): configure the Blue reader to read only a CSN on the smartphone.

Identification modes and communication distances

For each identification mode the communication distance is adjustable.

❖ **Card:**

By placing the smartphone in front of the reader.

- Contact: smartphone must be in contact with the reader.
- Up to 0.2m: smartphone must be in an area of 0.2m around the reader
- Up to 0.3m: smartphone must be in an area of 0.3m around the reader.
- Up to 0.5m: smartphone must be in an area of 0.5m around the reader

❖ **Slide:**

Slide: By placing your hand close to the reader without taking out your smartphone.

External detection: Works by changing the potential applied to the LED2 input (see details below):

- Very short
- Short
- Medium
- Long
- Very long

Not available for ARC1S neither ARCS keypad in Card or Key mode.

❖ **Tap Tap:**

By tapping your smartphone twice in your pocket for near or remote opening.
The communication distance can be:

- Up to 3m
- Up to 5m
- Up to 10m
- Up to 15m.

❖ **Hands free:**

By simply passing in front of the reader.
Communication distance around the reader:

- Up to 3m
- Up to 5m
- Up to 10m

❖ **Remote:**

By controlling your access points remotely.
Communication distance around the reader:

- Up to 3m
- Up to 10m
- Up to 15m
- Up to 20m

❖ **Remote button selection**

If the identification mode "Remote" has been activated, it allows to associate the current configuration to the Remote button 1 or Remote button 2.

Notes:

The notion of distance in Bluetooth® corresponds to an area around the reader, not just in the front.
Reading distances depend on the environment, on the position smartphone // reader ...

<u>It is recommended to do on-site testing to evaluate the settings.</u>

Warning

When Architect® Blue readers are installed close to each other, detection distances must be defined to accommodate the distance between the readers to avoid cross readings.

Notes:

- The NFC-HCE option for "NFC Mobile ID" is not a SECard option. It has to be activated in STid Mobile ID® app (activated by default).
  This feature is only available for Android phones.

- "NFC Mobile ID" is not compatible with STid Settings app.

❖ **External event detection using reader input:**

Hand (slide mode) information is given by capacitive sensor or input LED2 level on ARCS reader.

If enabled: information is given by LED2 level.

- LED2 no connected or connected to high level = Hand not present
- LED2 connected to the GND = Hand present.

For example: connect a detection system to the LED2. When people are detected, the smartphone reading is activated.

❖ **Unlocking smartphone required by the reader: security option**

- If checked: the smartphone must be unlocked (with PIN code or other unlocking option depending on the smartphone) to authenticate with the reader.

- If unchecked: unlocking the smartphone is not required to authenticate with the reader.

❖ **NFC SAK/ATQA values adding**

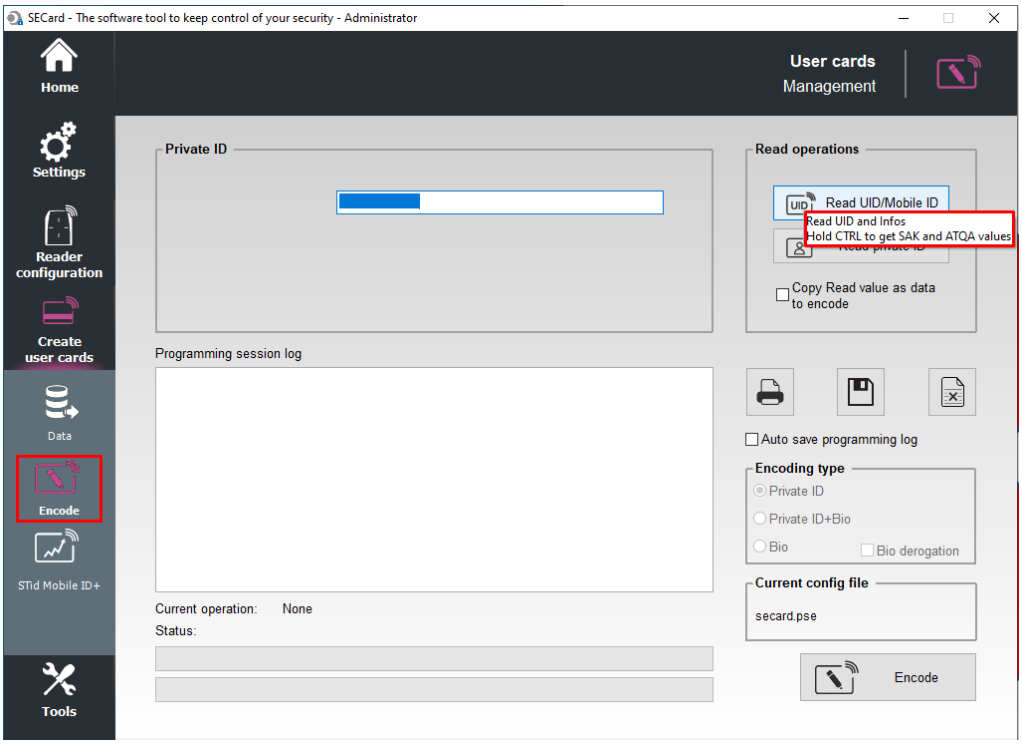
In RFID a chip is identified by two parameters ATQA and SAK. These parameters must be known to the readers for read the identifiers.

Smartphones in NFC mode meet this same rule. Some ATKA + SAK are already implemented in STid readers.

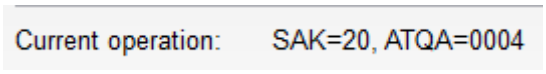
To ensure the compatibility of the readers with the reading of new smartphones in NFC mode, these fields make it possible to set up three values of ATQA and SAK**.**

How to know these values for your smartphone:

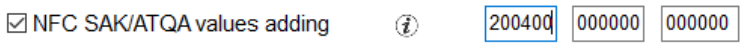
- Enabled the NFC on the smartphone
- Go to Create user cards



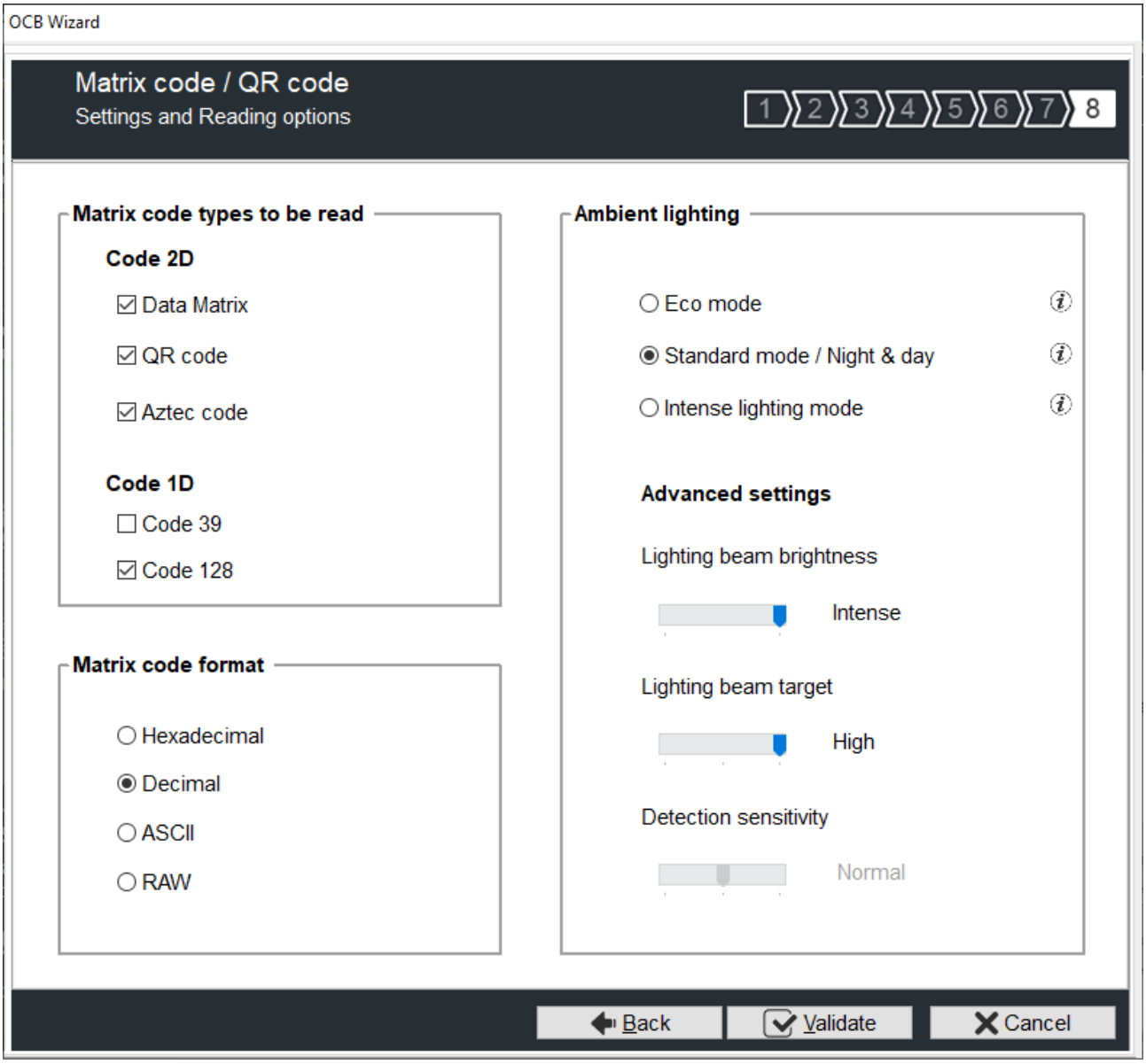
- Present the smartphone to SECard encoder and hold CTRL + click on Read UID button
- Result



- Enter this value in the field:



OCB - Step 8 *Adding functionality 3.6*



- **MATRIX / QR code type selection**
  Select the code type to be read:

Data Matrix	QR Code	Aztec code	Code 128	Code 39
				
123456	123456	123456		

❖ **MATRIX / QR code format**

Select the format of the matrix / QR code to be read.

The maximum size of the code depends on the format chosen:

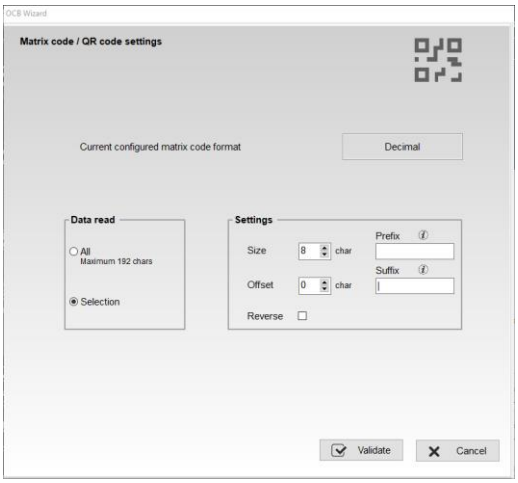
Format	Size in characters	Size in bytes	
Hexadecimal	96	48	
Decimal	25	10	De 0 à 120892581961462917470617 5 0x0 à 0xFFFFFFFFFFFFFFFFFFFF
ASCII	192	48	
Raw	192		

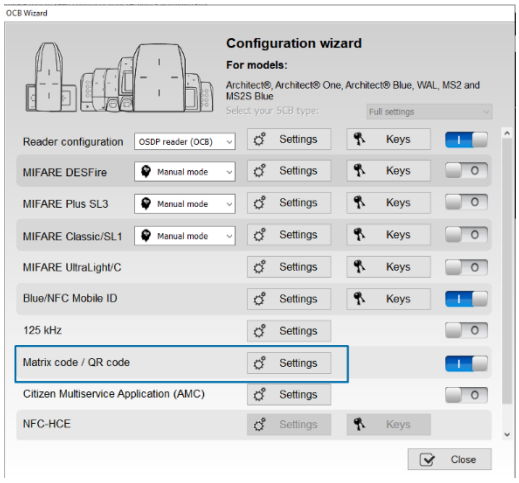
Note: only the characters list below are authorized in ASCII:

Value	ASCII character	Valeur	ASCII character	Valeur	ASCII character
30	0	38	8	61	a
31	1	39	9	62	b
32	2	41	A	63	c
33	3	42	B	64	d
34	4	43	C	65	e
35	5	44	D	66	f
36	6	45	E		
37	7	46	F		

Note: if the code to read is not in the code type set in the wizard, the code is not read. For example, if decimal type is set and the code to read contain letter the code will not read.

To read a specific part of the data code go to the settings Matrix / QR code:





❖ **Ambient lighting**

- Eco mode: for low and normal light environments
- Standard mode / Night day: for all lighting conditions
- Intense lighting mode: for indoor and outdoor environments with full sun exposure or direct lighting on the reader.

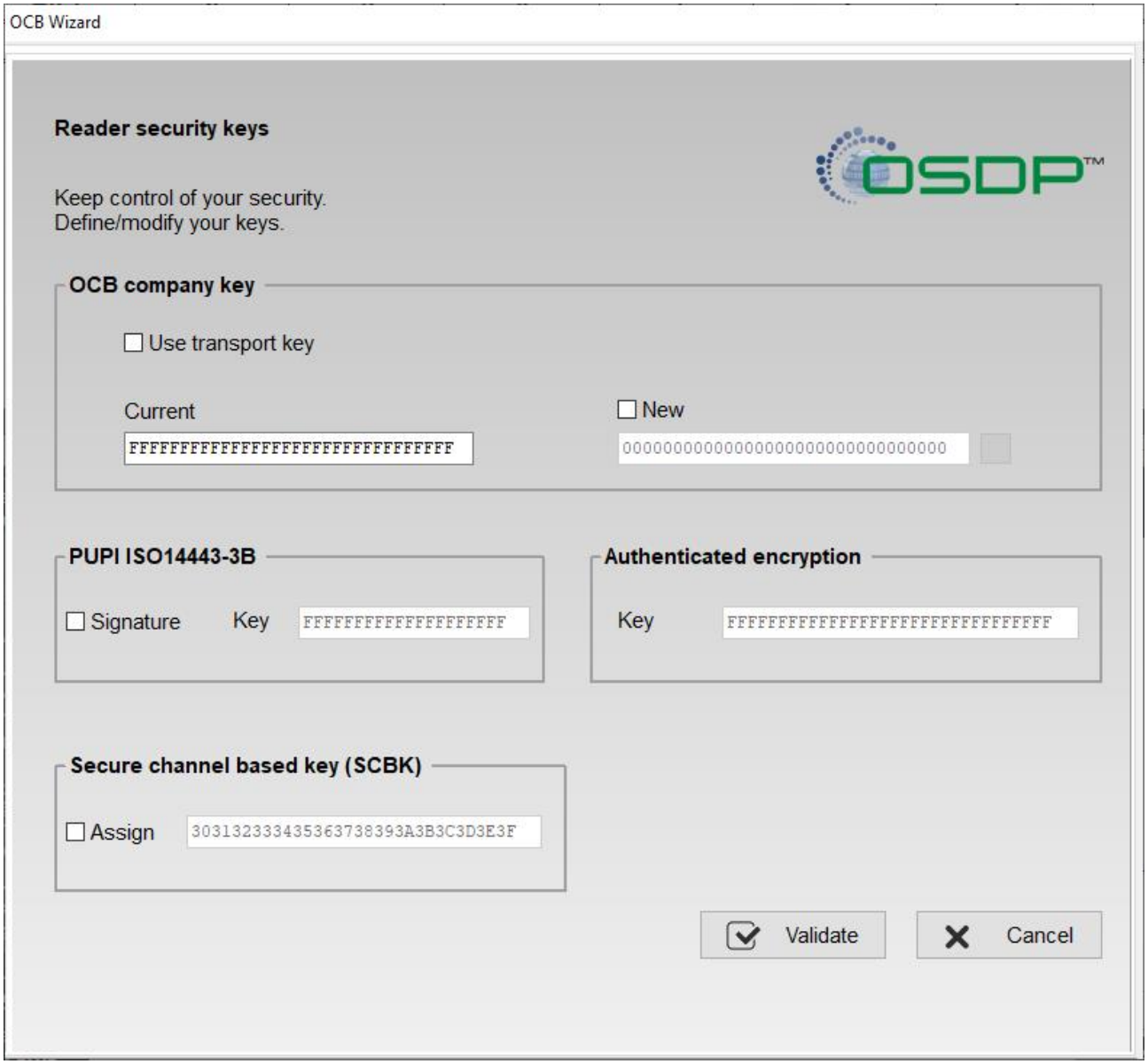
❖ **Advanced settings**

Lighting beam brightness	Control the power of the spot which illuminates the code	Normal		Intense
Lighting beam target	Control the power of the laser which targets the code	Low	Normal	High
Detection sensitivity	Control the sensitivity of the trigger to start scanning the code	Low	Normal	Max

Click the button 

to complete the reader configuration settings.

III. 4 - OCB Wizard: reader security keys



Attention: the osdp™ readers, in factory configuration, are in the transport key (key value not known).

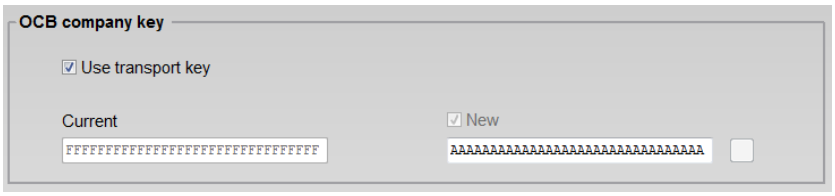
Warning

The OCB company key is important and should definitely be known by the administrator. It protects the data from the "OCB" and allows changes to the configuration of readers.

If you lose this key, the reader cannot be reconfigured for another "OCB" and will must be reset at the factory.

Configure a factory reader

Check "Use transport key" and "New" and enter a value in the field.

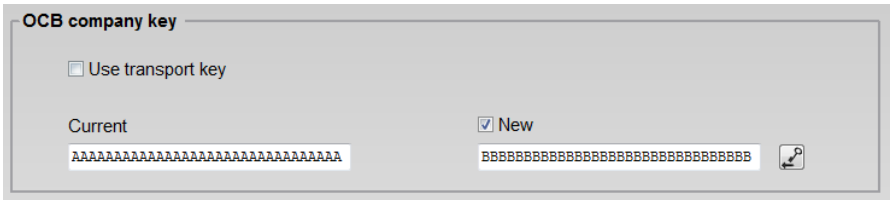


When this OCB configuration card is presented is to the reader, the security key of the reader takes the value of the new field (ex: 0xAA…AA).
This configuration card is usable on the factory readers and on the readers having already been configured by this card.

OCB « Transport key » to « key 0xAA…AA »	Reader with transport key	**OK**
	Reader already at the key 0xA…AAA	**OK**
	Reader with another key value	**NOK**

Modify the key of a reader

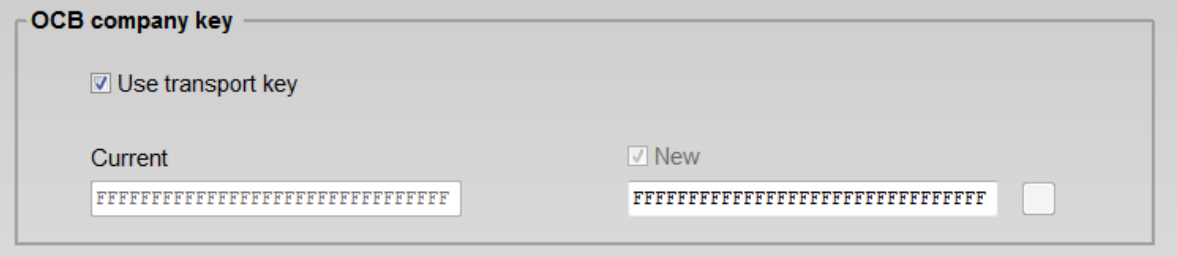
Enter the reader's key value in the current field and the value of the new key. When this configuration card is presented to the reader, the security key of the reader takes the value of the new field (ex 0xBB ... BB) only if the current key value is that known by the reader.



OCB « key 0xAA…AA » to « key 0xBB…BB »	Reader with transport key	**NOK**
	Reader with key 0xAA…AA	**OK**
	Reader with key 0xBB…BB	**OK**
	Reader with another key value	**NOK**

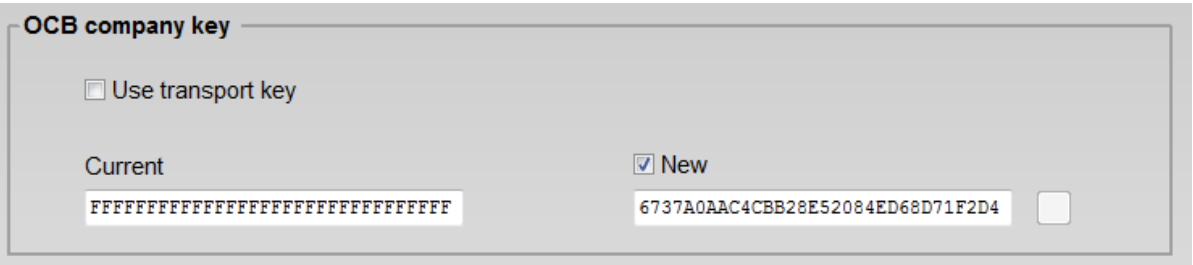
Recommended procedure in the test phase

Step1: create an OCB badge to pass the reader from transport key to the key 0xFF…FF:



- Label this badge to identify it.
- Present the OCB badge to the reader, wait for the BIPS to take into account.
- The reader is now at the key 0xFF ... FF.
- You can re-encode this badge in order to make changes to the reader settings and do configuration tests without losing the reader security key.
- When the configuration is validated proceed to step 2 to secure the reader with a different key from FF.

Step2: create an OCB badge to pass the reader from 0xFF…FF to a new key



- Label this badge to identify it.
- Present the OCB badge to the reader, wait for the BIPS to take into account.
- The reader is now at the new value key.

PUPI ISO 14443-3B

Enter the key used for the signature calculation, called “secret key” (10 bytes).

Authenticated encryption:

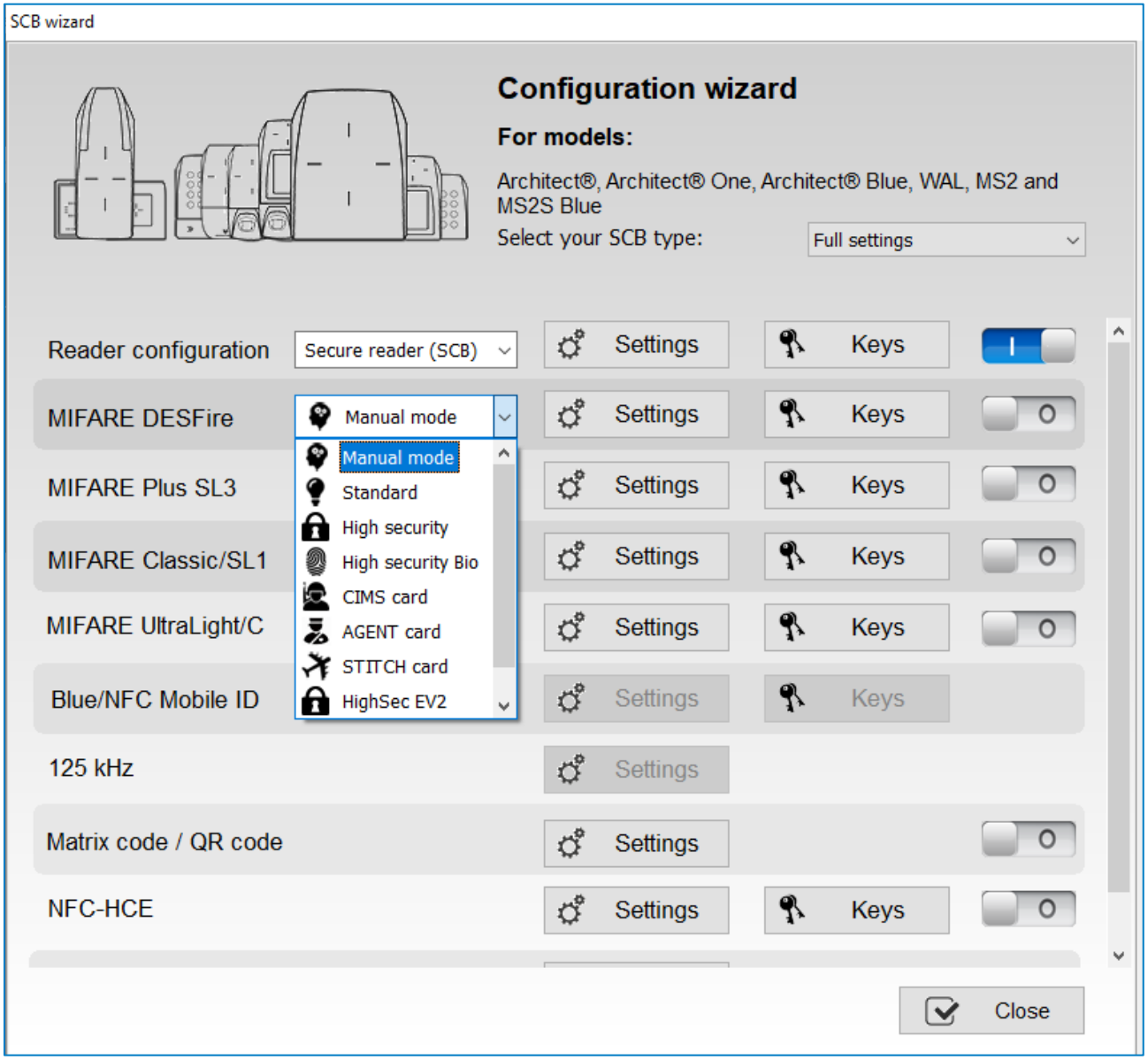
Enter the authenticated encryption key.

Secure channel based key (SCBK)

Assign with OCB configuration card the secure channel base key.

Click the button  **to complete the key settings.**

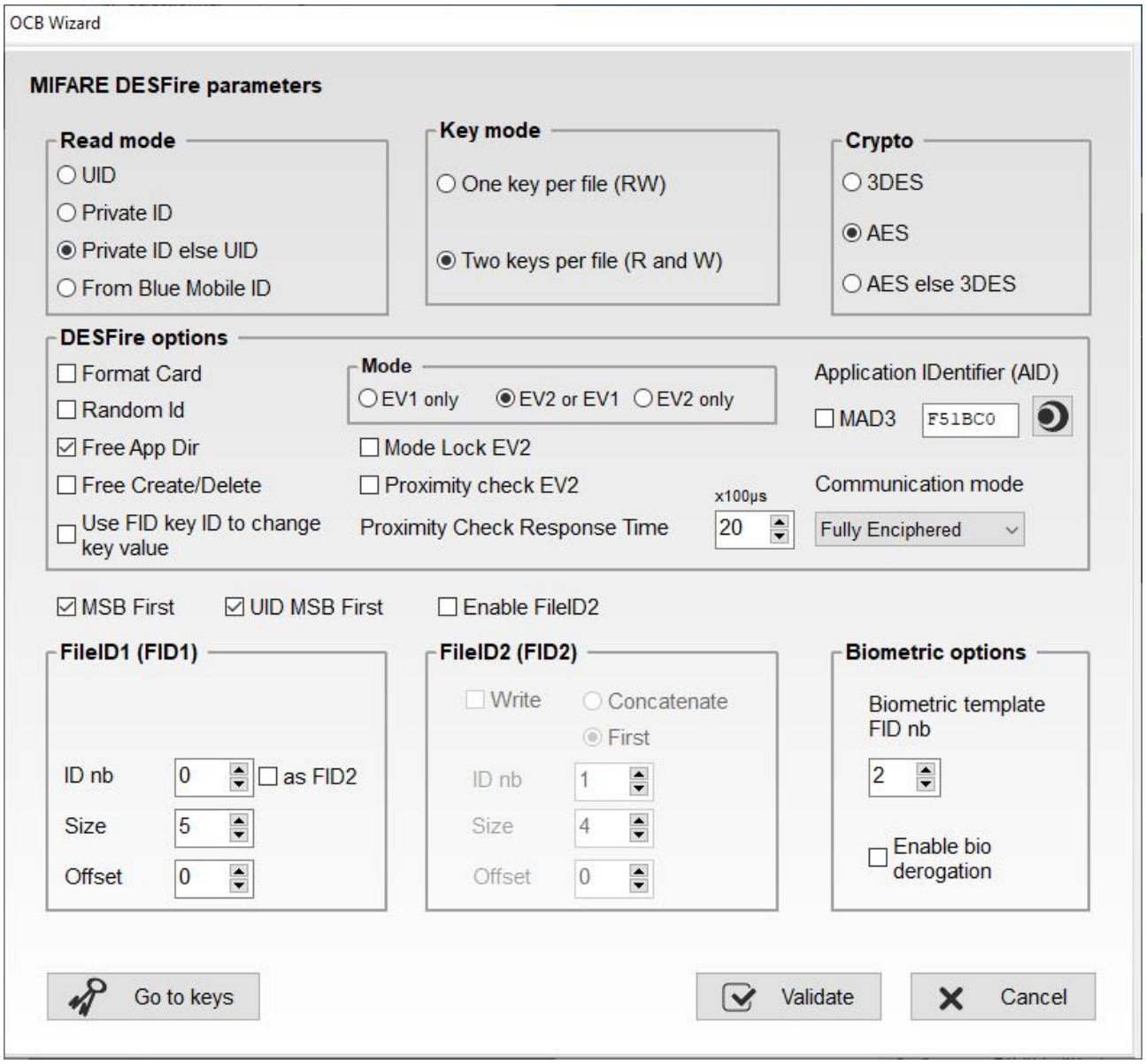
III. 5 - MIFARE® DESFire®: settings



To help user with the settings of the DESFire® chip, a drop-down menu offers pre-configurations. Depending on the selected configuration, the parameters are automatically selected, and key values are generated randomly, it is always possible to view and / or make changes using the Settings and Keys buttons.

Manual Mode: all parameters and keys are to be entered manually.
Standard: corresponds to a standard secure level configuration.
High Security: corresponds to a high security configuration with Key Diversification.
High security Bio: corresponds to the high secure mode with biometric settings.
HighSecEV2: corresponds to a high security configuration with Key Diversification and Proximity Check.
HighSecEV2 Bio: corresponds to a highSecEV2 mode with biometric settings.

The three modes CIMS, AGENT and STITCH, corresponding to specific French cards.



Read mode

- ❖ UID: Reader configured in “read-only serial number”.
- ❖ Private ID: Reader configured in “read-only private code”.
- ❖ Private ID else UID: Reader configured in “read-only private code”. If it is not found or if the security settings are incorrect, then the reader will read and return the UID.
- ❖ From Blue Mobile ID*: Reader configured in “read-only Blue mobile ID code”.

Key mode

- ❖ One key per file (RW): Use one key per file used for reading and writing.
- ❖ Two key per file (R & W): Use two keys per file. A key used for reading, the second for reading and writing.

Crypto

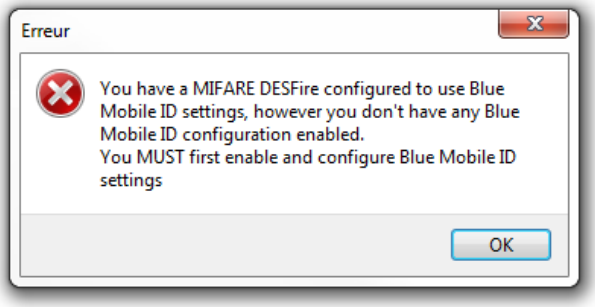
Choose the authentication method to use.

- 3DES
- AES
- AES but 3DES: In this case the reader will accept two authentication methods. First authentication AES, second in 3DES. The key value must be the same.

It is also possible to modify the authentication method; you must change the value of the Card Master Key by checking New and writing the value and selecting the authentication method.

*From BlueMobileID

- If this mode is select, a Blue configuration must be enabled; if you select this option without Blue configuration you have the error:



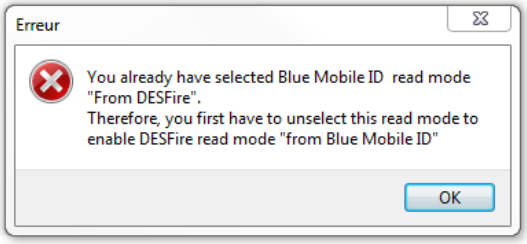
- In this mode, the DESFire parameters are automatically determined and inherited from the Blue configuration.
  These settings cannot be changed:

  - ✓ Crypto method: AES
  - ✓ AID: 0xF"site code Blue configuration"0
  - ✓ MSB First
  - ✓ RandomID: no
  - ✓ Enable FID2: no
  - ✓ Data type: Raw
  - ✓ FID1: 0
  - ✓ Size and offset same as Blue configuration

  These settings can be changed:

  - ✓ Format Card
  - ✓ FreeAppDir
  - ✓ Biometric template FID nb

- If FromBlueMobileID is select and BlueMobileID is configured on FromDESFire:



DESFire® options

- **Format card**:

If this option is enabled, DESFire® EVx chips will be formatted before encoding.
For this it is necessary to enter the current value of the Card Master Key of the chip.

> **Warning**
>
> This option will completely erase the data (applications and files) of the chip but not the current key.

- **Random Id**:

If this option is enabled, the DESFire® EV1 / EV2 chips will be configured in Random Id mode. It means the chip serial number sent for each “Scan” will be different and coded on 32 bits.

> **Warning**
>
> This option is irreversible. The Random ID cannot be disabled afterwards.

- **Free App dir**:

If this option is enabled, reading the list of applications included in the chip will be possible without authentication.
This option is enabled by default on the chip DESFire® EV1/EV2.

- **Use FID key ID to change key value**:

By default in SECard a change of key value file requires a preliminary authentication with the Master Key Application.
If this option is enabled, SECard will authenticate with the key to change.
To use this option with a chip that has been encoded but not with SECard, requires that the application has been created with the access rights to the "Configuration Changeable OK" otherwise it will format the chip or delete the application.
In the case of encoding maps agents this option must be enabled.

- **Free C/D**:

On the DESFire it’s possible to choose the settings of application.
By default SECard create Application with Free Create/Delete. To create / delete file, authentication with Application Master key is not required.

If this box is check application will be created without Free Create/Delete. To create / delete file, authentication with Application Master key is required.

- **Communication mode:**

On the DESFire® EV1/EV2, it’s possible to choose the communication mode with the file.
There are three different modes: Plain, MACed or Fully Enciphered.

- **Plain**: communication in plain.
- **MACed**: communication in plain with signature DES/3DES or AES.
- **Fully Enciphered**: communication fully enciphered in DES/3DES or AES.

This setting is applied to the encoding and to the reading.

> **Warning**
>
> The default communication mode in SECard is Fully Enciphered up to SECard versions < 3.0.0

❖ **Application IDentifier**:

If "MAD3" is checked, then the value of the identifier of the application will be four characters long, but it real value will consist of six, SECard forcing the first character to the value "F" and the last to "0" .
Example: For *Application IDentifier* "51BC", application really created will be "F51BC0".

If this box is unchecked, the field of AID is no longer restrained and completely customizable by the user, and then it is possible to set it to 6 characters long

❖ **Mode for reading**

The DESFire® EV2 offers security features (Secure messaging EV2) that we will call here Mode Ev2: including the prohibition of dialogue in EV1 and 3DES.

EV1 only:	Reader configured to read Ev1 and EV2 in EV1 mode. A not locked EV2 will be read as an EV1. A locked EV2 will not be read.
EV2 or EV1:	Reader configured to read EV2 (locked or not) and EV1. Reader will try to communicate in EV2 mode, if he fails it tries in EV1.
EV2 only:	Reader configured to read EV2 only. An EV1 will not be read.

❖ **Mode for encoding**

EV1 only:	Encode only in EV1 mode. A not locked EV2 will be encoded as an EV1. A locked EV2 will not be encoded.
EV2 or EV1:	Encode an EV1 in EV1 AES mode and an EV2 (locked or not) in EV2 mode.
EV2 only:	Encode only in EV2 mode. An EV1 will not be encoded.

❖ **Lock EV2 Mode (Secure messaging)**

Only available for EV2 chip. During the encoding, the chip will be configured to communicate only in Secure Messaging EV2. It will no longer be able to talk in EV1 or 3 DES.

Warning
This operation is definitive, no possible 'CANCEL'.

❖ **EV2 Proximity check / Proximity check Response Time**

Enables protection against relay attacks.
Puts tighter timing constraints on the permitted round-trip delay during authentication, in order to make it harder to forward messages to far-away cards or readers via computer networks.

The maximum acceptable time for exchange of the Proximity Check is user-defined (multiple of 100 micro seconds).

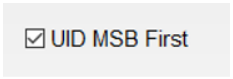
MSB First

If the box is checked, the reader reads the identifier Most Significant Byte First.
If the box is unchecked, the reader reads the identifier Least Significant Byte First.

For STid reader, the MSB First is default mode.

UID MSB First

If “Read mode” is “Private ID else UID”, define the reading for Private ID **and** for UID.
With this option, you can separately define the reading direction for the private ID and the UID.



If the box is checked, the reader reads the UID Most Significant Byte First.
If the box is unchecked, the reader reads the UID Least Significant Byte First.

Enable FileID2

Activate the settings of the second file.

SECard allows the user to encode two files with two possibilities**:**

- Reserve the space for the second file without encoding it.
- Write the second file at the same time than the first.

FileID1(FID1)

Set the first data file:

- Data type: Choose the data type **to read**:
  - Raw: if data in the card have been written in hexadecimal.
  - ASCII: if data in the card have been written in ASCII Decimal – max 17 digits (8 bytes).(for ex: 0x313131 written in the card will be read 111 or 0x6F depending protocol chosen).
    Only available for ARC & ARC1 readers
- ID nb: Choose the number (0 to 31) of the file to be created into application.
- Size: Choose the size of ID to be encoded.
- Offset: Define an offset in the encoding from the first byte.
- As FID2: Encode the second file in a future encoding.

  Must report data (key, size, file number ...) of the second file in the field box FileID1. After this manipulation, the FID2 will be ready to be encoded and read by the reader without reconfiguring by SCB card.

FileID2(FID2)

Set the second data file, if the box “Enable FileID2” is checked:

- ❖ Write: Encode the second file in the same time than the first. If the box is not checked, the second file is not encoded, but the settings are known by the reader.
- ❖ ID nb: Choose the number (0 to 31) of the file to be created into application.
- ❖ Size: Choose the size of ID to be encoded.
- ❖ Offset: Define an offset in the encoding from the first byte.
- ❖ Concatenate: This feature informs to tell the reader that it must read the files FID1 and FID2. The information brought up by the reader will be then concatenated (the first file and second file). In this case of configuration, it is necessary that the global encoded data size (FID1 & FID2) match the size of outgoing protocol defined in the configuration of the reader. (Example: for a Wiegand 3CB 5 bytes, the total size of both files should be 5 bytes or less). In the opposite case, the reader will truncate the FID2 data. In this mode, the file FID2 is also automatically written at first encoding if the box “Write” is checked.
- ❖ First: In this mode, the reader automatically reads the first file found using security parameters. If authentication with the file FID1 is not possible (bad key values for example), the reader will then attempt to read the second file.

Note:
File 1 and 2 are Standard data files (StandardDataFile) of 48 bytes each.
RF communication is according the choice of user.

Both numbers of the two files must be different from the number of biometric file otherwise numbers will be highlighted in red.

Warning

In the case of using two files and when the "Write" is activated (Concatenate or First), it is important that the sizes defined in the field “size” of the files 1 and 2 correspond to those to be encoded.

For this, the addition of insignificant 0 may be necessary
Example: for an ID 0x11 0x22, if the defined size is 3 bytes, i twill then fill 0x00 0x11 0x22.
.

Biometric options

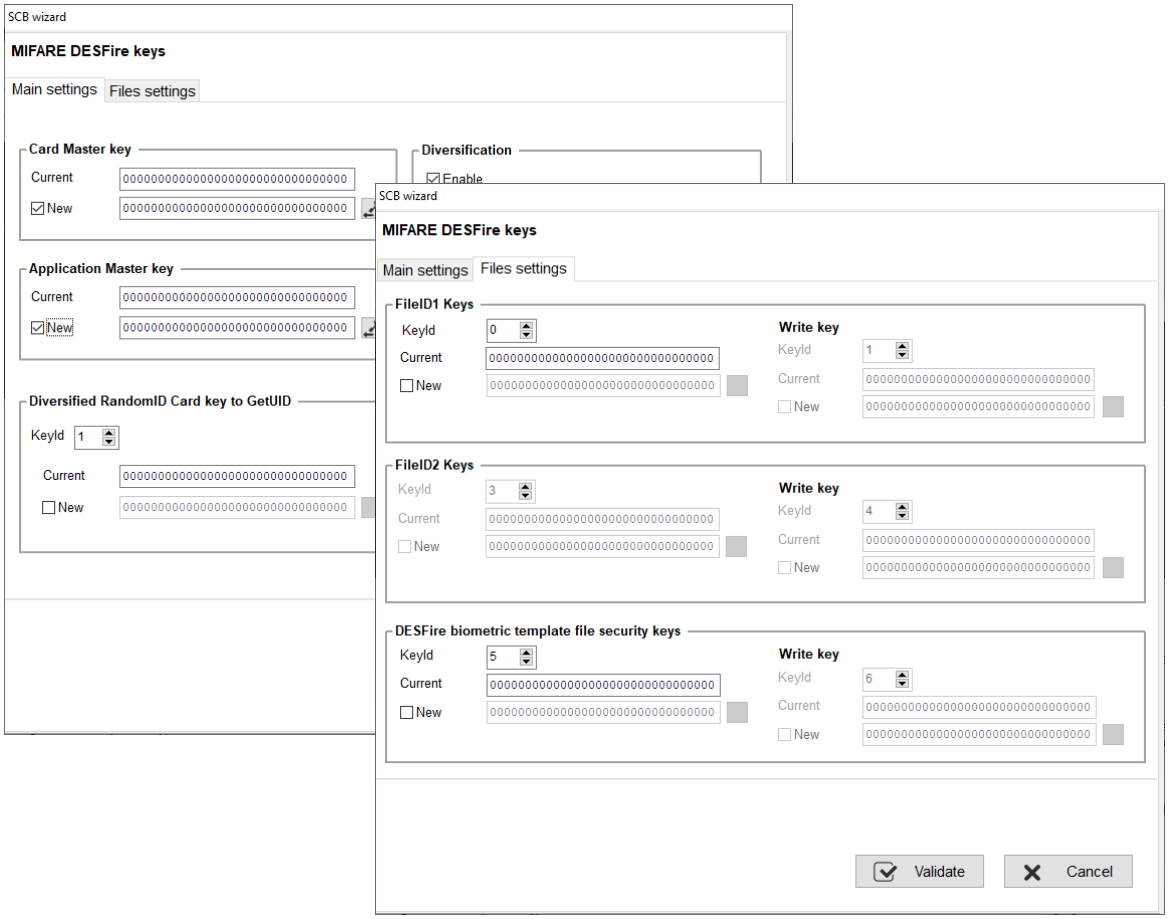
- ❖ Biometric template FID nb: Choose the number (0 to 31) of the file that will be encoded fingerprints.
- ❖ Enable bio derogation: refer to *T7.2 - Biometric derogation*.

Goto Keys: shortcut to the DESFire keys settings**.**

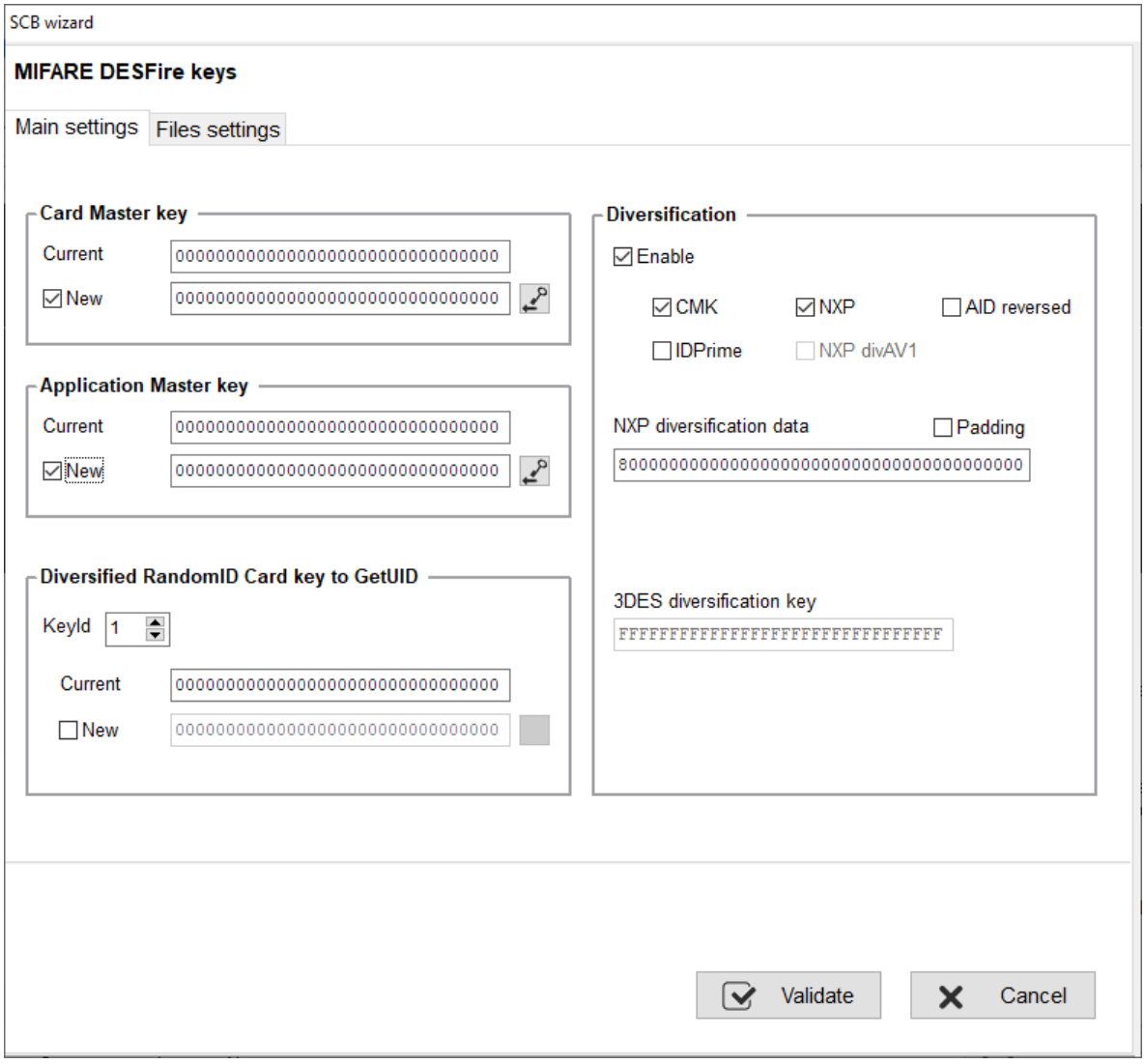
Click the button 

to complete the DESFire® settings.

III. 6 - MIFARE® DESFire®: keys



Define all the MIFARE® DESFire® keys.
For more information about the memory organization refer to *T3.2 - MIFARE® DESFire® and MIFARE® DESFire® EV1/2/3 chips* memory mapping.



Card Master key

Card Master key is the value of the master key of the chip MIFARE® DESFire® and MIFARE® DESFire® EVx.

Default value is « 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 » (16 bytes to 00h).
It is recommended to change its value to optimize security.

Application Master key

Application Master key is the value of the key of the application that has been defined within the settings MIFARE® DESFire® and MIFARE® DESFire® EVx.

Default value is « 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 » (16 bytes to 00h).
It is recommended to change its value to optimize security.

Diversified RandomID Card Key to GetUID

In the case of RandomID card and diversification, it's necessary to authenticate with the card to get the UID with GetUID command.

By default, the key used to make the authentication is the Card Master Key (CMK), if you don't know this key defined another key to authenticate.
This key is created during encoding only if RandomID is select in settings and box "New" is checked.

Note: if you don't enter a new value with box new check, the GetUID used CMK key.

Diversification

- ☑ Enable

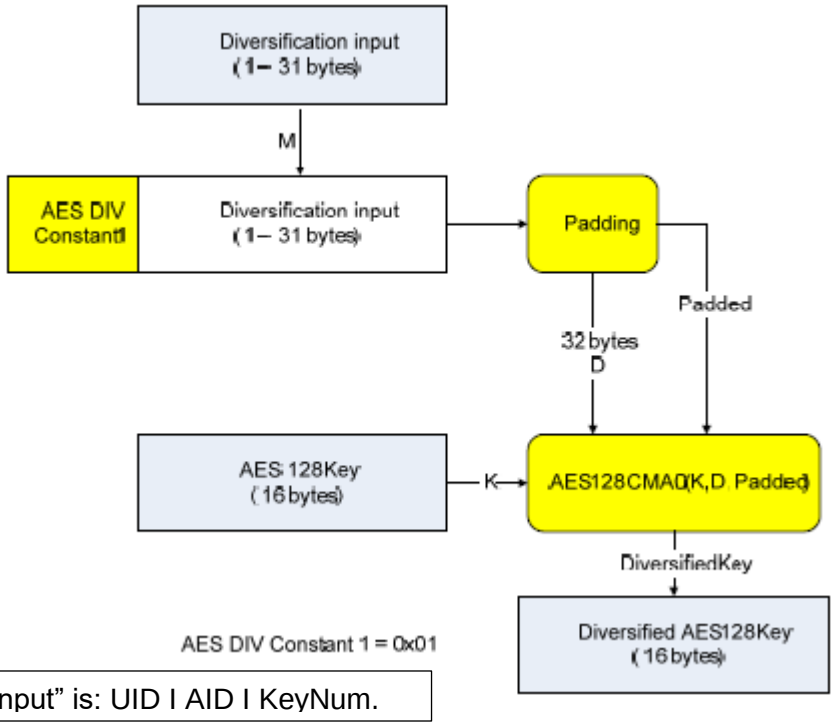
This function allows you to use another key than the one known by the user. To do this, the encoder uses the algorithm defined in the box "*Crypto"* in the DESFire® settings, to generate another key.

- If the current algorithm is the 3DES, the generated key is a function of 3DES encryption key set in the 16-byte "3DES key diversification" field. It is necessary that the first 8 bytes of this key are different to the last 8 bytes.
- If the current algorithm is AES, the key will be generated based on the user key and other parameters. In this case, the "key 3DES diversification" field is grayed.

- ☑ CMK — diversify the Card Master Key.
  To deactivate diversification applied to the Card Master Key, it is necessary to uncheck the "CMK" option and format the chip via the option "Format the card". Furthermore, you have to change the keys.

- ☐ NXP — Diversified key according to NXP-AN-165310.

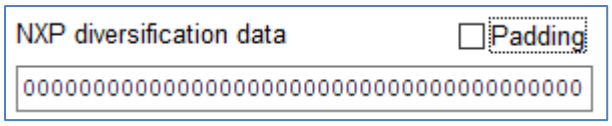
☑ NXP — Diversified key according to NXP-AN10922 method.



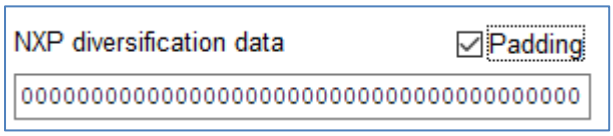
"Diversification input" is: UID I AID I KeyNum.

❖ 

Diversified key according to NXP-AN10922 method with reversed AID (LSB / MSB) before the computation of the diversified key.
Ex. AID = 10 C5 FB or AID = FB C5 10.

❖ 

Specifies the 20-byte input used in NXP AN-10922 diversification (use CMAC K1*).

❖ 

Specifies the 20-byte padding used in NXP AN-10922 diversification (use CMAC K2*).

* RFC 4493:

```
   Subkey Generation Algorithm

The subkey generation algorithm, Generate_Subkey(), takes a secret
key, K, which is just the key for AES-128.

The outputs of the subkey generation algorithm are two subkeys, K1
and K2.  We write (K1,K2) := Generate_Subkey(K).

Subkeys K1 and K2 are used in both MAC generation and MAC
verification algorithms.  K1 is used for the case where the length of
the last block is equal to the block length.  K2 is used for the case
where the length of the last block is less than the block length.
```

Note: in order to authenticate with the French Card CIMS you MUST use one of these methods.

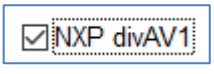
Note:

* For diversification to be effective it is necessary to also check the "New" key boxes to diversify and enter the value of the key.

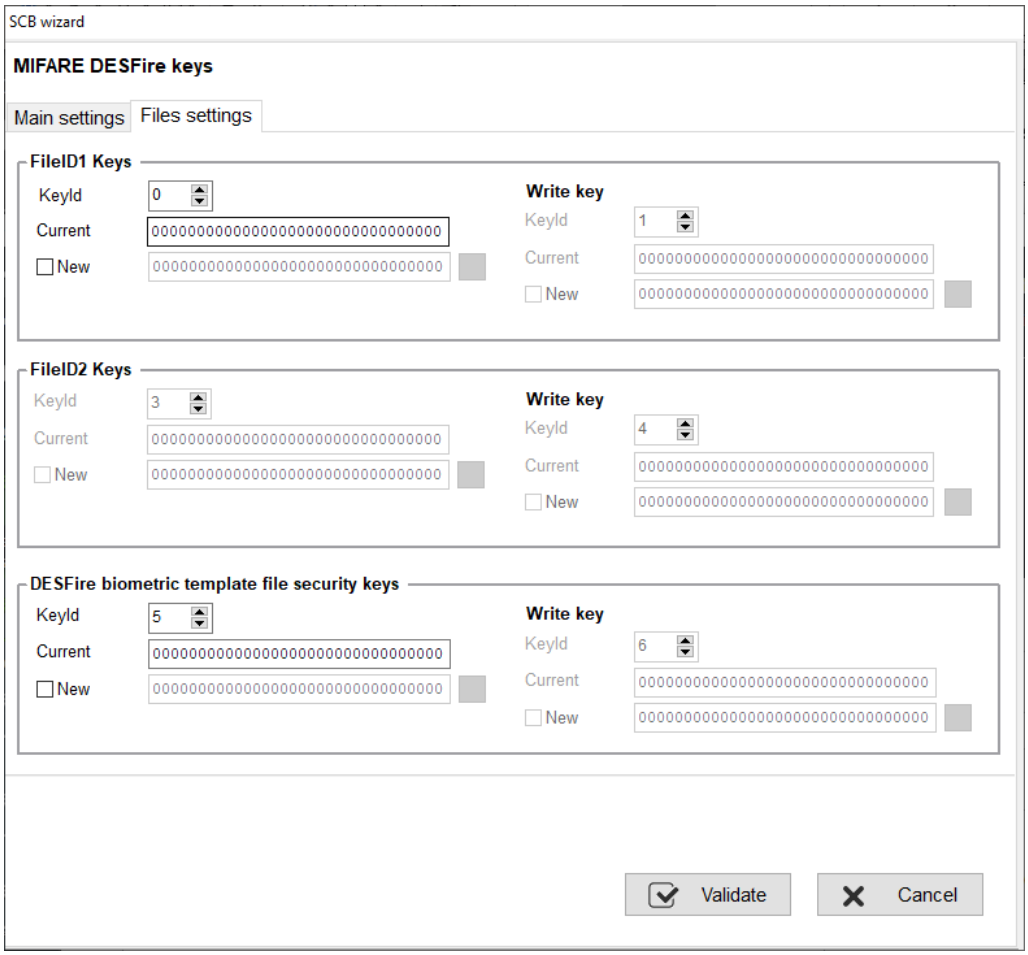
* It is possible to use the diversification and Random Id options at the same time in a configuration. However, the *Card Master Key* won't be diversified.

❖ 

Check this box **to read** card encoded with specific Gemalto MD3811 diversification (1 I UID I Padding & Card UID Len=4) **only to read encoded card not for encoding**.

❖ 

Diversified key according to NXP-AN-0148 (3DES divAv1)



FileID1 Keys / FileID2 Keys

Set the number key and key value for data files.
Warning, the key number 0 is the Application Master Key.

If using “One key per file” the section “Write key” is grayed.

To change a key value, in the "Current" field fill the current key and then checked "New" and fill in the field with the value of the desired key.

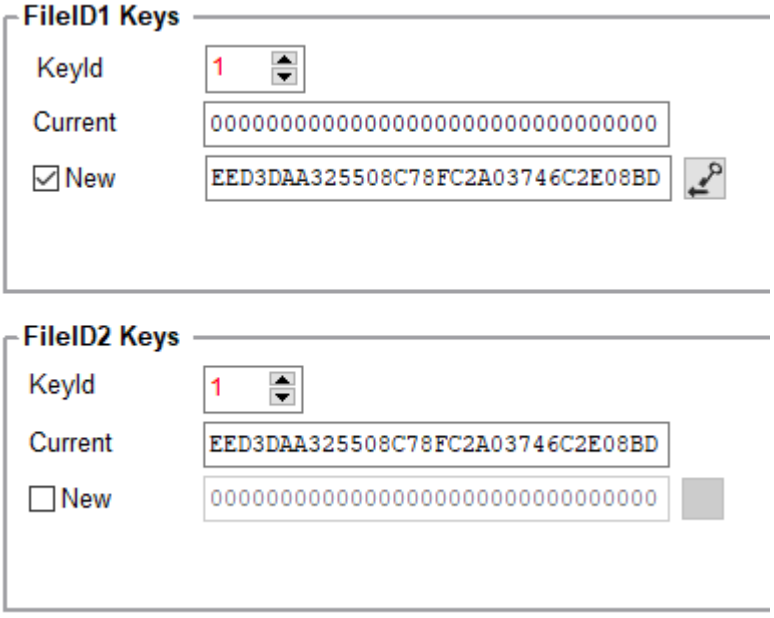
Default key are 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00.

Note:

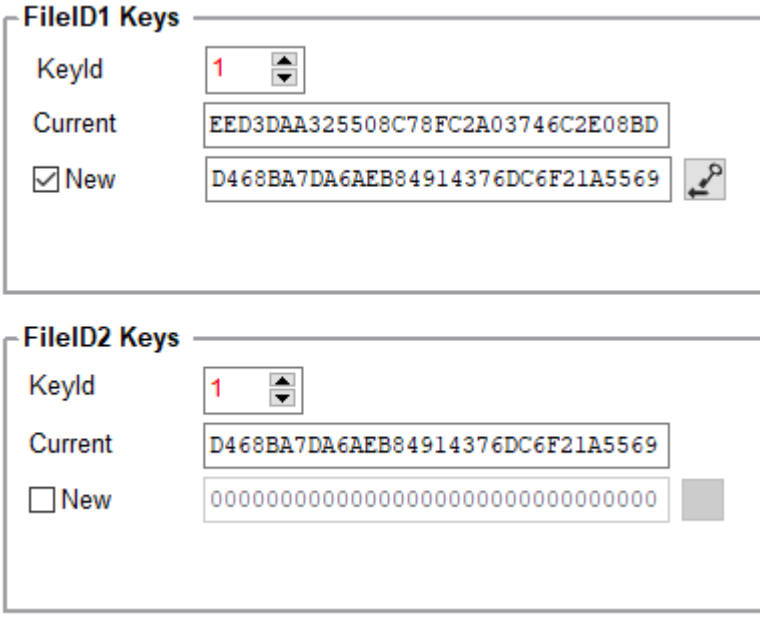
From SECard 3.0.0, it is not required to write the value of New in Current to re-encode the card.

- **Particular case:** it is possible to use the same key for file 1 and file 2.

  In this case, the key fields must be filled in as below:

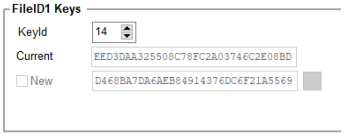


To change the value of the key, the key fields must be filled in as below:



- **Free Read**

  To read a file encoded with Free Read use the key number 14.
  The key field is grayed out.



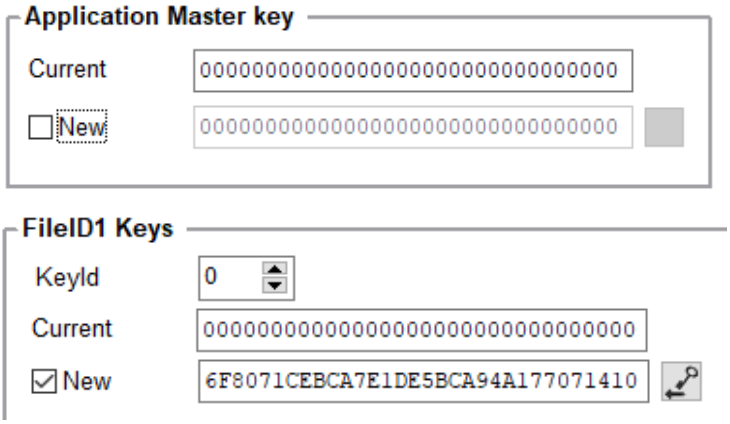
  When this key is used for reading key, the reading does not require authentication.

- **Using a single key to manage application and file security**

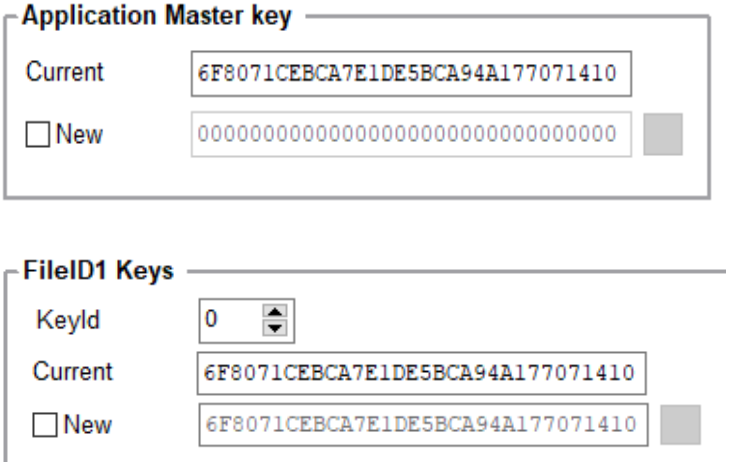
With SECard ≥ 3.0.0, you can use the Application Master Key (0) to manage the security of the application and file 1. File 2 must not be activated.

Case of One key per file (RW):

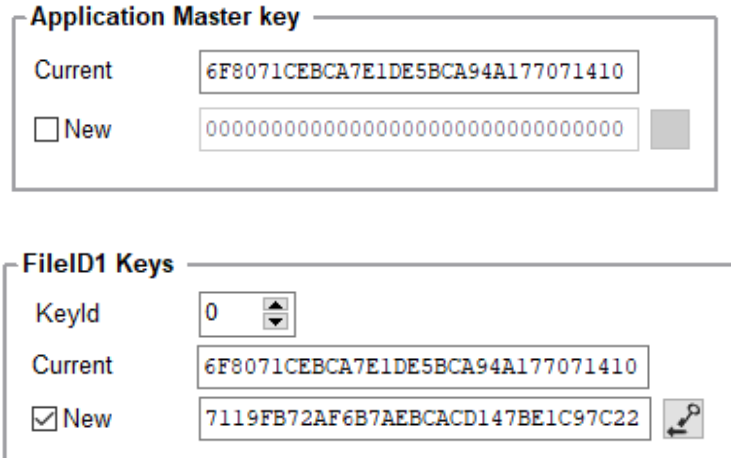
First encoding



Second encoding with the same key value

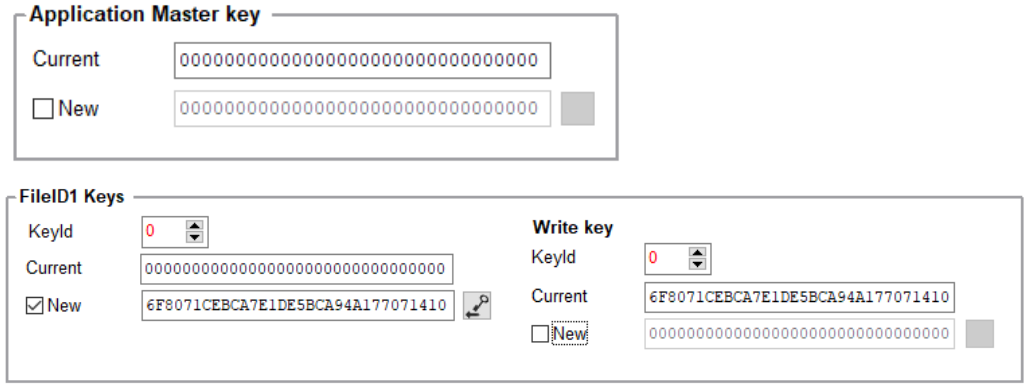


Second encoding with change key value

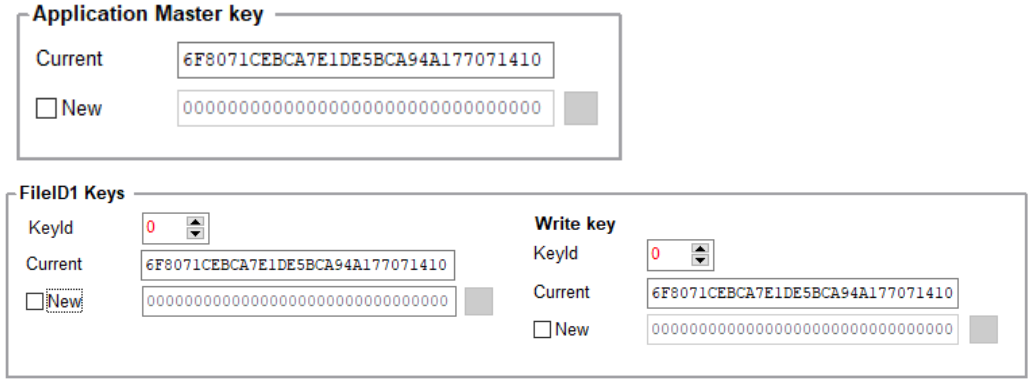


Case of two keys per file:

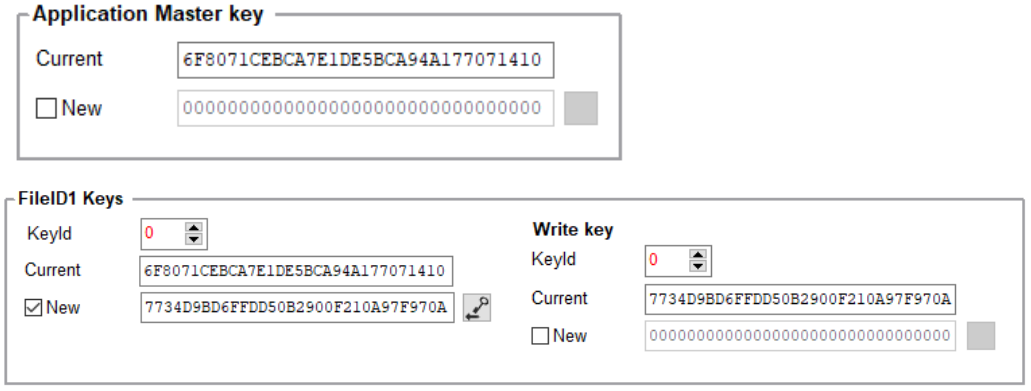
First encoding on virgin card



Second encoding with the same key value



Second encoding with change key value



DESFire® biometric template file security keys

Set the key number and key value for biometric file.

If using “One key per file” the section “Write key” is grayed.

To change a key value, in the "Current" field fill the current key and then checked "New" and fill in the field with the value of the desired key.

Default key are 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00.

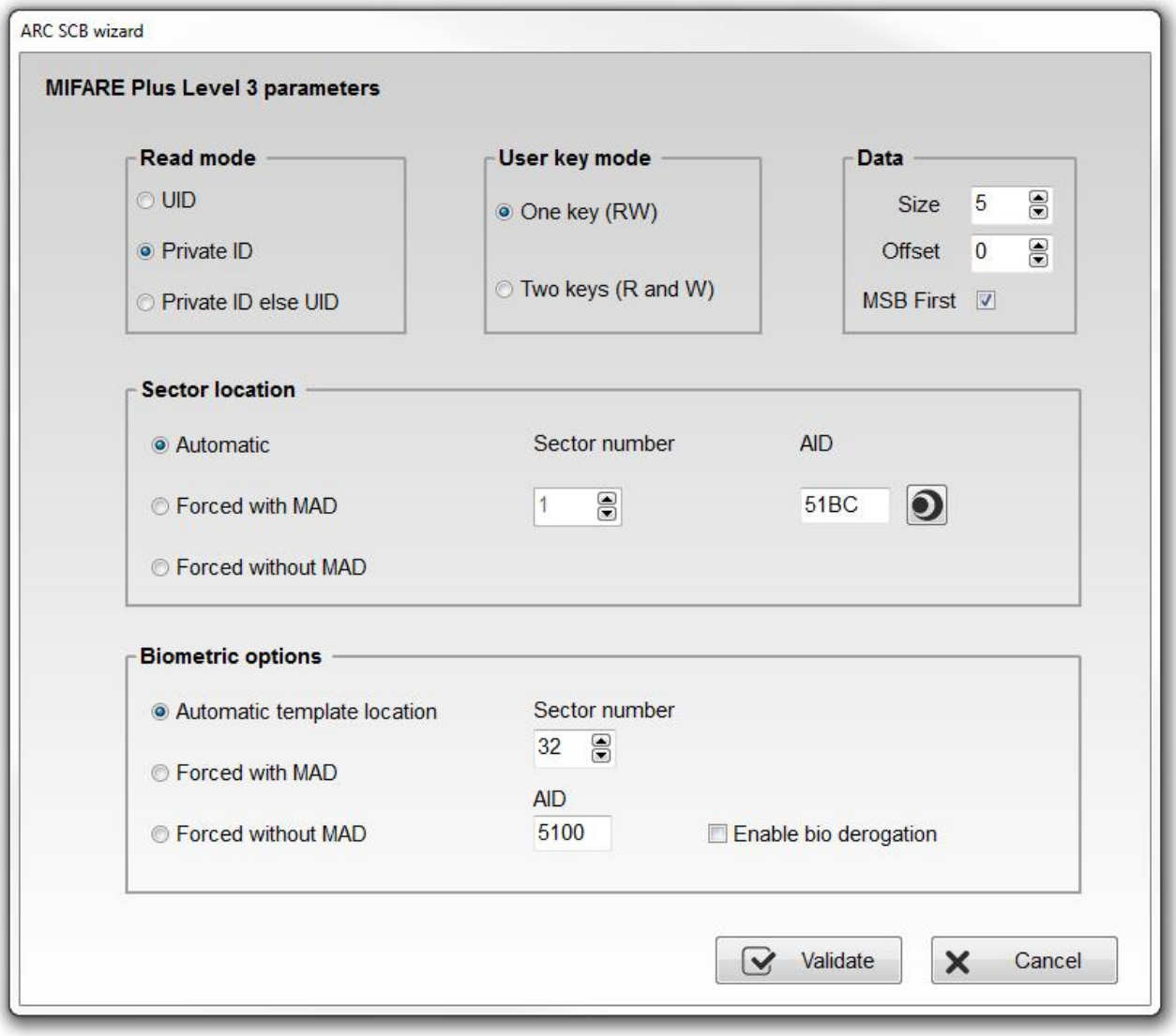
Note:

If in DESFire® settings the Read mode is “From Blue Mobile ID”, file ID1 keys are automatically determined according to Blue configuration keys.

Click the button 

to complete the DESFire® EVx keys.

III. 7 - MIFARE Plus® SL3: settings



Read mode

- UID: Reader configured in “read-only serial number”.
- Private ID: Reader configured in “read-only private code”.
- Private ID else UID: Reader configured in “read-only private code”. If it is not found or if the security settings are incorrect, then the reader will read and return the UID.

User Key mode

- One key (RW): Use one key per sector used for reading and writing.
- Two keys (R et W): Use two keys per sector. A key used for reading, the second for reading and writing.

Data

- Size: Determines the length of the ID read in the sector. The value corresponds to the protocol selected in the configuration of the reader. However, it is possible to choose a different size by entering another value, in this case the reader will read the ID to the size specified in this field and will return to the format defined by the protocol.
- Offset: Define an offset in the encoding from the first byte.
- MSB First: If the box is checked the reader reads the identifier Most Significant Byte First. If the box is unchecked the reader reads the identifier Least Significant Byte First.

Sector location

Define the sector to encode datas and/ or read by the reader.

MAD (Mifare® Application Directory) is a "table of contents" which reference applications (information) written in the areas of users' card through an AID (Application Identifier. Cf. AN103787).

It is completely customizable and is divided into two parts: the cluster code and application code.

The MIFARE Plus® 2k chip has 32 sectors (0 à 31). It can be used with MAD1 (sector 0 to manage sectors 1 to 15) and MAD2 (sector 16 to manage 17 to 31).

The MIFARE Plus® 4k chip has 40 sectors (0 to 39).It can be used with MAD1 (sector 0 to manage sectors 1 to 15) and MAD2 (sector 16 to manage sectors 17 à 39). Only the first 31 sectors are managed by SECard.

The MAD is protected by a read key (Key A) and a write key (Key B). Defaults are:

- ✓ "A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7" for key A
- ✓ "FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF" for key B

These key values are those recommended by *NXP* application note which allows at all users to access the MAD.

With this method (MAD and AID) a reader can retrieve a user code in cards that have been encoded at different memory areas with personal data at different location (in memory card).

- ❖ Automatic + AID:
  In this mode, the user does not have to worry about the location of data. The "SCB" and the user card are created with the following parameters:
  - ❖ First free sector available in card is chosen by SECard by MAD scanning.
  - ❖ AID defined in "AID" field is transmitted to the reader by the "SCB".
  - ❖ The user MAD card is programmed with AID in the corresponding position in the first sector available using the default keys:
    - Read key (key A) "A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7" cannot modified
    - Write key (key B) "FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF" can be modified
  - ❖ The reader identifies the user card sector to read by searching the AID in the MAD.

- ❖ Forced with MAD + sector number + AID:
  In this mode, sector number will be forced by SECard and use to encode user ID, but AID select in "AID field will be written in MAD at right location (depending the sector number forced).
  Reader configured with these parameters will only use forced sector number and NOT MAD to find the sector to read.

- ❖ Forced without MAD + sector number:
  In this mode, no MAD management is performed. Only the parameter "sector number" is considered to find the location of data in the chip.
  The reader reads the information in this sector. For the sector 0, only blocks 1 and 2 will be read.

Note: AID 51BC displayed by default in the "AID" field is the value of the Application Identifier STid.

Biometric option

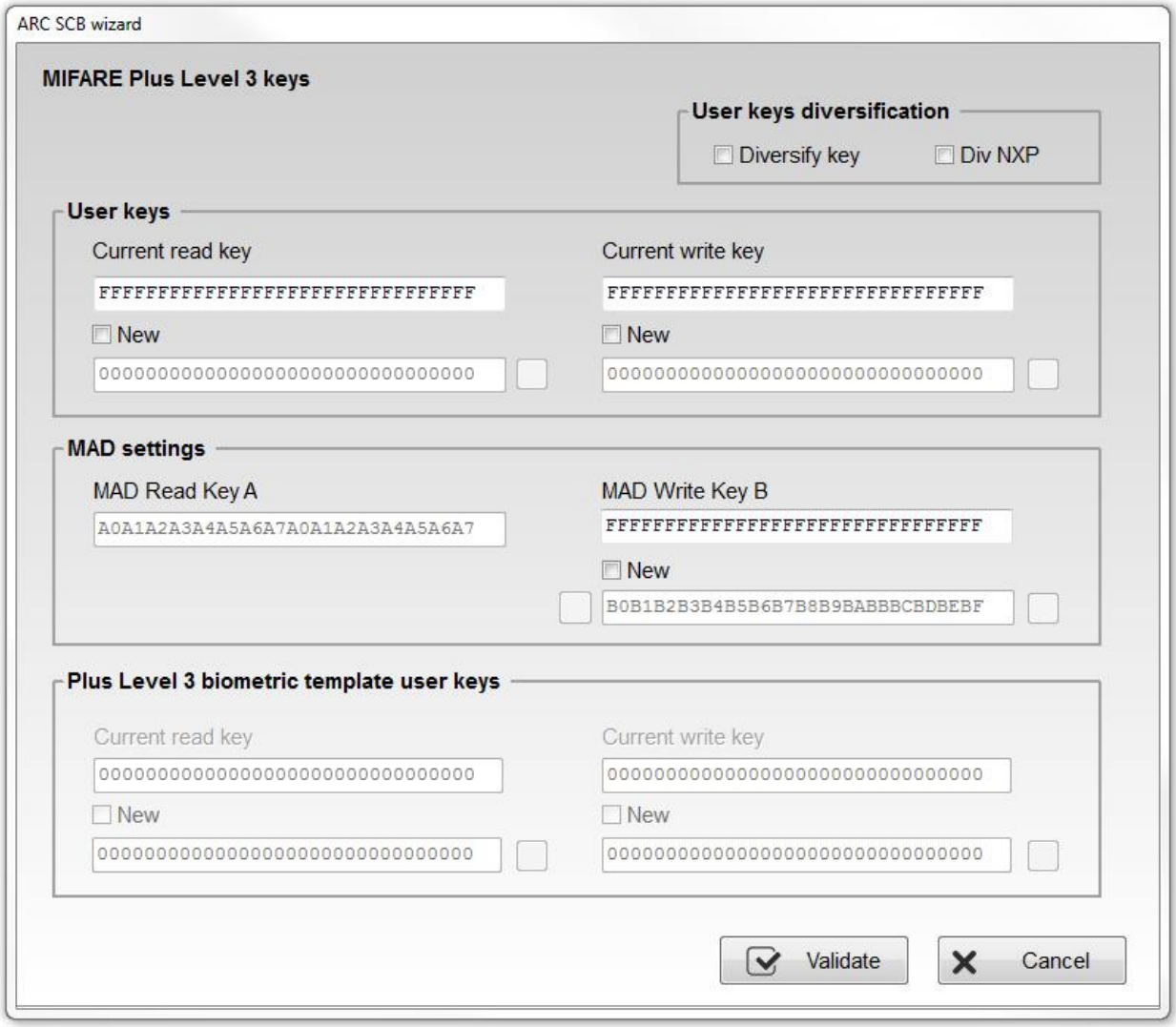
Fingerprints to encode will be registered in sectors 32 to 39 of chips MIFARE Plus® Level 3. Options “Auto”, “Forced with MAD” and “Forced without MAD” same principle as above.
In the case of the use of the MAD with AID, the AID value must be different from that used for the private ID.
Note: biometrics encoding is only possible on chips MIFARE Plus® Level 3 4KB of memory.

- Enable bio derogation: refer to *T7.2 - Biometric derogation*.

Click the button 

to complete the MIFARE Plus® Level 3 settings.

III. 8 - MIFARE Plus® SL3: keys



User keys diversification

- Activate / desactivate key diversification.
  This function allows you to use another than the one key than known by the user. To do this, the encoder uses the AES algorithm to generate another key. To that diversification is effective it is necessary to check the "New" key boxes to diversify and enter the value of the key.

- *"NXP"* diversify the key according to NXP-AN10922 method. If this option is not selected the keys will be diversified according to the NXP-AN165310 method.
  AES_CMAC(K,1|UID|blocNb).

User keys

Keys to protect the sector containing the private ID.
Enter the value of the current key and change it.

Note: From SECard 3.0.0, to re encode a MIFARE Plus®, it is not required to put the value from field New to field Current.

MAD settings

This box is available only if the location of the sector was set to "Automatic" or "Forced with MAD" mode.

Key A, reading MAD is automatically forced to the value "A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7."

Key B, writing MAD is by default FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF, it is possible to change by completing the field New of MAD Write key B.

During a management MAD, key sectors "0" and "16" change. The access conditions are:

- One read key, key A: “A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7”.
- One write key, key B: “FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF”.

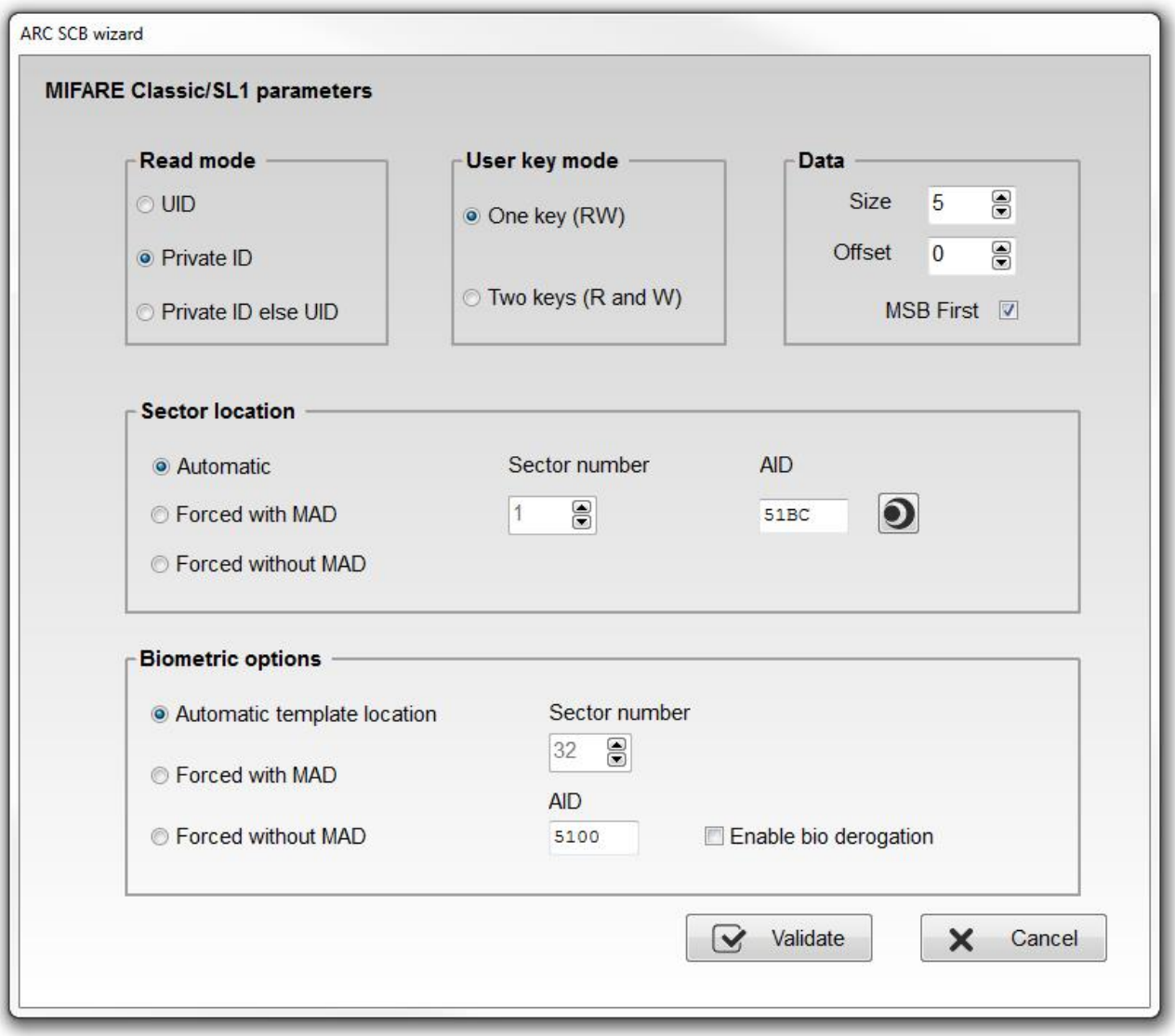
Plus Level 3 biometric template user keys

Key to protect the sector containing biometric information.
Enter the current value of the key and change it.

Click the button 

to complete the MIFARE Plus® Level 3 keys.

III. 9 - MIFARE® Classic/SL1: settings



Read mode

- ❖ UID: Reader configured in “read-only serial number”.
- ❖ Private ID: Reader configured in “read-only private code”.
- ❖ Private ID else UID: Reader configured in “read-only private code”. If it is not found or if the security settings are incorrect, then the reader will read and return the UID.

User Key mode

- ❖ One key (RW): One key per sector used for read and write operations.
- ❖ Two keys (R et W): Two keys per sector. A key used for read operation, the second one for read/ write operations.

Data

- ❖ Size: Determines the length of the ID read in the sector. The value corresponds to the protocol selected in the configuration of the reader. However, it is possible to choose a different size by entering another value, in this case the reader will read the ID to the size specified in this field and will return to the format defined by the protocol.
- ❖ Offset: Define an offset from the first byte, before encoding.
- ❖ MSB First: If the box is checked the reader reads the identifier Most Significant Byte First. If the box is unchecked the reader reads the identifier Least Significant Byte First.

Sector location

Define the sector to encode data and/or to read data by the reader.

MAD (Mifare® Application Directory) is a "table of contents" which reference applications (information) written in the areas of users' card through an AID (Application Identifier. Cf. AN103787).

It is completely customizable and is divided into two parts: the cluster code and application code.

The MIFARE® Classic 1k has 16 sectors (0 to 15). It can be used with MAD1 Sectors (1 to15) are available for data, sector 0 is occupied by the MAD.

The MIFARE Plus® 2k chip has 32 sectors (0 to 31). It can be used with MAD1 (sector 0 manage sectors 1 to 15) and MAD2 (sector 16 to manage sectors 17 to 31).

The MIFARE® Classic / MIFARE Plus® 4k chip has 40 sectors (0 to 39). It can be used with MAD1 (sector 0 manage sectors 1 to 15) and MAD2 (sector 16 manage sectors 17 to 39). Only the first 31 sectors are managed by SECard.

The MAD is protected by a read key (Key A) and a write key (Key B). Default values are:

- ✓ "A0 A1 A2 A3 A4 A5" for key A
- ✓ "FF FF FF FF FF FF" for key B

These key values are those recommended by *NXP* application note which allows at all users to access the MAD.

With this method (MAD and AID) a reader can retrieve an user code in cards that have been encoded at different memory areas with personal data at different location (in memory card).

- ❖ Automatic + AID:
  In this mode, the user does not have to worry about the location of data. The "SCB" and the user card are created with the following parameters:
  - ❖ First free sector available in card is chosen by SECard by MAD scanning.
  - ❖ AID defined in "AID" field is transmitted to the reader by the "SCB".
  - ❖ The user MAD card is programmed with AID in the corresponding position in the first sector available using the default keys:
    - Read key (key A) "A0 A1 A2 A3 A4 A5" can be modified
    - Write key (key B) "FF FF FF FF FF FF" can be modified
  - ❖ The reader identifies the user card sector to read by searching the AID in the MAD.

- ❖ Forced with MAD + sector number + AID:
  In this mode, sector number will be forced by SECard and use to encode user ID, but AID select in "AID field will be written in MAD at right location (depending the sector number forced).
  Reader configured with these parameters will only use forced sector number and NOT MAD to find the sector to read.

- ❖ Forced without MAD + sector number:
  In this mode, no MAD management is performed. Only the parameter "sector number" is considered to find the location of data in the chip.
  The reader reads the information in this sector. For the sector 0, only blocks 1 and 2 will be read.

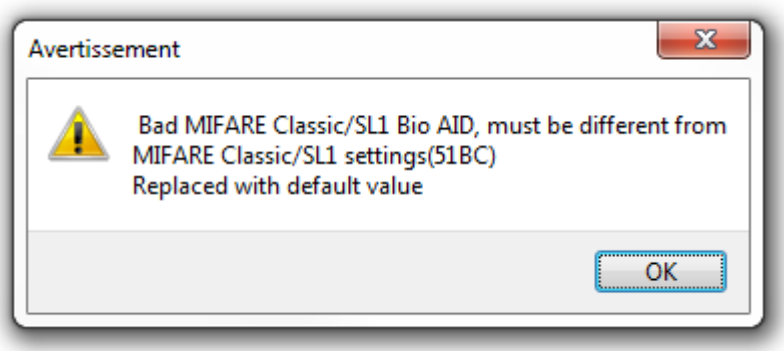
Note: AID 51BC displayed by default in the "AID" field is the value of the Application Identifier STid.

Biometric options

Only available for MIFARE® Classic 4ko.

Define the sector (>=32) to encode template and/or to read template by the reader.

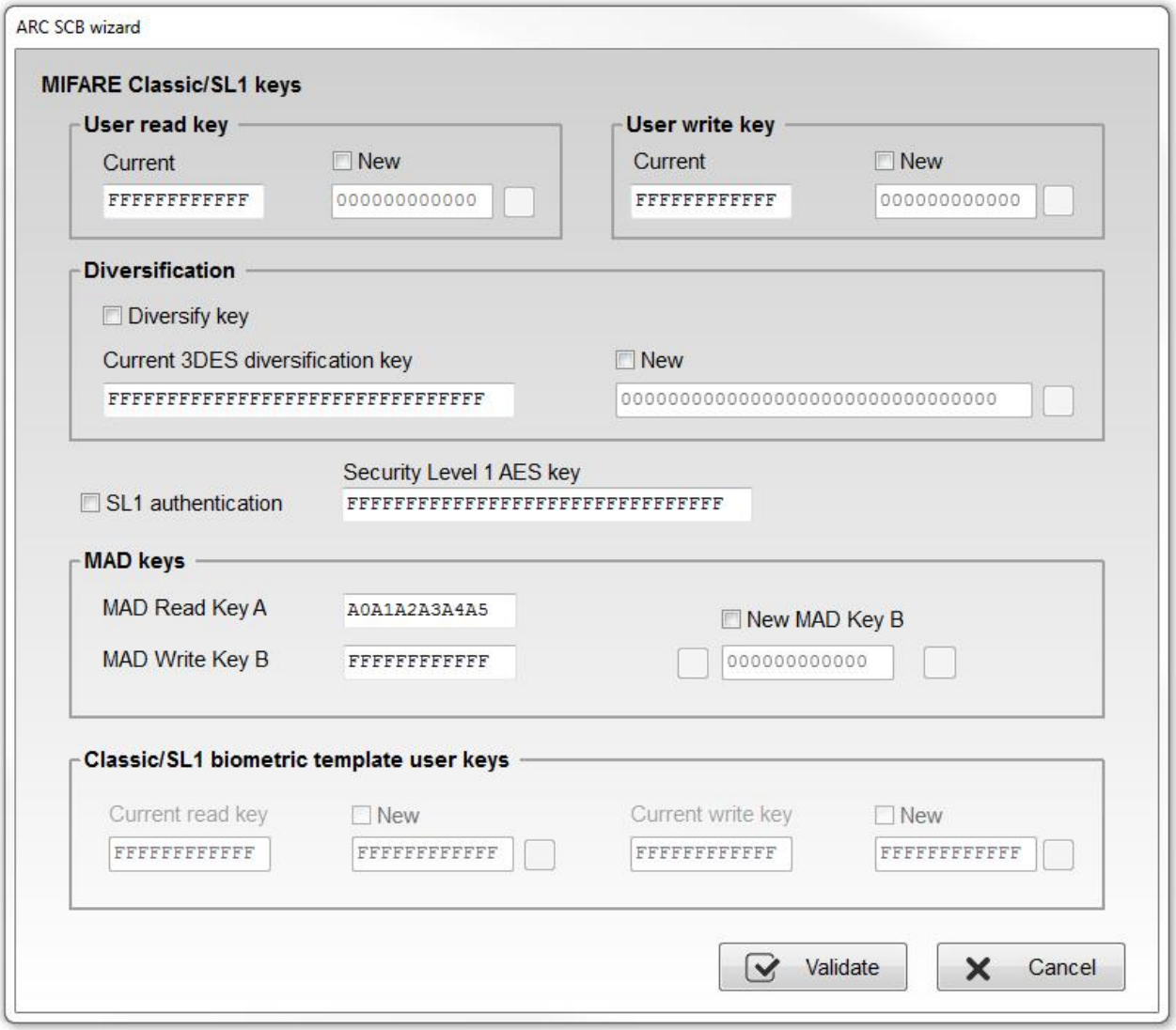
If the MAD used, it must be different than MAD used for data.



- Enable bio derogation: refer to *T7.2 - Biometric derogation*.

Click the button Validate **to complete MIFARE® Classic/SL1 settings.**

III. 10 - MIFARE® Classic /SL1: keys



User read key / User write key

Keys to protect the sector containing the private ID.
Enter the value of the current key and change it.

Note: the default keys for a blank card are either "FF FF FF FF FF FF" or "A0 A1 A2 A3 A4 A5" according to the original supplier of the card.

Diversification

- Activate / deactivate the key diversification.
  This function allows you to use a different key than known by the user. For this, the encoder uses the diversification algorithm to generate a new key. It will be function of block number, the serial number, user key and a 3DES encryption key of 16 bytes. To be effective it is necessary to check the "New" key boxes to diversify and enter the new value of the key.

Note: it is possible to deactivate the key diversification. For this, you must recreate the "SCB" by unchecking the "Diversification" box and indicating in the first field the value of the key 3DES. It will be necessary later to encode the user card again without this option.

The diversification algorithm used is the one recommended by NXP (AES-CMAC – NXP AN165310).

It's AES_CMAC(K,1|UID|blocNb) with K the key to diversify.

SL1 authentication

Activate the AES authentication for MIFARE Plus® Level 1 chip. It is used to secure authentication chip / reader by an encryption algorithm.

Only available for "*Private ID"* and "Private *ID else UID". (*UID will be sent in this mode if the reader is unable to authenticate*).*

Warning

This key is important and should definitely be known to the administrator
A MIFARE Plus® Level 1 with another AES key value cannot authenticate with the reader.

If this option is used, the reader can no longer read private code of MIFARE® Classic

To disable this option, it is necessary to recreate / reconfigure the card "SCB" by unchecking "*SL1 authenticate"*.

For an encoding of Mifare® Classic 7 bytes CSN, it is necessary to desactivate the "*Autocard Type*" and to choose "*Classic/Plus L1*".

MAD keys

This box is available only if the location of the sector was set to "Automatic" or "Forced with MAD" mode.

Key A, reading MAD is by default "A0 A1 A2 A3 A4 A5", it is possible to use a different key by modifying the value in the field.

Key B, writing MAD is by default "FF FF FF FF FF FF", it is possible to change by completing the field New of MAD Write key B.

During a management MAD, key sectors "0" and "16" change. The access conditions are:

- One read key, key A: "A0 A1 A2 A3 A4 A5".
- One write key, key B: "FF FF FF FF FF FF".

Note: from NXP AN-10787 Rev07 7 July 2010 document, key A is fixed to A0A1A2A3A4A5A6A7.

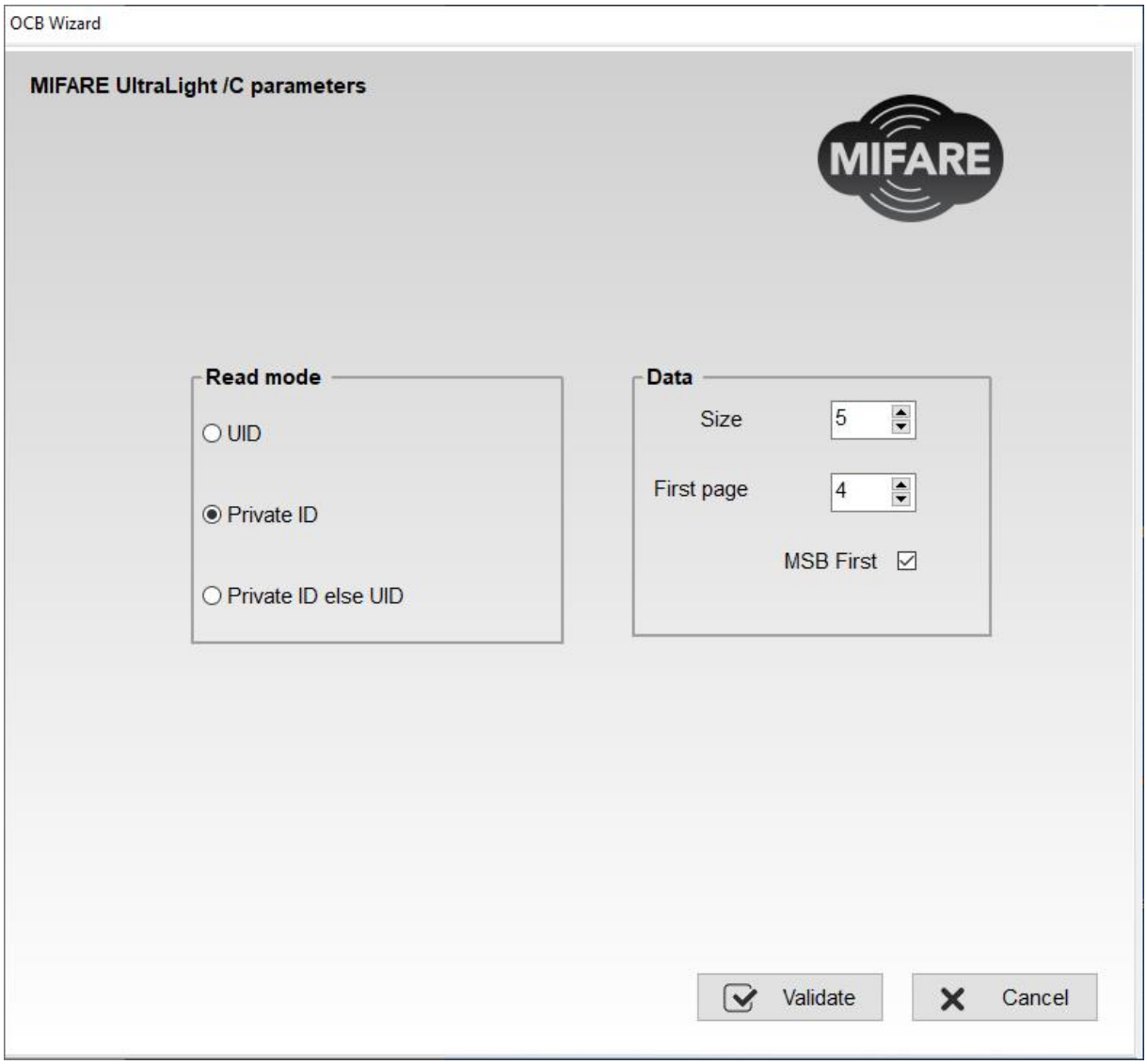
Classic/SL1 biometric template user keys

Keys to protect the sector containing the template.
Enter the value of the current key and change it.

Click the button 

to complete MIFARE® Classic/SL1 keys.

III. 11 - MIFARE Ultralight® C: settings



Read mode

- UID: Reader configured in “read-only serial number”.
- Private ID: Reader configured in “read-only private code”.
- Private ID else UID: Reader configured in “read-only private code”. If it is not found or if the security settings are incorrect, then the reader will read and return the UID.

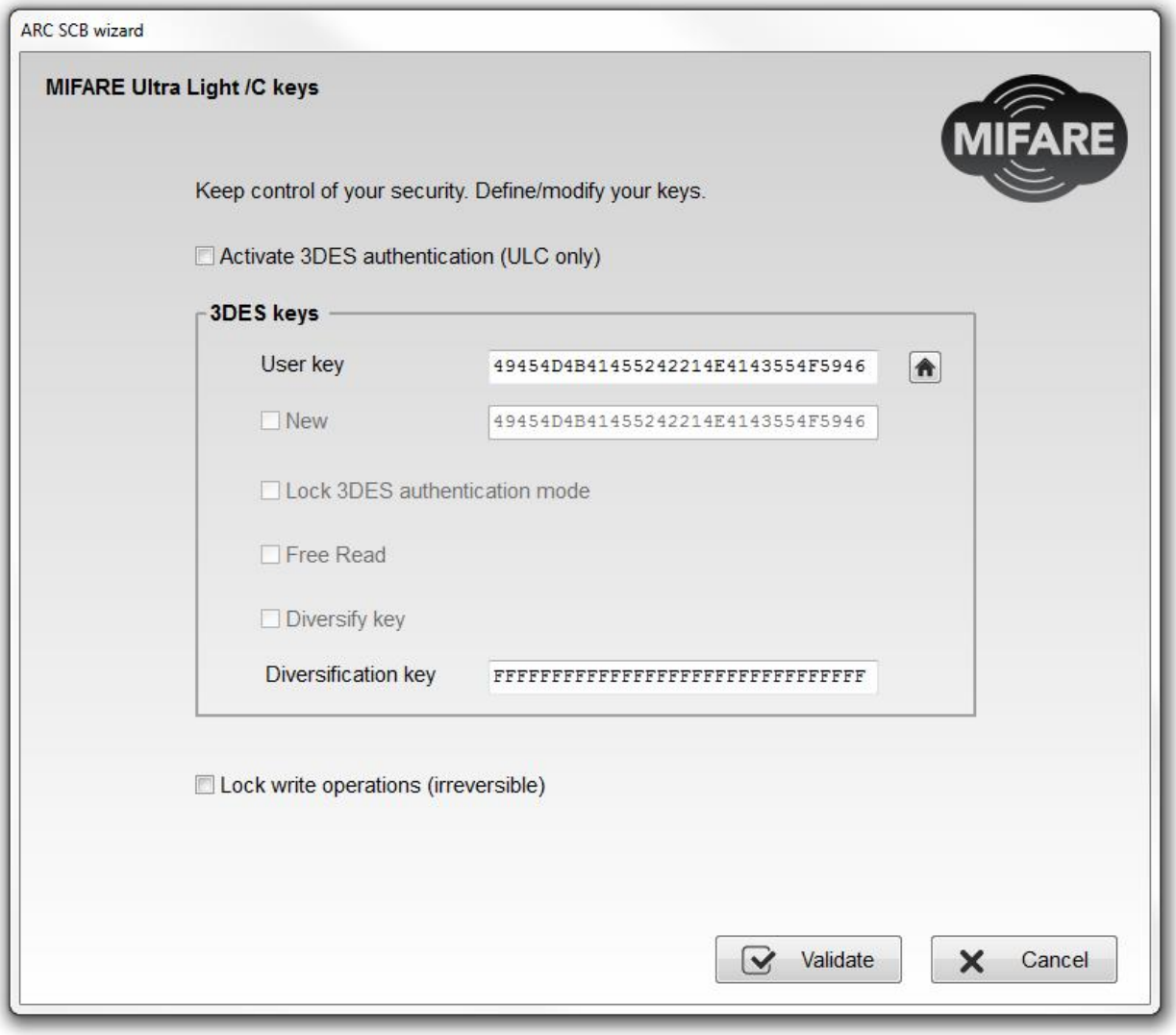
Data

- Size: Determine the length of the ID read. The value corresponds to the protocol selected in the configuration of the reader. However it is possible to choose a different size by entering another value, in this case the reader will read the ID to the size specified in this field and will return to the format defined by the protocol.
- First page: Define the first page where the private ID will be encode / read. In addition, 3DES authentication changes will be effective from this value to the last page.
- MSB First: If the box is checked the reader reads the identifier Most Significant Byte First. If the box is unchecked the reader reads the identifier Least Significant Byte First.

From SECard V3.0.0, the first accessible page becomes the page 3. **Warning: it’s an OTP page. Re-encoding is not possible in this case.**

Click the button Validate **to complete MIFARE Ultralight®/C settings.**

III. 12 - MIFARE Ultralight® C: keys



Activate 3DES authentication (ULC only)

Activate/ deactivate 3DES authentication between MIFARE Ultralight® C chip and the reader.

User key

Fields reserved for common values of 3DES keys and change.
Default user key is: *49454D4B41455242214E4143554F5946*.

Lock 3DES authentication mode

If this option is selected, it will be necessary to use 3DES authentication with MIFARE Ultralight® C chip (**this action is irreversible**).

Free read

If this option is selected and if “Lock 3DES authentication mode” is not selected, it will NOT be necessary to use 3DES authentication with MIFARE Ultralight® C chip to read encoded data.

Diversify keys

Activate key diversification.

With the diversification function, it is possible to use a different key from that known by the user. For this, the encoder uses a diversification algorithm in order to generate a key based on the serial number, the user key and a 3DES encryption key.

Lock write operations (irreversible)

Prohibit all write operations on the chip. It will be read only mode (**this action is irreversible**).

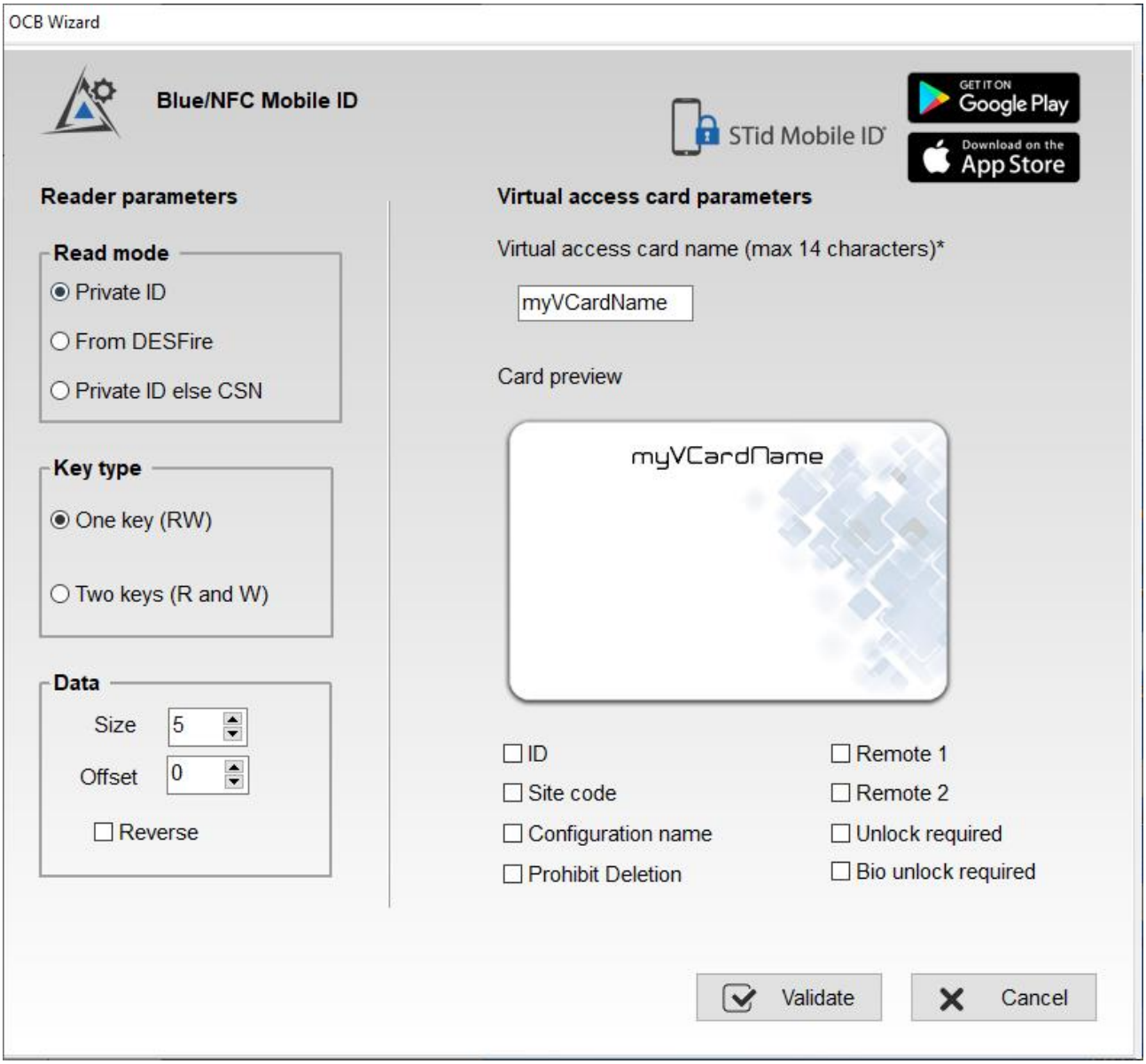
Click the button 

to complete MIFARE Ultralight®/C keys.

III. 13 - Blue/NFC Mobile ID: settings

III.13.1 - STid Mobile ID®

- **Read mode: Private ID**



Reader configured in “read-only private ID”.

Key type

- One key (RW): Use one key for reading and writing.
- Two keys (R & W): Use two keys. A key used for reading, the second for reading and writing.

Data

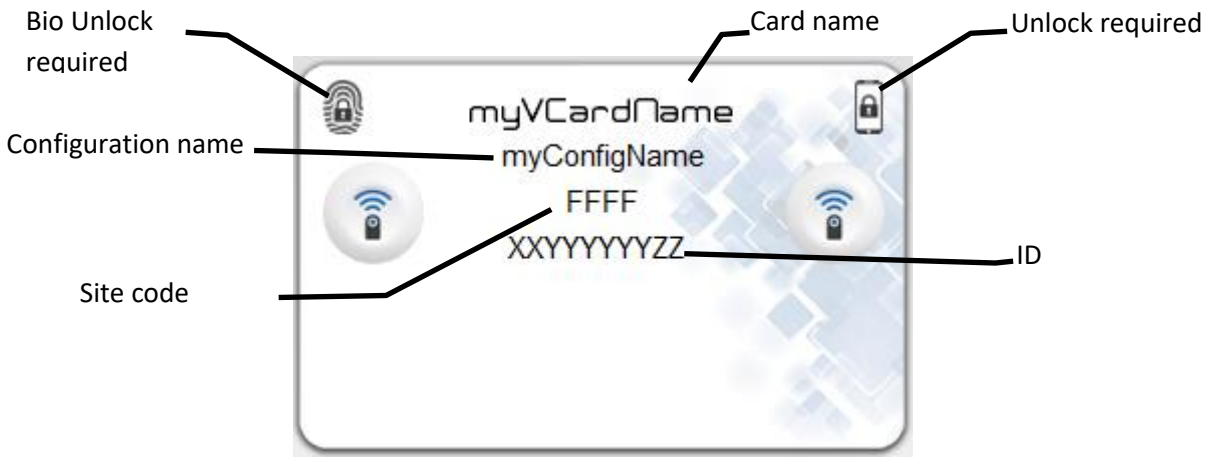
- Size: Determines the length of the ID.
  In SCB, Size must be equal to the protocol size in SCB-Step3.
- Offset: Define an offset from the first byte before reading.
- Reverse: If the box is checked the reader reads the identifier Least Significant Byte First. If the box is unchecked the reader reads the identifier Most Significant Byte First.

Virtual access card parameters

Customize virtual access card by selecting the parameters to be displayed.
Virtual access card name: Enter the name of the virtual access card. 14 characters max.

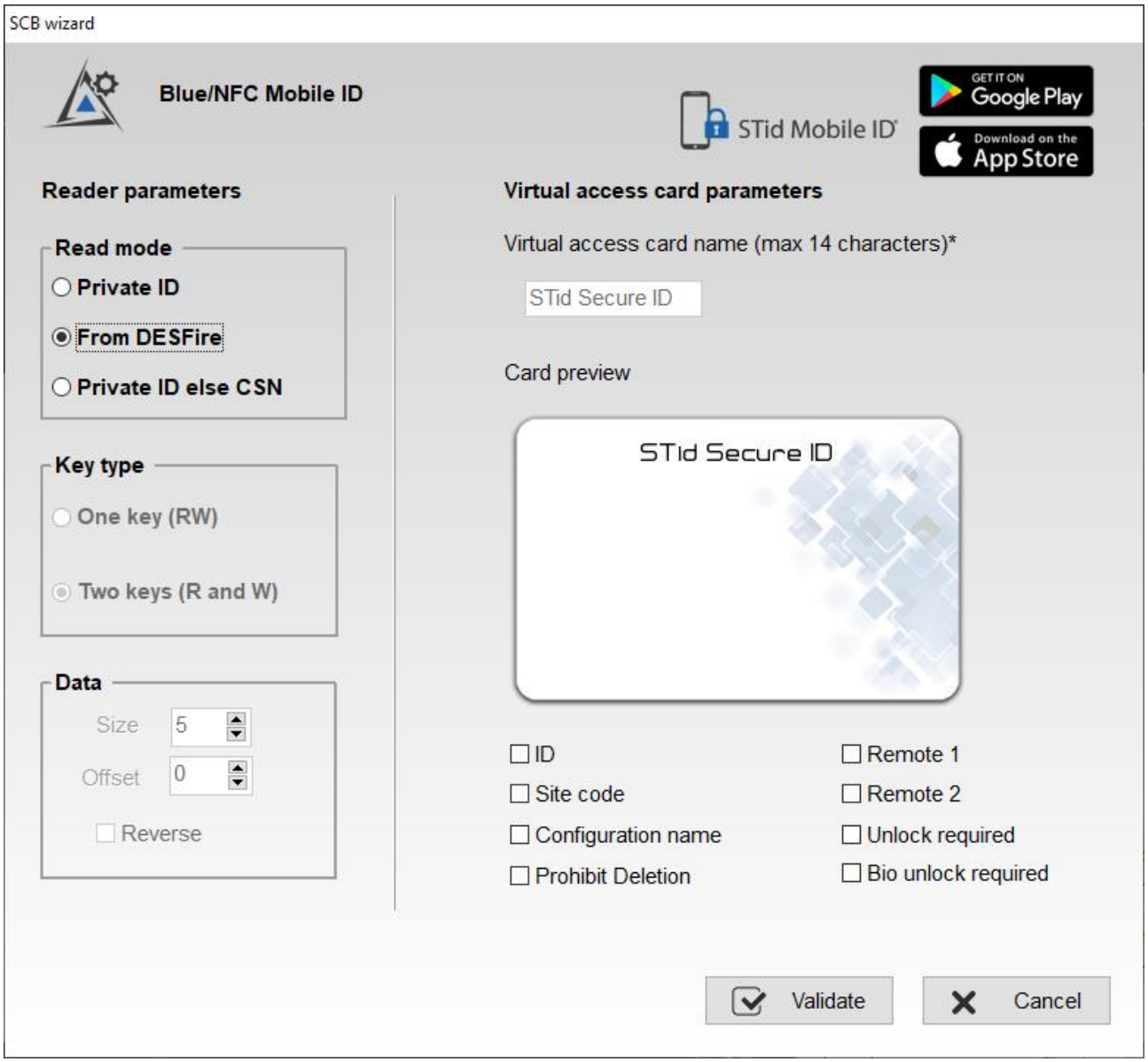
Note: In case where the user has several virtual access cards on his smartphone, choose a significant name to the access card.

Non-contractual picture

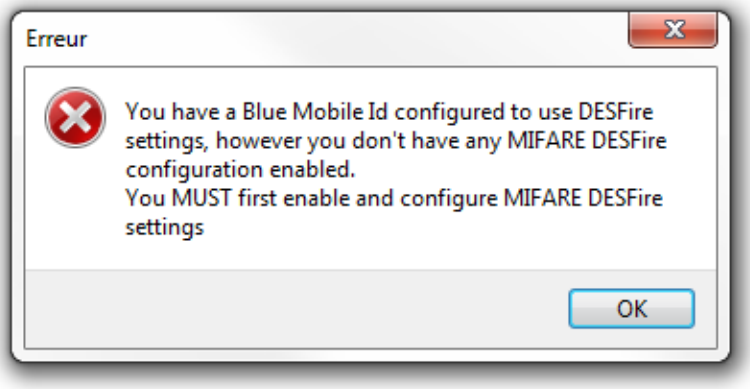


<u>Prohibit Deletion</u>: prohibit the deletion of the virtual access card by the user. Only the administrator, via SECard (Settings / Credits / Delete your virtual access card) can delete it.

❖ **Read mode: from DESFire**



❖ If this mode is selected, a DESFire® configuration must be enabled; if you select this option without DESFire® configuration enabled you have the error:

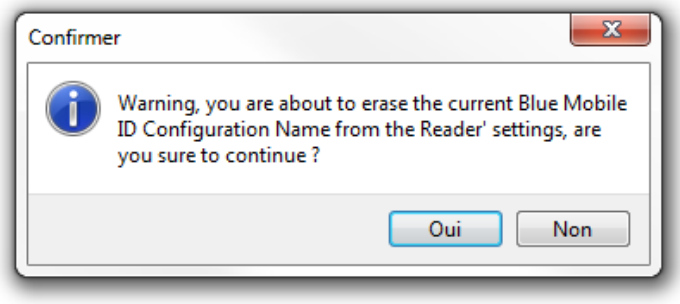


❖ In this mode, the Blue Mobile ID parameters are automatically determined and inherited from the DESFire® configuration.

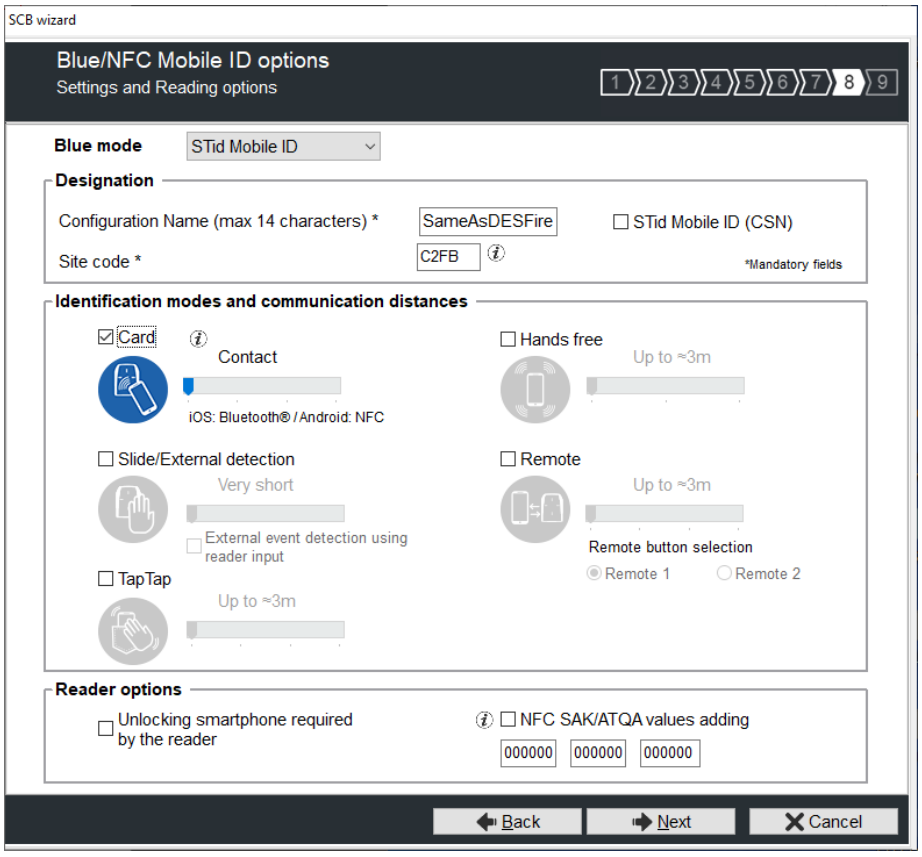
These settings cannot be changed:

- ✓ Reverse no: MSB First
- ✓ Key type, Size and offset same as DESFire® configuration.

Warning



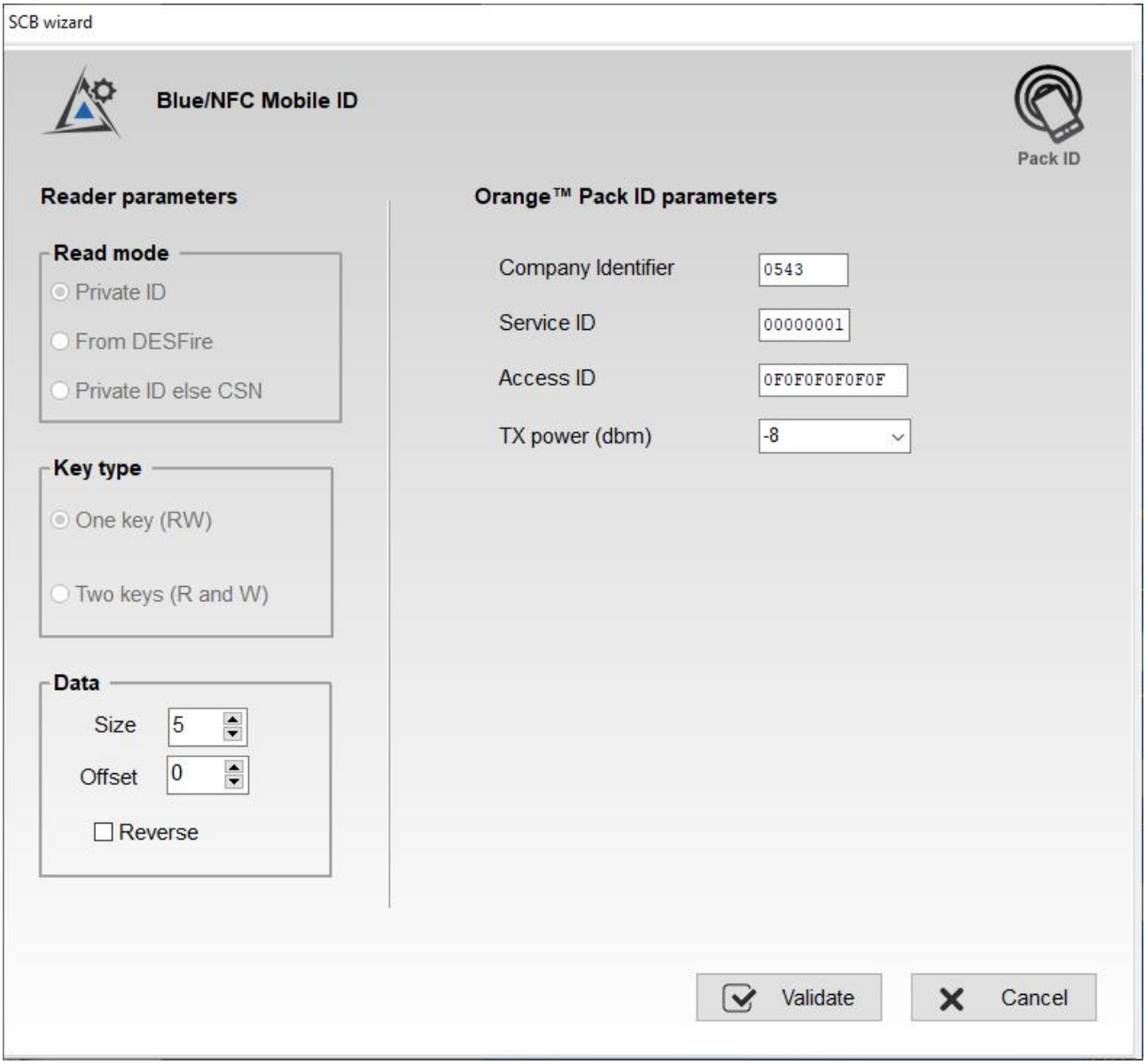
Note: Reader parameters are modified and the configuration used is SameAsDESFire.



❖ **Read mode: Private ID else CSN**

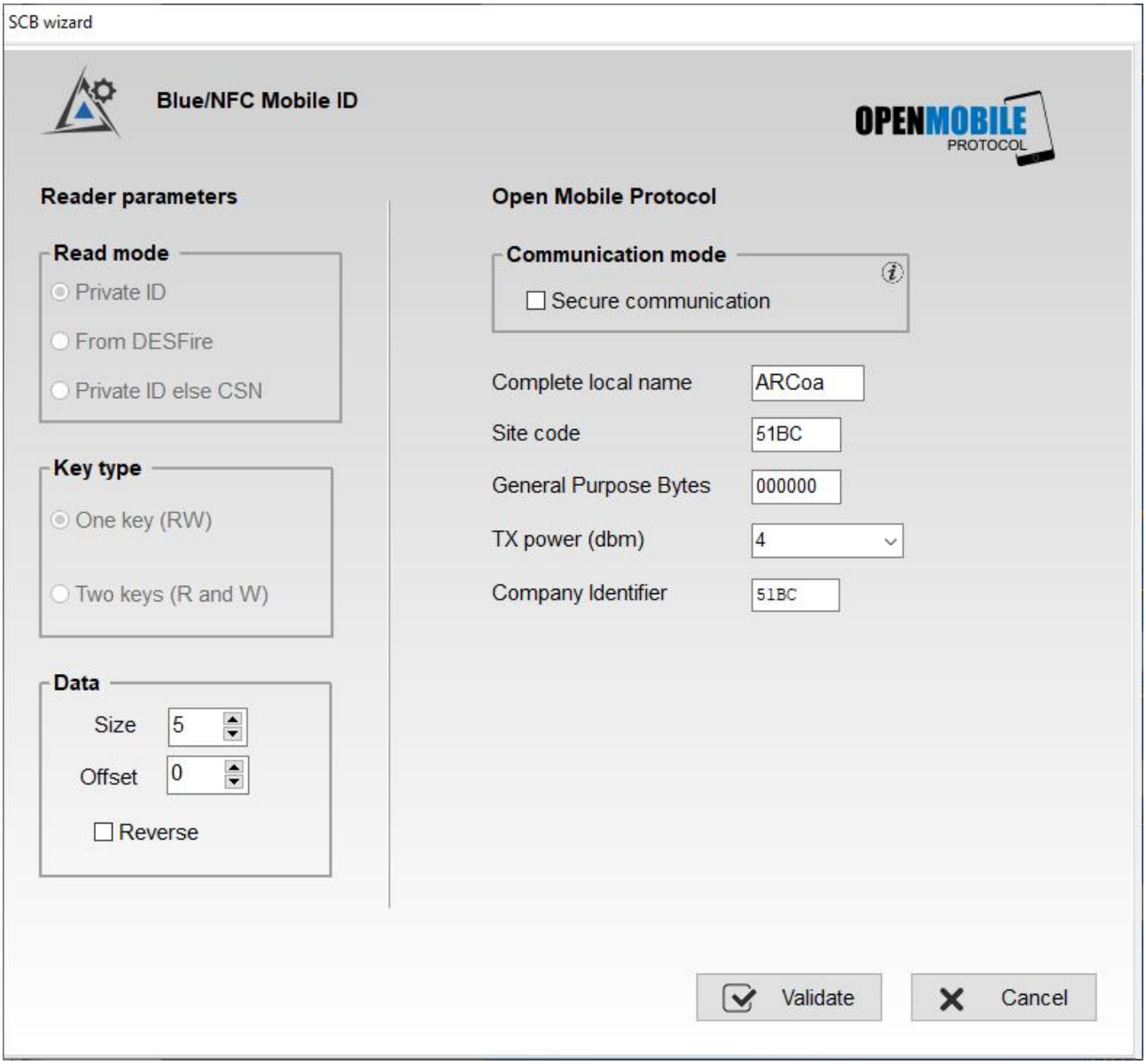
Reader configured in “read-only private virtual card”. If it is not found or if the security settings are incorrect, then the reader will read and return the STid Mobile ID® CSN.

III.13.2 - Orange™ Pack ID



- Company Identifier: manufacturer data on 2 bytes.
- Service ID: manufacturer data on 4 bytes to differentiate the customers of Pack ID.
- Access ID: manufacturer data on 6 bytes to identify the access zone controlled by the reader.
- Tx power: change the power level of the reader (default 4 dbm). Possible values: -16, -12, -8, -4, 0 and 4 dbm.

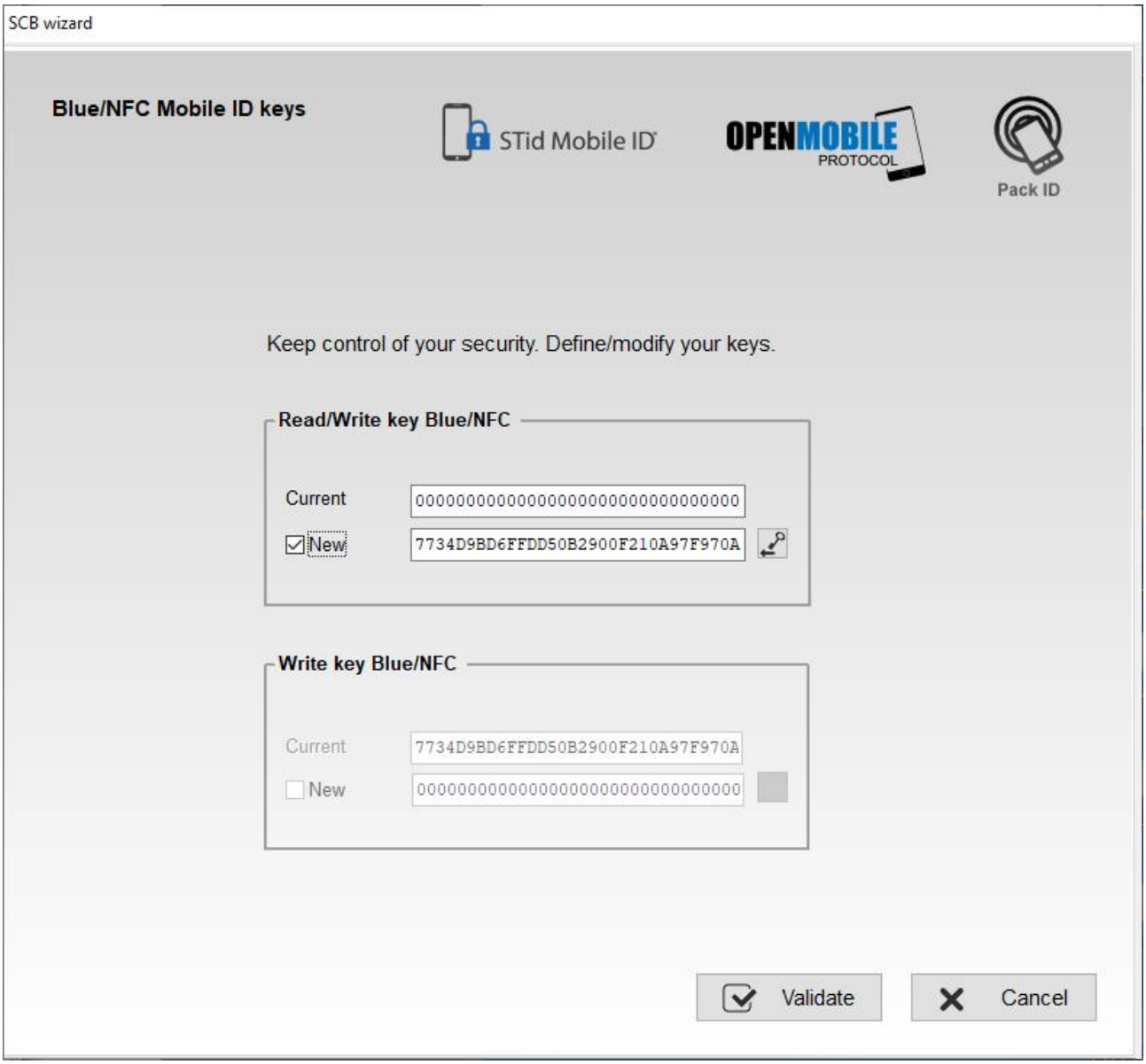
III.13.3 - Open Mobile Protocol



For information about Open Mobile Protocol, contact your STid sales representative.

Click the button  **to complete Blue Mobile ID settings.**

III. 14 - Blue/NFC Mobile ID: Keys



Set the key value for Blue/NFC Mobile ID data.

If using “One key RW” the section “Write key” is grayed.

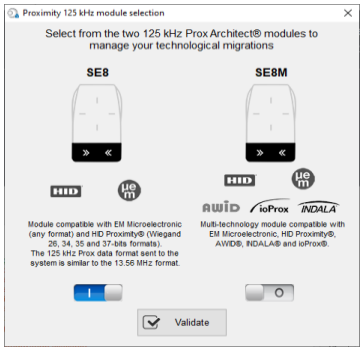
To change a key value: fill the current key in the "Current" field and then check "New" and fill the value of the desired key in the field.

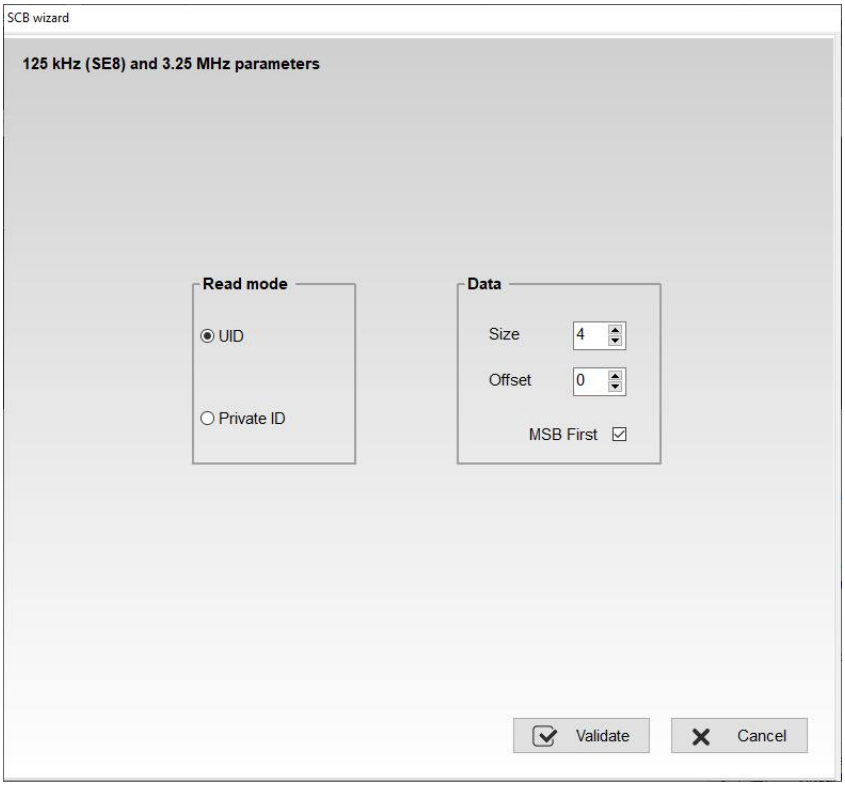
Default keys are 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00.

III. 15 - 125 kHz: settings

The Settings screen depend on the SE8 module selected in Reader configuration Wizard step 2

III.15.1 - SE8





Configure reader settings related to EM4102 chip, EM4x50, HID 125, Nedap.

Read mode

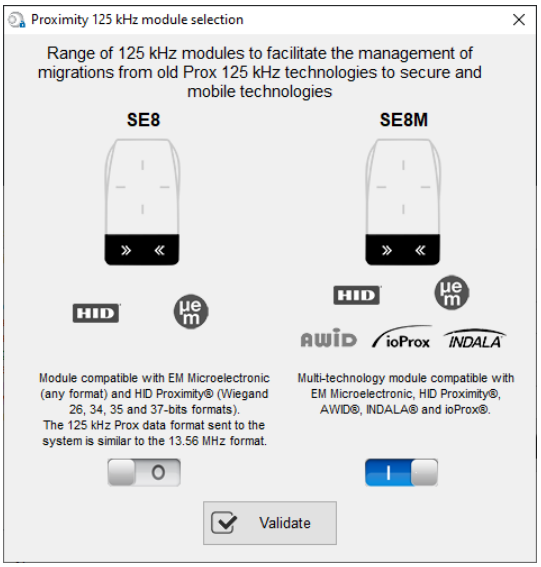
- UID: Reader configured in “read-only serial number”.
- Private ID: Reader configured in “read-only private Id” with determine size and offset. Allows to manage the particular functioning of the 2H.

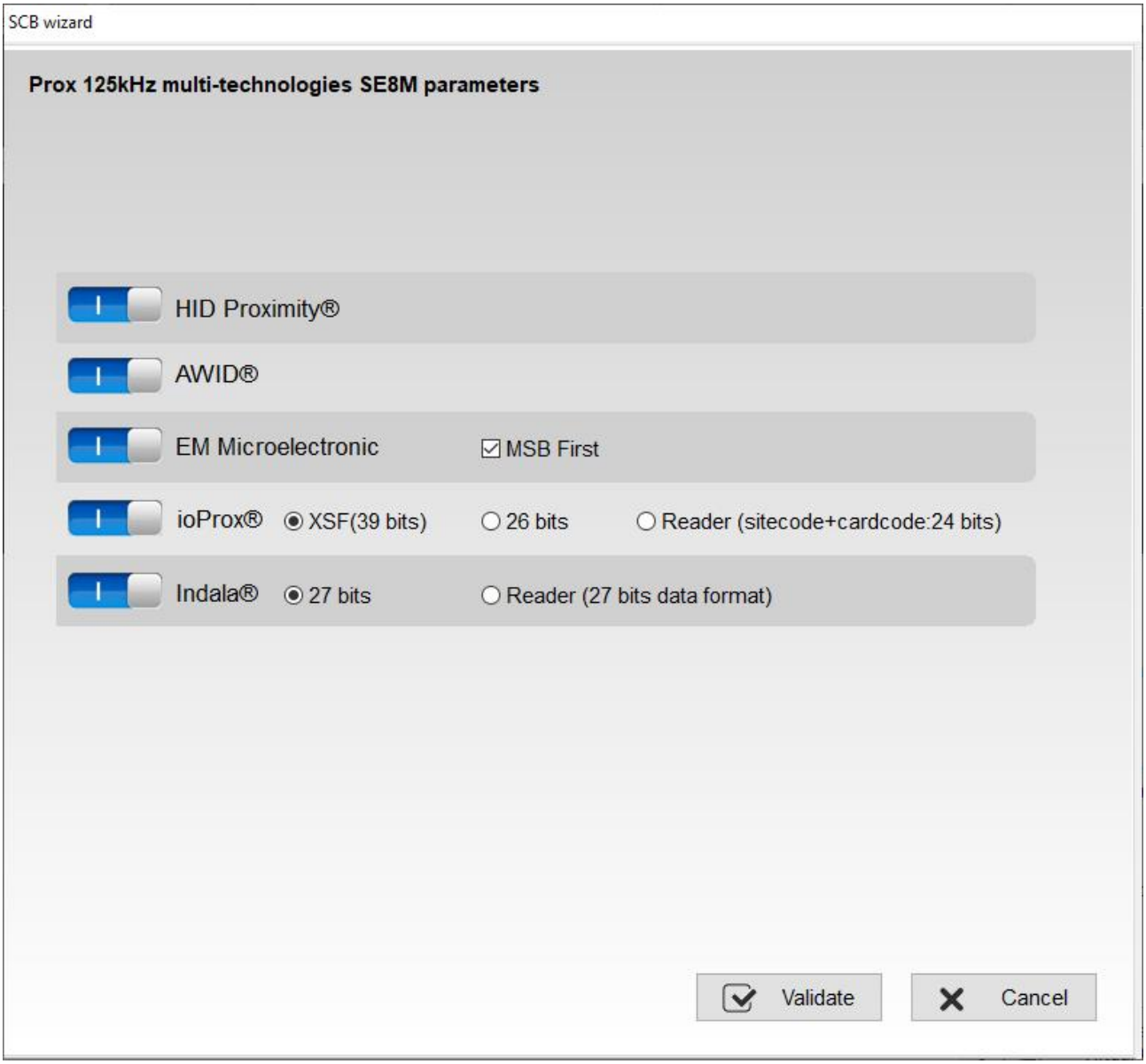
Data

- Size: Determine the length of the ID read. The value corresponds to the protocol selected in the configuration of the reader. However, it is possible to choose a different size by entering another value, in this case the reader will read the ID to the size specified in this field and will return to the format defined by the protocol.
- Offset: Allow to shift the private number to be read from the byte "0".
- MSB First: If the box is checked the reader reads the identifier Most Significant Byte First. If the box is unchecked the reader reads the identifier Least Significant Byte First.

Click the button  **to complete 125 kHz settings.**

III.15.2 - SE8M


Proximity 125 kHz module selection
Range of 125 kHz modules to facilitate the management of migrations from old Prox 125 kHz technologies to secure and mobile technologies
SE8
SE8M
HID
HID
AWID
ioProx
INDALA
Module compatible with EM Microelectronic (any format) and HID Proximity® (Wiegand 26, 34, 35 and 37-bits formats). The 125 kHz Prox data format sent to the system is similar to the 13.56 MHz format.
Multi-technology module compatible with EM Microelectronic, HID Proximity®, AWID®, INDALA® and ioProx®.
Validate


SCB wizard
Prox 125kHz multi-technologies SE8M parameters
HID Proximity®
AWID®
EM Microelectronic
MSB First
ioProx®
XSF(39 bits)
26 bits
Reader (sitecode+cardcode:24 bits)
Indala®
27 bits
Reader (27 bits data format)
Validate
Cancel

❖ HID Proximity®

The output protocol depends on the encoded card format.

The output protocol selected on Configuration reader wizard step 3 is not consider.

❖ AWID®

The output protocol depends on the encoded card format.

The output protocol selected on Configuration reader wizard step 3 is not consider.

❖ EM Microelectronic

The output protocol is the output protocol reader selected on Configuration reader wizard step 3.

MSB First

If the box is checked, the reader reads the identifier Most Significant Byte First.
If the box is unchecked, the reader reads the identifier Least Significant Byte First.

❖ ioProx®

Message structure

Bit 1 ...Bit 5 (6 bits)	Bit 6 ... Bit 38 (data)			Bit 39 (1 bit)
	Bit 6...bit 13 (8 bits)	Bit 14...Bit 21 (8 bits)	Bit 22...Bit 38 (16 bits)	
Size of data card	*Family code*	*Site Code*	*Card code*	*Odd parity on the 38 bits*

Example:

39 size	0x01 family code	0x73 (site code)	26414 = 0x672E	Parity
10 0111	0000 0001	0111 0011	0110 0111 0010 1110	0

◉ 26 bits

Message structure

Bit 1	Bit 2 ... Bit 25 (data)		Bit 26
	Bit 2...Bit 9	Bit 10...bit 25	
Even parity from bit 2 to bit 13	*Site code*	*Card code*	*Odd parity from bit 4 to bit 25*

✓

Example: 

Parity	0x73 (site code)	26414 = 0x672E	Parity
1	0111 0011	0110 0111 0010 1110	0

◉ Reader (sitecode+cardcode:24 bits)

SiteCode + Card code are sent within a frame according the output protocol reader selected on Configuration reader wizard step 3.

❖ Indala

◉ 27 bits

Message structure

Bit 1 ...Bit 27 (27 bits)
Card data

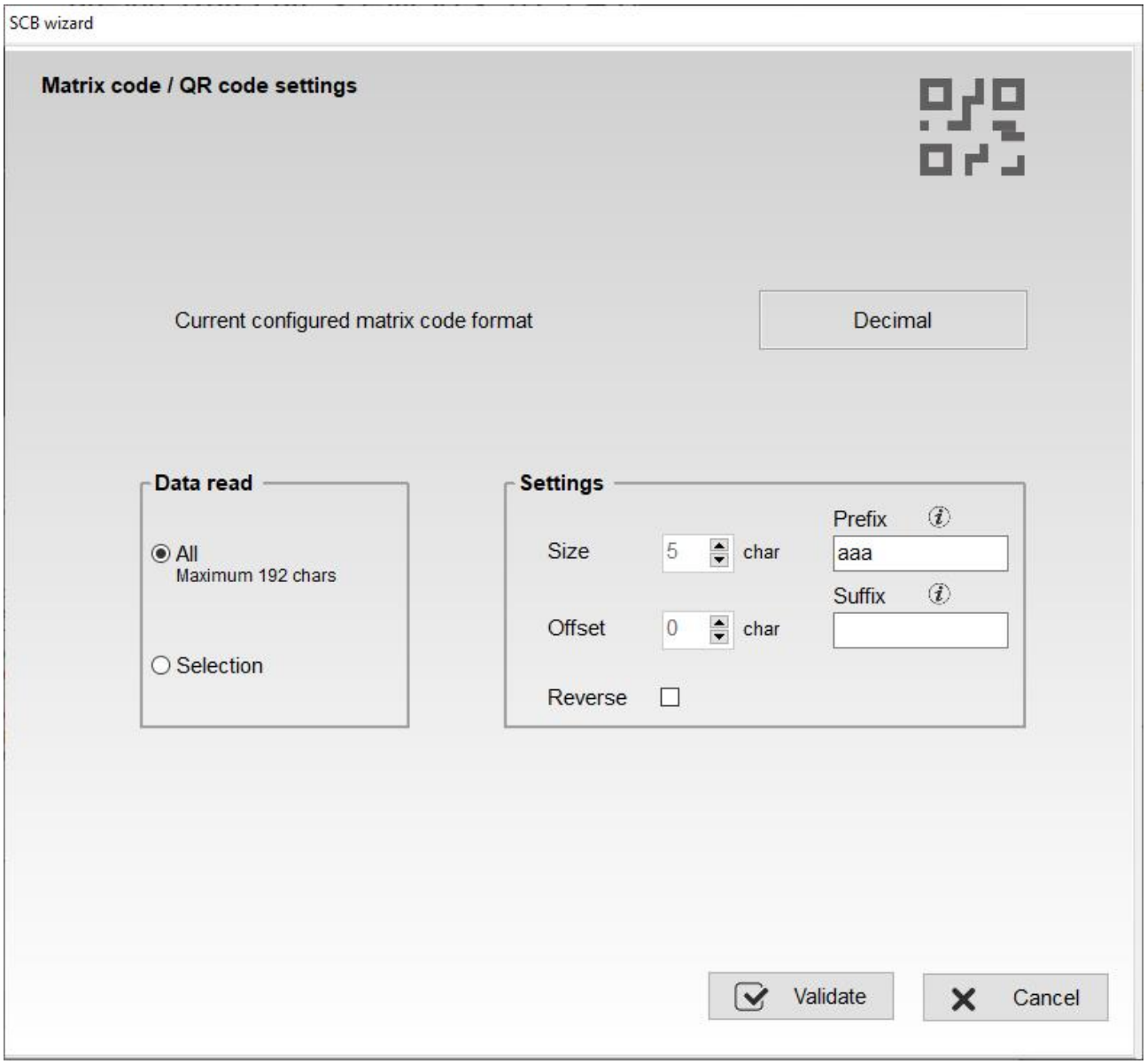
Example: 

19030 = 0x0004A56
000 0000 0000 0100 1010 0101 0110

◉ Reader (27 bits data format)

27 bits card code are sent within a frame according the output protocol reader selected on Configuration reader wizard step 3.

III. 16 - MATRIX code / QR Code: settings *Adding functionality 3.6*



- **All**: Read the complet string
- **Selection**: Read a string with size and Offset defined.
  - If Size is set to 0, there is no filtering on the character string, the character string is completely read. It is possible to have a size 0 and set an offset.
  - Reverse: allows you to reverse the code read according to the defined format of the QR Code

Example :

- Decimal: read the decimal code, convert to hexadecimal then invert byte by byte
  - 1234 => 0x04D2 => 0xD204
- Hexadecimal: read the hexadecimal code, then invert byte by byte
  - 1234 => 0x1234 => 0x3412
- ASCII: reading the ascii code, converting to hexadecimal then inverting byte by byte
  - 31323334 => 0x1234 => 0x3412

Note: if the code type to read is not the code type set in the wizard, the code is not read. For example, if decimal type is set and the code to read contain letter the code will not read.

❖ **Prefix / Suffix** :

The prefix and / or suffix can be used to read only data that contains specific start and / or end text characters or to find the ID number in a longer text string.

The prefix / suffix characters will be deleted from the data read.

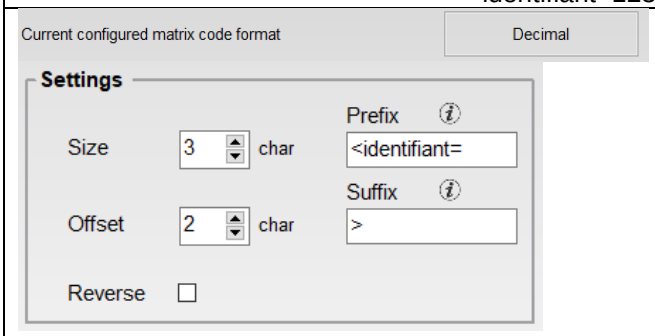
The prefix / suffix need not necessarily be at the start or at the end of the data read.

If the prefix and / or suffix is not identified in the data, the ID is considered invalid.

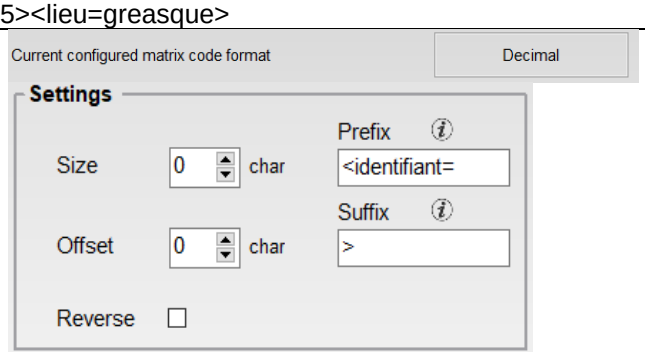
The management of the prefix and / or suffix is complementary to the other identifier processing parameters such as size and offset.

The maximum size of the prefix and suffix is 20 bytes each.

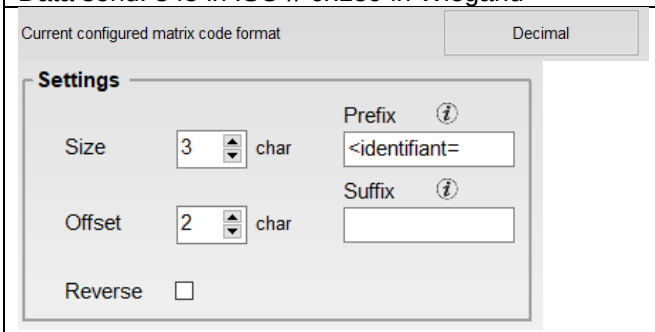
<identifiant=12345><lieu=greasque>



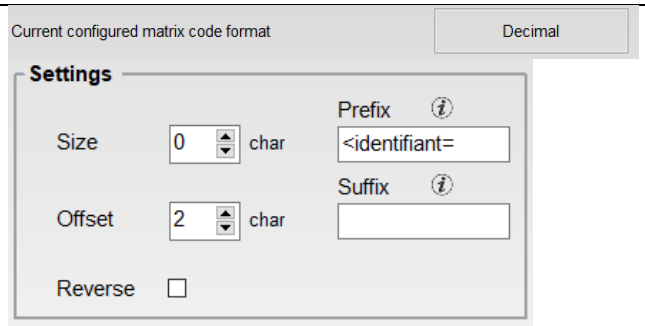
Data read between Prefix and Suffix: 12345
Application Offset 2, data: 345
Application Len 3, data: 345
Valid ID
Data send: 345 in ISO // 0x159 in Wiegand



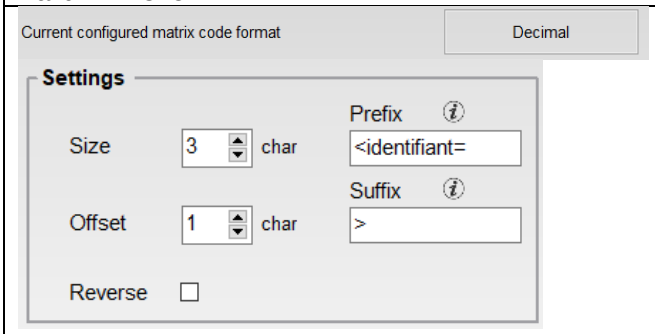
Data read between Prefix and Suffix: 12345
Valid ID = 12345 in ISO



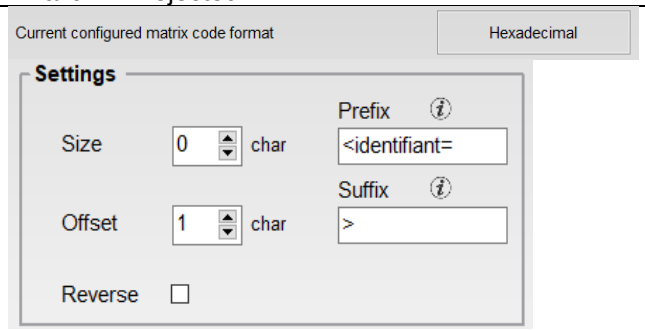
Data read after Prefix: 12345><lieu=greasque>
Application Offset 2, data: 345><lieu=greasque>
Application Len 3, data: 345
Valid ID = 345



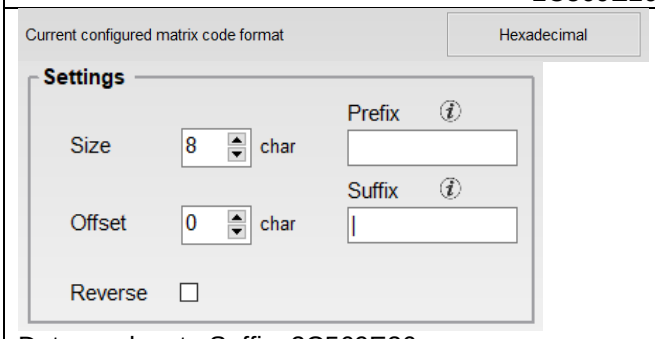
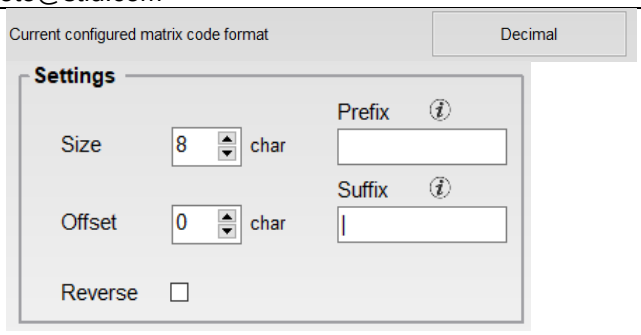
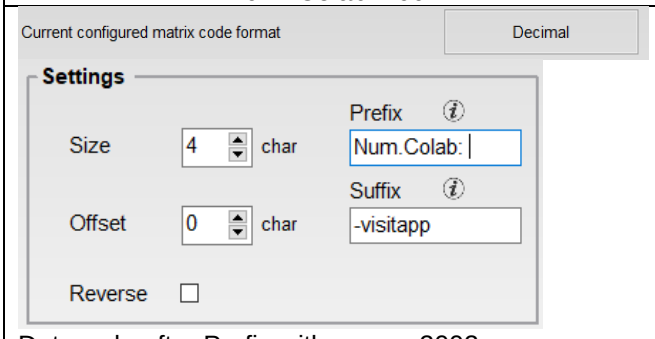
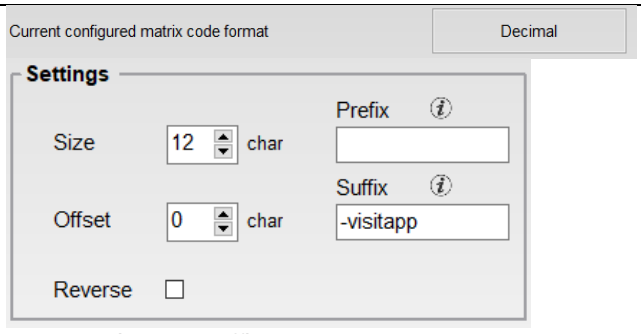
Data read after Prefix: 12345><lieu=greasque>
Application Offset 2, data: 345><lieu=greasque>
Application Len 0, data: 345><lieu=greasque>
Invalid ID: Rejected



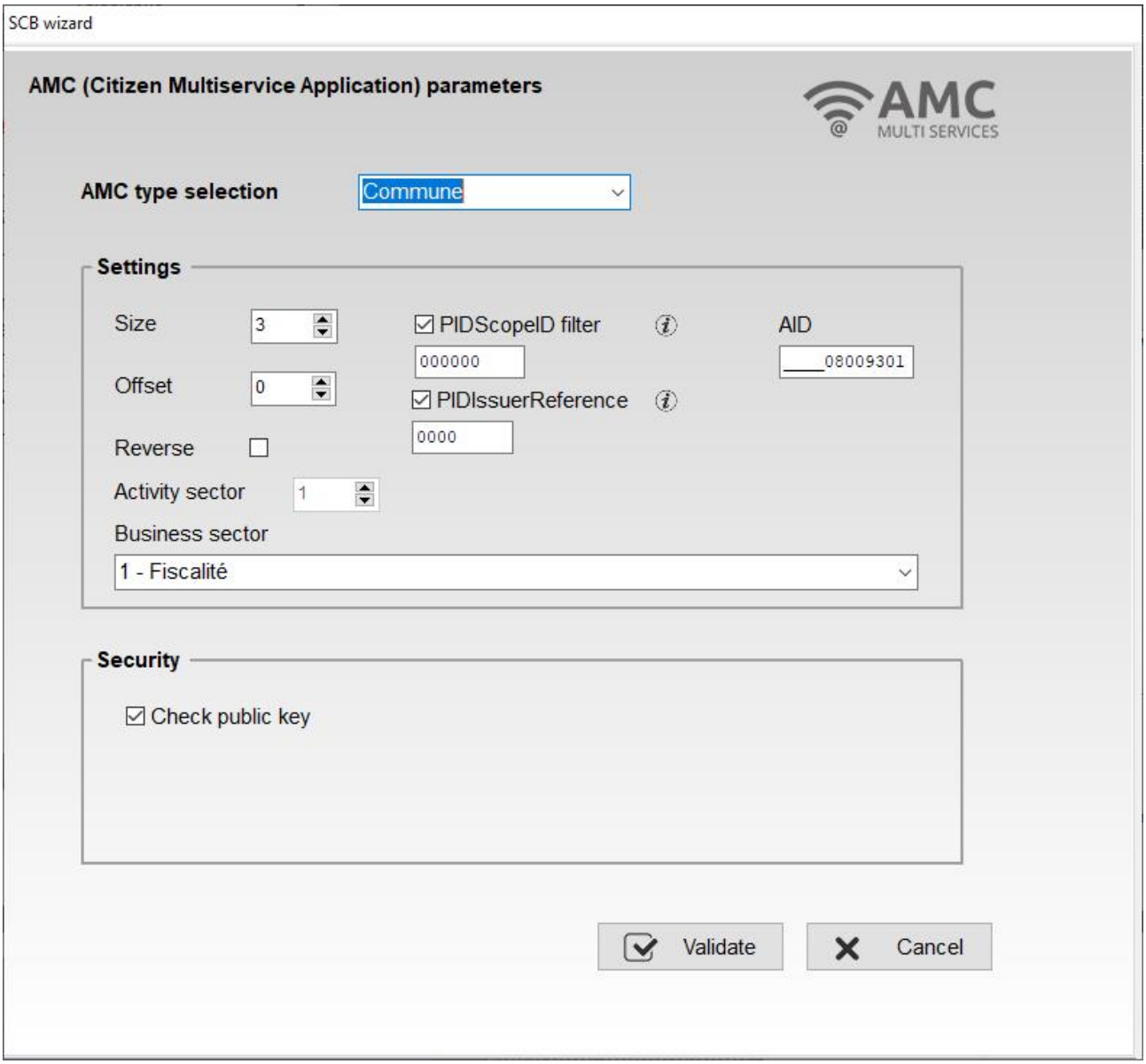
Data read between Prefix and Suffix: 12345
Application Offset 1, data: 2345
Application Len 2, data: 23
Valid ID = 23



Data read between Prefix and Suffix: 12345
Application Offset 1, data: 2345
Application Len 0, data: 2345
Valid ID
Data sent: 0x2345 in Wiegand // 9029 in ISO

2C569E26|toto@stid.com	
 Data read up to Suffix: 2C569E26 Application Offset 0, data: 2C569E26 Application Len 8, data: 2C569E26 Valid ID Data sent: 0x2C569E26 in Wiegand 743874086 in ISO	 Data read before Suffix: 2C569E26 Application Offset 0, data: 2C569E26 Application Len 8, data: 2C569E26 Invalid ID: Rejected cause decimal format selected
GABRIEL GRANADOS CHAVEZ Num. Colab: 2002	548704361841-visitapp
 Data reda after Prefix with space: 2002 . Application Offset 0, data: 2002 Application Len 4, data: 2002 Valid ID Data sent: 0x07D2 in Wiegand 2002 in ISO	 Data read up to Suffix: 548704361841 Application Offset 0, data: 548704361841 Application Len 12, data: 548704361841 Valid ID Data sent: 0x7FC1541D71 in Wiegand 548704361841in ISO

III. 17 - Citizen Multiservice Application (AMC): settings *New 3.6*

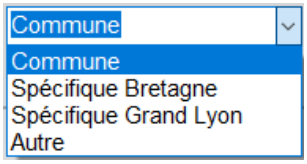


The Multi-Service Citizen Application (AMC) standard describes a technical framework for the management of services in the territories (local authorities, universities, etc.) using a single medium (card, mobile).

You will find all the useful information on the site: https://www.adcet.com/fr/

Note: When the AMC type is activated, the reader no longer returns the PUPI number of ISO2B badges, even if the ISO2B type is activated in SECARD.

❖ **AMC type selection**



The system allows auto-configuration on an existing ServiceScopeID or manual entry of the information needed to read the ID.

The AMC application designates all the data contained in the medium to manage a group of services, as well as the resources provided by this medium for the management of this data (files, security mechanisms, etc.).

AMC file structures can be either "Commune" or “Spécifique”.

❖ **AID (Application IDentifier) AMC**

Table of registered AIDs:

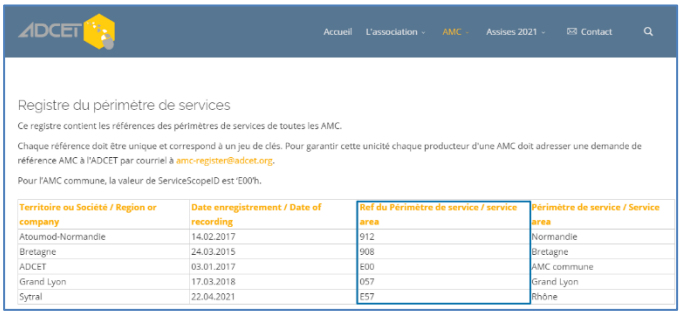
AMC	AID	
Commune	08009301	
Bretagne	30059381	
Grand Lyon	080093F0D057	
Autre	aaaa bbbb [cccc]	Le cccc field is optional

For specific unregistered AIDs, it is recommended to comply with ISO / IEC 7816-5 to avoid AID conflicts.

❖ **PIDScopeID Filter**

Three bytes defining the value of the Service Scope (ServiceScopeID). The values are indicated on the ADCET site. For France, add 0x250 in front.

AMC	PIDScopeID
Commune	0x 250E00
Bretagne	0x 250908
Grand Lyon	0x 250057
Autre	0x dddddd



❖ PIDIssuerRefer filter

The data present in an AMC is written by a "data transmitter".

This transmitter is identified by a unique reference, the data sender reference or IssuerReference (2 bytes).

Region or company	PIDIssuerRefer
Grand Lyon	1057
Gemalto	E002
Otipass	E101
ADCET	FEF0
Idemia	E001
Grand Poitiers	1076
Bordeaux Métropole	0033
Paragon-Id	E003
Atoumod-Normandie	1912
Bretagne	00EB
Métropole européenne de Lille	1053
Amiens Métropole	1006
Evreux Portes de Normandie	1047
Grand Avignon	1013
Wizway	E102
Conduent	E103
Calmell	E004
SELP	E005
Mairie de Lille	0053
SMIRT	1377
COMMUNAUTÉ D'AGGLOMÉRATION DE NEVERS	1068
SMTC	1039

❖ Activity sector

The Predefined IDs structure of a “AMC commune” must contain exactly 35 identifiers (PIDCount = 35, total of the structure = 357 bytes) with references 1 to 35, and which correspond to the CNIL and ADCET sectors of activity, then to RFU identifiers.

Authentication of the Predefined IDs data structure is accomplished through a signature verification process that requires reading the entire structure.

Service sectors and position of identifiers for AMC, Commune, Bretagne and Grand Lyon:

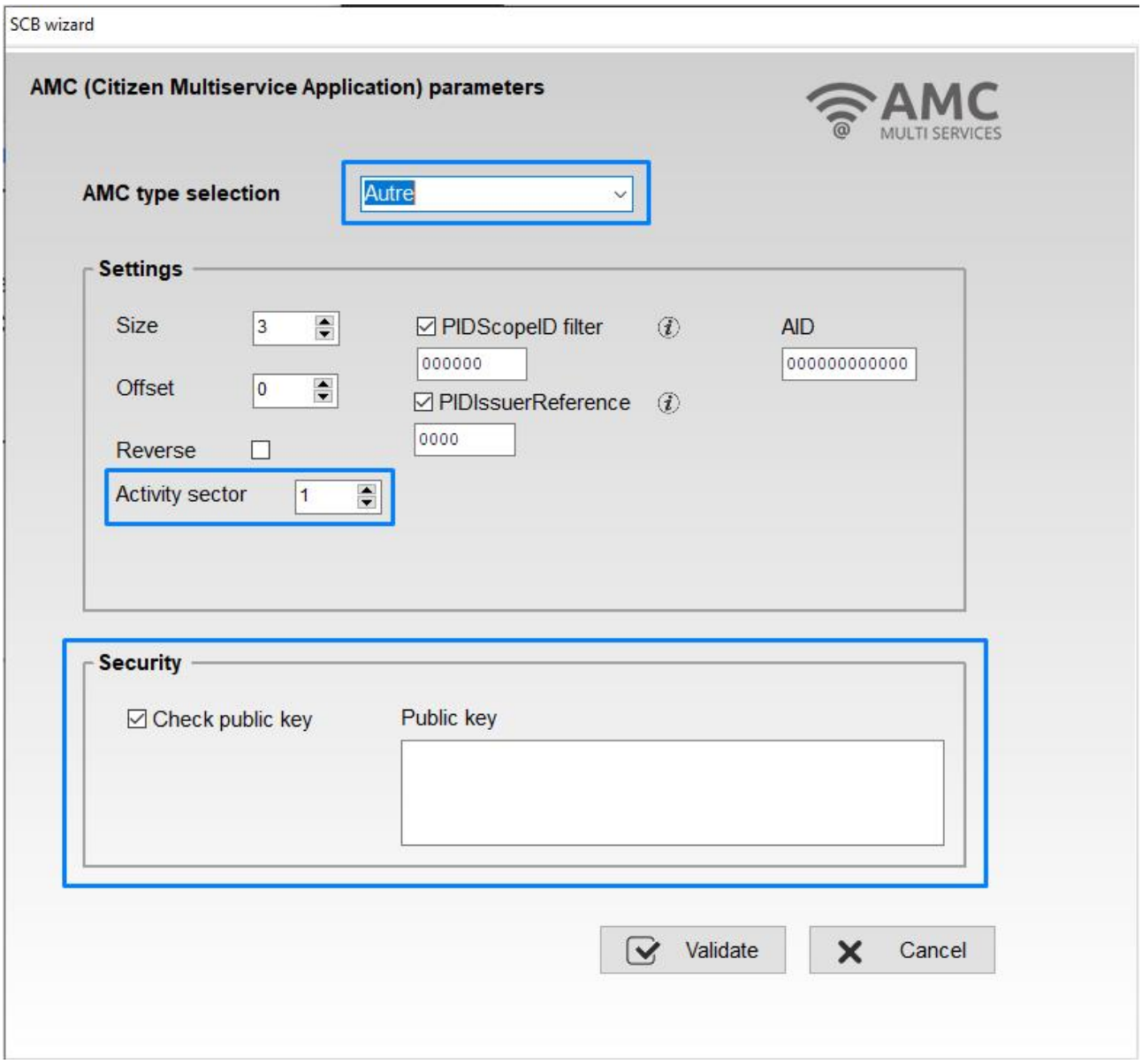
Sector	Number
Fiscalité	1
Travail et social	2
Santé	3
Transports	4
Etat civil et citoyenneté	5
Relations avec les élus	6
Prestations scolaires et périscolaires, activités sportives et socioculturelles	7
Economie et urbanisme	8
Polices spéciales et voirie	9
Relations avec les usagers	10
Service agents (non défini par la CNIL)	11

❖ **Security**

Validation of the signature.

For AMC, Commune, Bretagne and Gran Lyon, the public key is known, on the other hand for AMC other the public key must be filled in the field.

For AMC other, select a business sector number and enter the public key.

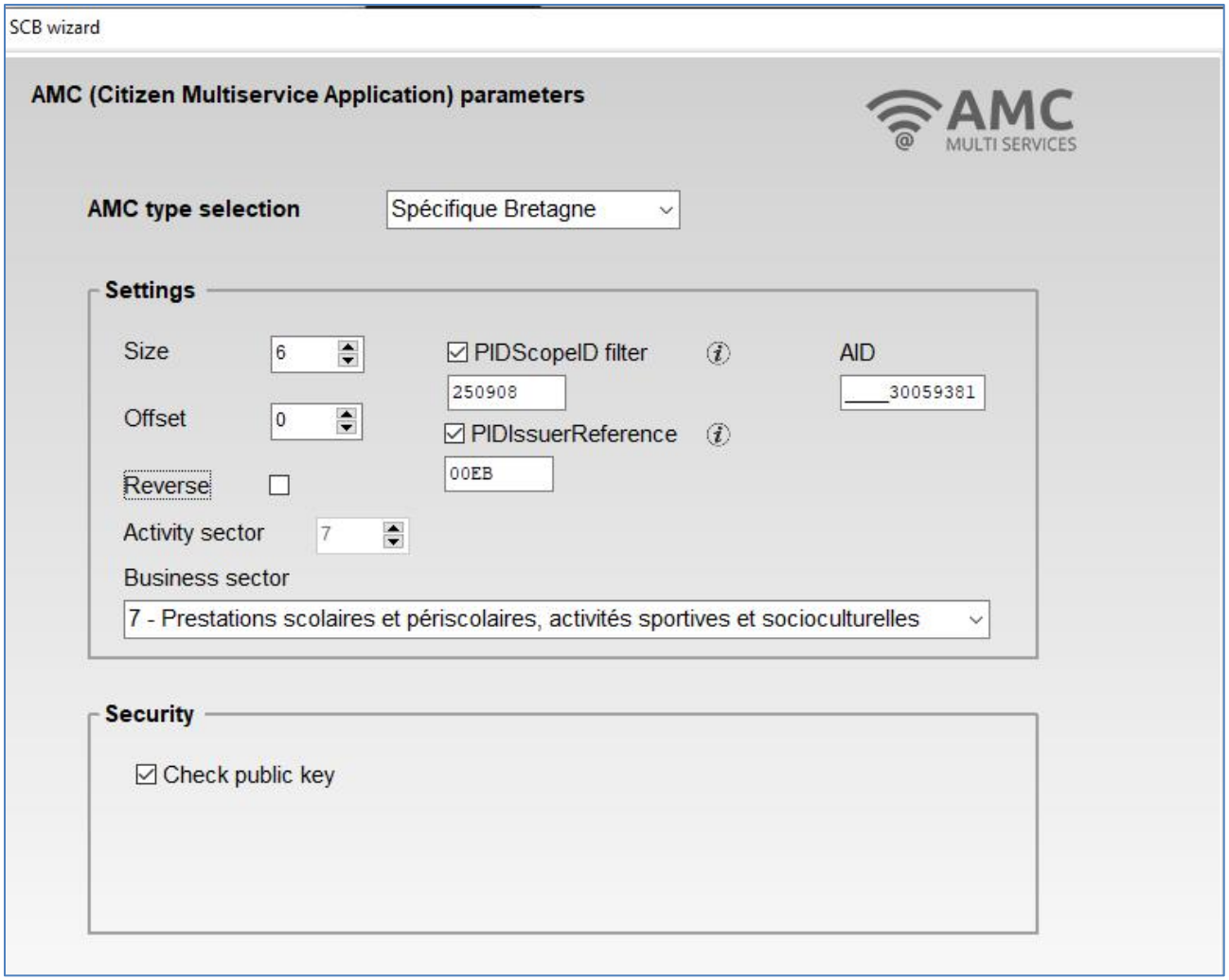


❖ Size: Determines the length of the ID.

❖ Offset: Define an offset from the first byte before reading.

❖ Reverse: If the box is checked the reader reads the identifier Least Significant Byte First.
If the box is unchecked the reader reads the identifier Most Significant Byte First.

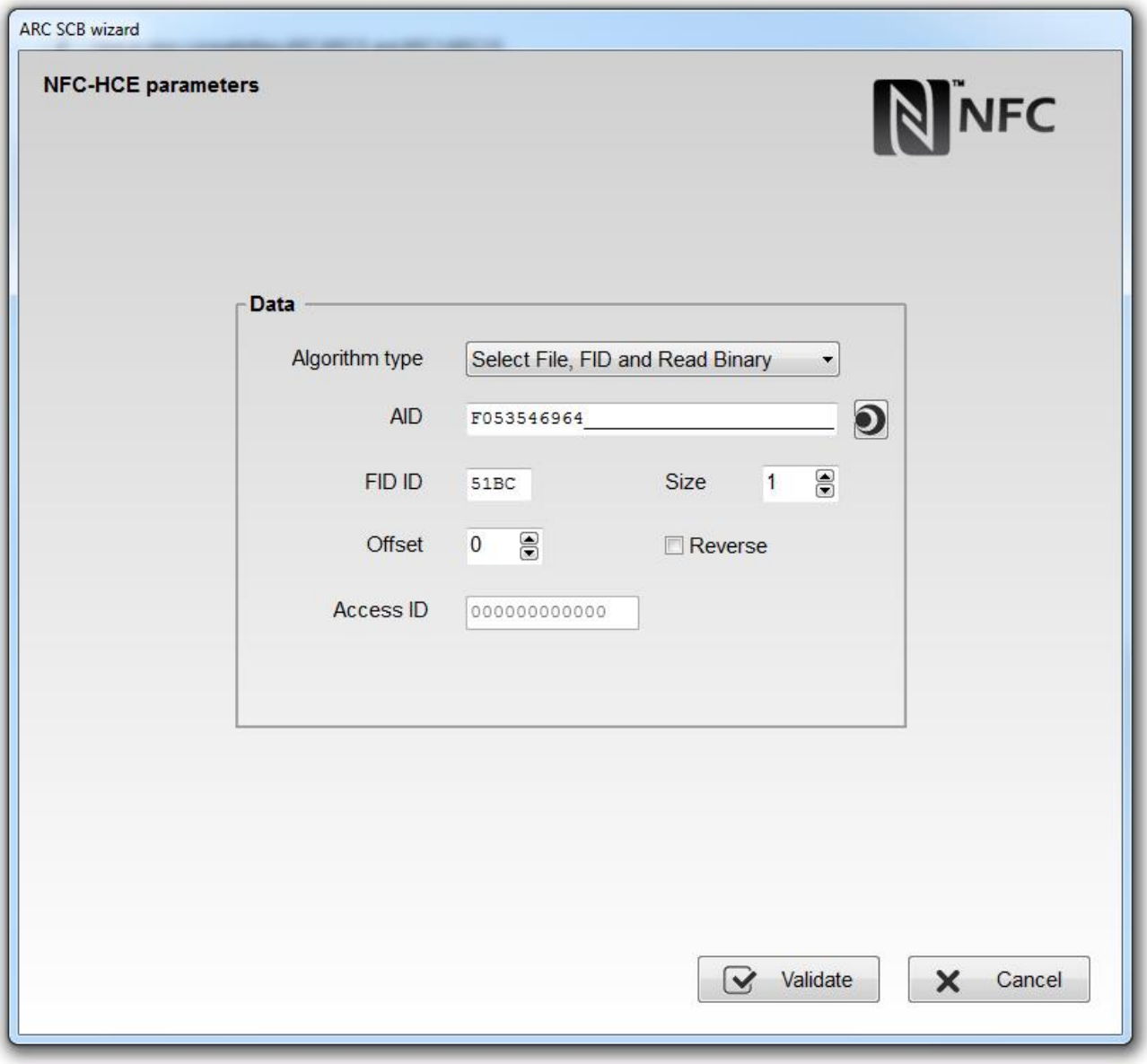
Example with Korrigo badge



ID distributed by reader: **00EBE4F8C7D8**

III. 18 - NFC-HCE: settings

Please check the compatibility between Blue/NFC Mobile ID and NFC-HCE.



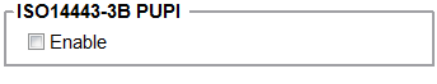
APK (mobile application) and Android Smartphone with HCE supported are required (OS version ≥4.4.x).

Smartphones tested compatible: Samsung S4, S5 & S6, LG G3, Nexus 6, Sony Xperia Z1 and Huawei P8 Lite.

You must develop your APK according to one of two available algorithms or use Orange™ Pack ID APK.

Warning

Disable reading PUPI in the Wizard.



❖ **Algorithme type:** Select File, FID and Read Binary

The exchanges between the RFID reader and smartphone are made according to ISO7816. The operating mode is “Select File AID + Select File FID ID + Read binary (size + offset)”.

Commands must be implemented in the APK are:

- SELECT FILE 0xAID (DESFIRE ISO FILE): An AID has at least 5 bytes and may consist of up to 16 bytes.

  command APDU: 00A4040005AID

  response APDU: 9000

- SELECT FILE 0xFID ID (DESFIRE ISO FILE ID): File ID to be read on 2 bytes.

  command APDU: 00A4000002FIDID

  response APDU: 9000

- READ BINARY xx bytes

  command APDU: 00B000000Size

  response APDU: xxxxxxxxxx9000 with xx = ID on size bytes

SECard parameters:

- **AID** An AID has at least 5 bytes and may consist of up to 16 bytes
  Default = 0xF053546964
- **FID ID** File ID to be read on 2 bytes. Default = 0x51BC.
- **Size** Number of bytes of the ID (up to 48):
  - ❖ TTL Wiegand and Serial Hexadecimal: 1 to 48 bytes
  - ❖ TTL Iso and Serial Decimal: 1 to 10 bytes
- **Offset** First byte position of ID (0 to 48-Size). Default = 0.
- **Reverse** ☐ Reverse ID sends not reversed (Default)

  ☑ Reverse ID sends reversed

❖ **Algorithme type:** Select File only

Command must be implemented in the APK is:

- SELECT FILE 0xAID (DESFIRE ISO FILE):

command APDU: 00A40400**Size**$_{AID}$AID

Size$_{AID}$*: 1 byte (0x05 up to 0x10)*

An AID has at least 5 bytes and may consist of up to 16 bytes

response APDU: ID9000

SECard parameters:

- **AID** — An AID has at least 5 bytes and may consist of up to 16 bytes
  Default = 0xF053546964
- **Size** — Number of bytes of the ID (up to 48):
  - ❖ TTL Wiegand and Serial Hexadecimal: 1 to 48 bytes
  - ❖ TTL Iso and Serial Decimal: 1 to 10 bytes
- **Reverse** — ☐ Reverse ID sends not reversed (Default)
  ☑ Reverse ID sends reversed

Note: the settings "Size" is used to check the Size ID read with the Size ID set in SECard.

❖ **Algorithme type:** Orange PackID

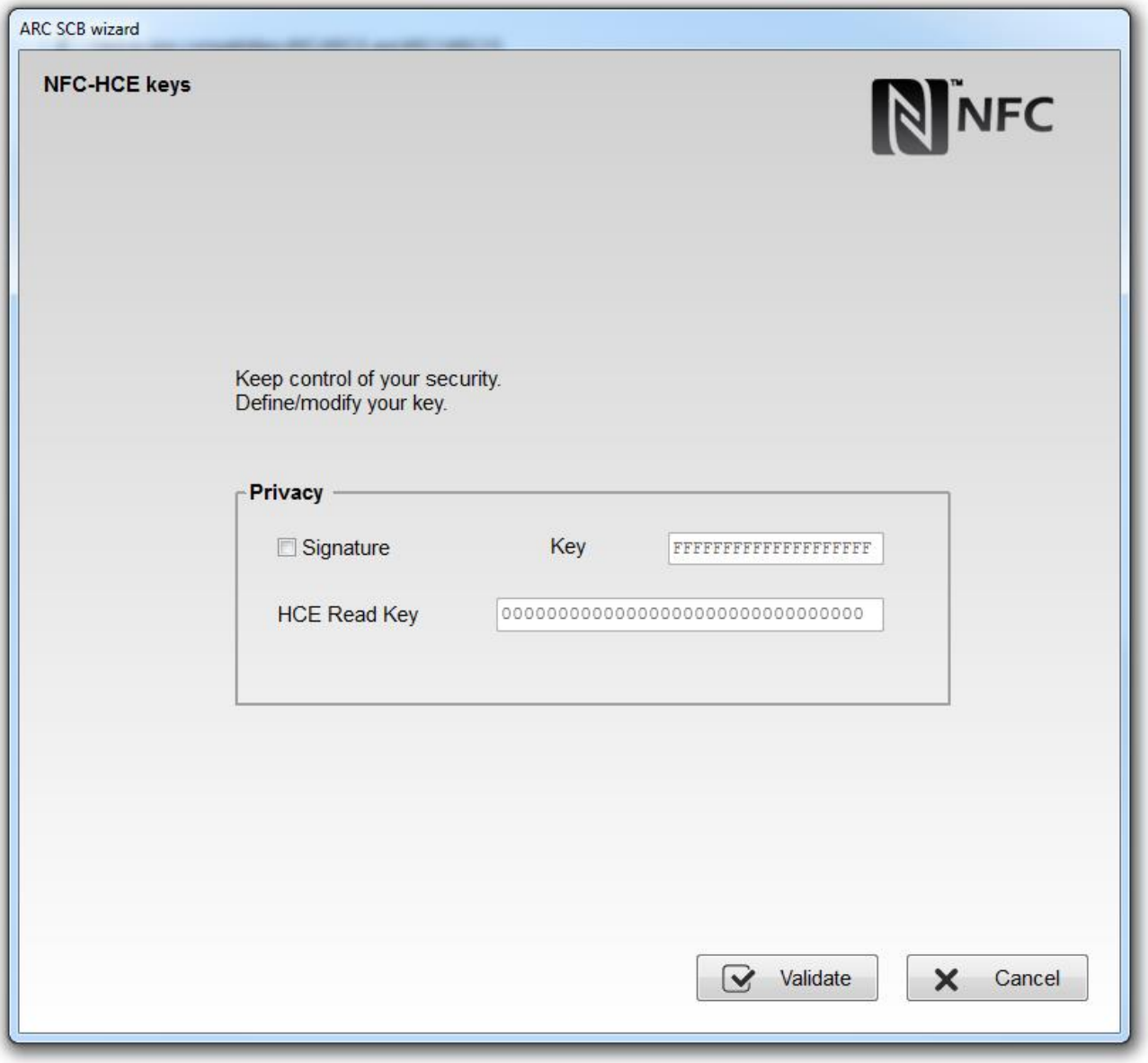
SECard parameters:

- **AID** — An AID has at least 5 bytes and may consist of up to 16 bytes
  Default = 0xF053546964
- **Size** — Number of bytes of the ID (up to 48):
  - ❖ TTL Wiegand and Serial Hexadecimal: 1 to 48 bytes
  - ❖ TTL Iso and Serial Decimal: 1 to 10 bytes
- **Reverse** — ☐ Reverse ID sends not reversed (Default)
  ☑ Reverse ID sends reversed
- **Access ID** — Value on 6 bytes to identify the access zone controlled by the reader.

Click the button Validate **to complete NFC-HCE: Settings**

III. 19 - NFC-HCE: Keys

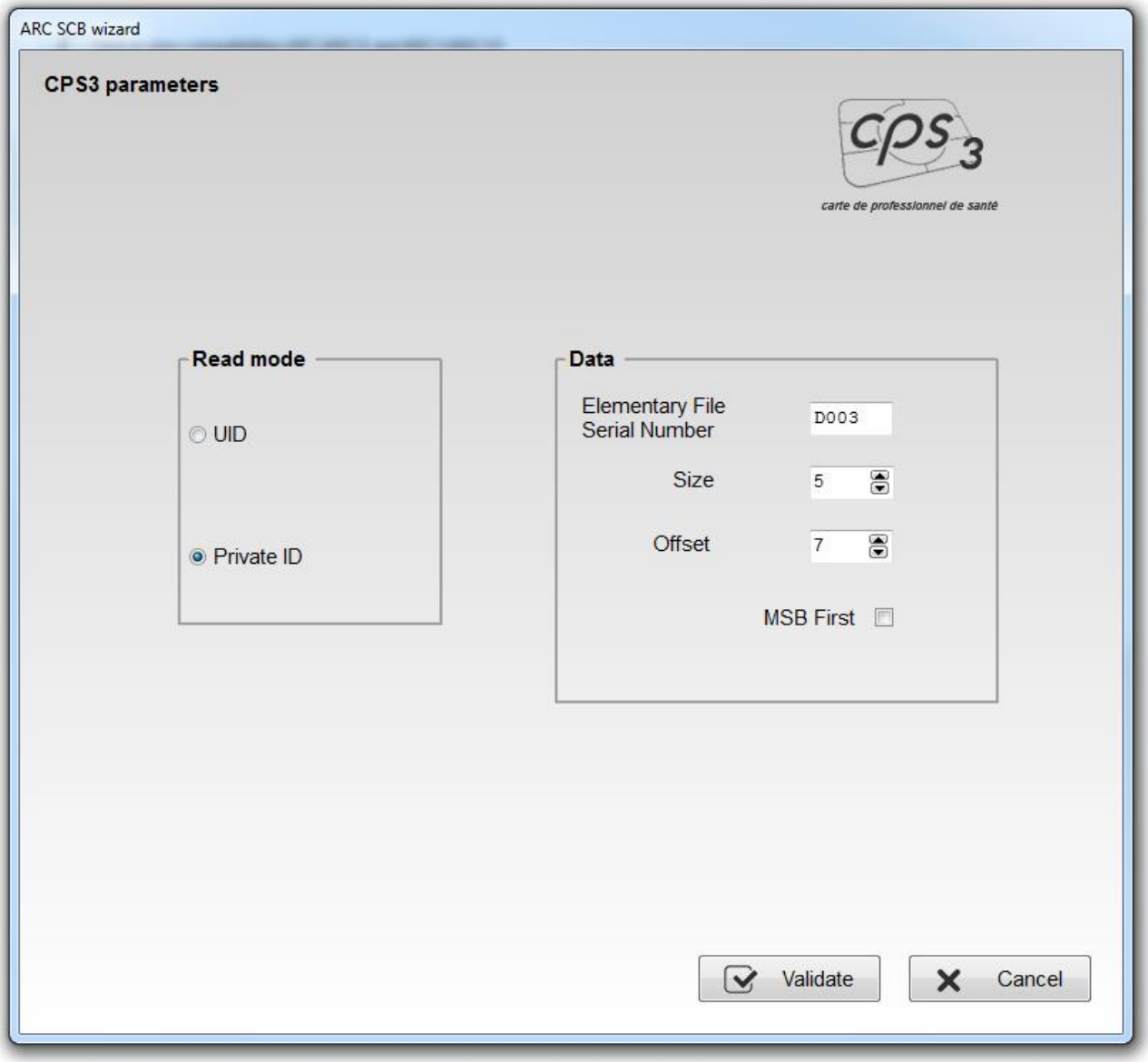
Please check the compatibility between Blue/NFC Mobile ID and NFC-HCE.



- **Signature** — Signature HCE ID it's send in plain mode (default).
  Signature An HMAC-SHA1 key on 10 bytes is used for signing the HCE ID.
- **Key** — 10 bytes key for signing.
- **HCE Read Key** — Only available for Orange™ Pack ID.
  Secret key for Access ID zone defined in settings.

Click the button Validate **to complete NFC-HCE: Keys**

III. 20 - CPS3: settings



Read mode

- UID: Reader configured in"read-only serial number".
- Private ID: Reader configured in "read-only private code".

In the case of the CPS3, UID is the protocolary identifier, which is the serial number of the chip.

Private Id corresponds to the technical identifier (serial IAS number), it is a 19 digit number consists of the following:

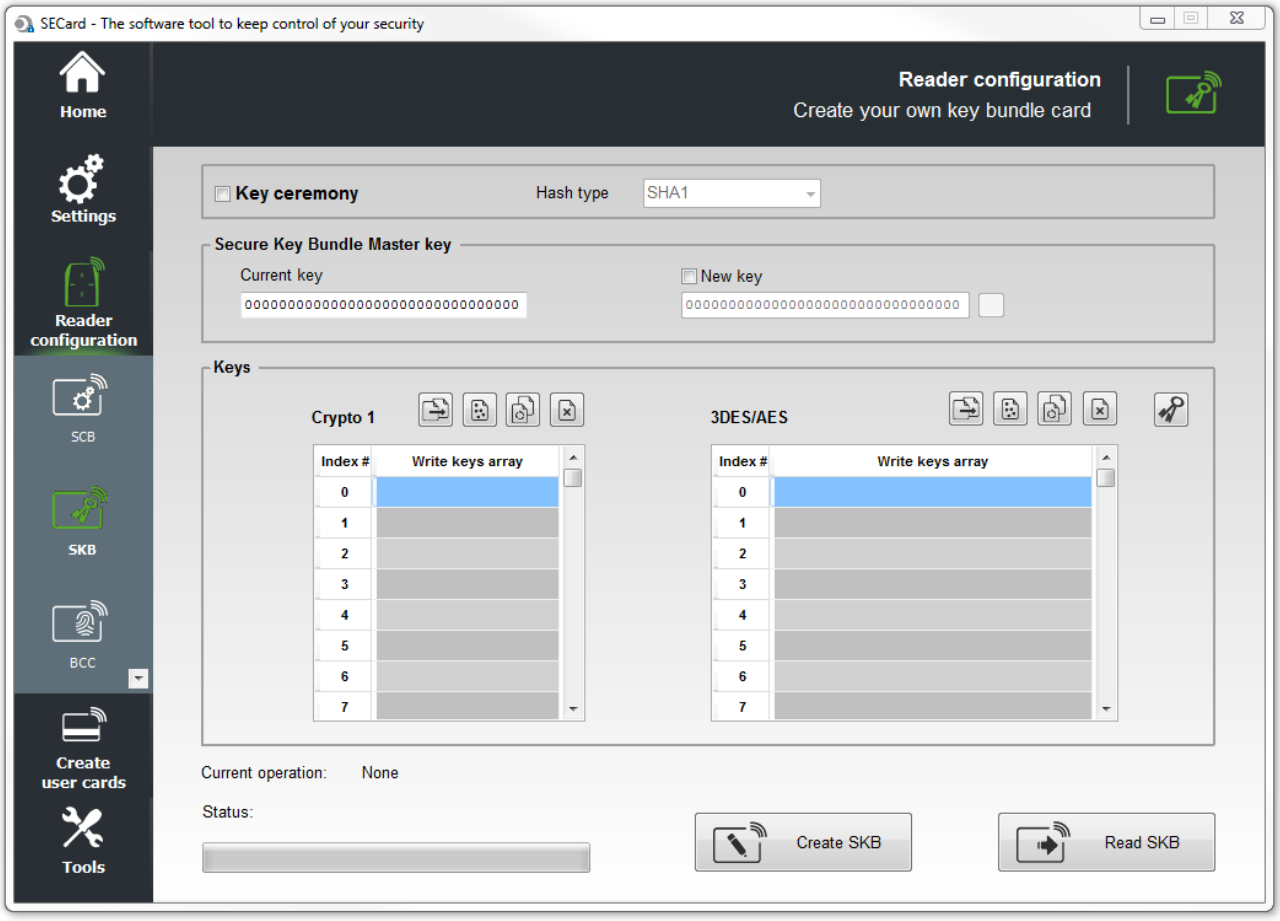
[Identifier ASIP (10)][Unique card number (8)][key(1)]

Its value is present in the Elementary File D003.

To recover the unique code of the card should read 5 bytes of the IAS with an offset of 7 bytes for not reading the id ASIP.
To read this ID, there is no authentication between the reader and the chip.

Click the button  **to complete CPS3 settings.**

IV. Reader configuration - SKB



SECard software has a module to create cards named "*SKB* (Secured Key Bundle)".
These cards contain 32 *Crypto1* keys and 32 *3DES/AES* keys. They are protected by a card master key « *SKB Master Key* ».

These cards are used by the following readers via command Load_SKB (see communication protocol 5AA-7AA):

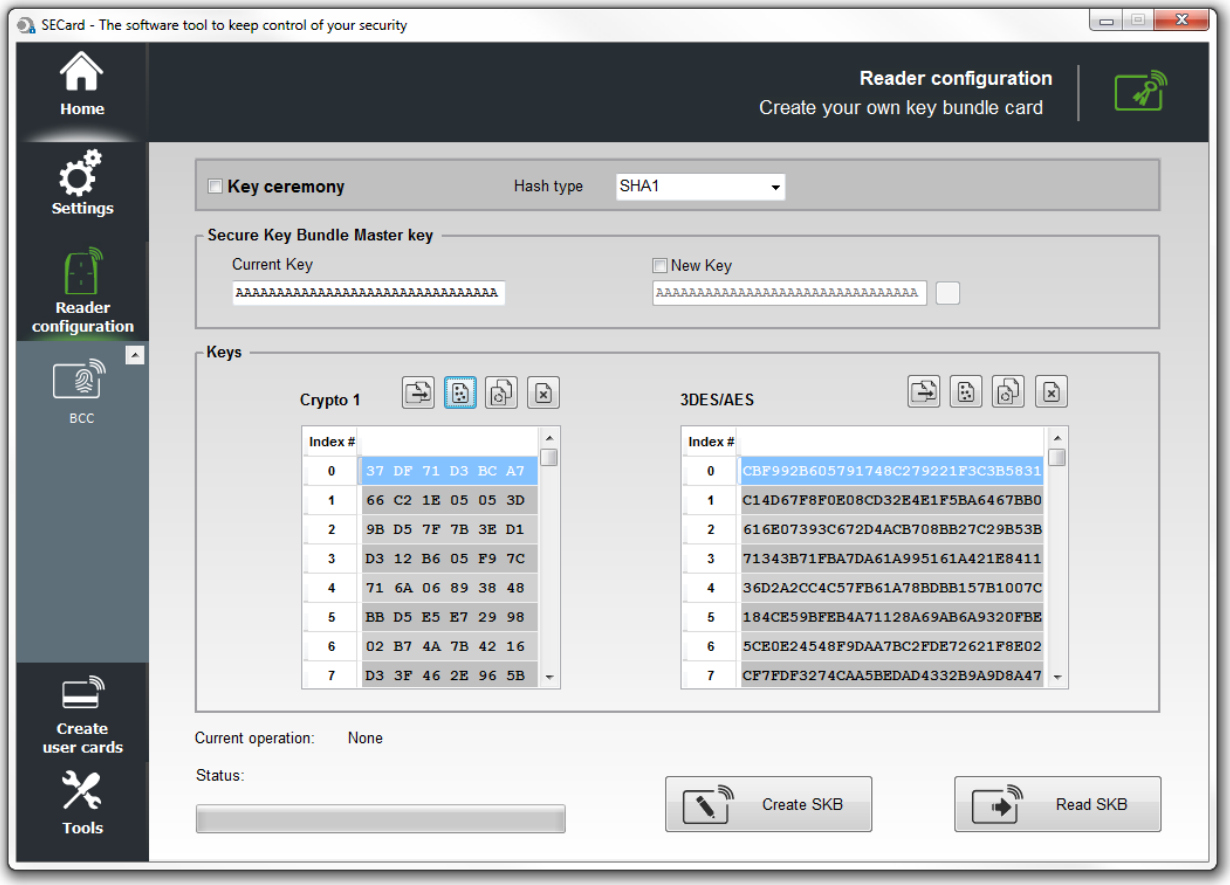
- ARC-W32-X-PH5-5AA-x — *Upgradable* reader – *RS232* – *Read / Write*
- ARC-W33-X-PH5-7AA-x — *Upgradable* reader – *RS485* – *Read / Write*
- WAL-W32-X-PH5-5AA-x — *Reader* – *RS232* – *Read / Write*
- WAL-W33-X-PH5-5AA-x — *Reader* – *RS485* – *Read / Write*
- ARCS-W33-X-PH5-7AA-x — *Secure Upgradable* reader – *RS485* – *Read / Write*
- ARC1S-W33-X-PH5-7AA-x — *Secure* reader – *RS485* – *Read / Write*
- STR-W35-E-PH5-5AA-1 — Desktop *reader* – *USB* – *Read / Write*
- STR-W32-E-PH5-5AA-1 — Desktop *reader* – *RS232* – *Read / Write*
- LXS/ ATX/ MXS / LXC / LXE-W32-E-PH5-5AA-x — *Prox Reader* – *RS232* – *Read / Write*
- LXS/ ATX/ MXS / LXC / LXE-W33-E-PH5-5AA-x — *Prox Reader* – *RS485* – *Read / Write*
- MS-W31-E-PH5-5AA-x — OEM reader – *RS232/TTL* – *Read / Write*

The feature of « *SKB* » is to provide a portfolio (bundle) of indexed keys (index from 0 to 31 for *Crypto1* and *3DES/AES*). Once stored in reader's EEPROM, it will be possible to access these keys by calling them in *SSCP®* command with their index value. Then no need to communicate the key values through the serial link. Note: timing to load SKB is 6 seconds.

Warning

It is necessary to create these cards with MIFARE Plus® Level 0, MIFARE® DESFire® EV1/EV2 or with a current SKB.

IV. 1 - Classic creation mode



Secure Key Bundle Master key

On a MIFARE® DESFire® EV1/EV2 blank card the default key is "00000000000000000000000000000000"

On a MIFARE Plus® Level 0 blank card the default key is FFFF…FFFF or A0A1A2….A15.

It is recommended to change this value for more security.

Keys

	Copy the values of table read keys to the array of keys to write.
	Fill “value to write” array with random keys values. These values are those written in the SKB card.
	Switch from array of keys write to array of keys to read.
	Delete all values of the array of keys to write.
	Indexed keys table for Encoding.

Crypto 1

Array reserved for key 32 key values Crypto 1.

3DES/AES

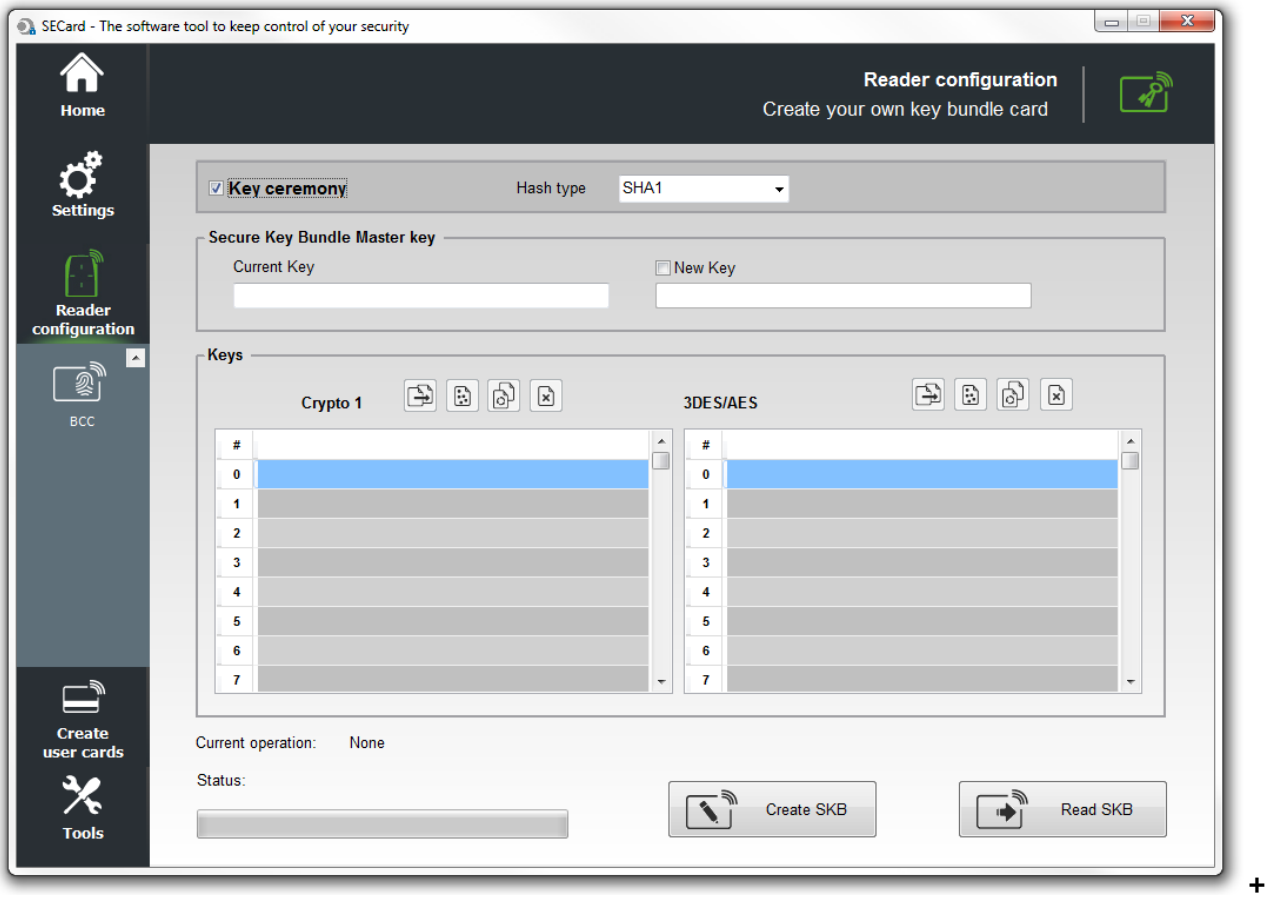
Array reserved for key 32 key values 3DES/AES.

IV. 2 - Key ceremony creation mode

With this Key ceremony, three holders are required to generate the SKB.

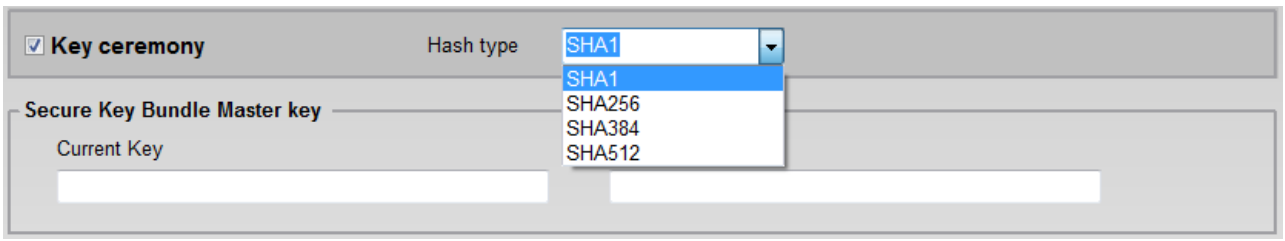
You can't write in the keys field; all field are automatically filled by the Key ceremony. The resulting value of a key is the XOR on the three keys. The value that appears in the field is the HASH of the resulting key.

Made the Key Ceremony for all Key you needed, if a field it's not used it's forced to 00…00.

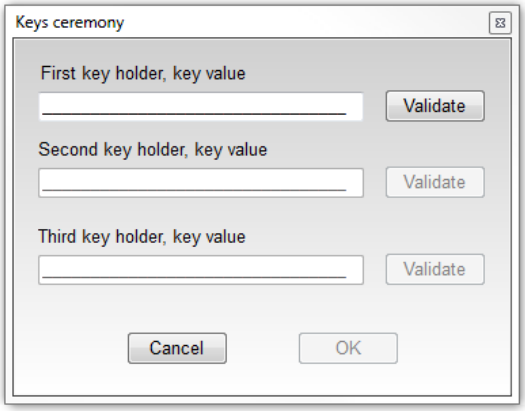


Example for SKB Master Key

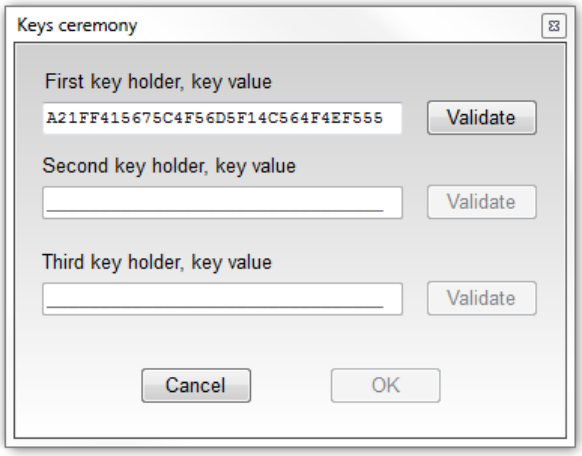
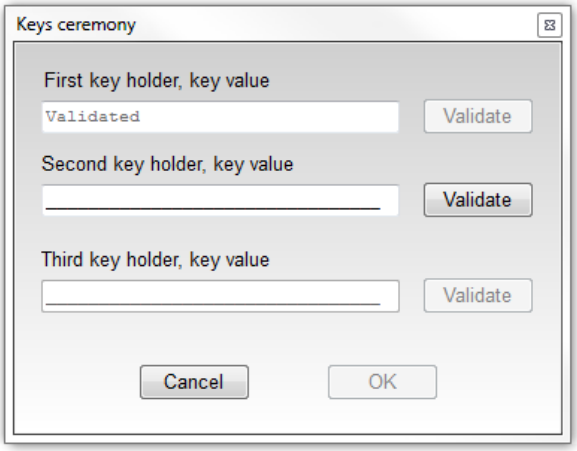
1- Select the Hash type wanted



2- Double click in Current Key field to open the Keys ceremony windows

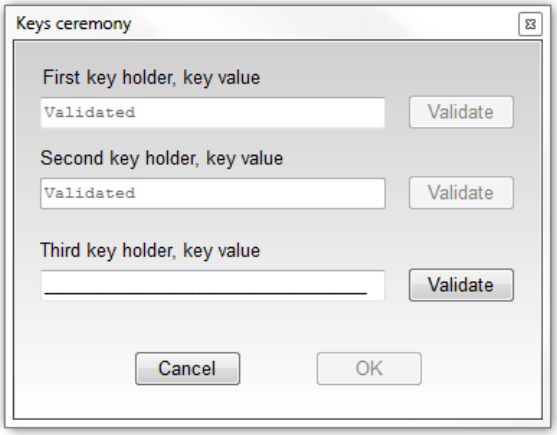


3- First key

Enter the first key	Click on Validate
	

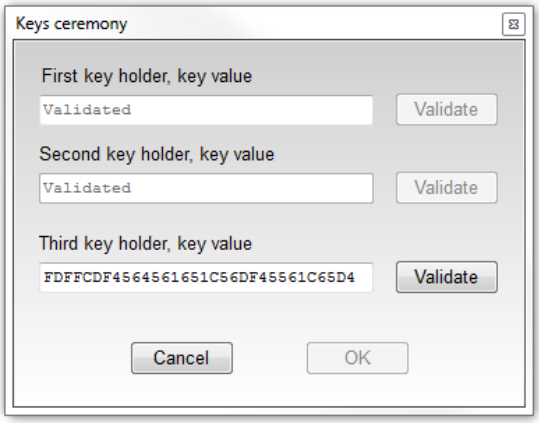
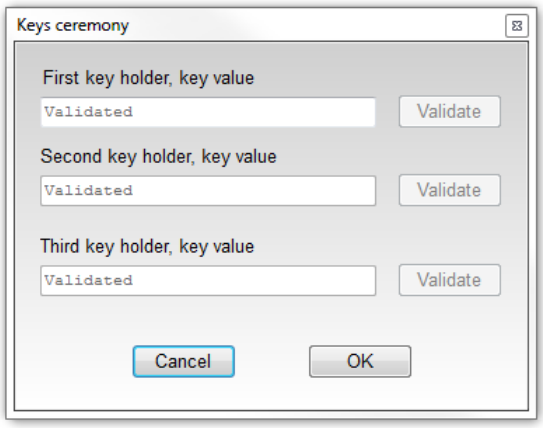
The value of the first key is then masked

4- Second key

Enter the second key	Click on Validate
	

The value of the second key is then masked.

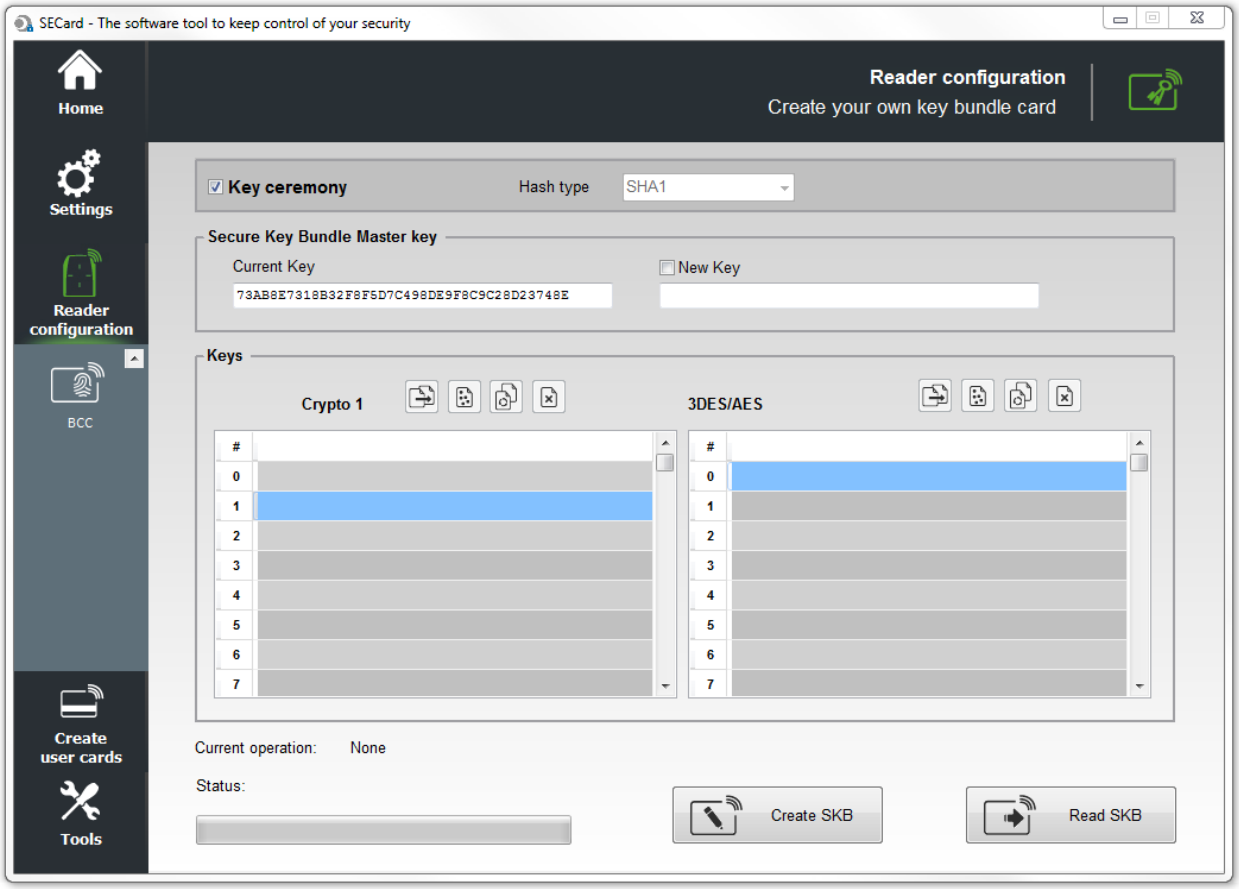
5- Third key

Enter the third key	Click on Validate
	

The value of the third key is then masked

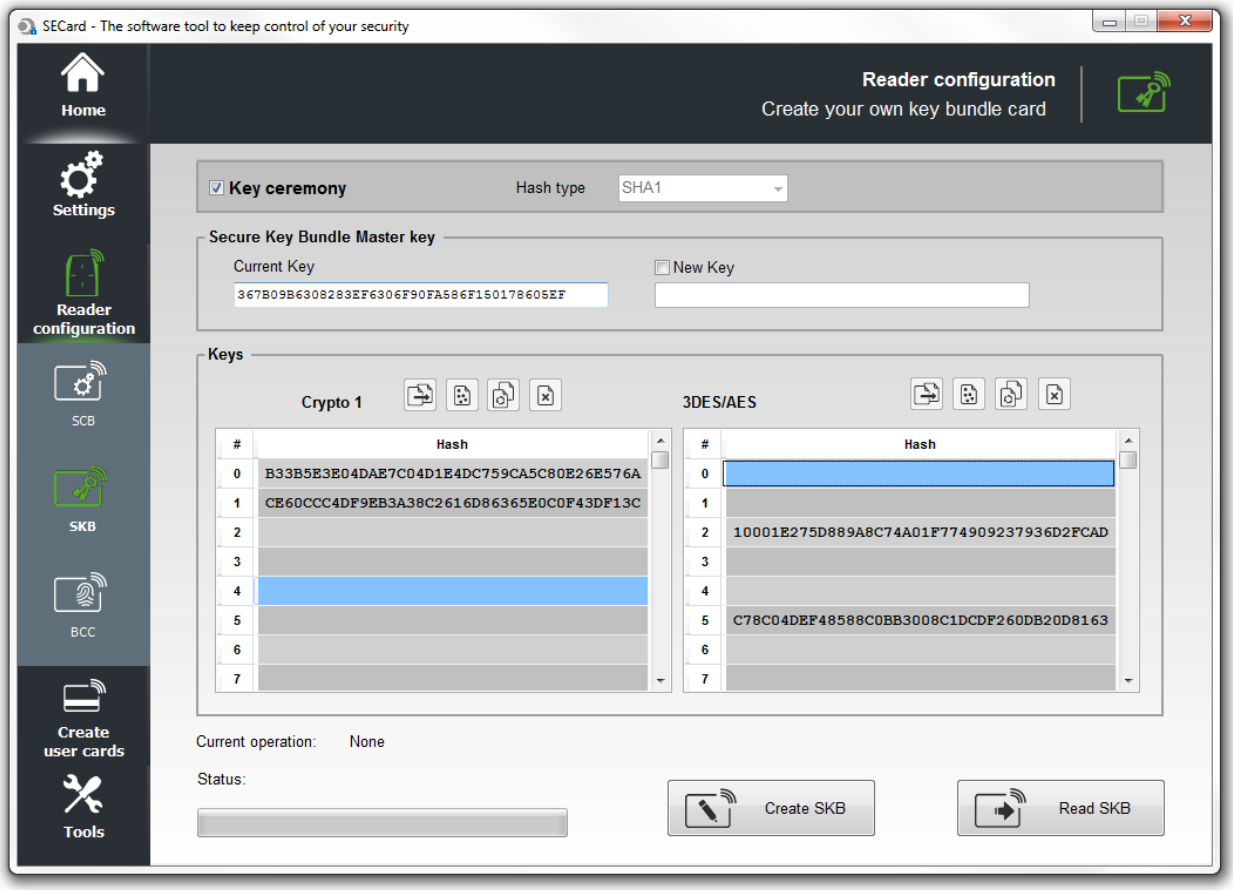
6- Click on OK to finish the key ceremony FOR Master key.

7- The key ceremony for Master Key is achieved and we can see the HASH of current SKB Master key



Repeat this operating mode for each key needed.

For example:



8- Create SKB

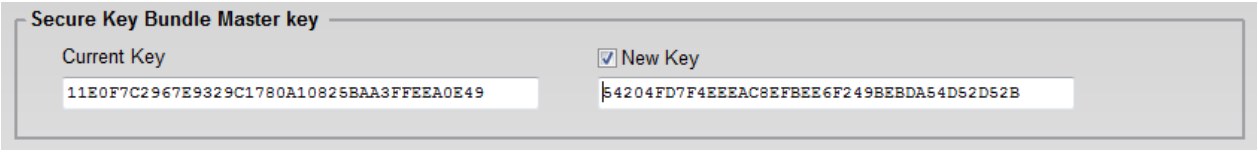
Once the key values needed are create, click on “Create SKB” to write the keys into the card.

Read SKB

Read again a SKB card: need to inform the master key of the card to read.

Change SKB Master Key

To change the current SKB Master key, double click in the New Key field, and go to step 2.



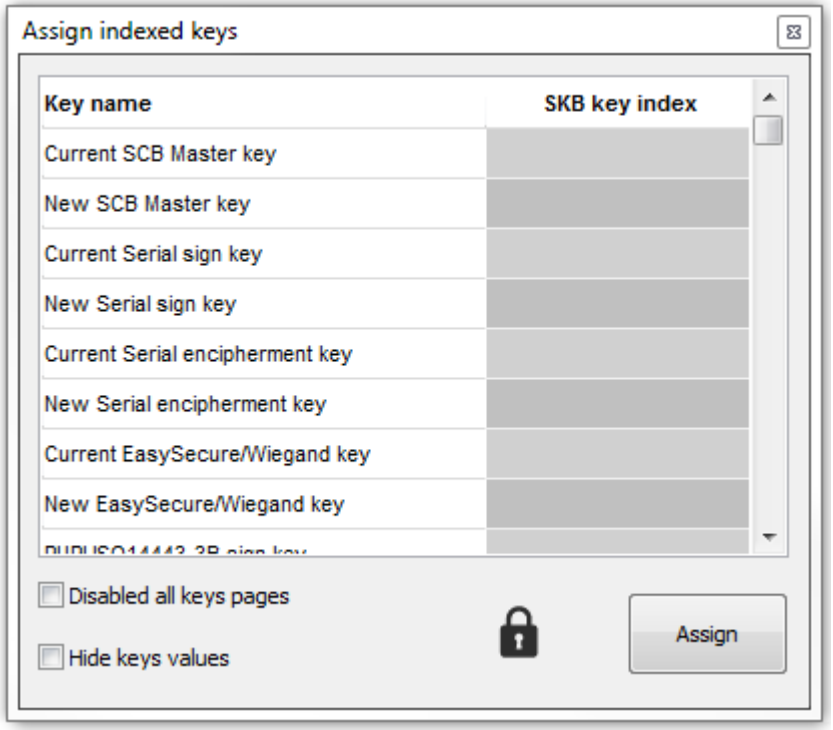
IV. 3 - Using indexed keys in the SECard configuration

From version 3.1, you can fill the key fields of the configuration wizard from a SKB badge.

The keys that can be assigned are:

- Reader keys
- DESFire keys
- Mifare Plus Level 3 keys
- UltraLight keys
- Mobile ID keys

To do this, click on  button, a window containing a table appears in order to assign an index to the different desired keys.



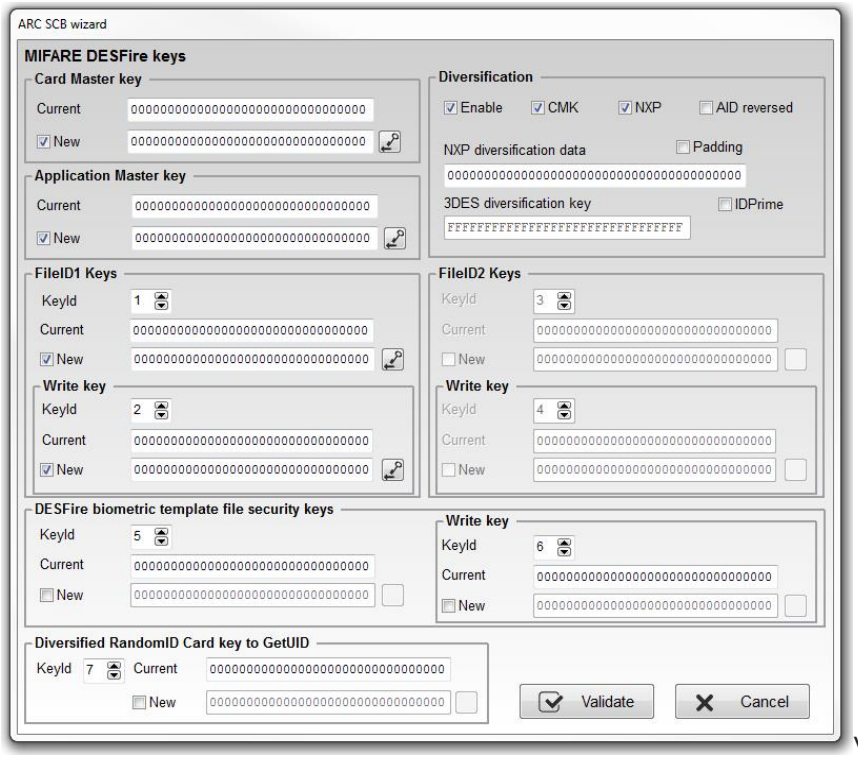
All fields are not to be filled in, only those useful for the current configuration.

Note: to make a key change, in the SCB wizard, check the New box next the field.

For example, the current SCB key is the default value and must be changed to the value of the key at index 2, check the box New to make the change effective:

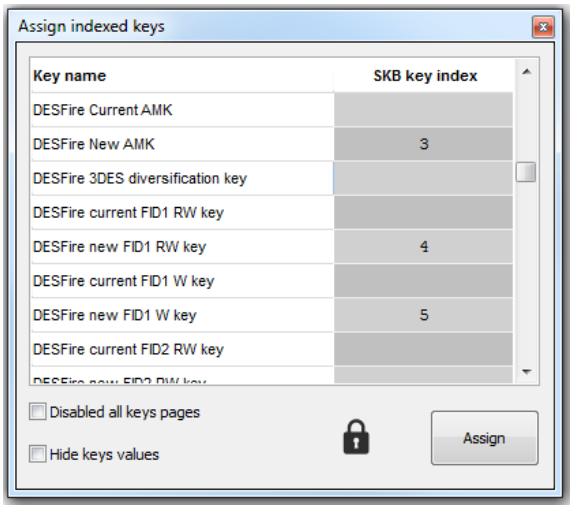
Example: keys to change: Card Master key, Application Master Key, Read and Write File ID1 Key for a virgin DESFire®.

1- In the SCB wizard, after DESFire® settings is ok, open the DESFire® Keys window and check the "New" box of all the fields concerned:

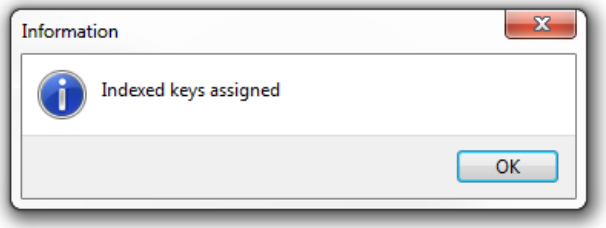


Validate

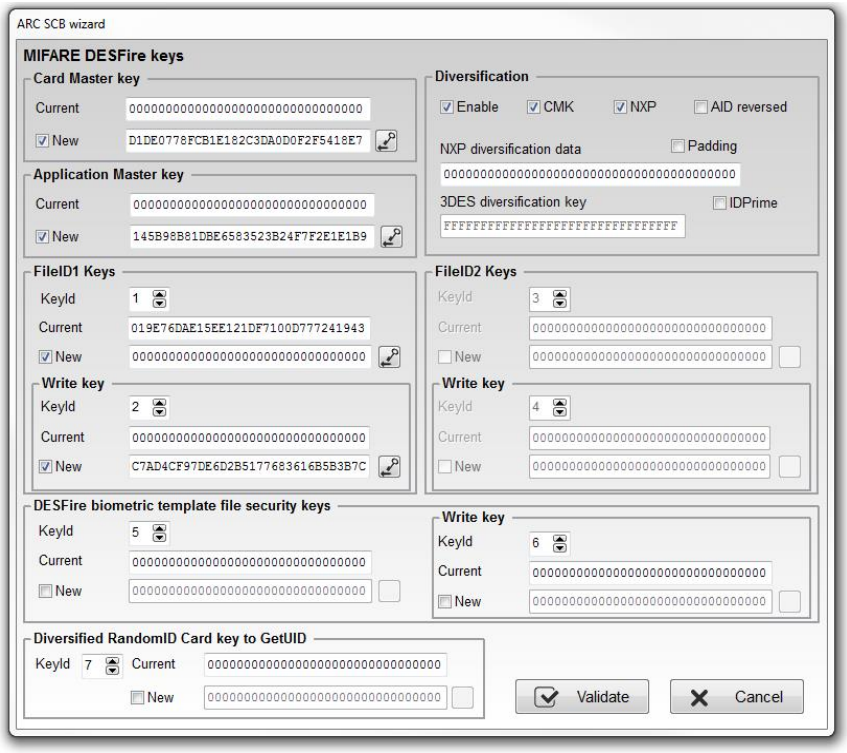
2- In the SKB window, load the SKB then open the assignment table and assign the index numbers of the keys



3- Click on Assign



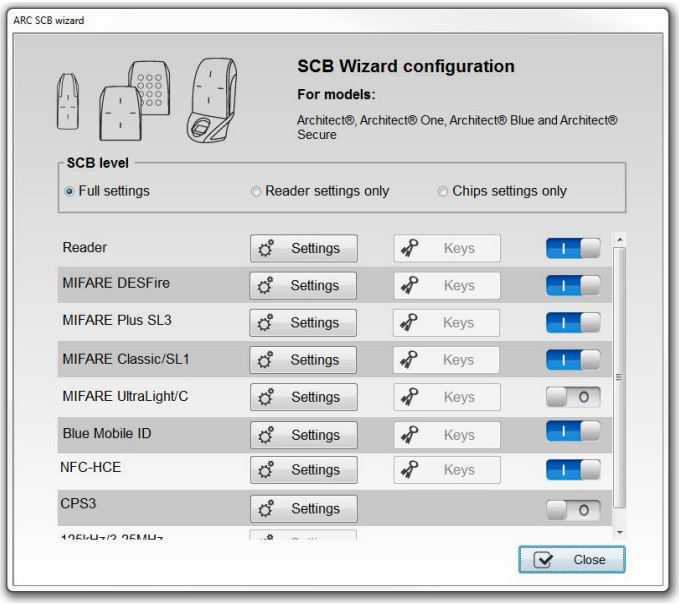
4- If “Disabled all keys pages” and “Hide keys values” were not checked during the assignment, the DESFire® key window will be:



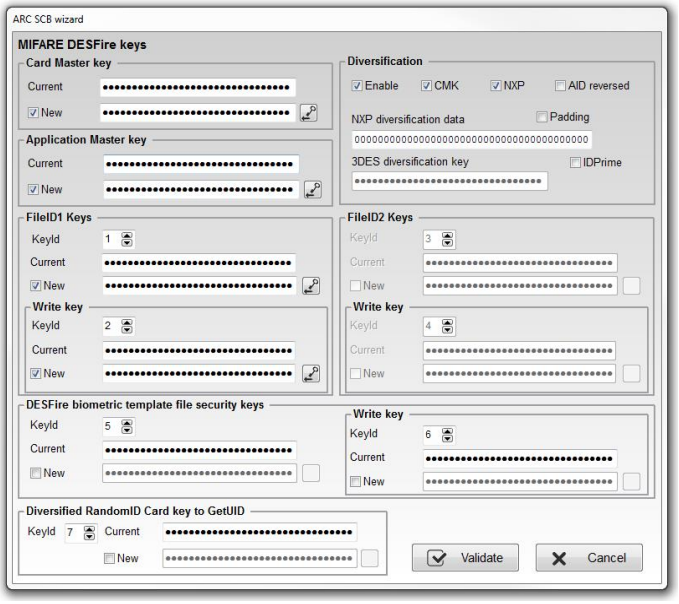
The value of the keys appears in the fields according to the values of the indexed keys.

0	00000000000000000000000000000000
1	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
2	D1DE0778FCB1E182C3DA0D0F2F5418E7
3	145B98B81DBE6583523B24F7F2E1E1B9
4	019E76DAE15EE121DF7100D777241943
5	C7AD4CF97DE6D2B5177683616B5B3B7C
6	AD00F30E724AB6C37449B8FE067548DF
7	7DA8639D08440AA8AE21BC7C7848B018

5- If “Disabled all keys pages” was checked during the assignment, the buttons giving access to the keys will be grayed out



6- If “Hide keys value” was checked during the assignment, the DESFire® key window will be:



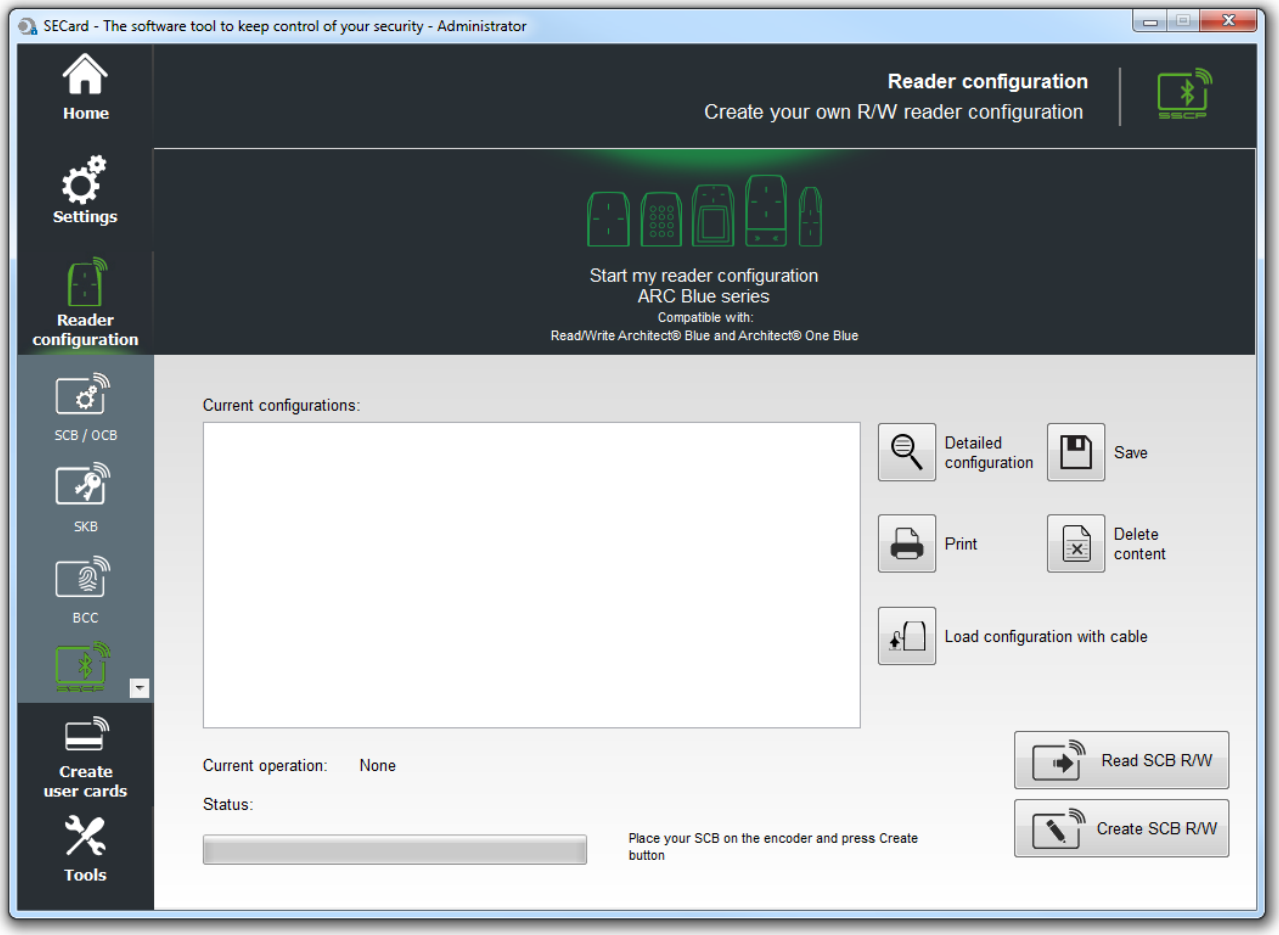
Note: it is possible to modify an Index or options “Disabled all keys pages”, “Hide keys value” by making the change and clicking Assign again.

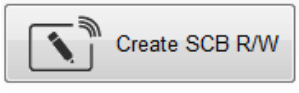
Warning

All key values set by this method in the configuration wizard will not be saved in the .PSE file.

V. Reader configuration – SCB R/W

The SCB R/W is a configuration badge for ARC R/W Bluetooth®, that allows to configure the Blue/NFC of the reader.

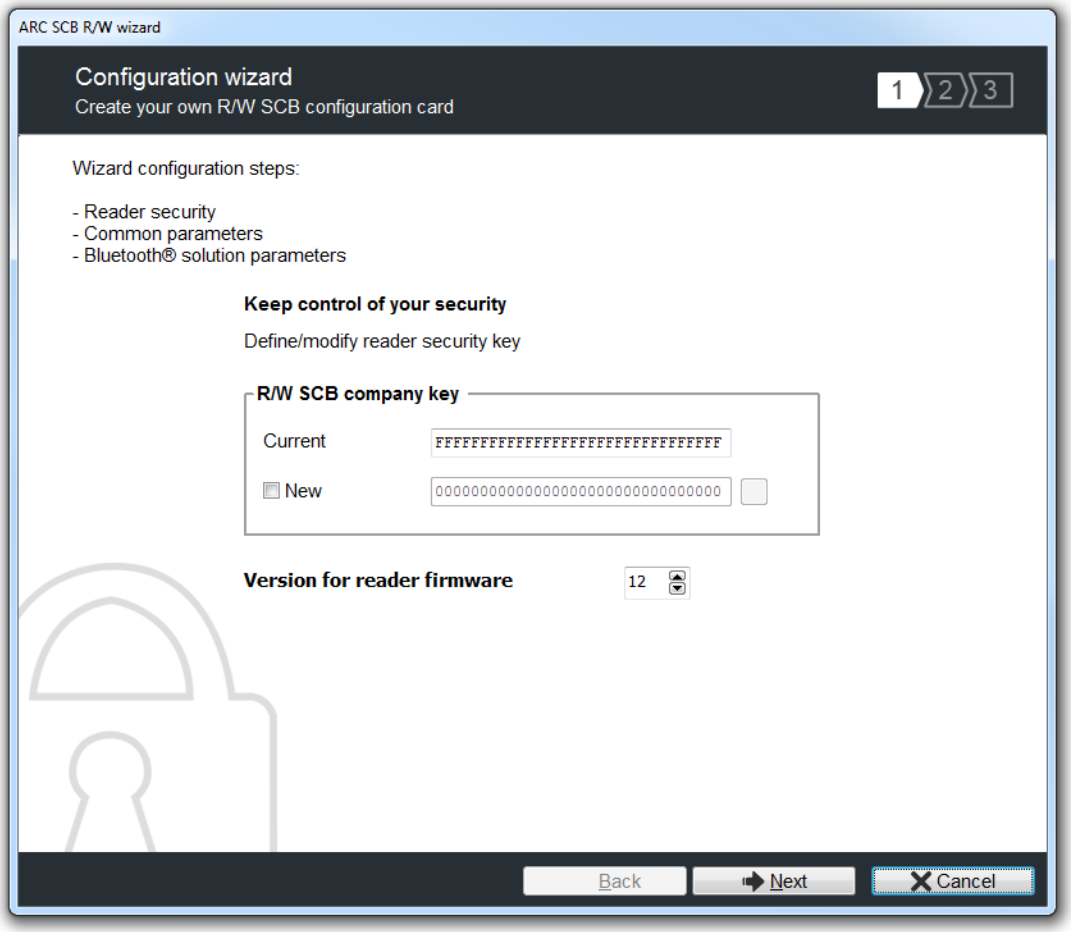


	Open the configuration wizard for readers
	Print the configuration list displayed.
	Save in .rtf file the configuration list displayed.
	Clear the configuration list displayed.
	Display details information of current configuration.
	Load the configuration to the reader by serial link.
	Read a SCB R/W configuration card. Use SCB Company Key defined in the configuration wizard.
	Create a SCB R/W configuration card with parameters defined in the configuration wizard.

V.1 - Configuration Wizard

The reader configuration is done in 3 steps. To move from one stage to another, you must click on “Next”.

1 2 3 Click here	Reader security
1 2 3 Click here	Common parameters
1 2 3 Clich here	STid Mobile ID® settings
1 2 3 Clich here	Orange™ Pack ID settings
1 2 3 Clich here	Open Mobile Protocol settings



SCB R/W company key

Configurable readers with SCB R/W card are initially supplied with default configuration (factory key 0XFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF).
These can be configured by a " SCB R/W " with 0xFF…FF in current key to a new company key.

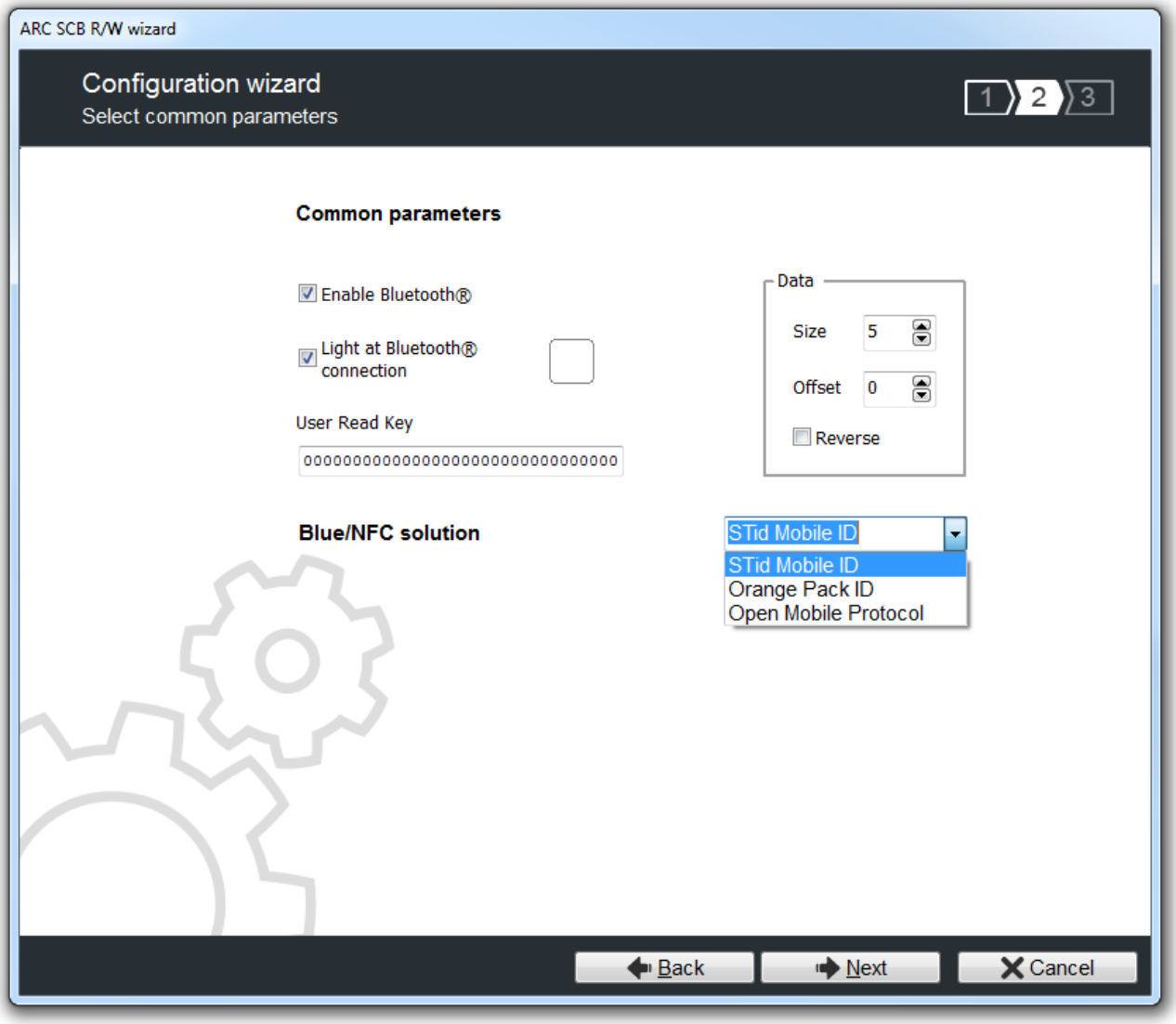
After the initial configuration and in order to reconfigure the reader, it will be necessary to present to the reader " SCB R/W " **with a company key similar to that recorded by the reader.**

Warning

This key is important and should definitely be known by the administrator. It protects the data from the " SCB R/W " and allows changes to the configuration of readers.
If you lose this key, the reader cannot be reconfigured for another " SCB R/W " and will must be reset at the factory.

Version for reader firmware

The available functionalities and the compatibility of SCB R/W depend on reader firmware generation.

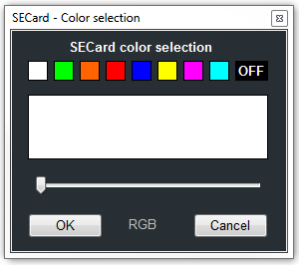


Enable Bluetooth®:

Activate / disactivate STid Mobile ID® or Orange™ Pack ID or Open Mobile Protocol (Blue and NFC). If is disactivate, there is no Bluetooth® transmission.

Light at Bluetooth® connection:

Flash LED when smartphone start connection on the reader. The color can be selected by clicking on the right square.



This action, independent of the detection of the virtual badge, informs the user that the communication between the smartphone and the reader is in progress.

User Read Key:

Set the read key value for Blue/NFC Mobile ID data.

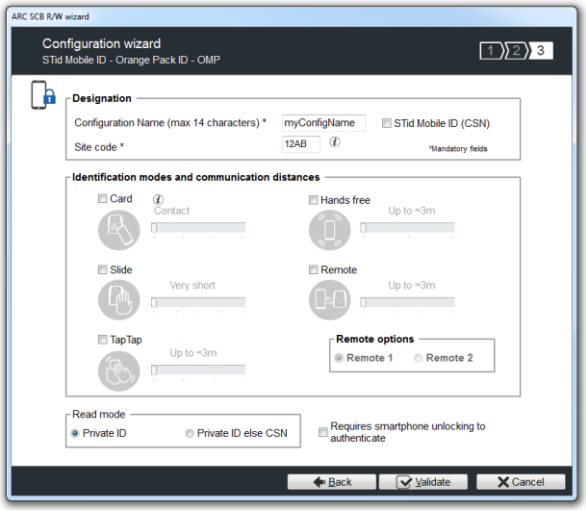
Data:

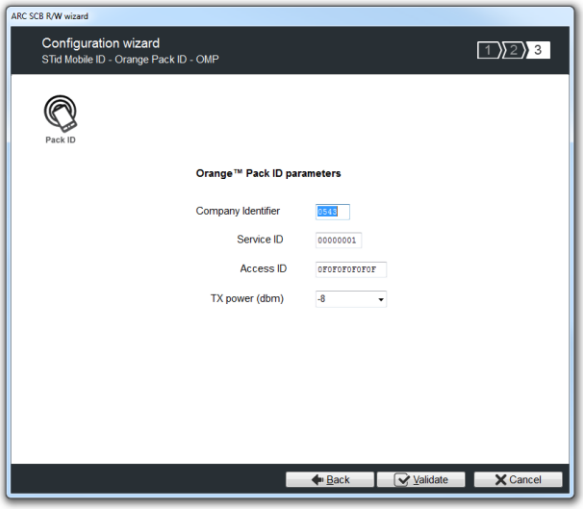
- ❖ Size: Determines the length of the ID.
- ❖ Offset: Define an offset from the first byte before reading.
- ❖ Reverse: If the box is checked the reader reads the identifier Least Significant Byte First.
  If the box is unchecked the reader reads the identifier Most Significant Byte First.

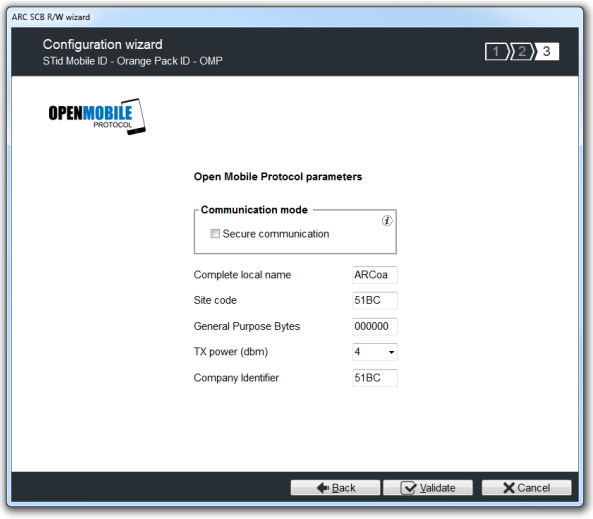
Blue/NFC solution:

Configure the reader to read STidMobile ID or Orange™ Pack ID or Open Mobile Protocol.

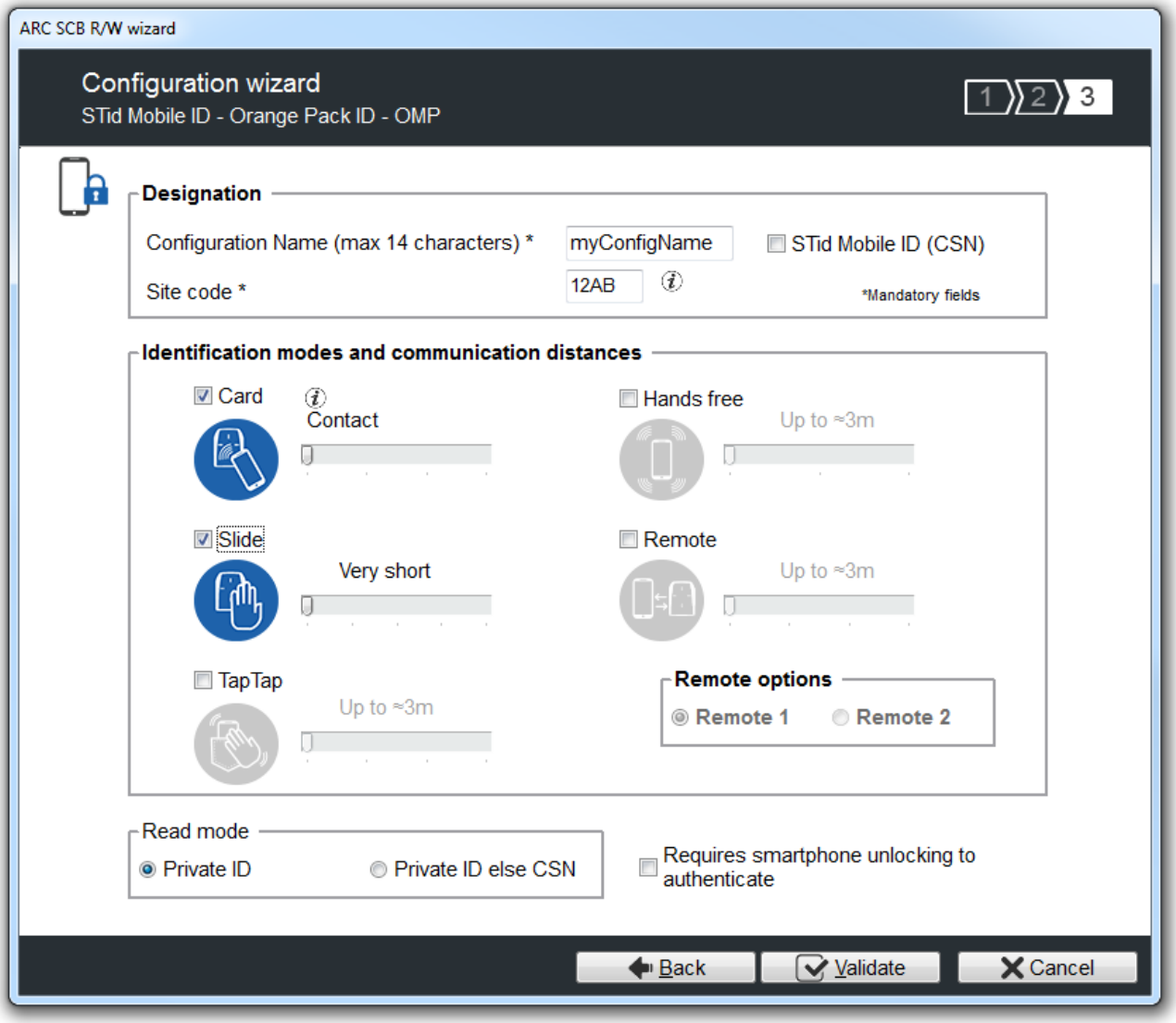
This choice impacts the screen wizard Step 3:





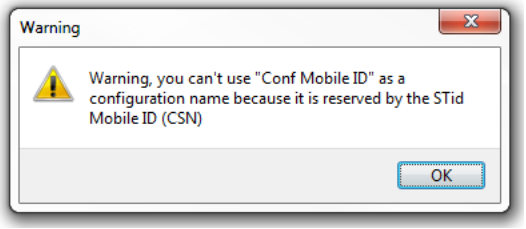


Step3 - Blue Mode STid Mobile ID®



Designation

- Configuration Name: enter the name of the configuration Mobile ID Secure Plus: 14 characters max.
  Note: configuration name “Conf Mobile ID” is reserved to STid Mobile ID®.



- Site Code: 2-bytes data used for the site code of the configuration.
  Note: site code 51BC is reserved for STid Mobile ID®.

- STid Mobile ID® (CSN): configure the Blue reader to read only a CSN on the smartphone.

Identification modes and communication distances

For each identification mode the communication distance is adjustable.

❖ **Card:**

By placing the smartphone in front of the reader.

- Contact: smartphone must be in contact with the reader.
- Up to 0.2m: smartphone must be in an area of 0.2m around the reader
- Up to 0.3m: smartphone must be in an area of 0.3m around the reader.
- Up to 0.5m: smartphone must be in an area of 0.5m around the reader

❖ **Slide:**

By placing your hand close to the reader without taking out your smartphone.
The distance between the smartphone and the reader can be:

- Very short
- Short
- Medium
- Long
- Very long

Not available for ARC1S neither ARCS keypad in Card or Key mode.

❖ **Tap Tap:**

By tapping your smartphone twice in your pocket for near or remote opening.
The communication distance can be:

- Up to 3m
- Up to 5m
- Up to 10m
- Up to 15m.

❖ **Hands free:**

By simply passing in front of the reader.
Communication distance around the reader:

- Up to 3m
- Up to 5m
- Up to 10m

❖ **Remote:**

By controlling your access points remotely.
Communication distance around the reader:

- Up to 3m
- Up to 10m
- Up to 15m
- Up to 20m

❖ **Remote options**

If the identification mode "Remote" has been activated, it allows to associate the current configuration to the Remote button 1 or Remote button 2.

Notes:

The notion of distance in Bluetooth® corresponds to an area around the reader, not just in the front.
Reading distances depend on the environment, on the position smartphone // reader ...

<u>It is recommended to do on-site testing to evaluate the settings.</u>

Warning
When Architect® Blue readers are installed close to each other, detection distances must be defined to accommodate the distance between the readers to avoid cross readings.

Read mode

- **Read mode: Private ID**
  Reader configured in read private virtual card.

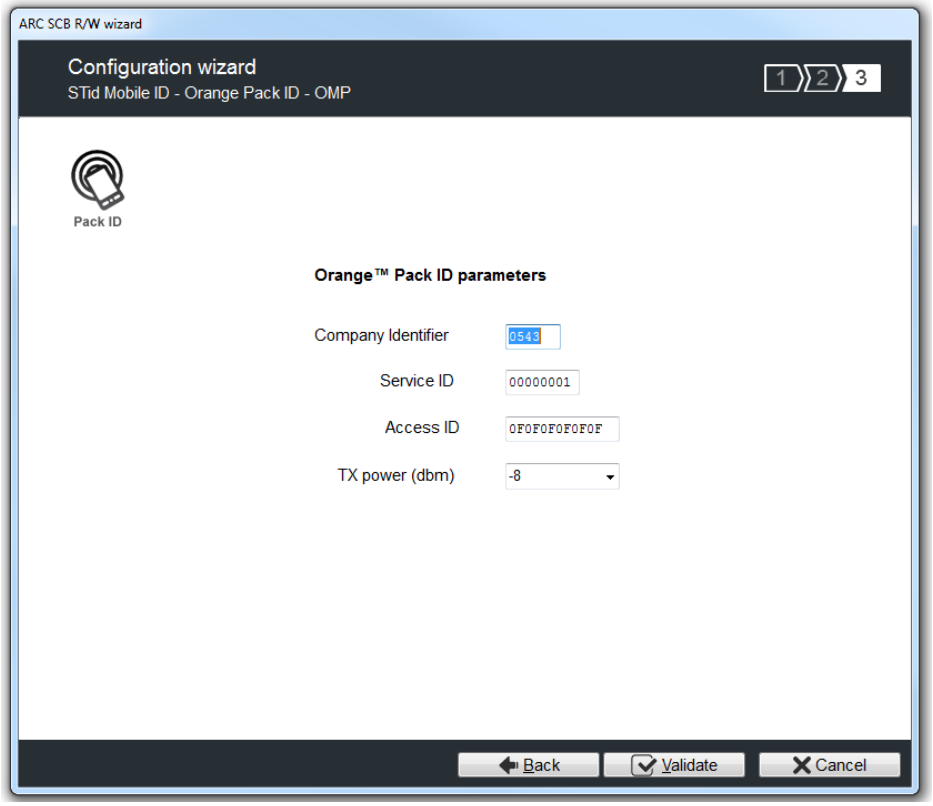
- **Read mode: Private ID else CSN**
  Reader configured in read private virtual card. If it is not found or if the security settings are incorrect, then the reader will read and return the STid Mobile ID® CSN.

Requires smartphone unlocking to authenticate: security option

- If checked: the smartphone must be unlocked (with PIN code or other unlocking option depending on the smartphone) to authenticate with the reader.

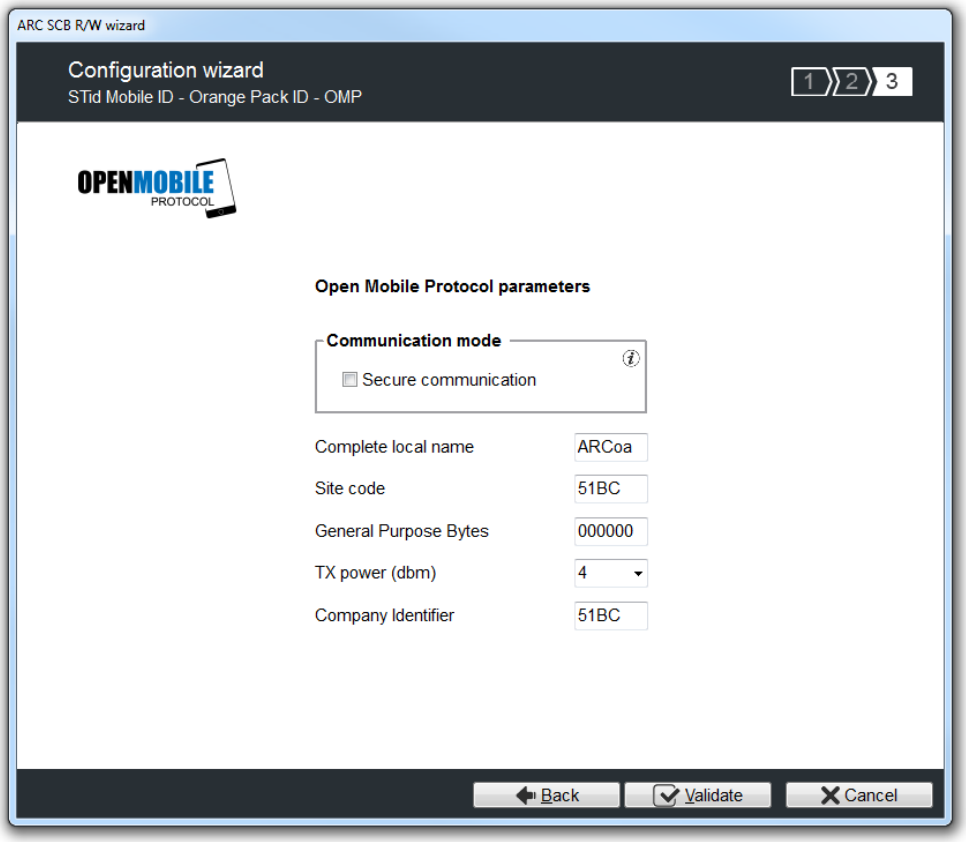
- If unchecked: unlocking the smartphone is not required to authenticate with the reader.

Step3 - Blue Mode Orange™ Pack ID



- **Company Identifier**: manufacturer data on 2 bytes.
- **Service ID**: manufacturer data on 4 bytes to differentiate the customers of Pack ID.
- **Access ID**: manufacturer data on 6 bytes to identify the access zone controlled by the reader.
- **Tx power**: change the power level of the reader (default 4 dbm). Possible values: -16, -12, -8, -4, 0 and 4 dbm.

Step3 - Blue Mode Open Mobile Protocol



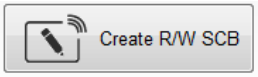
For information about Open Mobile Protocol, contact your STid sales representative.

Click the button 

to complete the reader configuration settings.

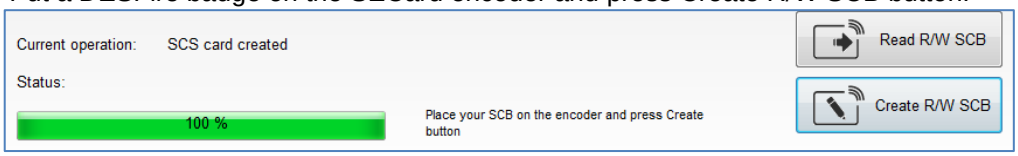
V.2 - Creating R/W SCB

Two possibilities to load the configuration into the reader:

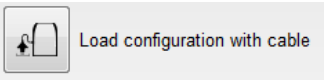
❖ 

R/W SCB configuration card must be created with MIFARE® DESFire® Ev1/ EV2 not locked 4ko and MIFARE® DESFire® Ev1/ EV2 not locked 8ko.

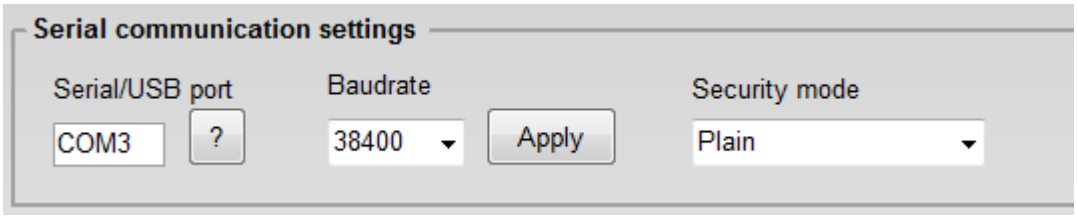
1- Put a DESFire badge on the SECard encoder and press Create R/W SCB button.



2- To load the configuration into the reader use SSCP® commands LoadConf_X (cf Spec_Protocole_5AA-7AA_MIFARE_GLOBAL_V1.17_EN.pdf)

❖ 

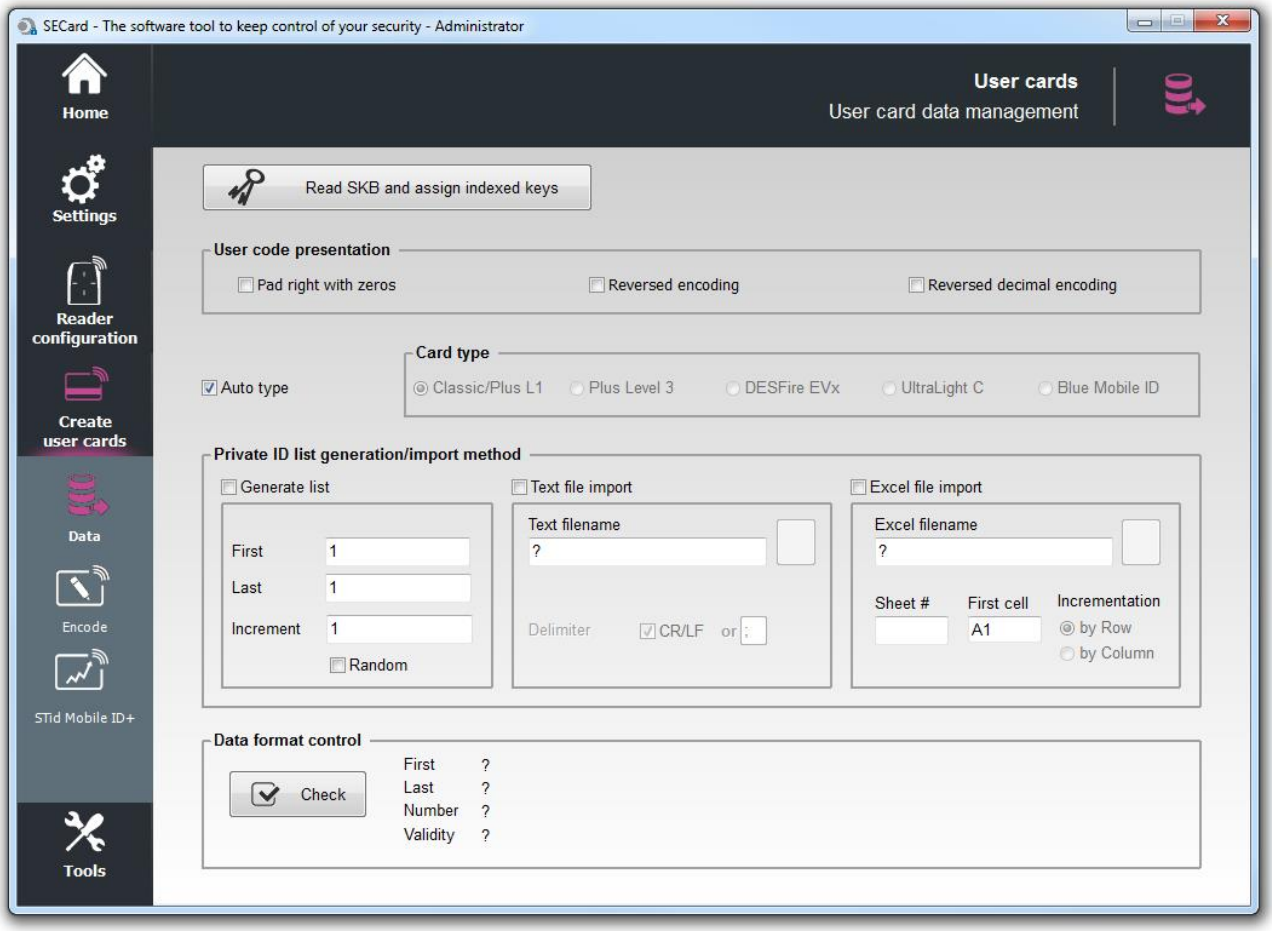
1- Connect the reader to configure to a port of the PC.
2- In “Serial communication settings” select the port number, the reader is a R/W reader so you can used CTRL+?



3- Press Load configuration with cable button.

VI. Create User cards

VII. 1 - Data



The encoding is done according to the settings defined in the "*SCB Wizard*".
The keys can be those defined in the configuration or read in a SKB card.

User code presentation

- Pad right with zeros:
  If the size of the number to be encoded is less than the size specified in the configuration, software will complete the number to encode with zeros in the most significant bits by default.

  If the "Pad right with zero" is checked the number to encode will be completed by zeros in the least significant bits.

- Reversed encoding:
  Reverse the hexadecimal writing.
  Example: number to encode ABCDEF10, with reversed encoding is: 10EFCDAB.

- Reversed decimal encoding (not alone, option to add with "Reversed encoding")
  Reverse the decimal writing. The decimal ID to encode is then convert in hexadecimal and then reversed.
  Otherwise the decimal value is inverted and then converted to hexadecimal.

Card Type

Auto type: If this box is checked, the encoder automatically detects the type of chip and encodes it according to its own parameters defined in “Wizard SCB”.

Warning

If chips are Mifare Plus® Level 0 AND Mifare Plus® Level 1 to be encoded as Mifare Plus® Level 1 AND Mifare Plus® Level 3, then you need to uncheck « *Auto type* » box and choose chip type to encode.
For an encoding of Mifare ® Classic 7 bytes CSN, it is necessary to deactivate the “*Auto Type*” and to choose “*Classic/Plus L1*”.

To encode the DESFire part on IDPrime card force to DESFire type.

Generate list

This mode is only available for standard sizes and custom sizes of private ID with length less or equal than 10 bytes in decimal and 48 in hexadecimal.

In each of the corresponding fields: enter the start, the end and increment of the list of numbers to encode.

Random

This option can be activate / deactivate only by Administrator. The increment field becomes the number of elements in the random value list.
Generate a random list of n values between the first and last value.
Note:

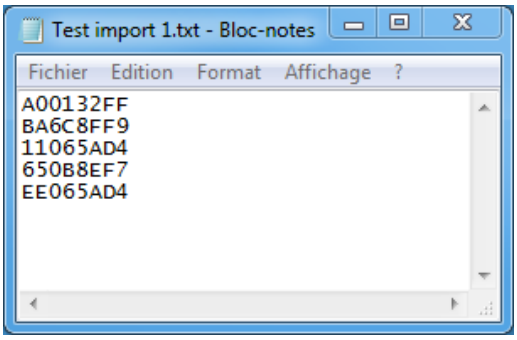
- ✓ The random list is not compatible with 26-bits Wiegand format.
- ✓ The maximum value is 0x7F FF FF FF (2147483647).

With this option the data encoded not appear in “Progressing session log” and it’s not possible for User to read it with “Read private ID”. Administrator can read the private ID by unchecking this option.
Warning: No duplicate check is performed.

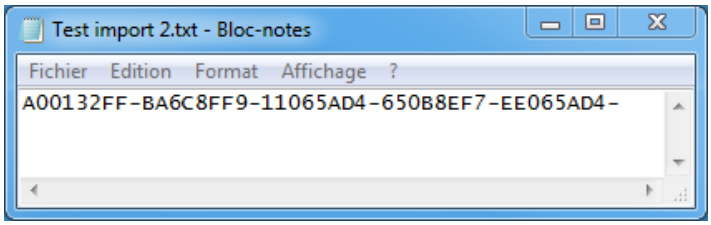
Text file import

To import a list in text format, that will be used for encoding users card.

Delimiter CR/LF



Delimiter « - »



Warning
The last number to be encoded must be followed by a delimiter.

Warning

The text import is not importing the values if:
- there are intermediate empty lines with the separator CR/LF
- there are multiple delimiters with another delimiter for example “ ;“ (ex:12313;12385485;;;5646;;12;041)

Excel file import

Import a list in Excel format, that will be used for encoding users card.

Indicate the page (sheet) in which the numbers are to be encoded and the first cell.

Increment per line: Use when the numbers are written in a column.
Increment per column: Use when numbers are written on one line.

Warning

Import from Excel is supporting only continuous list. If the user has inserted empty cells, then SECard will stop the encoding.

It is necessary to install Excel® before using this mode.

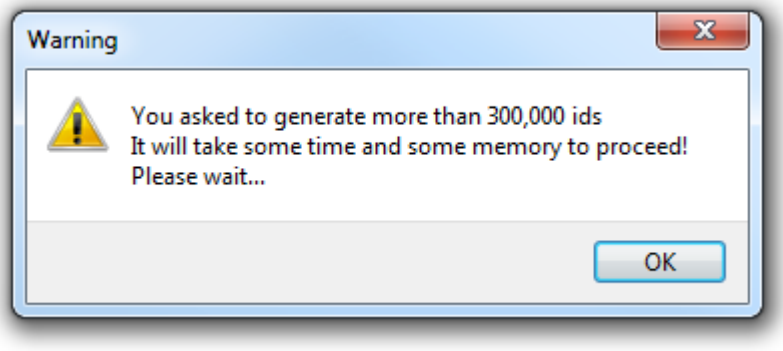
Data format control

Check the validity of number to encode. It is based only on the first and last values to be encoded.

Note:

* The software will check that the first and last values of text files and Excel. In any case, this function will check the maximum and / or minimum.

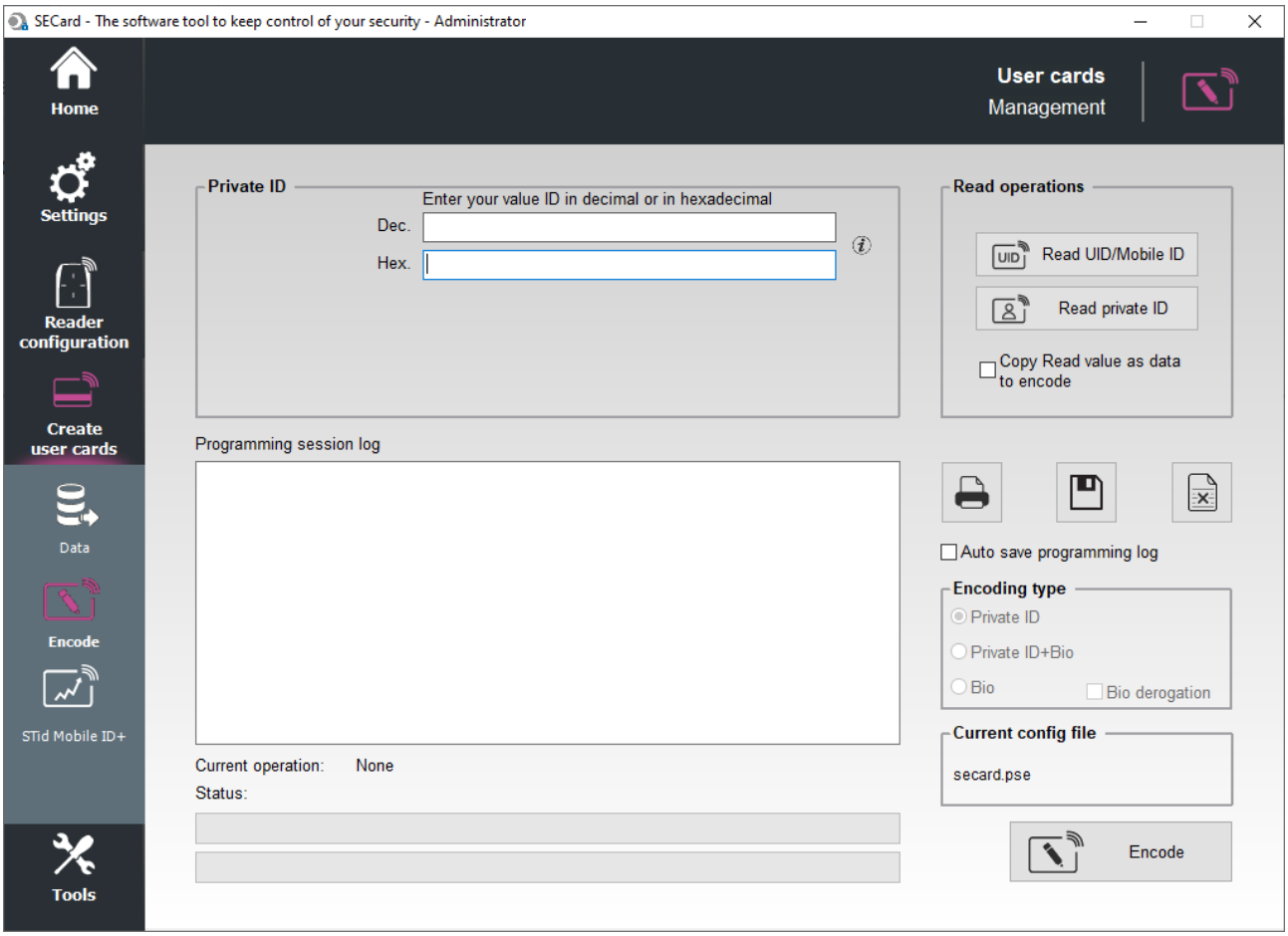
* If the number of identifiers is greater than 300,000, a message appears asking you to wait while checking and that it will require RAM resources of your computer.



Read SKB and assign indexed keys

In the case where the keys required for encoding are contained in a SKB badge, the SKB badge must be read to temporarily load the keys in SECard

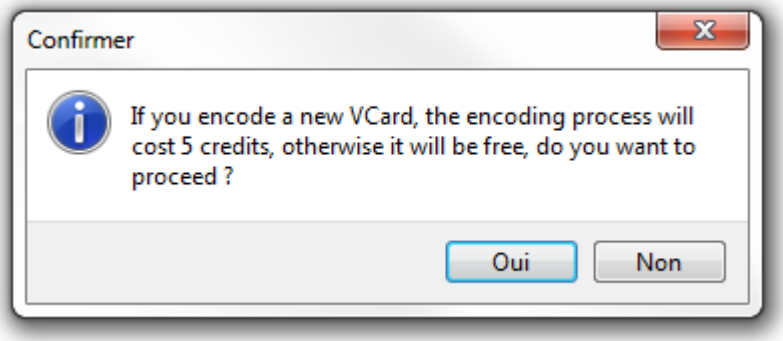
VII. 2 - Encode *Adding functionality 3.6*



Once the setup application finished and the numbers to be encoded determined, IDs can be encoded.

To encode an ID on a Smartphone it is necessary to install STid Mobile ID® from the AppStore or PlayStore.

Encode VCard



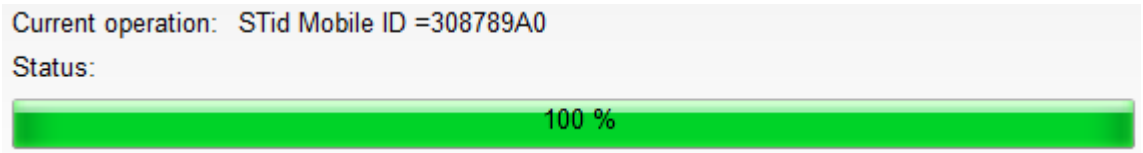
- If it's a new VCard the encoding process will cost 5 credits.
- If the VCard is already encoded in the smartphone and you just want to change the value of Private ID the encoding process will be free.

Private ID

- If "Generat list" or "Text file import" or "Excel file import" has not been selected in data, allows to enter a private ID, it is simply necessary to write the number in the suggested field.
- If "Generat list" or "Text file import" or "Excel file import" has been selected in data, the field is not accessible.

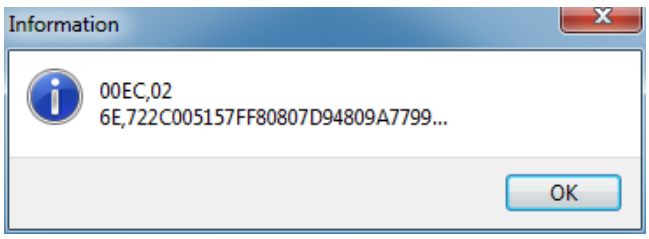
Read operations

- Read UID/Mobile ID: Read UID and chip type of the card detected by the encoder.
  Ex:

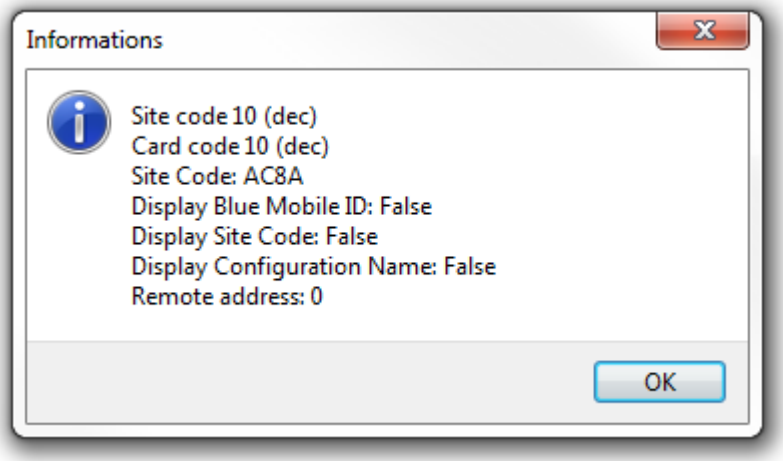


- Read private ID: Read a private ID or templates of the card detected by the reader according to the current configuration, and if the "Copy Read value as data to encode" is checked, the read value is copied into the field to encode.

  Example read template:



Example Read private Mobile ID:



	Print users operations.
	Save users operations.
	Delete users operations.

Auto save programming log

If this option is activated, all the operations done are saved in a RTF file. It will be located in the same directory than the .pse settings.

Encoding type

- Private ID: Encode only private ID.
- Private ID + Bio: Encode private ID and biometric.
- Bio: Encode only biometric.

Bio derogation: only avaialble if bio derogation has been enable in the Biometric options of the chip. In this case, a derogation will be encoded in the badge and the encoding process will not require presentation of the finger of the user.

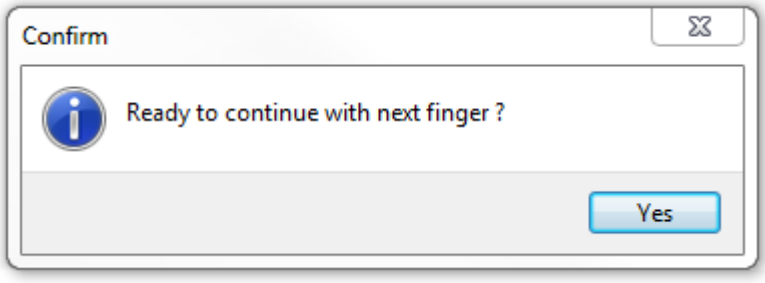
Current config file

Specifies the configuration file currently loaded in SECard and in which the identifiers will be encoded.

Biometric fingerprints encoding

When biometric configuration is enabled and the encoding selected "Bio" or "Private ID + Bio", the software SECard open a window to capture fingerprints.	Then place your finger on the biometric sensor encoder. It must be in red light to indicate that it is ready to read the fingerprint.	When the fingerprint is read, it is displayed on the window and the bar on the right shows the progress of the analysis.
		

Once the fingerprint is read, the software will ask you to place another finger if the configuration requests it.



If the finger is not placed well, the software will inform you about the problem by indicating you a good placement:

Warning

The biometric sensor has to be connected to an USB port.
The finger has to be clean.
The surface of the sensor has to be clean.

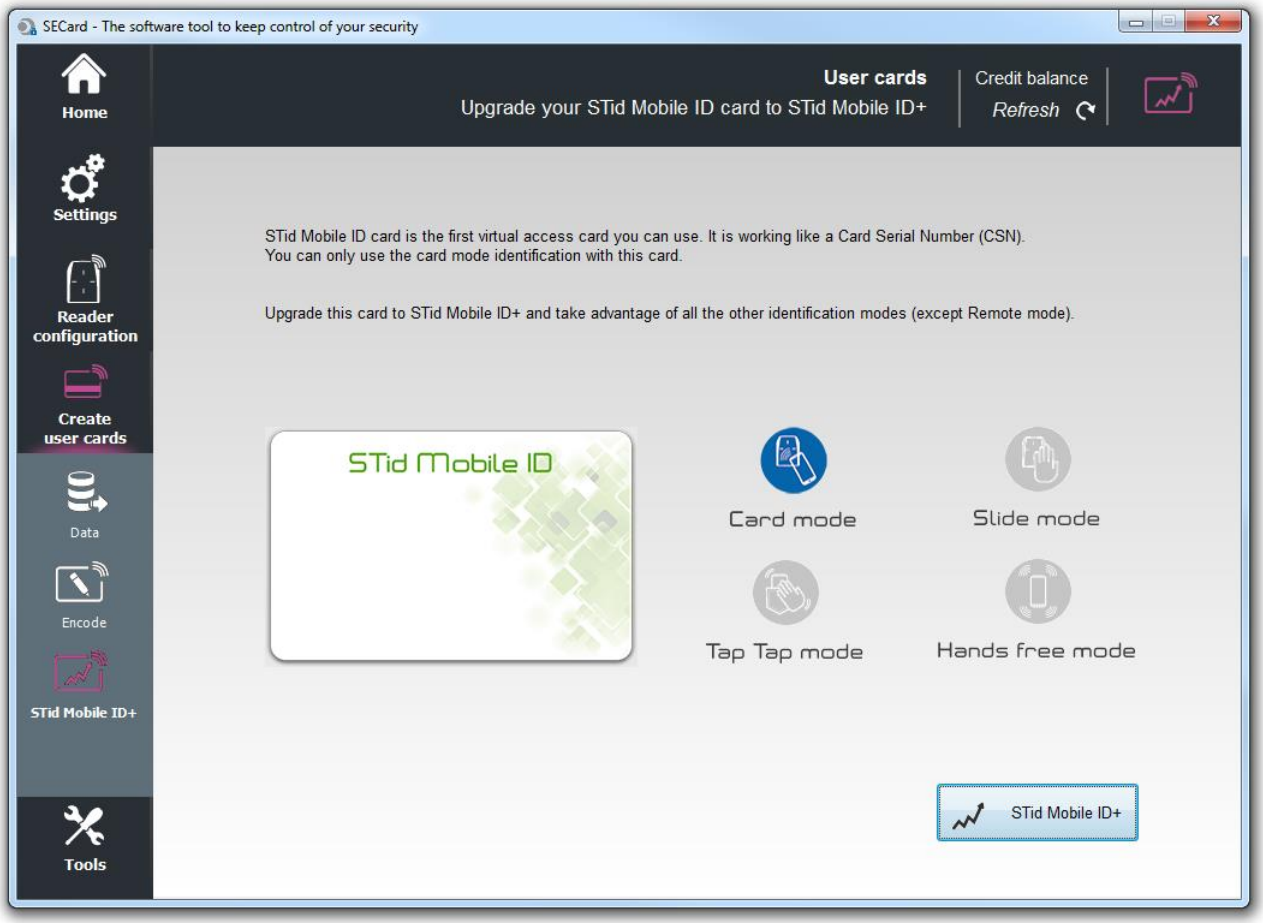
VII. 3 - STid Mobile ID+

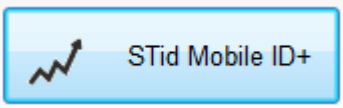
When “STid Moible ID” application is installed on the smartphone, the first Mobile ID card available is “STid Mobile ID”.

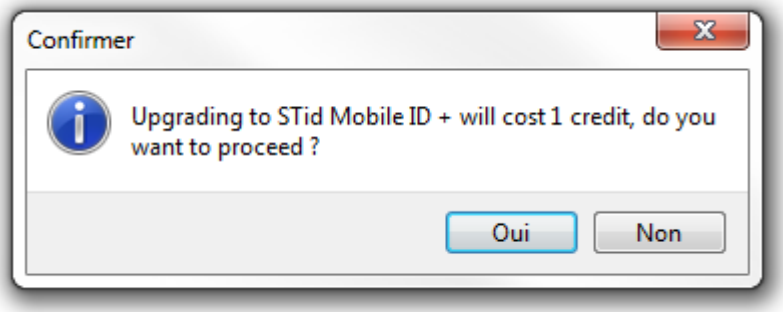
This card it is working like a Card Serial Number.

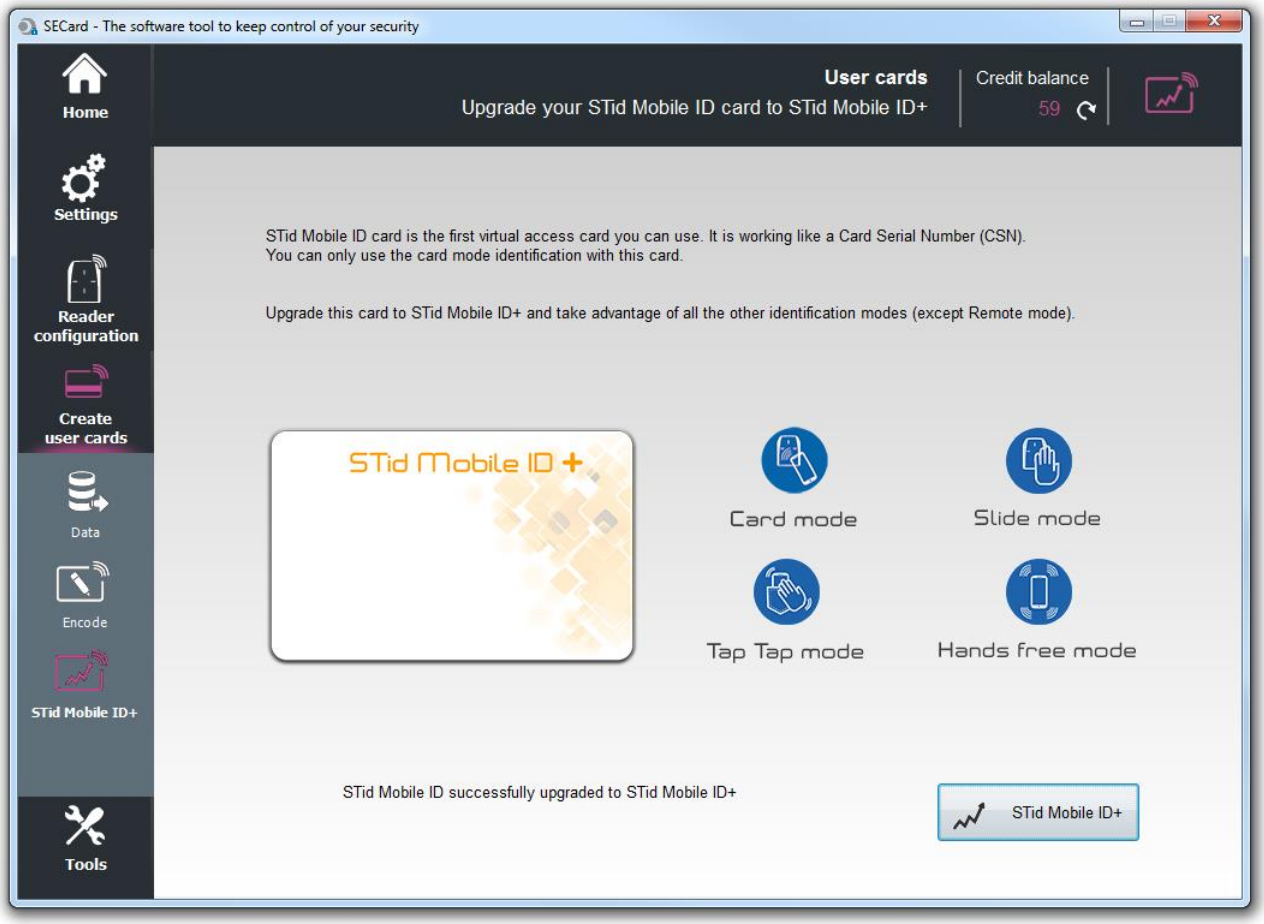
Only the “card mode”detection is authorized.

To take the advantage to Slide mode, Tap Tap mode and Hands free mode you can upgrade the STid Mobile ID® to STid Mobile ID+. This upgrading will cost 1 credit.



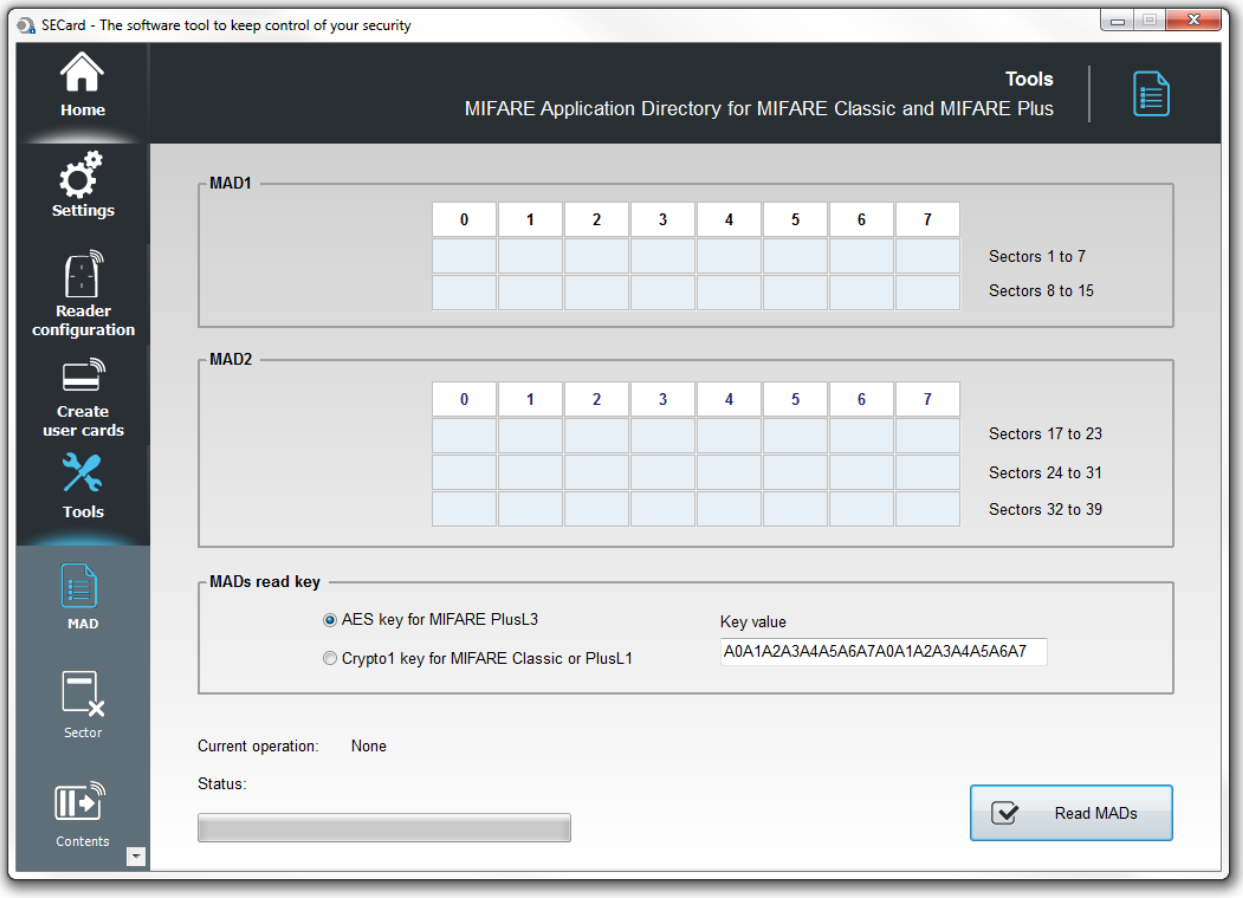
Click the button  **to upgrade Vcard.**


Confirmer
Upgrading to STid Mobile ID + will cost 1 credit, do you want to proceed ?
Oui
Non


SECard - The software tool to keep control of your security
Home
Settings
Reader configuration
Create user cards
Data
Encode
STid Mobile ID+
Tools
User cards
Upgrade your STid Mobile ID card to STid Mobile ID+
Credit balance
59
STid Mobile ID card is the first virtual access card you can use. It is working like a Card Serial Number (CSN).
You can only use the card mode identification with this card.
Upgrade this card to STid Mobile ID+ and take advantage of all the other identification modes (except Remote mode).
STid Mobile ID +
Card mode
Slide mode
Tap Tap mode
Hands free mode
STid Mobile ID successfully upgraded to STid Mobile ID+
STid Mobile ID+

VII. Tools

VII. 1 - MAD



Scan a MIFARE® Classic or MIFARE Plus® chip, to read the contents of the MAD and display current AID codes location.

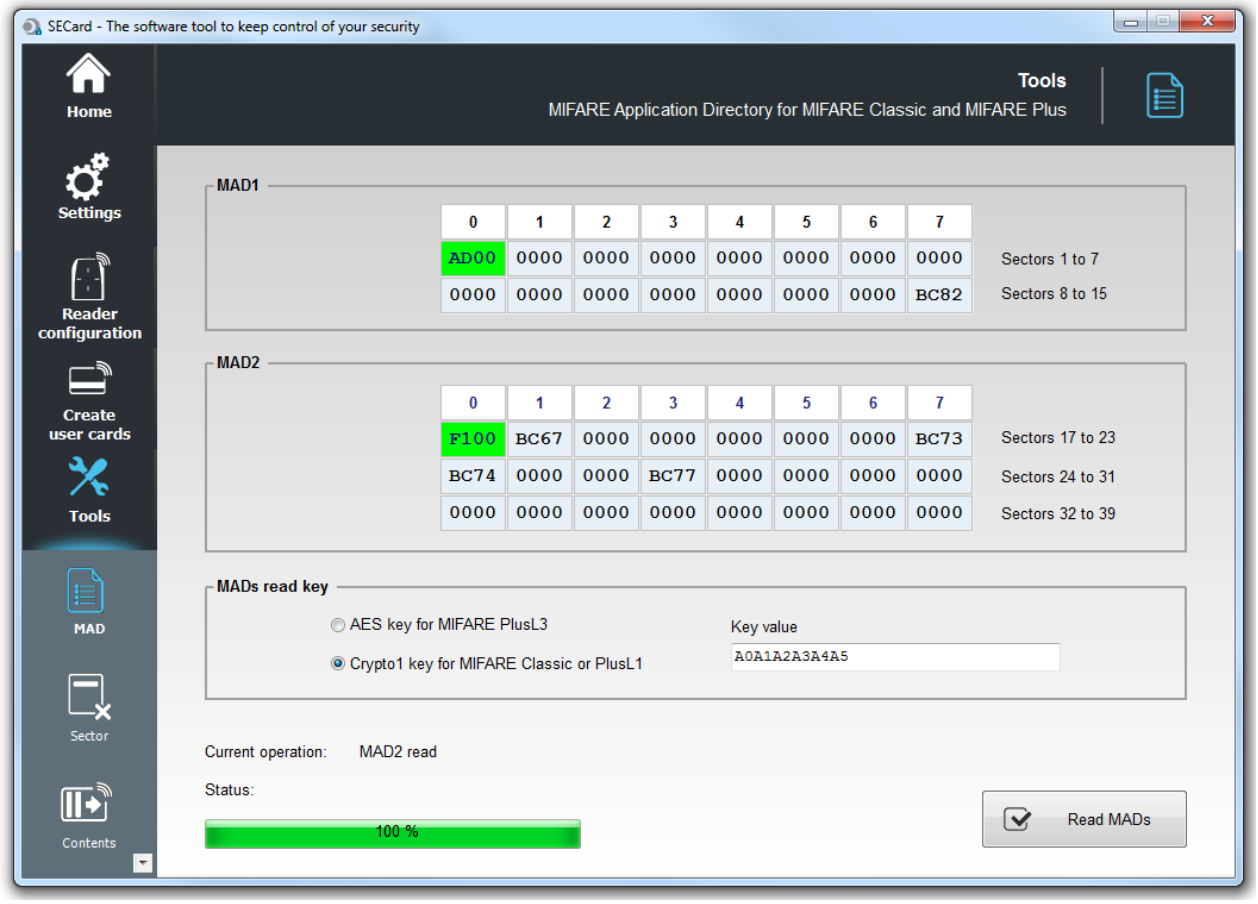
A MAD location containing an AID code means that an application use this sector.
Sectors 0 and 16 are not usable because they store the MAD1 and MAD2 information.

It is necessary to enter the MAD read key value in the "MADs read key" and to select the type of key used:

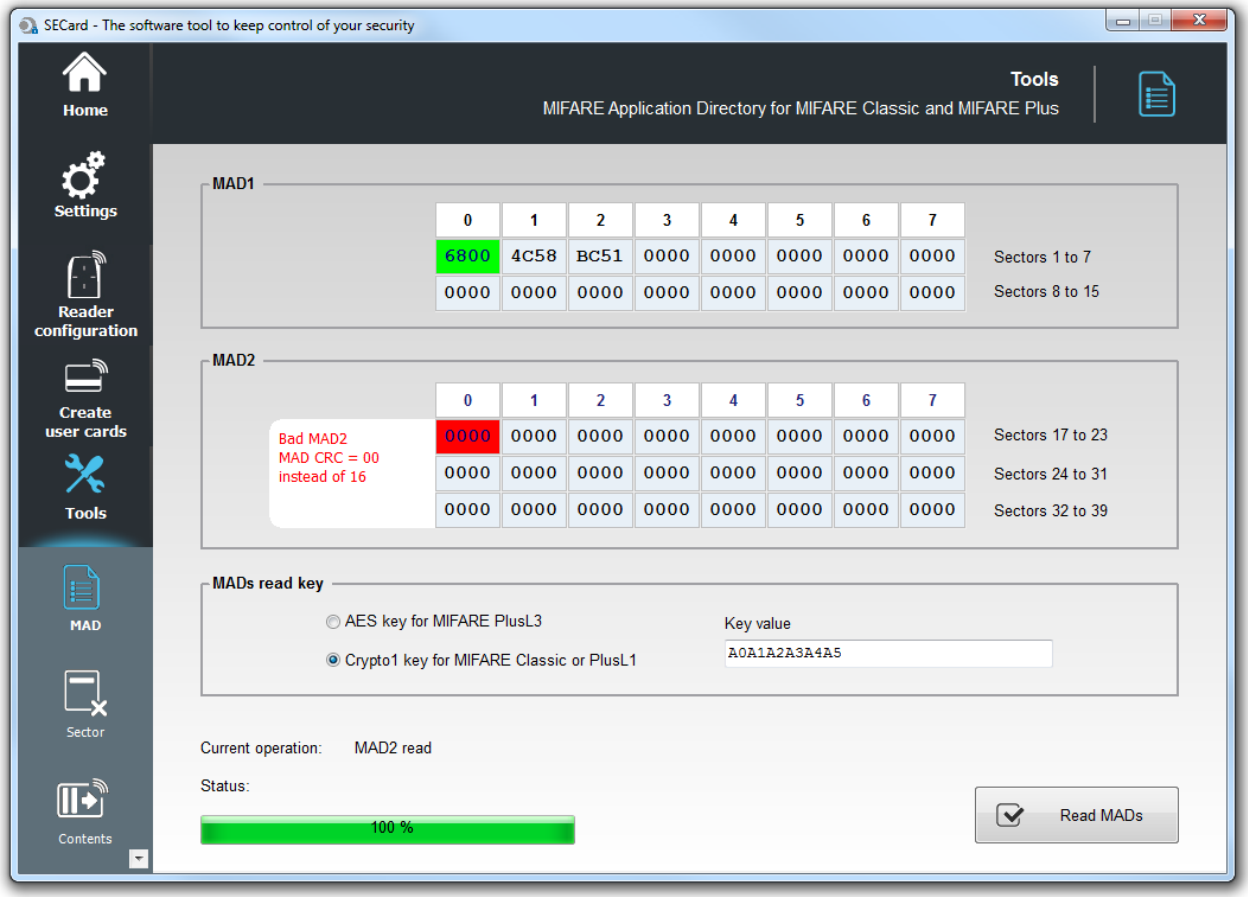
For MIFARE® Classic or MIFARE Plus® Level1, Crypto 1 key default is A0A1A2A3A4A5.

For MIFARE Plus® Level 3 AES key default is A0A1A2A3A4A5A6A7A0A1A2A3A4A5A6A7.

Successful MAD scan

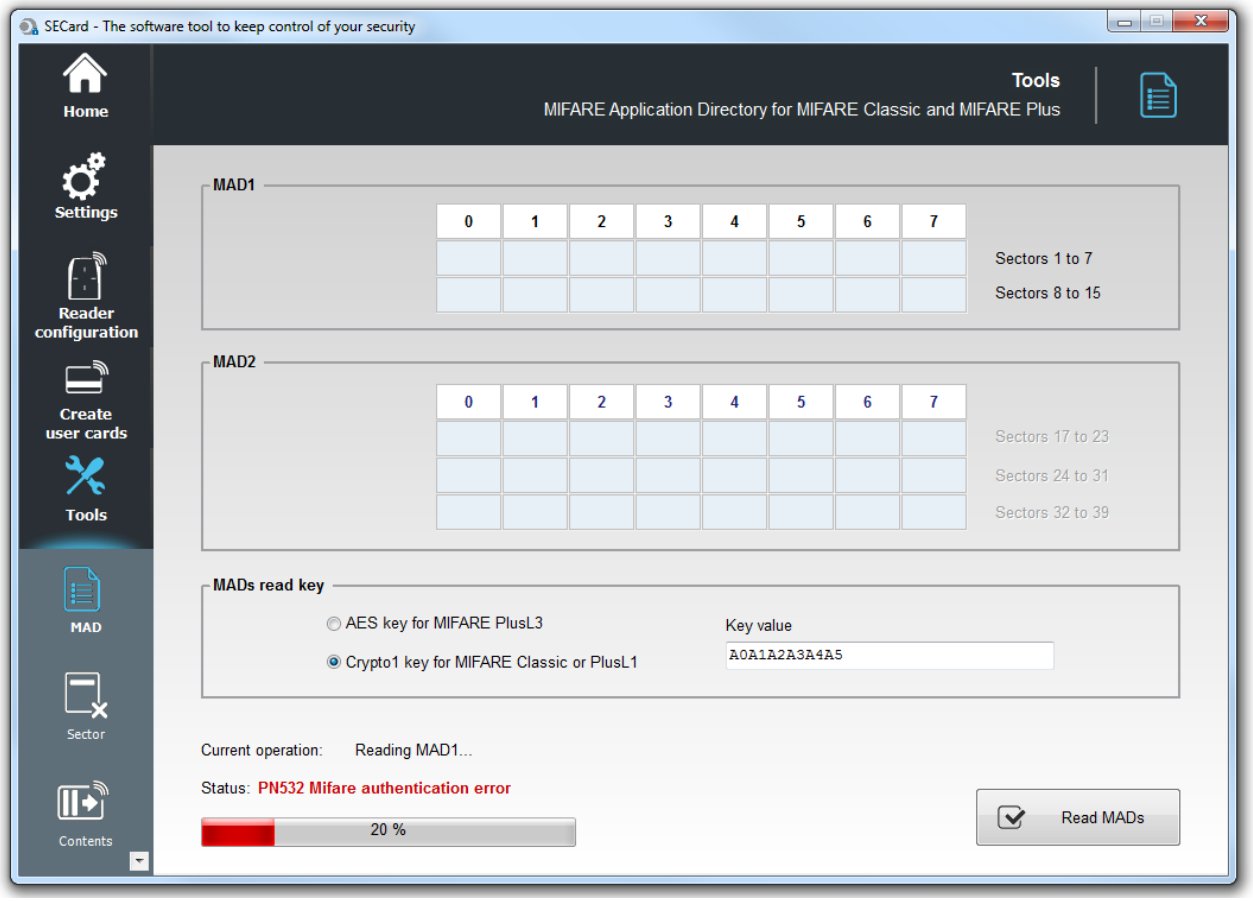


Successful scan MAD but MAD settings NOT OK

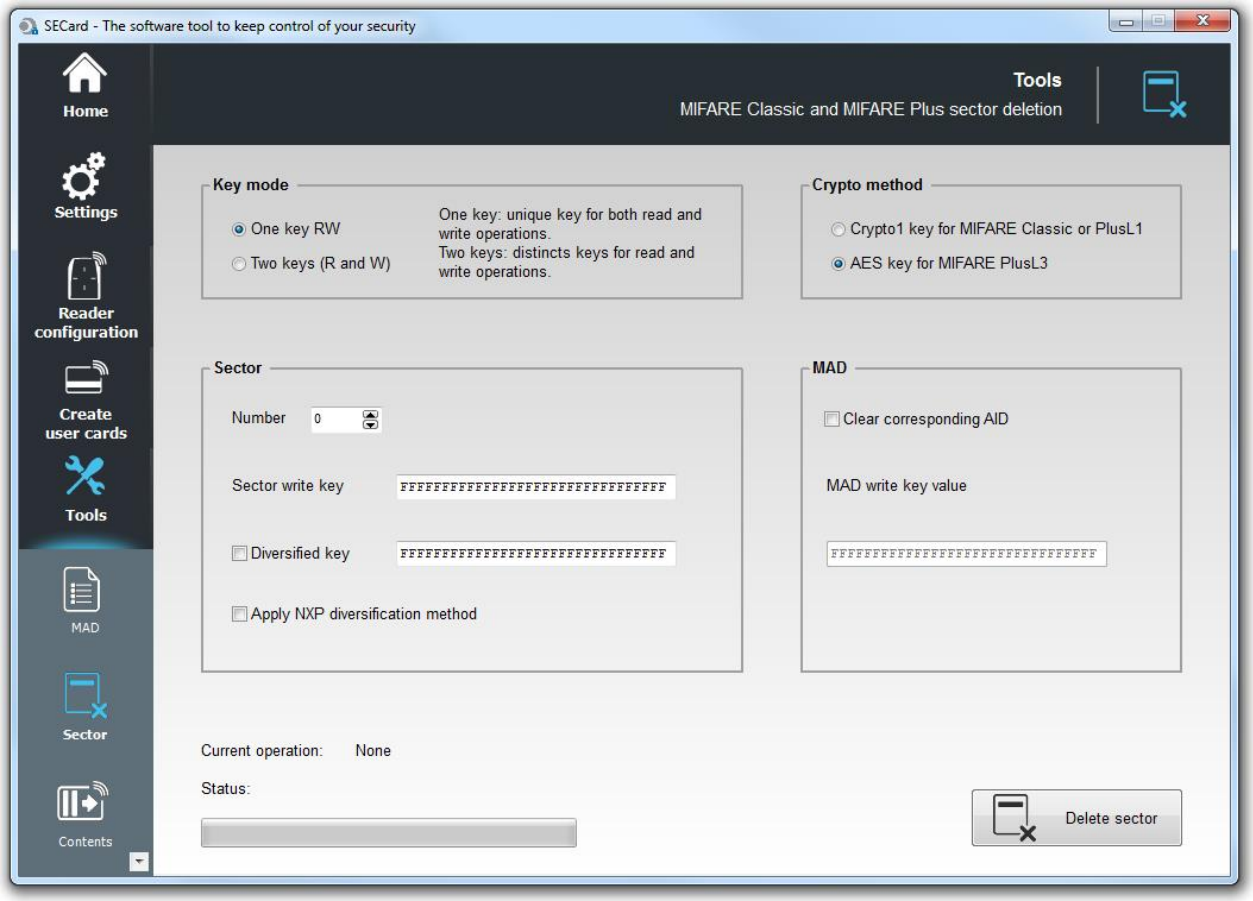


Encoded CRC+Info hasn't the right value. Performs encoding with SECard to correct the problem.

Failed to scan MAD: MAD not used or bad read key.



VII. 2 - Sector



Erase one sector of MIFARE® Classic or MIFARE Plus®.

Key mode

Choose the mode in which the sector to be erased has been encoded: one key or two key.

Crypto method

Choose the crypto method for the current chip.

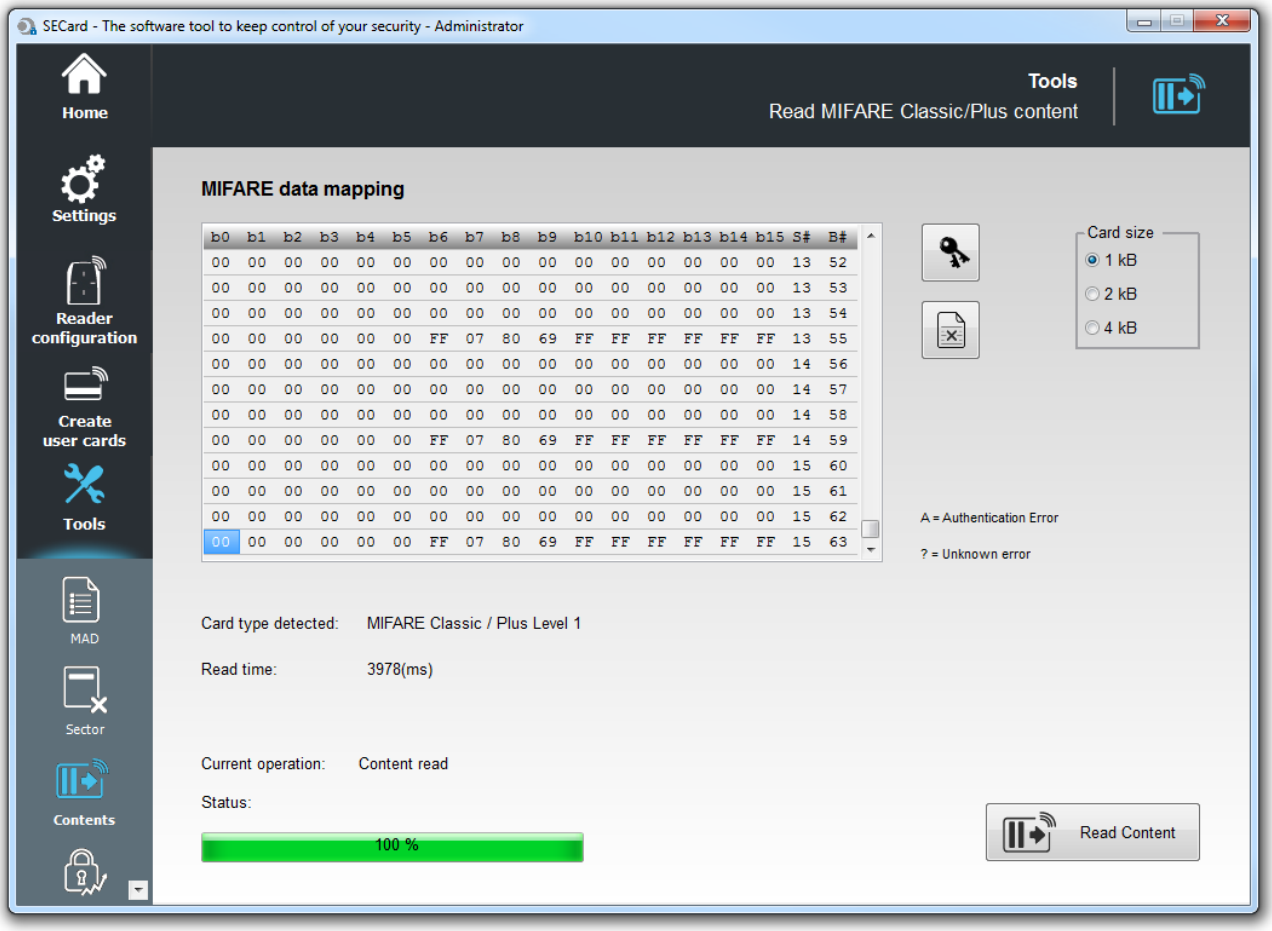
Sector

Choose the sector number to erase and the write key.
It is also necessary to check the "Diversified key" box and fill in the field the value of key if the encoding was performed with a value of diversified key (Apply the method of diversification NXP if diversification has been made by this method check).

MAD

It is possible to clear the corresponding AID in MAD. For this it is necessary to select « *Clear corresponding AID* » and to enter MAD write key value.

VII. 3 - Contents



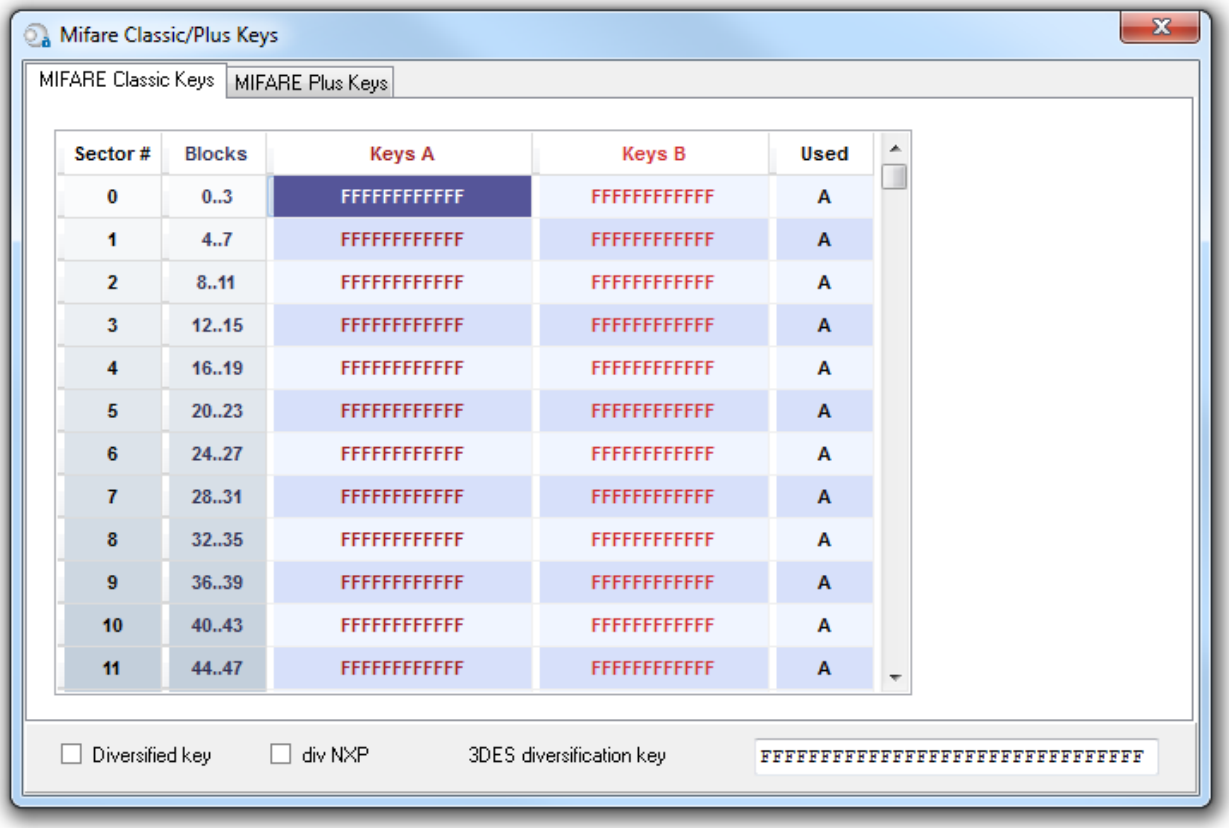
Read the contents of MIFARE® Classic or MIFARE Plus® chip.

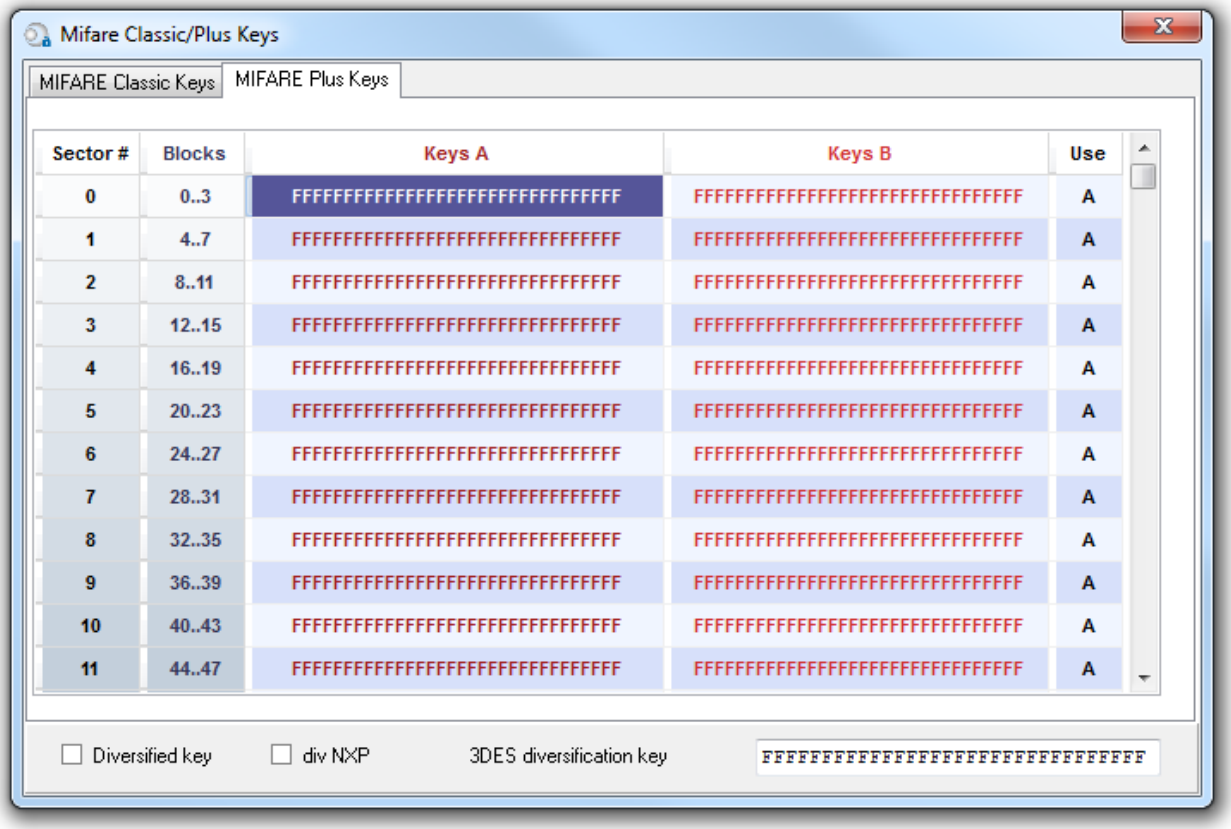
 Clear the contents of windows.

Card Size
Choose the size of the memory chip read.

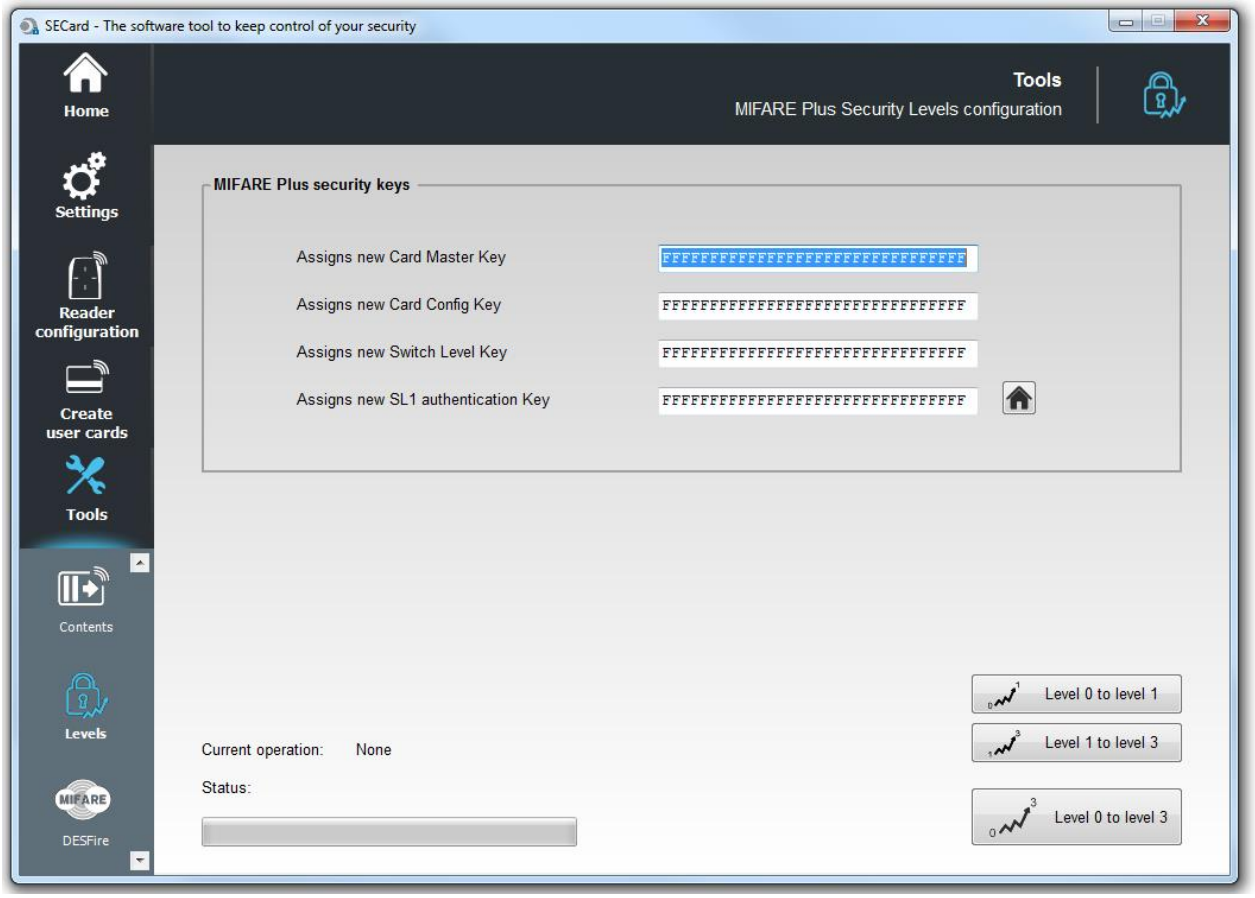
Note:
It is possible to stop reading using the "Esc" button on the keyboard.

Enter read keys sector(s) and type of key (A read/write key in mode one key or key B read/write key in mode two keys), diversification option is also available:





VII. 4 - Levels



Switch manually the security level of MIFARE Plus® chip:

- From Level 0 to Level1
- From Level 1 to Level 3
- From Level 0 to Level 3

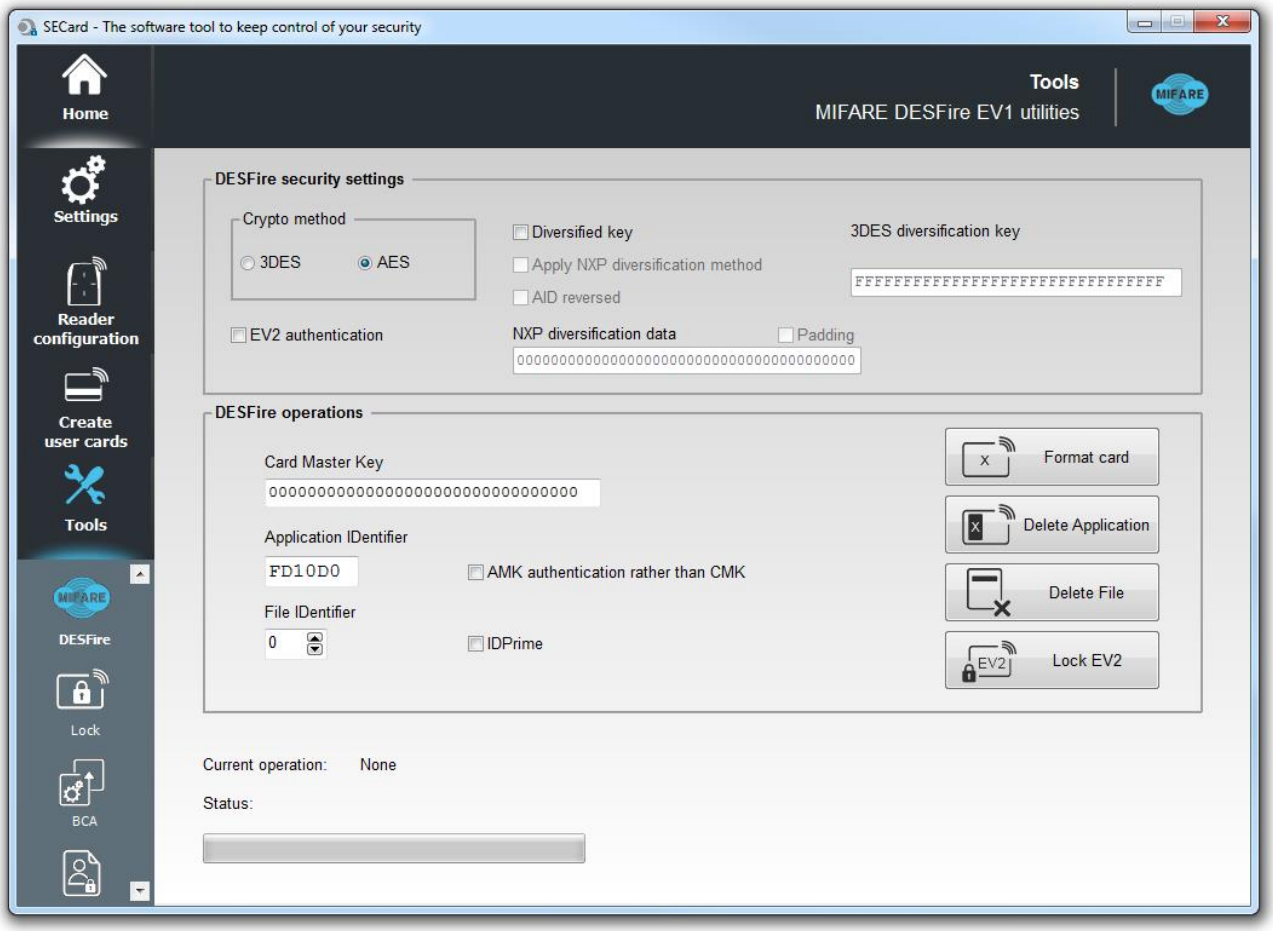
To perform a change of level, it is necessary to fill the four key fields.

MIFARE Plus® chip keys defaults are:"FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF", it is recommended to change to optimize security.

Warning

Card can only be switched upwards to higher security level.

VII. 5 – MIFARE® DESFire®



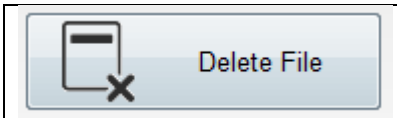
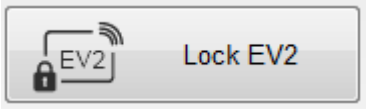
Format the chip, delete an application created on the MIFARE® DESFire® EV1/EV2 chip or delate file into an application.

DESFire® security settings

Choose the authentication method used for the master key and select the possible options for diversification.

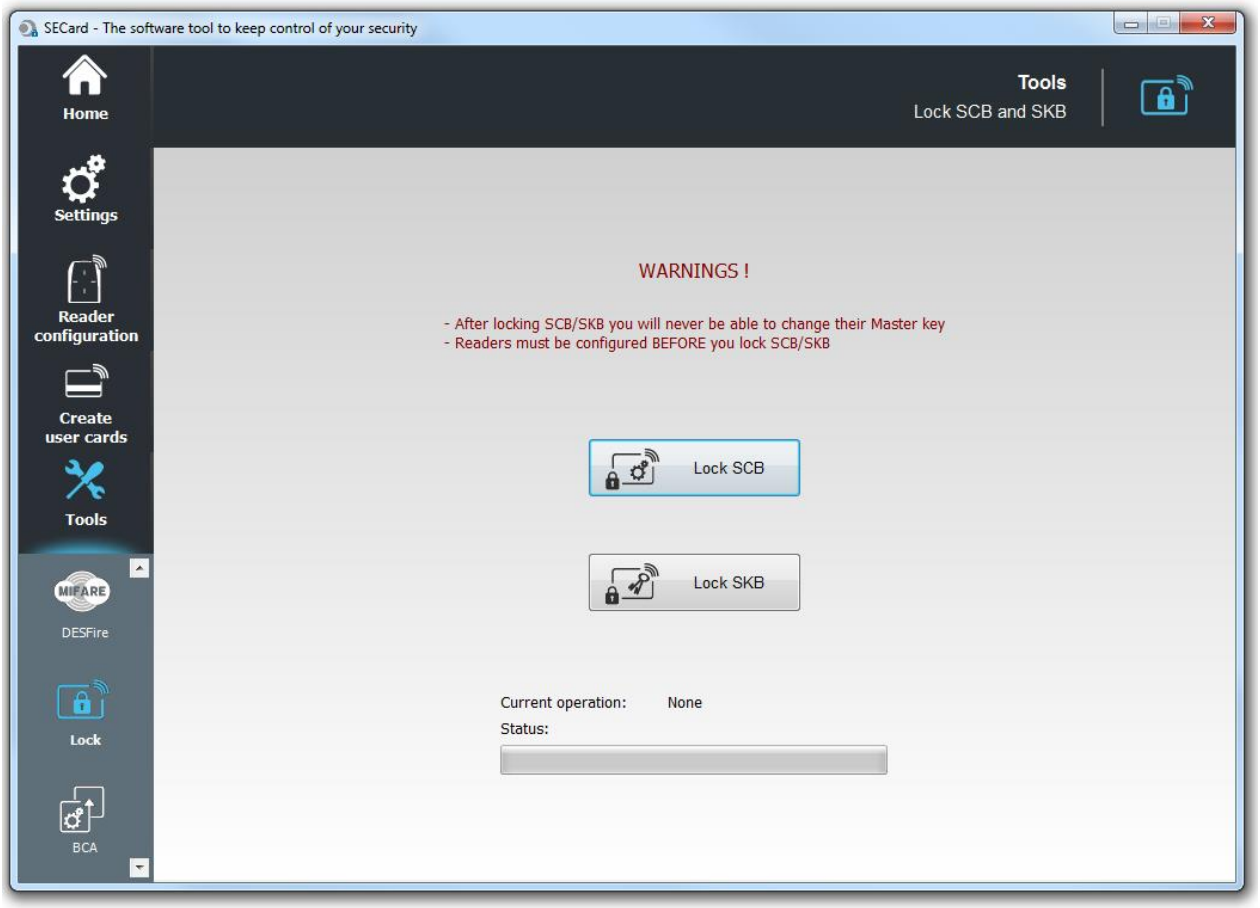
DESFire® operations

Format card	- Select security settings of DESFire (cryptographic method, diversification, if . - Set the Card Master key value. **Warning** When you format the chip, all data will be lost. Formatting does not change the master key.
Delete Application	- Select security settings of DESFire (cryptographic method and diversification. - Set the Card Master key value or application master key value according the settings of your chip. - Set the application identifier (AID) **Warning** When you delete an application, all included files will be deleted

	- Select security settings of the application containing the file (cryptographic method and diversification. - Set the Card Master key value or application master key value - Set the application identifier (AID) - Set the file ID number to delete.
	Locks a DESFire® EV2 in Secure messaging EV2 mode. The communication with the chip can then be done only in EV2. - Set the Card Master key value. - Select the crypto of the card master key **Warning** **This operation is definitive, no possible 'CANCEL'**

To delete an application or a file on IDPrime card, tick the IDPrime box to work with DESFire® emulation.

VII. 6 - Lock



Lock SCB and SKB cards, this will permanently lock the possibility to change further the master key of cards.

Once the SCB card locked, it will be only possible to configure the readers that have been configured with this configuration card, it will not be possible anymore to configure readers with factory key or another key.

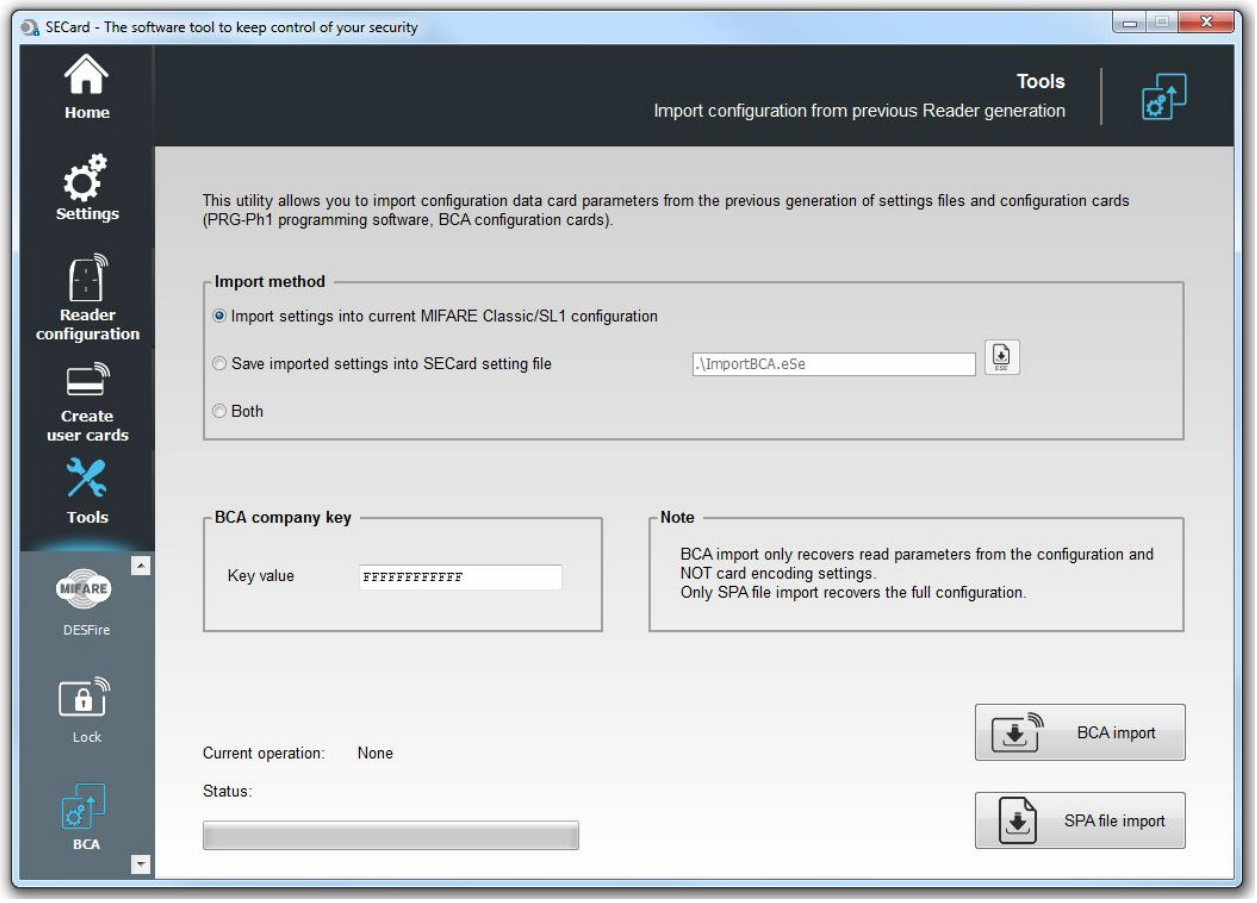
Warning

Before the lock operation, it is necessary to configure the readers by these cards.
If not, these cards will be unusable.

Warning

This operation is definitive, no possible 'CANCEL'.

VII. 7 - BCA



The new generation of standard readers (E) must be configured to read a private ID in the MIFARE® classic chip as the previous generation (A).

Two import tools are proposed, according to a BCA configuration card or a .spa configuration file create with PRG-PH1.
In both cases, only MIFARE® Classic configuration is imported.

Import method

1 - Import settings into current MIFARE® Classic/SL1 configuration:
The MIFARE® Classic parameters are filled into this dedicated window of “SCB” wizard.

2 - Save imported settings into SECard settings file:
The MIFARE® Classic parameters are saved into a new .eSe file (ImportBCA.eSe by default), different from the one used for the general configuration.

Both = 1 + 2

BCA company key

It is absolutely necessary to know the company key of BCA card to enter it in this field.
BCA company key on 6 bytes will be imported into the SCB key field with a zero padding left to reach 16 bytes.

The key values of BCE card will be copied in the array of values read "Crypto1keys" of SKB card. The SKB master key will be defined with SECard.

BCA import

Imports **only** the parameters necessary for the readers to read user cards.

Warning

Some parameters are not taken into account (these are not referenced in the BCA) such as key changes and MAD parameters.

This import does not allow tocreate new user cards.

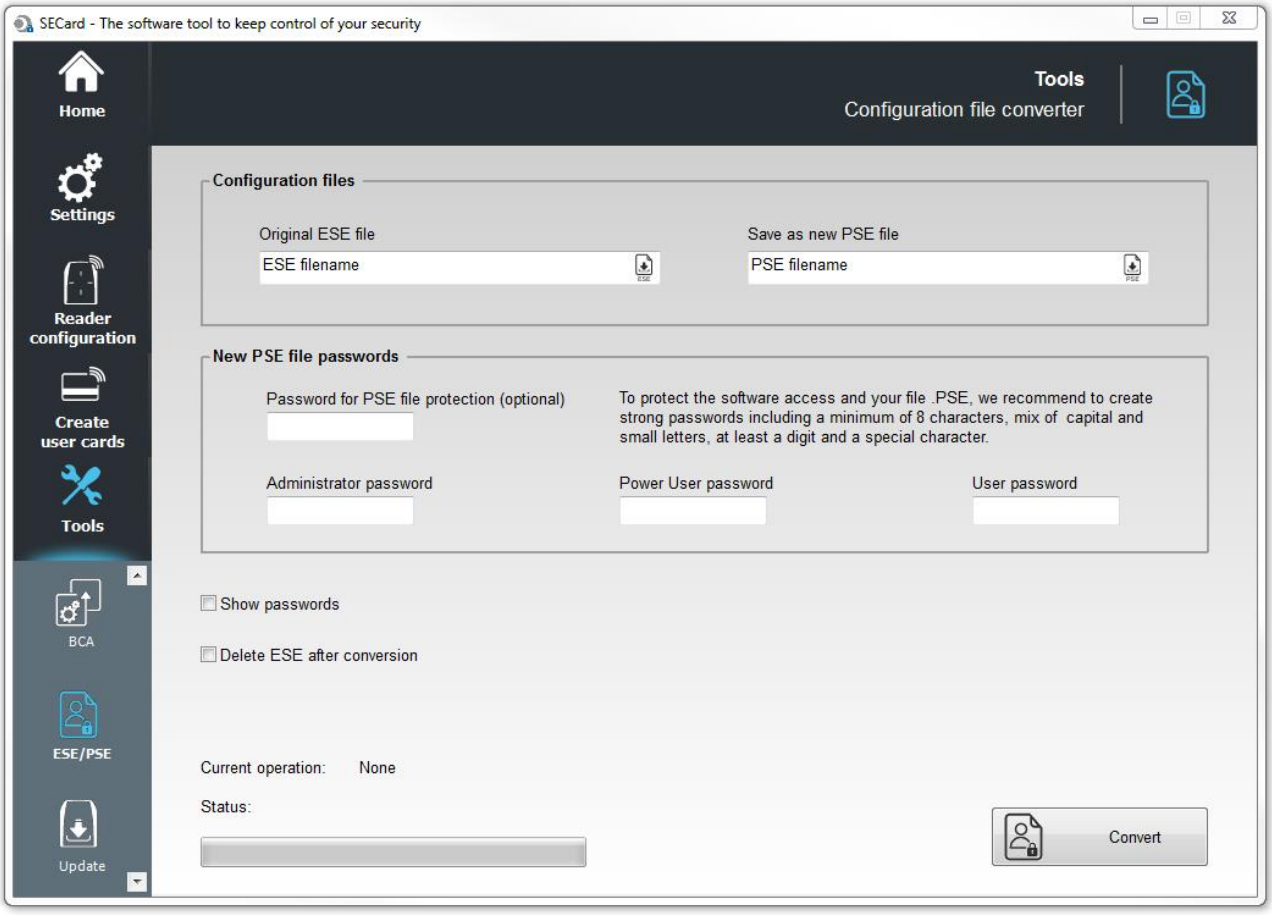
SPA file import

Imports **all** the parameters necessary for the reader to read user cards **AND** all write parameters needed to create new users cards.

Note:

* Secure Plus parameters will not be imported because this functionality is differently implemented in SECard
* If .spa file is protected by password it is required to enter it.

VII. 8 - ESE/PSE



Configuration files created with previous version of SECard were ".eSe" files. From V2.0.x version, the configuration files format are ".PSE Protected Settings".
Login and read passwords are into this file.

This tool allows you to import ".eSe" configuration files and convert them into ".pse" by adding logins and read passwords.

Configuration files

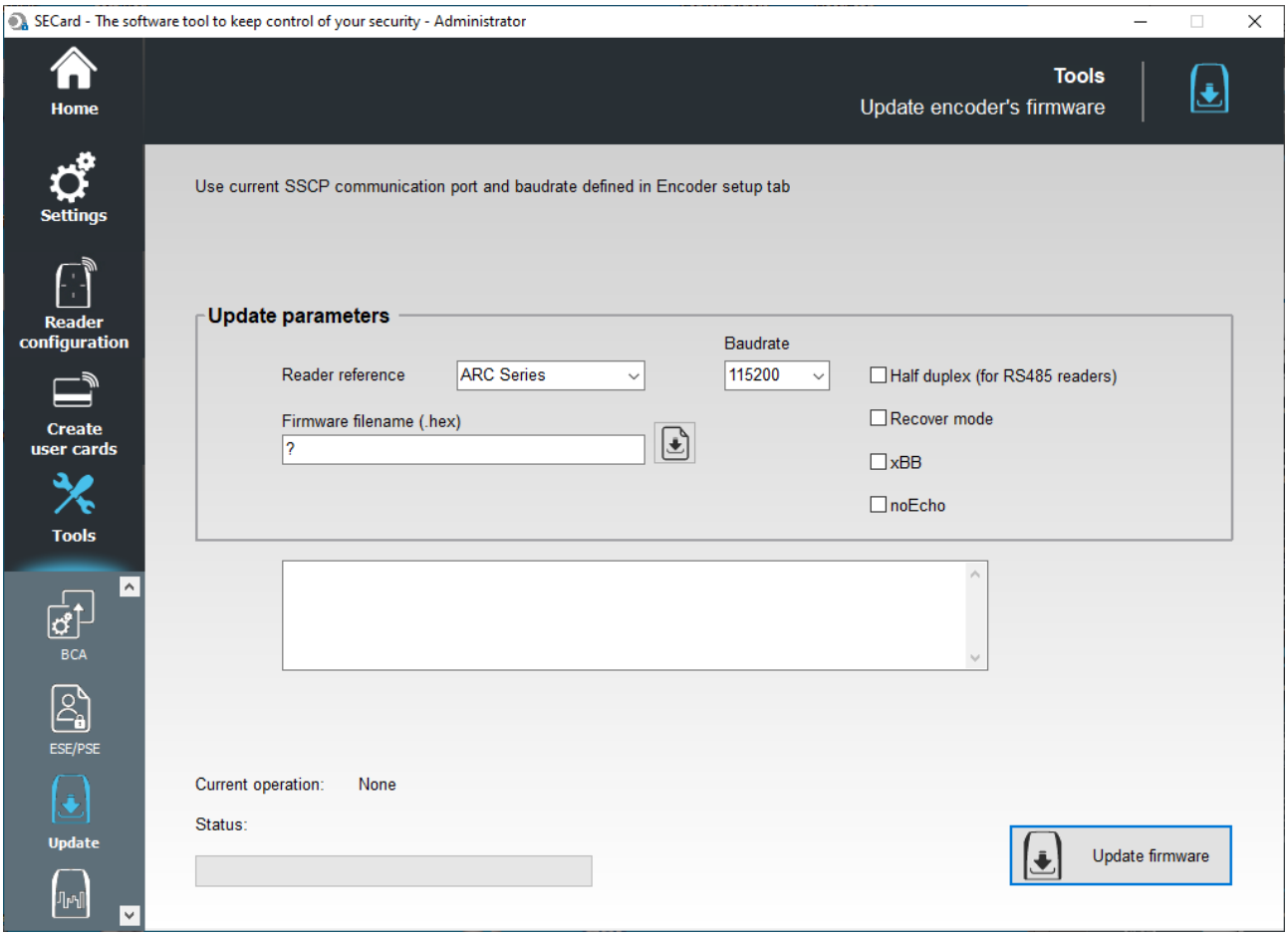
Select the ".ese" configuration file to import, and assign a new ".pse" name.

New PSE file passwords

It is necessary to enter Administrator, Power User and User passwords.

Note: to show passwords, check the "Show passwords" before assigning the first password.

VII. 9 - Update



Upgrade the firmware of readers **with a series connection**.

Warning: DLL FlashMagicARM, FlashMagicARMCortex and nrfutil.exe (present in the root folder SECard) are required.

The communication port is to be set in the Setting tab ***II.*** *1* - Encoder.

Update parameters

- Reader reference: choose the reader reference to upgrade.
- Baudrate: choose de baudrate of reprogramming.
- Firmware filename: download the firmware file.
- Half Duplex (RS485 readers).
- Recover mode: if programming failed, retry with “recover mode” checked (only for R/S 31 readers).
- xBB: check this case if the reader is a 5BB or 7BB protocol (firmware min Z05).
- noEcho: "removes" echo from reprog commands and therefore greatly reduces reprog time.

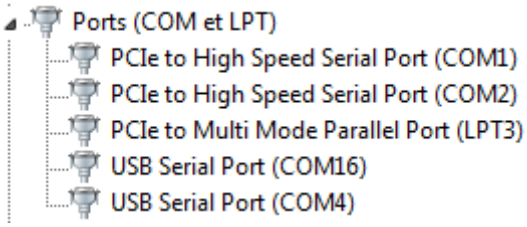
When all parameters are filled, power on the reader and click the Update button:

- while the LED blinks orange for serial readers
- at any time for TTL readers

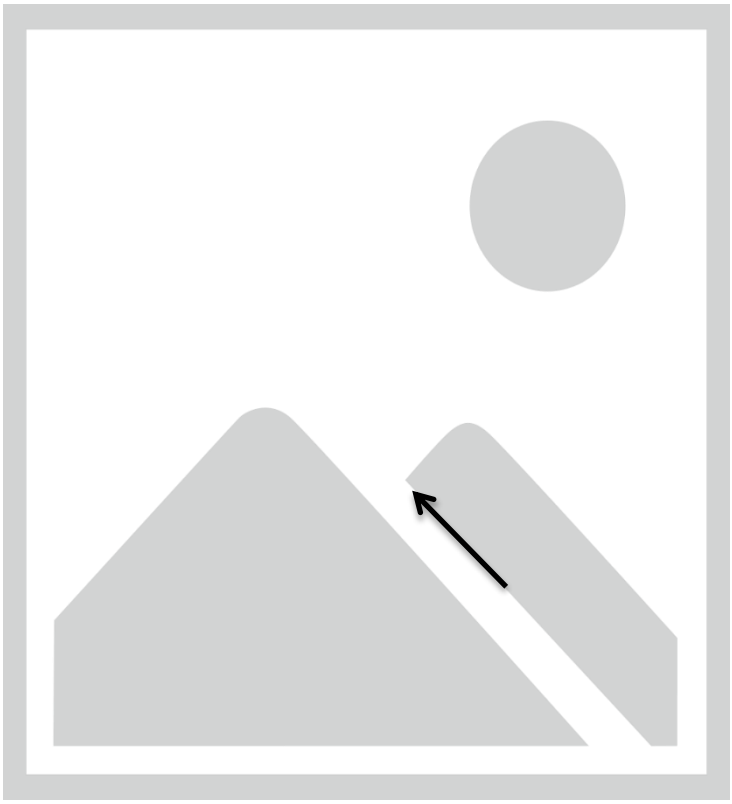
Note: for RS485 readers, use a fast interface (by default, baudrate set to 38400).

Update a read/write reader: example ARCW33APH57AA

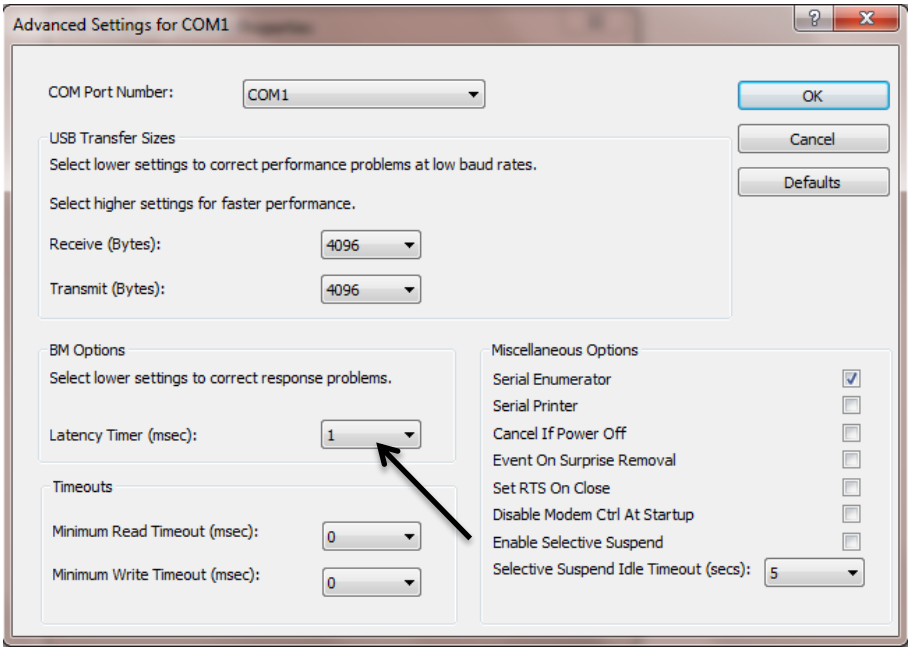
Communication port setting for RS485/USB converter:



Double click on the good COM port number.



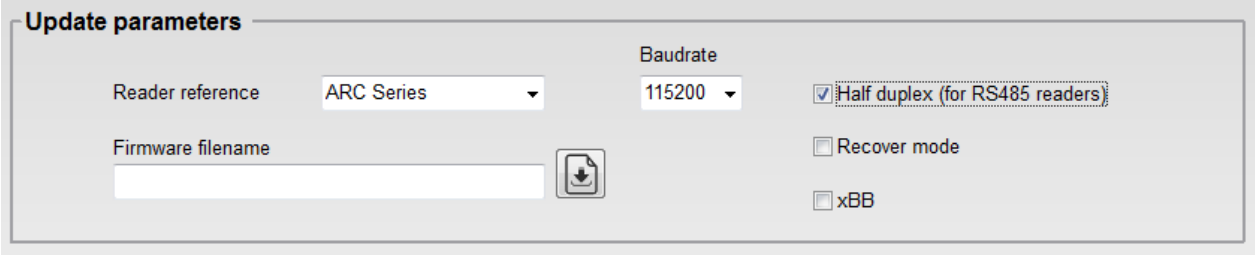
Open Advanced…



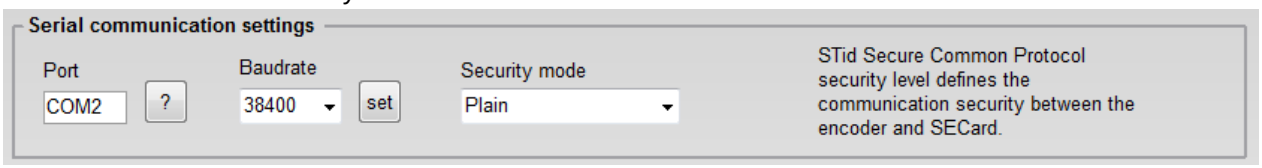
Put Latency on “1”

Update a read/write reader: example ARC-W33-A-PH5/7AA

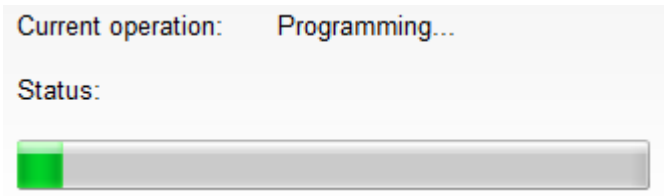
1- Select ARC series + Half Duplex + Load the firmware

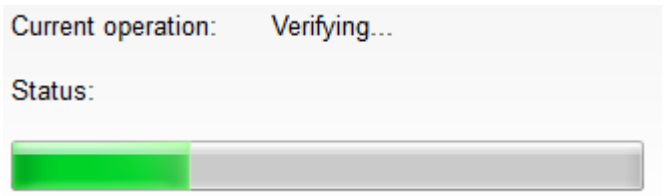


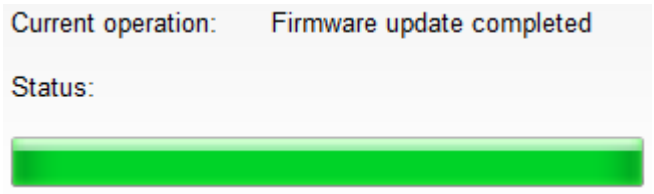
2- Configure the COM port
Note: with W reader you can use CTRL + ?



3- Click on Update Firmware, the LED reader light white (for ARC1/ARC1S the color LED is not define)

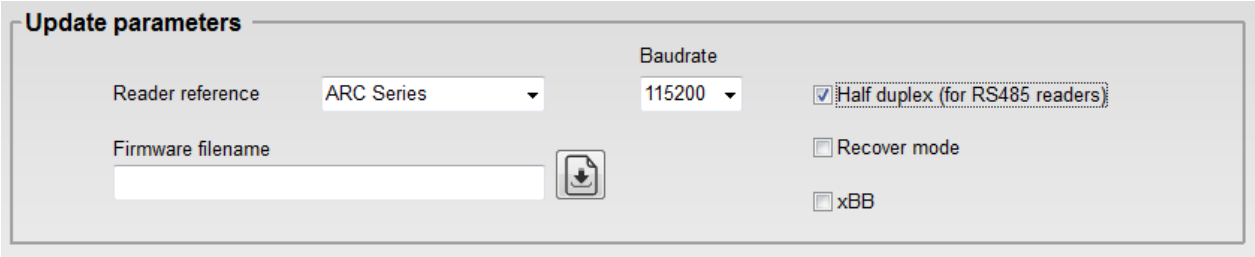






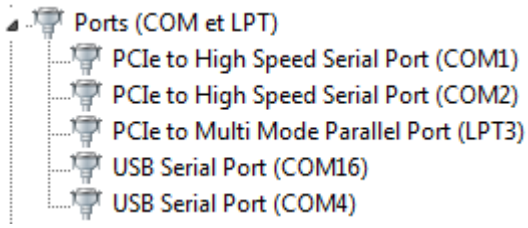
Update a read only serial reader: example ARC-R33-A-PH5/7AB

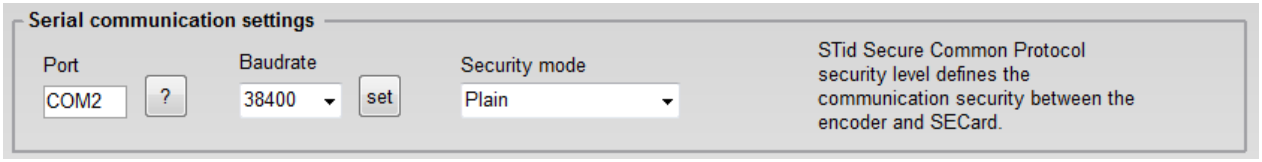
1- Select ARC Series + Half Duplex + Load the firmware



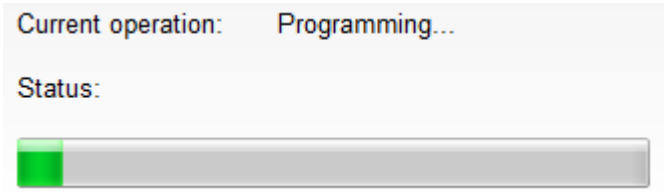
2- Configure the COM port at 38400 baud

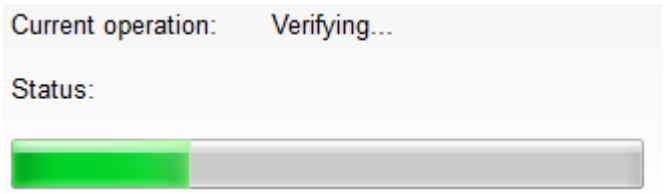
Note: with R reader search the com port number on your list:

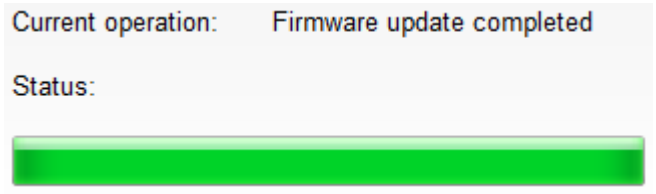




3- Power on the reader and click on Update Firmware while the LED blinks orange.

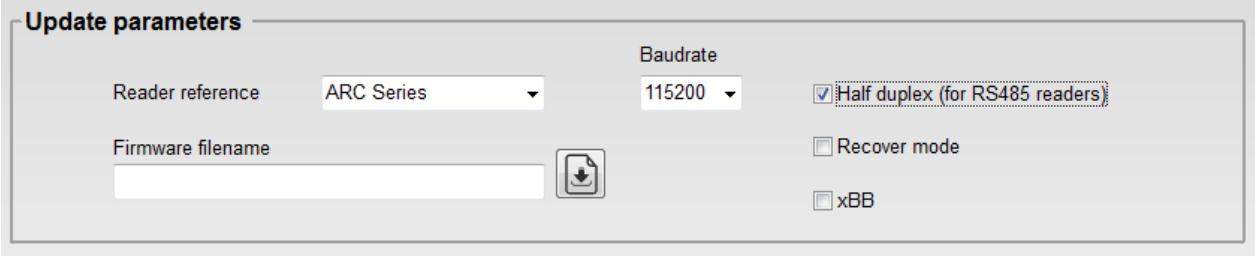






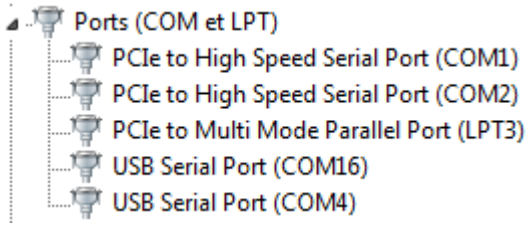
Update a read only TTL reader: example ARC-R31-A-PH5/2b

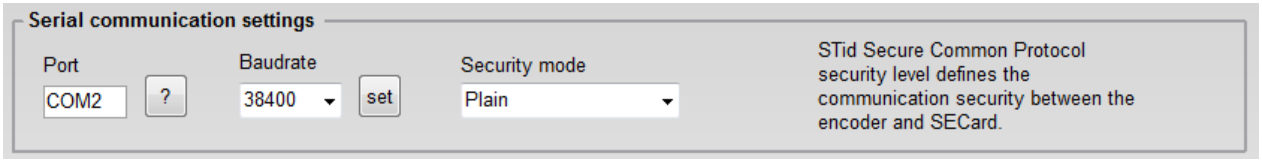
1- Select ARC Series + Half Duplex (the TTL reader are update by the RS485 serial link) + Load the firmware



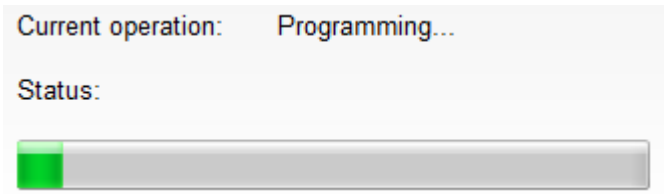
2- Configure the COM port at 38400 baud

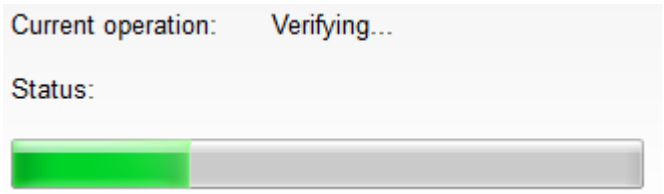
Note: with R reader search the com port number on your list:

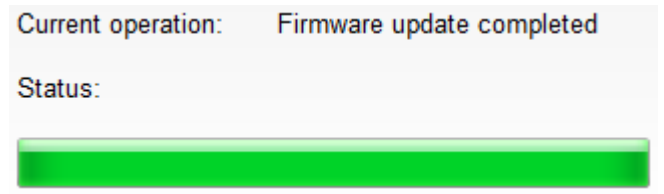




3- Click on Update Firmware.

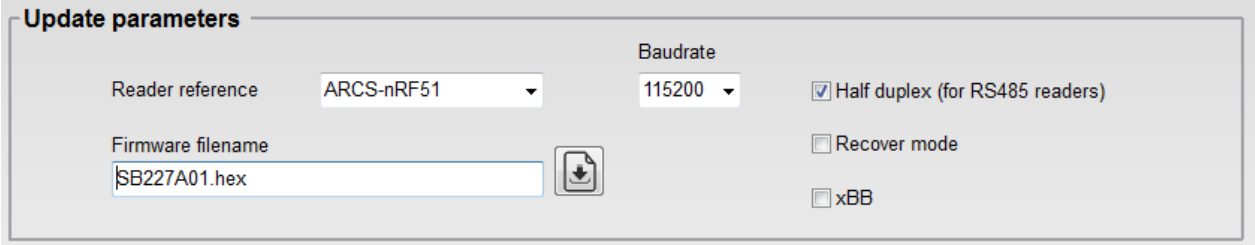




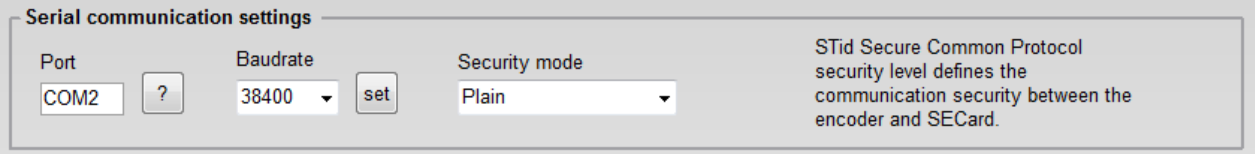


Update the BTSmart chip: example with ARCS-R31-A-BT1/xx

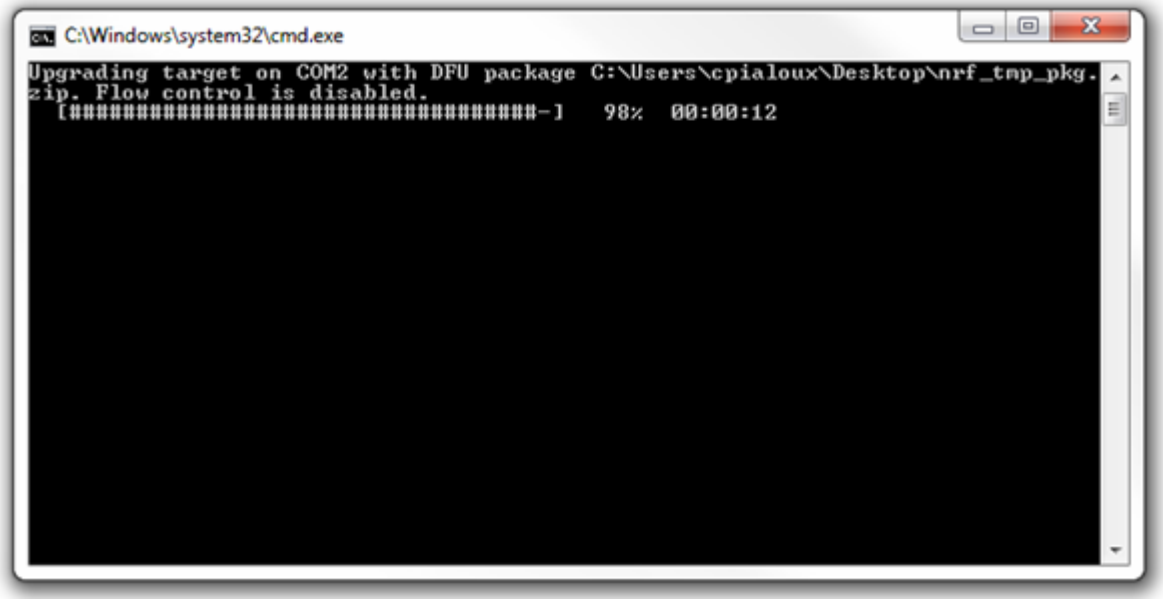
1- Select ARCS-nRF51 + Half Duplex (the TTL reader are update by the RS485 serial link) + Load the firmware

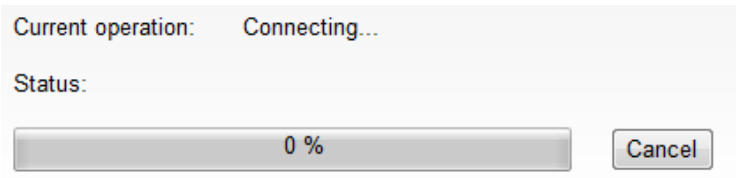


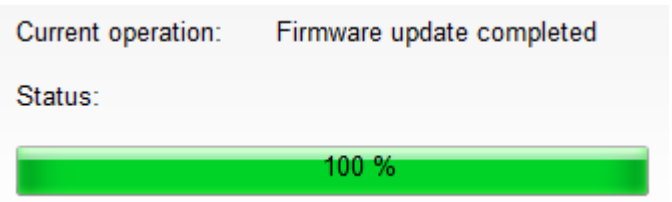
2- Configure the COM port at 38400 baud



3- Click on Update Firmware.
A DOS Windows will open:

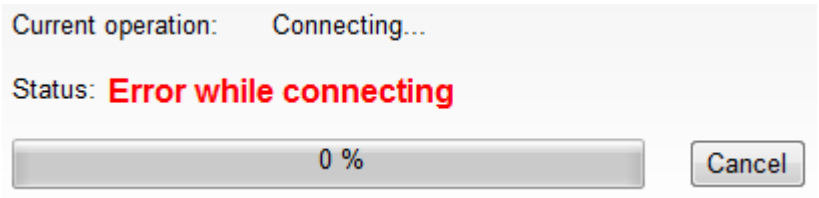






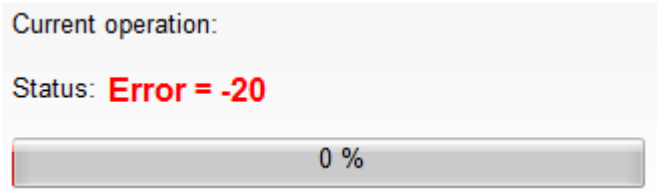
Update error message

❖



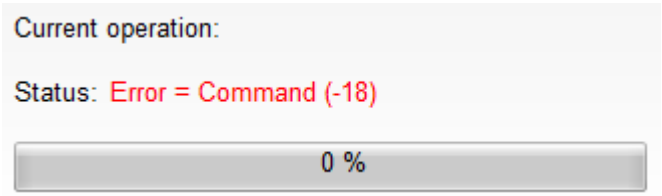
- ❖ Check the COM port number
- ❖ Check the Baudrate
- ❖ Click on Update while the LED blinks orange for serial reader

❖ During update if connection is break or power is off you have the message:



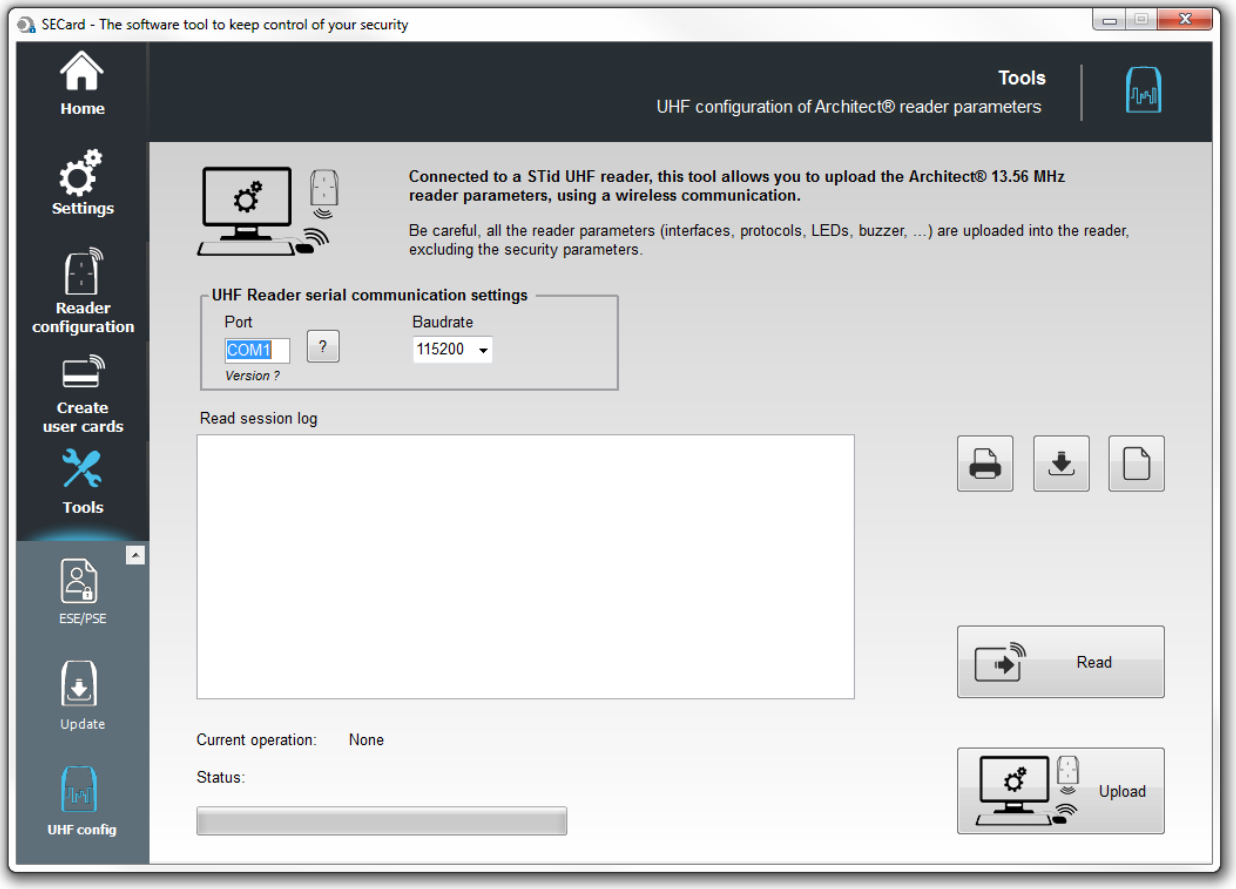
In this case you must power off the reader, select Recover mode, power on the reader and click on update firmware

❖



- ❖ Check if the DLL FlashMagicARM and/or FlashMagicARMCortex are present in the root folder SECard.

VII. 10 - UHF config



Read / write reader parameters of the current configuration in the UHF chip of ARC reader.

No key or any security is managed by this feature.

The tool uses the UHF write key filled in reader parameters to securely write the memory chip.

	Print user's operations.
	Save user's operations.
	Clear user's operations.

Enter the communication port and baudrate of UHF reader.

Warning

The read / write operations of the ARC UHF chip can only be done at power off, and with a UHF STid reader.

When the reader is power on, the UHF chip is automatically desactivate.

SECARD

USER MANUAL

Part 2: Technical

www.stid-security.com

T1 - SECard configurable readers

T1.1 - SCB configurable

SECard has a mode for creating SCB card (Secured Configuration Badge).
With "*SCB*" cards we can configure according to reader security settings, all Architect® and WAL read only STid readers.

Reference type: ARCS-**R**3x-X/BT1-xx or ARCS-**S**3x-X/BT1-xx

T1.2 - OCB configurable

SECard has a mode for creating OCB card (osdp™ Configuration Badge).
With "O*CB*" cards we can configure according to reader security settings, all Architect® and WAL osdp™ STid readers.

Reference type: ARCS-W33-x/BT1-**7OS** firmware Z05 min

T1.3 - SCB R/W configurable

SECard has a mode for creating SCB R/W card.
With " SCB R/W " cards we can configure according to reader security settings, read and write Bluetooth® Architect® STid readers.

Reference type: ARCS-W33-x/BT1-**7AA**

T2 - About readers

T2.1 - Powering up read only reader

At power up the reader enters an initialization phase:

1) Activating LED white and activates buzzer for 100 ms.

2) Activating LED and buzzer according the code to indicate reader type and firmware version.

3) LED is blinking 20 times (waiting for an update). **Only available for RS232, RS485 and USB readers**.

4) For ARCS Blue only: Activating white fixed LED during Bluetooth® initialization.

Firmware version is denoted by the following color codes:

Red = +10
Orange = +5
Green = +1
Firmware version must match with the one written on the label on the back of the reader.

Reader type is indicated by the buzzer following the code:

Long Beep = +5
Short Beep = +1

By adding beep heard (ex.1 long + 1 short = 6) the type of reader is obtained according to the table below:

Beep sum	Reader Type
1	R31/103 & Reader+INT-R33F/103
2	R31/PH1 only ARC1
3	R31/PH5 & R31/PH1 & Reader+INT-R33F/PH5
4	S31/PH5 & Reader+INT-S33F/PH5
5	Reader +INT-R33-E/PH5
6	R32/PH5 & R35/PH5 & R33/PH5
7	S32/PH5 & S35/PH5 & S33/PH5
8	Reader +INT-E-7AA/7AB
9	R33/PH1 only ARC1

T2.2 - Readers configuration

❖ R31/103 readers can only retrieve configuration from SCB after the initialization phase. So, you have to turn off reader, present a SCB, and turn the power on.
Other readers retrieve configuration without the need to restart.

To point out that reader successfully gets settings from SCB, reader beeps 5 times and LED is blinking quickly.

Reader give some information about retrieving settings from SCB:

- If the SCB version is greater than the SCB version defined by the firmware:
  ➔ LED is flashing red and buzzer is activated for 1 second.

- If the SCB version is compatible with the SCB version defined by the firmware:
  ➔ LED is flashing green and buzzer is quickly emitting 5 beeps.

❖ SE8/SE8M
If an old SCB/OCB that does not activate 125 kHz is presented in front of a reader equipped with an SE8M, the reader will operate normally at 13.56 MHz.

If a reader already has an old configuration and an SE8M is then connected to the reader, the SE8M will not work until a new SCB/OCB is presented in front of the reader.

If a reader equipped with an SE8M receives an SCB/OCB with activation of an SE8, the 125kHz of the SE8M will not be activated. Same operation, if a reader equipped with an SE8 receives a configuration for an SE8M. ➔The reader will flash red 3 times to indicate that the wrong type of reader has been activated by the SCB/OCB. The 13.56 MHz part will be functional.

T2.3 - ARC1 reader

❖ Specific reference ARC1-R31-A/PH1-xx and ARC1-R31-B/PH1-xx are able to read:

- MIFARE® Classic - Chip serial number or private Id
- MIFARE Plus® - Only chip serial number
- MIFARE® DESFire® EV1 - Only chip serial number
- MIFARE Ultralight® C - Only chip serial number
- CPS3 - Chip serial number or private Id contained in an Elementary File
- ISO14443-3B - Chip serial number PUPI

❖ Other ARC1 references read the same chip than other readers.

Note:
ARC One reader is configured as an ARC reader except in these three cases:

- If the Pulse mode is selected, the ARC1's LED will be fixed on the selected color.

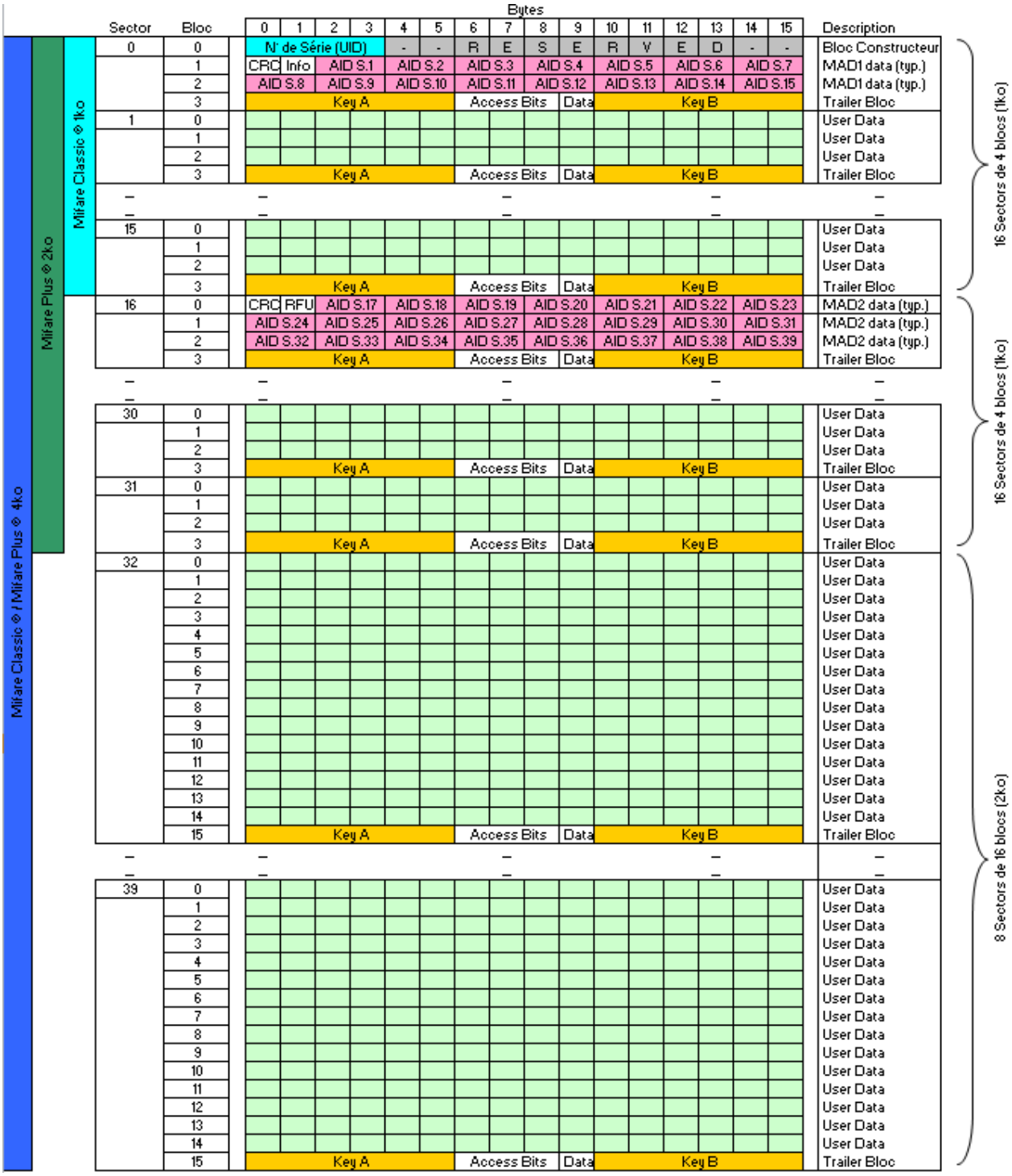
- If the ECO mode is selected, only the Scan time will be impacted (no impact on the LED brightness).

- If Biometric, Keypad and/or Touch Screen options are activated, they will not be taken into account.

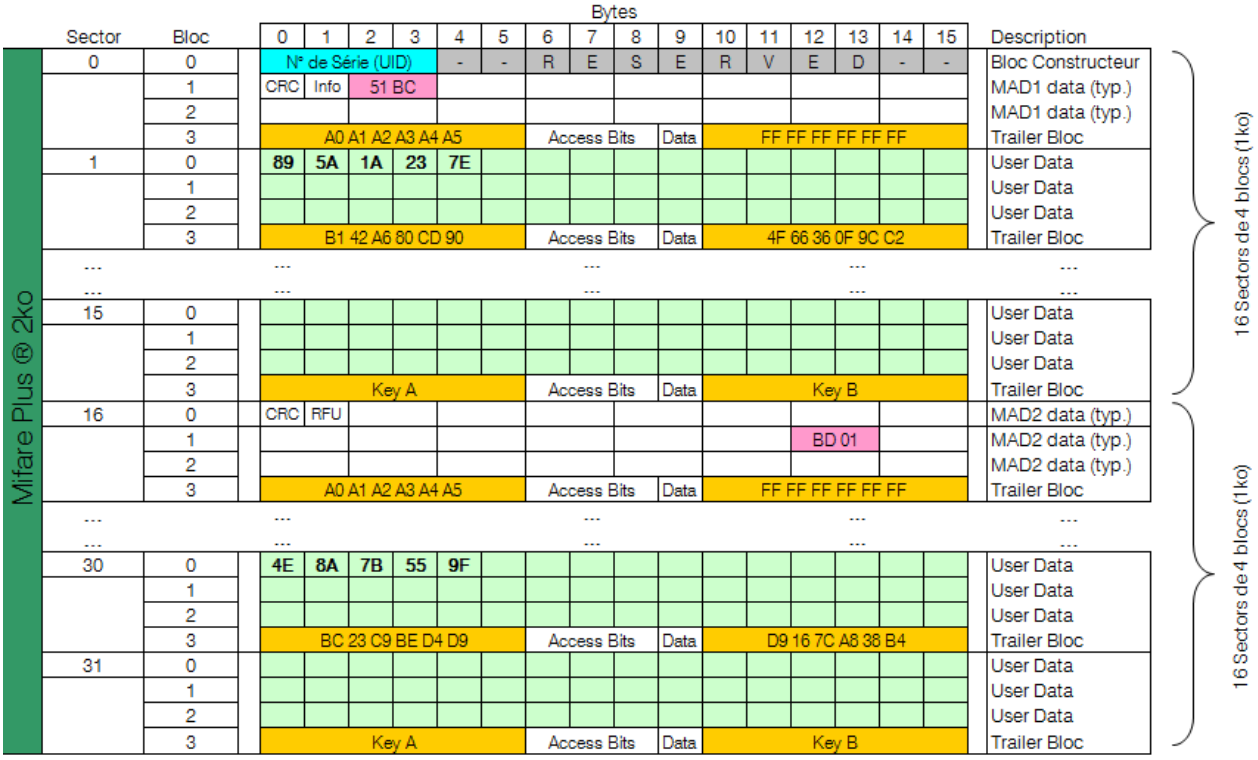
T3 - About RFID chips

T3.1 - MIFARE® Classic and MIFARE Plus® memories mapping

Global memory map



Example of partitioned memory: MIFARE Plus® Level 1



In this case, MIFARE Plus® Level 1 chip contains two different encoded informations in sector 1 and 30, protected by two different keys.

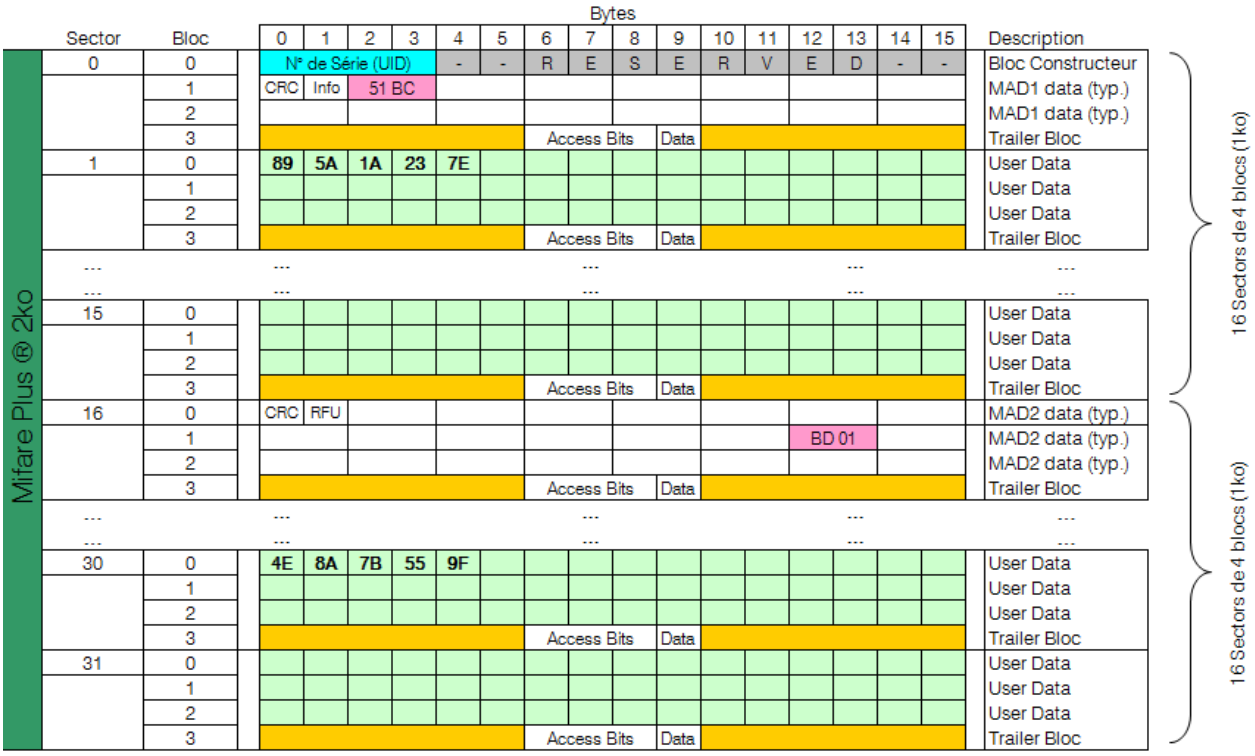
Each information is indexed in MAD at their respective location.

- ✓ Key A MAD: « *A0 A1 A2 A3 A4 A5* »
- ✓ Key B MAD: « *FF FF FF FF FF FF* »

- ✓ Sector 1 Key A: « B1 42 A6 80 CD 90 »
- ✓ Sector 2 Key B: « 4F 66 36 0F 9C C2 »

- ✓ Sector 30 Key A: « BC 23 C9 BE D4 D9 »
- ✓ Sector 30 Key B: « D9 16 7C A8 38 B4 »

Example of partitioned memory: MIFARE Plus® Level 3



In this case, MIFARE Plus® Level 3 chip contains two different encoded informations in sector 1 and 30, protected by two different keys.

Level 3 *AES* keys are not stored in the 4th bloc of each sector, but in a specific memory area.

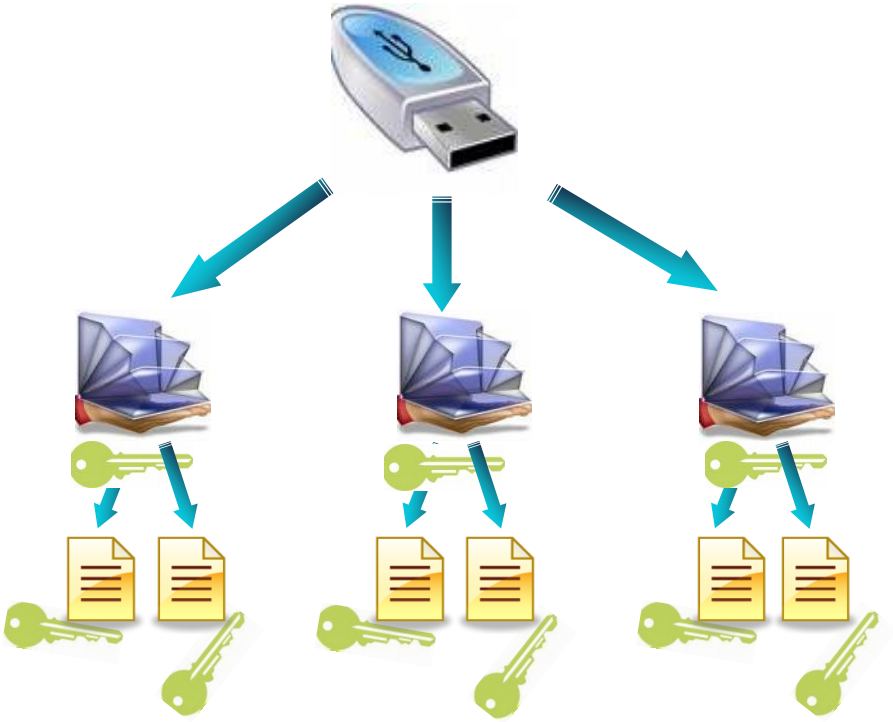
- ✓ Key A *AES* MAD: « *A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7* »
- ✓ Key B *AES* MAD: « *FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF* »

- ✓ Sector 1 AES Key A: « 11 10 8F 86 3E EA 98 5E CB 0C 4D 91 5E 0A 95 24 »
- ✓ Sector 1 AES Key B: « 9B E4 90 91 D7 45 B7 4A 7C 25 80 D3 52 5C 2D 6E»

- ✓ Sector 30 AES Key A: « 9A 55 AC 3F F7 AB 1C F5 BF 20 E6 73 60 29 F0 16 »
- ✓ Sector 30 AES Key B: « AA 20 40 AB FC 16 E2 49 BE FE 3F B3 42 5E 59 BE »

T3.2 - MIFARE® DESFire® and MIFARE® DESFire® EV1/2/3 chips memory mapping

Global memory mapping



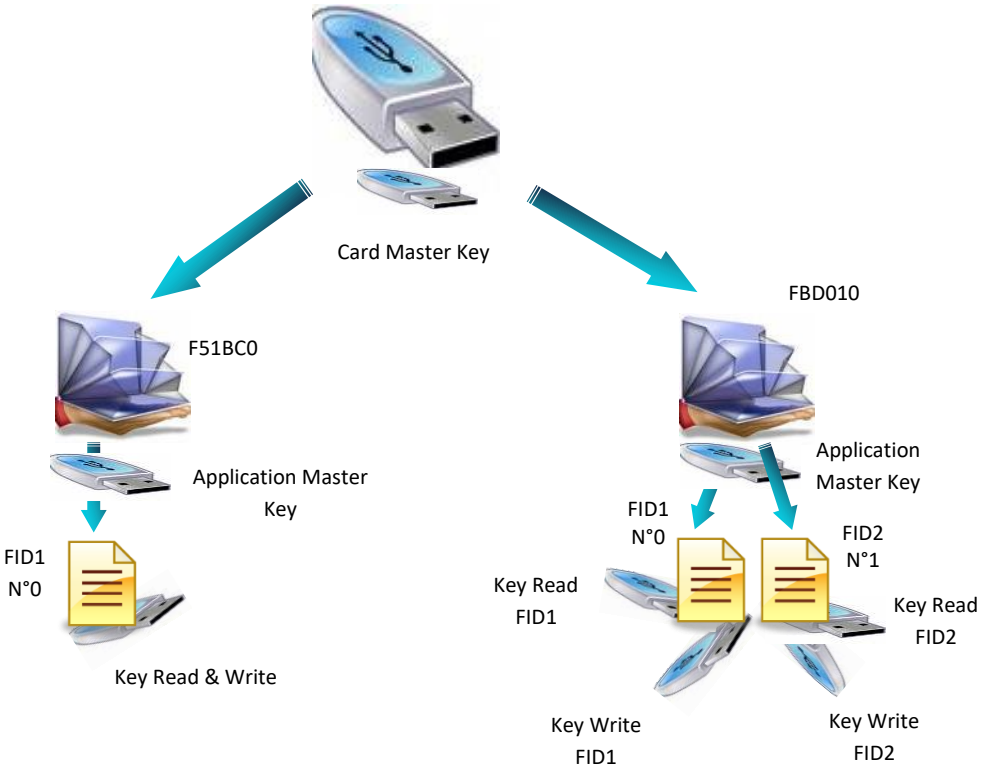
→ One root application.

→ Up to 28 applications.

→ Up to 32 files per application.

→ Up to 14 keys per application. Independent use for each file. (SECard use the maximum, 14 keys per application).

Example of partitioned memory



T3.3 - MIFARE Ultralight® and Ultralight® C memories mapping

Global memory mapping

			Bytes				
			0	1	2	3	Pages
Mifare UltraLight C ®	Mifare UltraLight ®	Chip serial Number 7 bytes	CSN0	CSN1	CSN2	BCC0	0
			CSN3	CSN4	CSN5	CSN6	1
		Internal Lock bytes	BCC1	INTERNAL	LOCK0	LOCK1	2
		OTP	OTP0	OTP1	OTP2	OTP3	3
		Data Read / Write	Data0	Data1	Data2	Data3	4
			...	...	...	...	...
			...	...	...	Data47	15
			Data48	Data49	...	...	16
			...	...	...	...	17
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	Data142	Data143	39
		Lock bytes Auth. Configuration Counter	LOCK / AUTH / COUNTER				40-43
		Security Key	3DES AUTHENTICATION KEY				44-47

- ✓ MIFARE Ultralight® and Ultralight® C memory is divided into *Pages* of 4 bytes each.
- ✓ Read/Write part starts at *Page* 4. *Page* 3 is an OTP zone (One Time Programming). It can be encoded only once.
- ✓ Locking write operations or blocking of authentication (Lock bytes) are always made from a age to the last.

  Example: Locking write operations or blocking of authentication (Lock bytes) are always made from a page to the last.

Example of partitioned memory

Mifare UltraLight C ®		Bytes 0	1	2	3	Pages
	Chip serial Number 7 bytes	CSN0	CSN1	CSN2	BCC0	0
		CSN3	CSN4	CSN5	CSN6	1
	Internal Lock bytes	BCC1	INTERNAL	LOCK0	LOCK1	2
	OTP	OTP0	OTP1	OTP2	OTP3	3
	Data Read / Write	0xFA	0x01	0x5B	0x9E	4
		...	...	...	...	...
		...	...	...	...	...
		...	...	...	...	...
		...	...	...	...	...
		...	...	...	...	...
		...	...	...	...	...
		...	...	...	...	...
		0x8F	0x61	0x40	0x1E	20
		...	...	...	...	...
		...	...	...	...	...
		...	...	...	...	...
		...	...	...	...	...
		...	...	...	...	39
	Lock bytes Auth. Configuration Counter	LOCK / AUTH / COUNTER				40-43
	Security Key	3DES AUTHENTICATION KEY				44-47

Unprotected

Protected

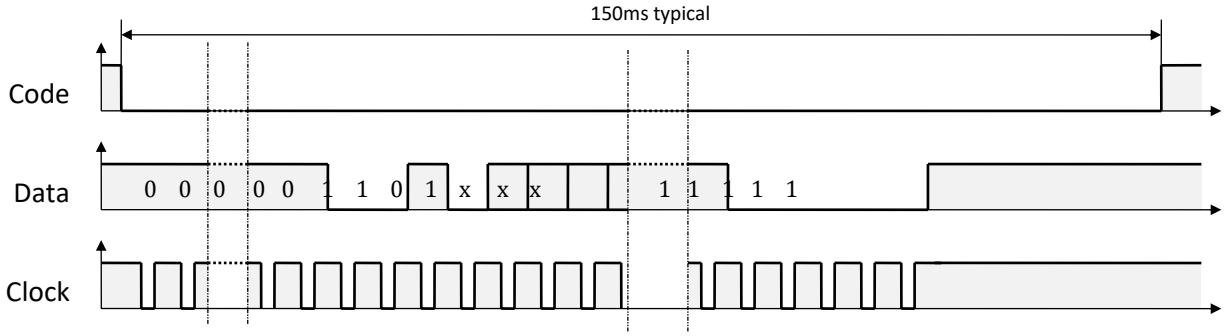
In the case above, the area from page 4 to page 41 included, is not read protected and do not require authentication with the 3DES key. The private code located in Page 4 will be readable without any constraint.

However, the area from Page 42 to Page 47 is protected. The private code located in Page 42 can only be read after authentication with the 3DES key.

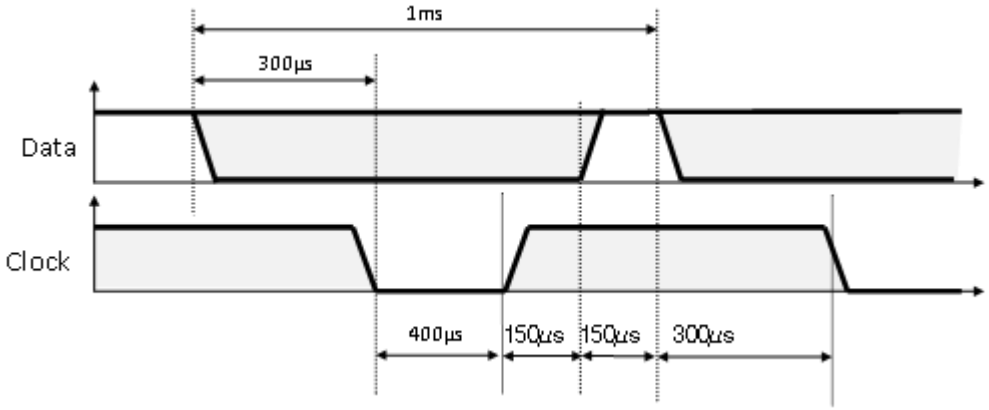
T4 - About TTL communication protocols

T4.1 - ISO2 Clock&Data protocol

Chronograms



Clock details



Message structure (*2B & 2H)*

Leading zeroes	*Start Sentinel*	*Datas*	*End Sentinel*	*LRC*	*Trailing zeroes*

Message description

The frame is made of a first series of 16 zero followed by synchronization characters of 5 bits (4 bits, LSB first, plus 1 parity bit). It ends the frame with trailing zero without a clock. The message consists of the following:

Start Sentinel:	1 character 1011b (0x0B) – parity bit 0. Transmission 1101 0
Data:	According to ID type: 13 or 10 decimal characters
End Sentinel:	1 character 1111b (0x0F) - parity bit 1. Transmission 1111 1
LRC:	1 control character, which is the « XOR » of all characters.

2B protocol (13 characters)

Reading an ID of 5 bytes (40 bits) and convert to decimal.

Variant	Decoding	Full frame of 112 bits	Values
2B	*Decimal (BCD)*	*13 characters*	*0 to 9*

Example:

For a hexadecimal user code of « 0x187E775A7F », the output code will be: « *0105200966271* ».
Frame sent by reader will be:

000...	1101 0	0000 1	1000 0	0000 1	1010 1	. . . .	0110 1	0100 0	1110 0	1000 0	1111 1	1111 1	000...
	B	*0*	*1*	*0*	*5*	*2 0 09 6*	*6*	*2*	*7*	*1*	*F*	*F*	
Zero	*S.S*	*Char.1*	*Char.2*	*Char.3*	*Char.4*	*Char ….*	*Char.10*	*Char.11*	*Char.12*	*Char.13*	*E.S*	*LRC*	*Zero*

2H protocol (10 characters)

Reading an ID of 4 bytes (32 bits) and convert to decimal.

Variant	Decoding	Full frame of 97 bits	Values
2H	*Decimal (BCD)*	*10 characters*	*0 to 9*

Example:

For a hexadecimal user code of « 0x06432F1F», the output code will be: « *0105066271* ».

Frame sent by reader will be:

000...	1101 0	0000 1	1000 0	0000 1	1010 1	. . . .	0110 1	0100 0	1110 0	1000 0	1111 1	0010 1	000...
	B	*0*	*1*	*0*	*5*	*0 6*	*6*	*2*	*7*	*1*	*F*	*4*	
Zero	*S.S*	*Char .1*	*Char .2*	*Char .3*	*Char .4*	*Char ….*	*Char .7*	*Char .8*	*Char .9*	*Char .10*	*E.S*	*LRC*	*Zero*

In the case of 5 bytes (40 bits) ID, reader will truncate the MSB byte (8 bits) before decimal conversion.

Specific reading for 125kHz identifier

Detection mode UID: 5-byte reading then converted to decimal and truncated to 10-characters

Detection mode Private ID: 5-byte reading then truncates to 4 and converted to decimal

2S Crosspoint protocol (10 characters)

Only available for low frequency part (125 kHz) of hybrid reader (BF5)

Variant	Decoding	Full frame of 112 bits	Values
2S	*Decimal (BCD)*	*9-10 characters*	*0 à 9*

BCD characters in frame are computed using:

- consider 3 Less Significant Byte.
- converting these hexadecimal byte into binary.
- inverting each bits of each byte

b7	b6	b5	b4	b3	b2	b1	b0		b7	b6	b5	b4	b3	b2	b1	b0		b7	b6	b5	b4	b3	b2	b1	b0
b6	b4	b7	b5	b1	b3	b0	b2		b6	b4	b7	b5	b5	b3	b0	b6		b1	b3	b1	b2	b4	b2	b0	b7
0	1	0	0	0	0	0	1		1	0	1	0	0	1	0	1		1	1	0	1	1	0	1	1
1	0	0	0	0	0	1	0		0	0	1	1	0	1	1	1		0	0	1	0	1	1	1	1

Byte [2] Byte [1] Byte [0]

- Converting binary value into hexadecimal then in BCD.

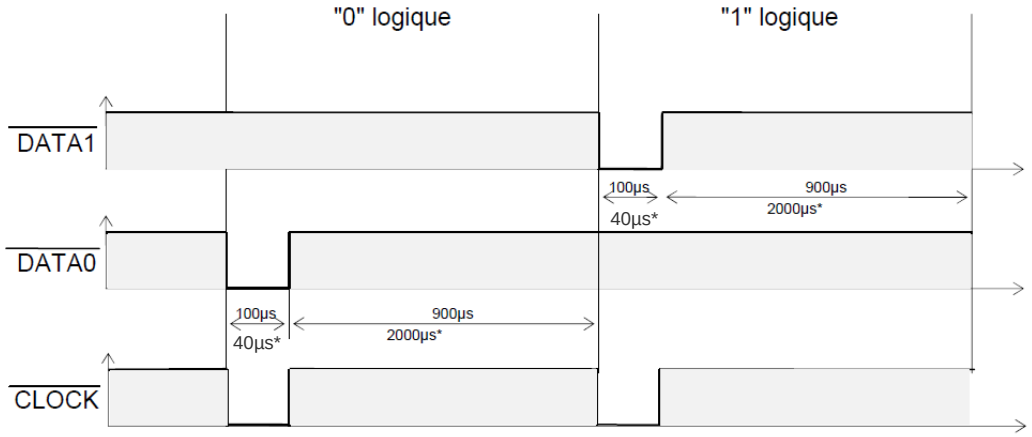
Example

For an id « 0x0A0041A5DB»:

SOURCE	41	A5	DB	0100 0001	1010 0101	1101 1011
Coding	82	37	2F	1000 0010	0011 0111	0010 1111

T4.2 - Wiegand Protocol

Chronograms



* variant 3i timings

Wiegand 3i protocol

Variant	Decoding	24 bits data	Values
3i	*Hexadecimal*	*6 characters*	*0 to F*

Message structure

Bit 1	Bit 2 ... Bit 25	Bit 26
Even parity from bit 2 to bit 13	*Data (24 bits)*	*Odd parity from bit 4 to bit 25*

Message description

The frame consists of 26 bits as follows:

First parity: *1 bit even parity of next 12 bit*
Data: *6 hexadecimal characters " MSB first "*
Last parity: *1 bit odd parity of previous 12 bits*

Example: for the hexadecimal code « *0x0FC350* », frame sent will be:

0	0000	1111	1100	0011	0101	0000	1
	0	*F*	*C*	*3*	*5*	*0*	
Parity	*Char.1*	*Char.2*	*Char.3*	*Char.4*	*Char.5*	*Char.6*	*Parity*

Note:
A site code is generally associated with the third octet (byte [2]). In the example above, it is 0x0F or 15 in decimal (up to 255 decimal - 0xFF in hexadecimal).

The card code is generally associated with the first and second byte (byte [1] and byte [0]). In the example above, it is 0xC350, 50000 in decimal (decimal max is 65535 - 0xFFFF in hexadecimal).

Wiegand 3CB protocol

Bit 1 ... Bit 40	Bit 41... Bit 44
Data « MSB first »	*LRC*

Message description

The frame consists of 44 bits as follows:

Data: 10 *hexadecimal characters « MSB first »*
LRC : *1 control char , all characters « XORed»*

Example: for the hexadecimal code « *0x01001950C3* », frame sent will be:

0000	0001	0000	0000	0001	1001	0101	0000	1100	0011	0011
0	*1*	*0*	*0*	*1*	*9*	*5*	*0*	*C*	*3*	*3*
Char.1	*Char.2*	*Char.3*	*Char.4*	*Char.5*	*Char.6*	*Char.7*	*Char.8*	*Char.9*	*Char.10*	*LRC*

Wiegand 3CA protocol

Bit 1 ... Bit 36	Bit 37... Bit 36
Data « MSB first »	*LRC*

Message description

The frame consists of 36 bits as follows:

Data: *8 hexadecimal characters « MSB first » (32 bits)*
LRC: *1 control char, all characters « XORed »*

Example: for the hexadecimal code « *0x001950C3* », the frame sent will be:

0000	0000	0001	1001	0101	0000	1100	0011	0010
0	*0*	*1*	*9*	*5*	*0*	*C*	*3*	*2*
Char.1	*Char.2*	*Char.3*	*Char.4*	*Char.5*	*Char.6*	*Char.7*	*Char.8*	*LRC*

Note: in the case of 5 bytes (40 bits) ID, reader will truncate the MSB byte (8 bits) before decimal conversion.

Wiegand 3LA protocol

Same as « *Wiegand 3CA* » WITHOUT LRC.

Wiegand 3LB protocol

Same as « *Wiegand 3CB* » WITHOUT LRC.

Wiegand 3T protocol

Bit 1 … Bit 8	Bit 9 … Bit 64	Bit 65… Bit 68
Chip type	*Data « MSB first »*	*LRC*

The frame consists of 68 bits as follows:

RFId Chip Type: *1byte (8 bits)*
Data: *14 hexadecimal characters « MSByte first » (56 bits)*
LRC: *1 control character, all characters (4 bits) « XORed»*

« *Chip type*» indicates the type of chip read by the reader:

Value	Chip
0x40	MIFARE® Classic
0x41	MIFARE® DESFire® / DESFire® EV1 & EV2 & EV3
0x42	125 kHz (EM/Nedap/HID)
0x43	MIFARE Ultralight® / Ultralight® C
0x44	MIFARE Plus® Level 0 / Level 2 / Level 3
0x45	PUPI ISO 14443-3B
0x46	CPS3
0x47	Moneo
0x48	AMC (Citizen Multiservice Application)
0x4A	3,25 MHz (only standard range
0x4E	HCE
0x50	Undefined chip
0x60	BLE (Bluetooth®)
0x70	Wrench
0x80	QR Code (en mode UID)

Example for MIFARE® DESFire® chip:

For the hexadecimal code « 0x80AF01001950C3 », frame sent will be 0x4180AF01001950C3 B.

Example for MIFARE® Classic chip:

For the hexadecimal code « 0xA771FE4C », frame sent will be 0x40 000000A771FE4C 6.

Note:

- ✓ It is not possible to force site code in « UID » mode.
- ✓ In « PrivateID » mode, there is no Chip type sent. Only data (8 bytes) are sent.

Wiegand 3Eb Protocol

Variant	Decoding	32 bits data	Values
34 bits	*Hexadecimal*	*8 characters*	*0 to F*

Message structure

Bit 1	Bit 2 ... Bit 33	Bit 34
Even parity from bit 2 to bit 17	*Data (32 bits)*	*Odd parity from bit 18 to bit 33*

Message description

The frame consists of 34 bits as follows:

First parity: *1 bit even parity of next 16 bit*
Data: *8 hexadecimal characters " MSB first "*
Last parity: *1 bit odd parity of previous 16 bits*

Wiegand 3W Protocol

Variant	Decoding	32 bits data	Values
35 bits	*Hexadecimal*	*8 characters*	*0 to F*

Message structure

Bit 1-2	Bit 3 ... Bit 34	Bit 35
2 Even parity	*Data (32 bits)*	*Odd parity 5*

Wiegand 3V Protocol

Variant	Decoding	32 bits data	Values
37 bits	*Hexadecimal*	*8 characters*	*0 to F*

Message structure

Bit 1	Bit 2 ... Bit 36	Bit 37
Even parity from bit 2 to bit 19	*Data (35 bits)*	*Odd parity from bit 19 to bit 36*

Message description

The frame consists of 37 bits as follows:

First parity: *1 bit even parity of next 18 bit*
Data: 9 *hexadecimal characters " MSB first "*
Last parity: *1 bit odd parity of previous 18 bits*

Exemple

For hexadecimal code« *0x 0F3129DD3B* », frame is :

1	111	0011	0001	0010	1001	1101	1101	0011	1011	0
	7	*3*	*1*	*2*	*9*	*D*	*D*	*3*	*B*	
Parity	*Char.1*	*Char.2*	*Char.3*	*Char.4*	*Char.5*	*Char.6*	*Char.7*	*Char.8*	*Char.9*	*Parity*

T4.3 - Enciphered Wiegand protocol

The S31 readers send the enciphered information on a 128 bits Wiegand + 4 bits LRC (LRC in plain). The *AES* algorithm is used for this encryption AES key is that defined in “easy secure or Wiegand encryption AES key”, it must necessarily be different from 0xFF…FF.

Each frame is composed by a 12 bytes data packet, a random value coded on 2 bytes and a CRC-CCITT 16 bits (polynomial 0x1021, Initial value 0xFFFF).

If an ID value is more than 12 bytes, several frames will be emitted as shown below:

Data 12 bytes	***Random value 2 bytes***	***CRC 2 bytes***

Frame1 enciphered

Data 12 bytes	***Random value 2 bytes***	***CRC 2 bytes***

Frame 2 enciphered

Data 12 bytes	***Random value 2 bytes***	***CRC 2 bytes***

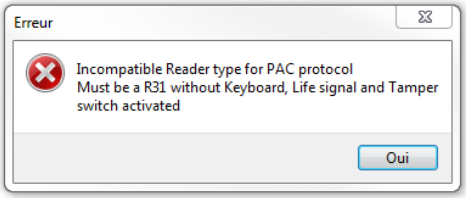
Frame 3 enciphered

T4.4 - PAC / PAC64 protocol

PAC/PAC64 protocols are available for read-only TTL readers (R31). There is no compatibility with the interfaces (INT or secure mode S31).

Several options are not supported in these protocols:

- No keypad mode.
- No management of life and tears signals.

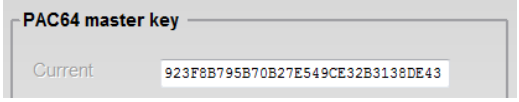


Protocole PAC

- Available for all types of chips.
- No authentication.
- Scramble output.
- 4-byte data transmitted on the Tx output of the reader.

Protocole PAC64

- Only available for DESFire® et Mobile ID.
- For UID DESFire: reading the UID after authentication with the card master key and then sending data obfuscated on the output Tx.
- For Private ID DESFire: read data based on SECard security principles and then send data obfuscated on the output Tx.
- For Mobile ID: read data based on SECard security principles and then send data obfuscated on the output Tx.
- The PAC64 key used for authentication and obfuscation is to be set in SECard:



- 7-byte data transmitted on the Tx output of the reader. Byte 8 is calculated by the protocol and corresponds to the encryptionindex.

T5 - Serial communication protocol

T5.1 - Unidirectional communication mode

In this mode, the data are sent plainly. The communication is made from the reader to the system.

LED and buzzer are managed by the reader through the configuration in the *SCB* card.

It is possible to configure the structure of the message sent by the reader through the box "*Serial configuration*" and with the following:

- ✓ No leading zero: Add on the frame leading zero (on start of frame).
- ✓ STX+ETX: Add STX (0x02) and ETX (0x03) on start and end of the frame.
- ✓ CR+LF: Carriage return option (0x0D + 0x0A)
- ✓ LRC: Checksum byte by XORing of all previously characters without the STX.
- ✓ ASCII: If this option is activated, the Data will be sent in ASCII mode.
- ✓ Base: Data sent in decimal or hexadecimal format.
- ✓ Baudrate: 9600, 19200, 38400, 57600 or 115200 bauds.

"Data" part is the identifier code read or keys reader Card or Key mode

1 byte	*X bytes**	*1 byte*	*1 byte*	*1 byte*	*1 byte*
STX	*Data**	*LRC*	*0x0D*	*0x0A*	*ETX*

**Concerning the keypad reader, refer to* *T6 - About keypad readers* T6 - About keypad readers

- ✓ Wrenching Signal: If the option is activated, and if the state on the input "*SW*" or of accelerometer changes, the reader will send the byte *0xAA*.

- ✓ Life signal: If the option *"Life signal"* is activated, the reader will send a byte every minute to indicate its presence:
  - Generic signal: 0x50
  - Specific signal LXS/MXS/ATX: 0x50
  - Specific signal LXE: 0x54
  - Specific signal MS: 0x52
  - Specific signal LXC: 0x55
  - Specific signal WAL: 0x56
  - Specific signal ARC: 0x61

Note:

- ✓ R33E/PH5 and S33E/PH5 readers are not addressable in this mode.
- ✓ The data size is doubled if the *ASCII* is activated.
- ✓ The field "*Size"* allows the modification of the data size sent by the reader.

For Prefix, Suffix, ID-Len and ID-TAG see SCB - Step 3 *Adding functionality 3.6*

T5.2 - Bidirectional communication mode

In this mode, the communication is done from the reader to the system for the transmission of the data and from the system to the reader for the LEDs and buzzer management.

In an idle state, the reader is going to manage the LEDs and buzzer according the configuration defined in the tab "*Default LED action*".

Maximum 2 readers on the same BUS is recommended.

When reading a valid code (depending on the configuration defined in the wizard SCB), it is transmitted to system by the reader. It is then possible at this time and for a period of 1.5s to command the buzzer and LED via the transmission of a frame of the system

Note: Sign, Enciphered and Sign AND Enciphered mode are accessible only with readers *S32E, S35E/PH5* and *S33E/PH5*.
At the powering and after configure reader with SCB, the reader initiates communication (depending on the mode) with the host. If an error occurs in the communication process, the initialization of the communication is restarted every minute.
In this mode, the communication is done according the STid *SSCP®* protocol. Consequently, it is possible to communicate in 4 different security modes:

- ✓ Plain
- ✓ Signed
- ✓ Encephered
- ✓ Signed and Encephered

✓ Plain

Data sent plainly

Complete frame sent by the reader

#02	Len	CTRL	CMD	Reserved	L_{out}	$Data_{out}$	CRC
1 byte	2 bytes	2 bytes	4 bytes	2 bytes	2 bytes	L_{out} bytes	2 bytes

Complete frame sent by the system

#02	Len	CTRL	ACK	L_{in}	$Data_{in}$	Status	CRC
1 byte	2 bytes	2 bytes	2 bytes	2 bytes	L_{in} bytes	2 bytes	2 bytes

✓ Signed

Data sent plainly and signed.
The signature algorithm used will be the reduced version of *HMAC-SHA-1*, i.e. the **first 10 bytes**).

Complete frame sent by the reader

#02	Len	CTRL	CMD	Reserved	L_{out}	$Data_{out}$	$HMAC\text{-}SHA\text{-}1_k$ (Commande)	CRC
1 byte	2 bytes	2 bytes	4 bytes	2 bytes	2 bytes	L_{out} bytes	10 bytes	2 bytes

Complete frame sent by the system

#02	Len	CTRL	ACK	L_{in}	$Data_{in}$	Status	Signature $HMAC\text{-}SHA\text{-}1_k$ (Réponse)	CRC
1 byte	2 bytes	2 bytes	2 bytes	2 bytes	L_{in} bytes	2 bytes	10 bytes	2 bytes

✓ **Enciphered**

Data sent enciphered.
The encryption algorithm used is *AES* using a 128 bits key

Complete frame sent by the reader

#02	Len	CTRL	C (Command)	..	C (Command) cont /end	Padding	Initialisation vector	CRC
1 byte	2 bytes	2 bytes	(k-1)*16 bytes	..	16-x bytes	X bytes	16 bytes	2 bytes

Complete frame sent by the system

#02	Len	CTRL	C (Respons)	..	C (Respons) cont /end	Padding	Initialisation vector	CRC
1 byte	2 bytes	2 bytes	(k-1)*16 bytes	..	16-x bytes	X bytes	16 bytes	2 bytes

✓ **Signed and enciphered**

Data sent signed and enciphered using the same algorithms described above.

Complete frame sent by the reader

#02	Len	CTRL	C (Command)	..	C (Command) cont/end	Padding	Initialisation vector	Signature	CRC
1 byte	2 bytes	2 bytes	(k-1)*16 bytes	..	16-x bytes	X bytes	16 bytes	10 bytes	2 bytes

Complete frame sent by the system

#02	Len	CTRL	C (Respons)	..	C (Respons) cont/end	Padding	Initialisation vector	Signature	CRC
1 byte	2 bytes	2 bytes	(k-1)*16 bytes	..	16-x bytes	X bytes	16 bytes	10 bytes	2 bytes

T5.2.1 Mutual authentication

The authentication and encryption communication system is based on two different session keys.

The two keys are generated during host / reader authentication from one random element and two known user keys for the reader and host.

A method for generating session keys ***(k_c, k_s)*** from user keys ***(K_c, K_s)*** therefore needs to defined (the user keys are used solely for generating session keys). This mechanism uses a specific encrypted dialogue for mutual authentication between the partners, before the session keys ***(k_c, k_s)*** are generated.
Where:

- ✓ ***k_s*** is the session key used for the *10-byte HMAC-SHA-1* signature algorithm
- ✓ ***k_c*** is the session key used for the *16-byte AES* cryptography algorithm
- ✓ ***K_s*** is the user key used to generate the *10-byte HMAC-SHA-1* signature key ***(k_s)***
- ✓ ***K_c*** is the user key used to generate the *16-byte AES* cryptography key ***(k_c)***

Warning

The default keys values are:

K_s = 0x FFFFFFFFFFFFFFFFFFFF

K_c = 0x FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

We recommend changing the default values to improve the security

The initialization of the mutual authentication is done by the reader when the field "*Security Mode*" is not "*Plain*". This procedure is described in the documentation of the protocol SSCP®:

- ✓ Spec_Protocole_5AA-7AA_MIFARE_GLOBAL_Vx.x.pdf

Please ask us for these documents.

T5.2.2 Message structure

The information transmitted by the host is formatted as follows:

#02	*Len*	*CTRL*	*CMD*	*Reserved*	*L_{out}*	*$Data_{out}$*	*CRC*
1 byte	2 bytes	2 bytes	4 bytes	2 bytes	2 bytes	L_{out} bytes	2 bytes

# 02	Start Of Frame (SOF) delimiter (on byte 02h)		
Len	Defines the length of the command to be sent (two bytes)		
CTRL	Two-byte word, with one byte that defines the serial link type used (RS485 or RS232) and one byte that defines the communication mode (plain text, encrypted, signed etc.…).		
	CTRL @	Defines the serial link type used (RS232 or RS485) (bit 0) and the reader address in the case of an RS485 link (bit 7 to bit 1)	*b7 – b1*: *Reader Adress RS485 1111 111 to 0000 000*; *b0*: *Serial link "0" RS232 "1" RS485*
	CTRL Mode	Defines the communication mode (one byte).	○ 00h ➔ Non-secure mode - message sent in plain text. ○ 01h ➔ Signed mode ○ 02h ➔ Encrypted mode ○ 03h ➔ Signed and encrypted mode
CMD	Four-byte word, with two bytes that define the command type (reader, *Mifare DESFire & DESFire Ev1, Mifare Classic, Mifare Ultralight C* or *Mifare PLUS*) and two bytes that define the Command code to be sent.		
	RFU	1 byte	00h
	Type	Defines the command type (one byte)	00h ➔ Reader command 01h ➔ *Mifare Classic* command 02h ➔ *Mifare DESFire & DESFire Ev1* command 03h ➔ *Mifare Plus* command 05h ➔ *Mifare Ultralight C* command 09h ➔ *CPS3* command 0Bh ➔ *Biometric* command
	Code	Defines the Command code to be sent to the reader (two bytes)	
Reserved	AAh 55h (two bytes).		
L_{out}	Defines the length of data sent by the host (two bytes)		
$Data_{out}$	Represents the data sent by the host (e.g. in the case of a write command) (L_{out} bytes).		
CRC	CRC-^{16}-CCITT [Len….Command] ***[Polynomial "$x^{16} + x^{12} + x^5 + 1$"*** 0x1021] ; ***Initial value 0xFFFF***		

The information transmitted by the reader is formatted as follows:

#02	*Len*	*CTRL*	*ACK*	*L_{in}*	*$Data_{in}$*	*Status*	*CRC*
1 byte	2 bytes	2 bytes	2 bytes	2 bytes	L_{in} bytes	2 bytes	2 bytes

<table>
<tr><td># 02</td><td colspan="3">Start Of Frame (SOF) delimiter (on byte 02h)</td></tr>
<tr><td>Len</td><td colspan="3">Defines the length of the command to be sent (two bytes)</td></tr>
<tr><td rowspan="3">CTRL</td><td colspan="3">Two-byte word, with one byte that defines the serial link type used (RS485 or RS232) and one byte that defines the communication mode (plain text, encrypted, signed etc.…).</td></tr>
<tr><td>CTRL @</td><td>Defines the serial link type used (RS232 or RS485) (bit 0) and the reader address in the case of an RS485 link (bit 7 to bit 1)</td><td>
<table>
<tr><th>b7 – b1</th><th>b0</th></tr>
<tr><td>Reader Adress RS485
1111 111 to 0000 000</td><td>Serial link
“0” RS232
“1” RS485</td></tr>
</table>
</td></tr>
<tr><td>CTRL Mode</td><td>Defines the communication mode (one byte).</td><td>o 00h ➔ Non-secure mode - message sent in plain text.
o 01h ➔ Signed mode
o 02h ➔ Encrypted mode
o 03h ➔ Signed and encrypted mode</td></tr>
<tr><td>ACK</td><td colspan="3">Start of Frame acknowledgement, identical to the Command code sent by host</td></tr>
<tr><td>L_{in}</td><td colspan="3">Defines the length of data to be received by the host (two bytes).</td></tr>
<tr><td>$Data_{in}$</td><td colspan="3">Data sent by the reader in response to the host command (L_{in} bytes).</td></tr>
<tr><td rowspan="4">Status</td><td colspan="3">Two-byte word, representing the status type (reader, Mifare DESFire & DESFire Ev1, Mifare Classic, Mifare PLUS or Mifare Ultralight C) and the command result code.</td></tr>
<tr><td>RFU</td><td>1 byte</td><td>00h</td></tr>
<tr><td>Type</td><td>Defines the command type (one byte)</td><td>00h ➔ Reader command
01h ➔ Mifare Classic command
02h ➔ Mifare DESFire & DESFire Ev1 command
03h ➔ Mifare Plus command
05h ➔ Mifare Ultralight C command
09h ➔ CPS3 command
0Bh ➔ Biometric command</td></tr>
<tr><td>Code</td><td colspan="2">Defines the error code sent (one byte)</td></tr>
<tr><td>CRC</td><td colspan="3">CRC-16-CCITT [Len….Command] [Polynomial “$x^{16} + x^{12} + x^5 + 1$” 0x1021] ; Initial value 0xFFFF</td></tr>
</table>

T5.2.3 Available commands in plain mode

Output_Protocol

Description

This command is sent by the reader when it reads a valid tag and / or pin number. It's transmitted in hexadecimal. This return of this function informs the reader on the state to be applied to LED and buzzer.

Reader: CTRL CMD AAh 55h L_{out} $Data_{out}$

CMD *2 bytes*: 01h 00h

L_{out} *2 bytes:* $Data_{Len}$ Equal to the number of bytes of Data

$Data_{out}$ *x bytes*: Id value read in hexadecimal.

System: CMD L_{in} LedColor LedDuration BuzzerDuration 00h 00h

CMD *2 bytes*: 01h 00h

L_{in}*2 bytes*: 00h 03h (LedColor + LedDuration + BuzzerDuration)

LedColor *1 byte:* Byte indicating the LED color.
[00h … 03h]

- 00h Led off
- 01h Green Led
- 02h Red Led
- 03h Orange Led

LedDuration *1 byte*: This byte defines the LED colour-change duration in multiples of 100 ms [00h … FFh] where the value FFh keeps the LED on with the same colour for an indefinite period (until the next reader reset or the next time a value other than FFh is sent).

BuzzerDuration *1 byte*: This byte defines the buzzer activation duration in multiples of 100 ms [00h … FFh] where the value FFh keeps the buzzer on for an indefinite period (until the next reader reset or the next time a value other than FFh is sent).

Note

The reader has a 1.5s timeout to receive the response of the system for the control of LEDs and buzzer. Once this deadline has passed, it will not accept any frame until the next issue of the Output_Protocol order.

Life_Signal

Description

This command is sent by the reader each minute to keep the system informed about its presence.

Reader: CTRL CMD AAh 55h L_{out} $Data_{out}$

CMD *2 bytes*: 01h 02h

L_{out} *2 bytes:* 00h 02h Equal to the number of bytes of Data

$Data_{out}$ *2 bytes:* 00h + XXh ; with XXh:

- 01h Generic signal
- 01h Specific signal for LXS/LXC/MXS/ATX
- 03h Specific signal for MS
- 05h Specific signal for LXE
- 06h Specific signal for LXC
- 07h Specific signal for ARC

System: CMD L_{in} 00h 00h

CMD *2 bytes:* 01h 02h

L_{in} *2 bytes:* 00h 00h

Note

It is necessary to activate this option through the SCB Wizard of SECard software.

Wrenching_Signal

Description

This command is sent by the reader when it detects a state changing on the input "*SW*". That informs the system about an potential wrenching of the reader.

Reader: CTRL CMD AAh 55h L_{out} 00h

CMD *2 bytes:* 01h 03h

L_{out} *2 bytes:* 00h 01h Equal to the number of bytes of Data

System: CMD L_{in} 00h 00h 00h 00h

CMD *2 bytes:* 01h 03h

L_{in} *2 bytes:* 00h 00h

Note

It is necessary to activate this option through the SCB Wizard of SECard software.

Read_input

Description

This command is sent periodically by the reader to the system. It allows the system to control the activation of the LEDs and buzzer.

Reader: CTRL CMD AAh 55h 00h

CMD *2 bytes:* 01h 04h

System: CMD L_{in} LedGreen LedRed Buzzer 00h 00h

CMD *2 bytes:* 01h 04h

L_{in} *2 bytes:* 00h 03h

LedGreen *1 byte*: 01h inactive
00h active

LedRed *1 byte* : 01h inactive
00h active

Buzzer *1 byte:* 01h inactif
00h actif

Note
It is necessary to activate this option with desired pooling through the SCB Wizard of SECard software.

T5.2.4 Available commands in secured communication modes

The following commands are available in secured SSCP® communication mode (i.e. Signed, Enciphered, Signed+Enciphered). In these communication modes you can also use all the command that use Plain mode.

Authenticate

Description
This command performs authentication for Signature AND/OR Encipherment with reader. It generates session's keys from user keys for selected SSCP® communication mode.

ResetAuthenticate

Description

This command reset authentication for Signature AND Encipherment between reader and host.

ChangeReaderKeys

Description

This command allows you to change user keys for Signature AND/OR Encipherment with reader.

They are described in *SSCP® documentation*:

- ✓ Spec_Protocole_5AA-7AA_MIFARE_GLOBAL_Vx.x_FR

Please ask us for these documents.

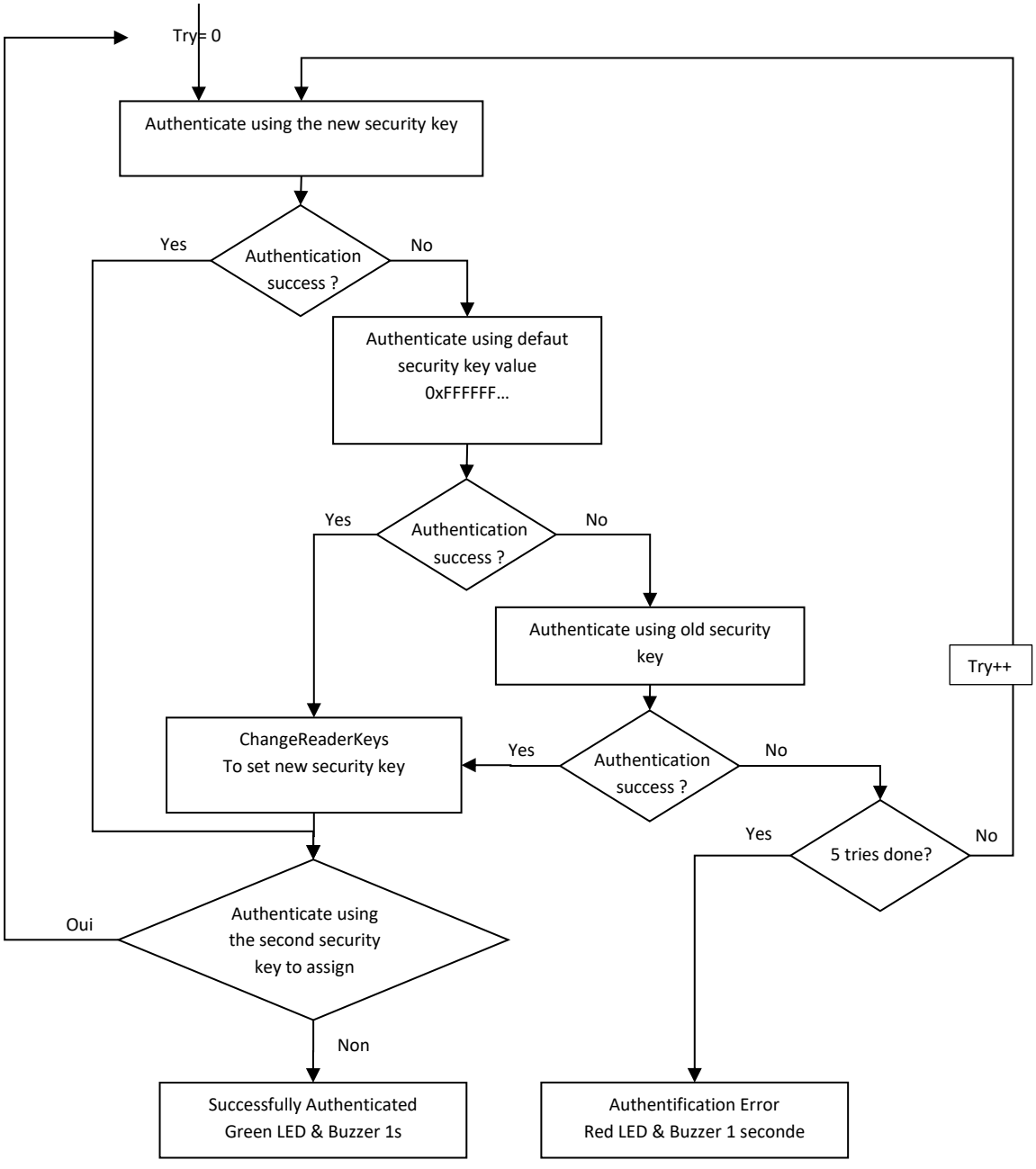
T5.2.5 Modification of the user keys

The encipherment *AES* "*Enc Key"* and signature "*Sign Key*" key be changed through SECard by ticking the case "*Change"* and filling the field with the new keys.

The modification is done through the specific reader command (***ChangeReaderKeys*** described in *SSCP®* documentations – transmitted signed and enciphered).
This procedure is sent to the system from the reader when it detects a changing through the *SCB* card.

The security key is:

- ✓ Enciphering key for Enciphered communication
- ✓ Signing key for Signed
- ✓ Both for Enciphered and Signed communication, in this case Authentication procedure has to be done two times, one per key.



T6 - About keypad readers

T6.1 - TTL Readers - R31 - Card OR Keys

The reader works in mode a Card OR Key. If a valid card is presented or if a key is pushed (according the encoding mode), the code will be sent immediately, followed by a short beep of the reader.

About the encoding mode type 4, a keys sequence written is confirmed by pushing the key '★'. In this case, the code is transmitted according the encoding mode. There is a Timeout between two keys pushing for 6 seconds. If it happens, the sequence is cancelled.

Formats available

- **'1': « 4 bits framed »**
  Value is coded by 4 bits which are sent within a frame according the chosen protocol.

Format ISO2 LSB … MSB		
'0'	0000	0x00
'1'	1000	0x01
'2'	0100	0x02
'3'	1100	0x03
'4'	0010	0x04
'5'	1010	0x05
'6'	0110	0x06
'7'	1110	0x07
'8'	0001	0x08
'9'	1001	0x09
'#'	1101	0x0B

In this case, 4 bits are sent LSB First within a frame according the chosen protocol. For more details, refer to the specification protocols.

Example: Frame of the key '5' according the protocol ISO2 / 2b.

000…	1101 0	1010 1	1111 1	xxxx x	000…
Zeros	**Start**	**'5'**	**End**	**LRC**	**Zeros**

Format WIEGAND MSB … LSB		
'0'	0000	0x00
'1'	0001	0x01
'2'	0010	0x02
'3'	0011	0x03
'4'	0100	0x04
'5'	0101	0x05
'6'	0110	0x06
'7'	0111	0x07
'8'	1000	0x08
'9'	1001	0x09
'#'	1011	0x0B

In this case, 4 bits are sent MSB First within a frame according the chosen protocol. For more details, refer to the specification protocols**.**

Example: Frame of the key '5' according the protocol Wiegand / 3i.

0	0000	0000	0000	0000	0000	0101	1
Parity	**'0'**	**'0'**	**'0'**	**'0'**	**'0'**	**'5'**	**Parity**

✓ **'2'** : **« 4 bits »**
Value is coded by 4 bits only which are sent according the chosen protocol.

Format ISO2 LSB … MSB		
'0'	0000	0x00
'1'	1000	0x01
'2'	0100	0x02
'3'	1100	0x03
'4'	0010	0x04
'5'	1010	0x05
'6'	0110	0x06
'7'	1110	0x07
'8'	0001	0x08
'9'	1001	0x09
'#'	1101	0x0B

In this case, 4 bits are sent LSB First within a frame according the chosen protocol. For more details, refer to the specification protocols.

Example: Frame of the key '4' according the protocol ISO2 / 2b.

0010
'4'

Format WIEGAND MSB … LSB		
'0'	0000	0x00
'1'	0001	0x01
'2'	0010	0x02
'3'	0011	0x03
'4'	0100	0x04
'5'	0101	0x05
'6'	0110	0x06
'7'	0111	0x07
'8'	1000	0x08
'9'	1001	0x09
'#'	1011	0x0B

In this case, 4 bits are sent MSB First within a frame according the chosen protocol. For more details, refer to the specification protocols**.**

Example: Frame of the key '4' according the protocol Wiegand / 3i.

0100
'4'

✓ **'3'** : **« 8 bits »**
Value is coded by 8 bits which are sent according the chosen protocol (default configuration)

Format ISO2 LSB … MSB		
'0'	11110000	0xF0
'1'	01111000	0xE1
'2'	10110100	0xD2
'3'	00111100	0xC3
'4'	11010010	0xB4
'5'	01011010	0xA5
'6'	10010110	0x96
'7'	00011110	0x87
'8'	11100001	0x78
'9'	01101001	0x69

In this case, 8 bits are sent LSB First according the timings of chosen protocol. For more details, refer to the specification protocols.

Example: Frame of the key '4' according the protocol ISO2 / 2b.

11010010
'4'

Format WIEGAND MSB … LSB		
'0'	11110000	0xF0
'1'	11100001	0xE1
'2'	11010010	0xD2
'3'	11000011	0xC3
'4'	10110100	0xB4
'5'	10100101	0xA5
'6'	10010110	0x96
'7'	10000111	0x87
'8'	01111000	0x78
'9'	01101001	0x69

In this case, 8 bits are sent MSB First according the timings of chosen protocol. For more details, refer to the specification protocols.

Example: Frame of the key '4' according the protocol Wiegand 3i.

10110100
'4'

✓ **'4'** : **« X touche Trame »**
4 bits keys framed – n keys within a frame according the chosen protocol.

Format ISO2 LSB … MSB		
'0'	0000	0x00
'1'	1000	0x01
'2'	0100	0x02
'3'	1100	0x03
'4'	0010	0x04
'5'	1010	0x05
'6'	0110	0x06
'7'	1110	0x07
'8'	0001	0x08
'9'	1001	0x09

In this case, 4 bits of n keys are sent LSB First within a frame according the chosen protocol. For more details, refer to the specification protocols. Only the keys '0' to '9' are available.

'★' Confirms the sequence. If **x=8**, the procedure is automatically confirmed and the code is sent.

'#' Cancels the current sequence.

Example: '4' '5' '9' '★' keys are pushed. The frame sent is 4 bits by keys according the protocol ISO2 / 2b.

000…	1101 0	0010 0	1010 1	1001 1	1111 1	xxxx x	000…
Zeros	**Start**	**'4'**	**'5'**	**'9'**	**End**	**LRC**	**Zeros**

Format WIEGAND MSB … LSB		
'0'	0000	0x00
'1'	0001	0x01
'2'	0010	0x02
'3'	0011	0x03
'4'	0100	0x04
'5'	0101	0x05
'6'	0110	0x06
'7'	0111	0x07
'8'	1000	0x08
'9'	1001	0x09

In this case, 4 bits of n keys are sent MSB First within a frame according the chosen protocol. For more details, refer to the specification protocols. Only the keys '0' to '9' are available

'★' Confirms the sequence. If **x=8**, the procedure is automatically confirmed and the code is sent.

'#' Cancels the current sequence.

Example: '4' '5' '9' '★' keys are pushed. The frame sent is 4 bits by keys according the protocol Wiegand 3i.

0	0000	0000	0000	0100	0101	1001	1
Parity	**'0'**	**'0'**	**'0'**	**'4'**	**'5'**	**'9'**	**Parity**

Note

✓ *Maximum number of key = 8*

✓ ***xmax** = 6 maximum number of key for Wiegand 3i protocol. In this case values of keys are not automatically sent. It is necessary to confirm the sequence.*

T6.2 - TTL - R31 Reader – Keys AND Card

A keys sequence is requested (1 up to 9 keys depending of the configuration with keys **'1'** up to **'9'** only). There is a timeout of 6 seconds between the strikes of 2 digits. If the timeout is reached or keys **'★'** and **'#'** are pushed, the entire operation is aborted and needs to be entered (indicated by a sound and the red Led blinks).

When the pin number has been entered, the CLA is waiting for a card and for 6 seconds, for a card. During this waiting, the buzzer beeps.

All the data are sent when the sequence (card AND keys) is complete according the current protocol.

Key n°1 *4 bits Format*	Key n°2 *4 bits Format*	…	Identifier *n bits Format* *protocol size*

Example:
3 keys: 7, 8, 9 / Identifier 0x11223344 in hexadecimal, 287454020 in decimal
3CB-Wiegand protocol ➔ ouput = 0x**789***0011223344*(+LRC)
Iso 2b protocol ➔ output = **789***0000287454020*

T6.3 - TTL - R31 Reader – Keys OR Card - 26-bits Wiegand mode *New 3.6*

In this mode, the PIN code is sent to the system in the form of a badge identifier attached to a site code defined in the "Site code (FC)" field.
#: validate the entry of the PIN code.
*: cancels the entry of the PIN code entered previously, the reader emits 4 beeps to indicate that it has been taken into account.

bit 1	bit 2 ... bit 9	bit 10 ... bit 25	bit 26
Even parity on bit 2 ... bit 13	*Site Code FC (0 u pto 255) Configured in SECard bit 2 = MSB*	*PIN code (0 up to 65 535) Entered on keypad bit 10 = MSB*	*Odd parity on 14 ... bit 25*

The PIN code "65,535" is reserved to indicate an error:
- The # key is pressed first without a code to return.
- The entered PIN code = 0
- The PIN code is greater than or equal to "65 535"

Parity is calculated by the reader.
The time for saving a key press in memory (without pressing # or *) is 6 seconds.
If this time is exceeded, the reader beeps 4 times to indicate that the time-out has been reached.
On a Screen reader in Scramble mode, by pressing the # key, the reader scrambles the keyboard.

Example with FC=121 and PIN Code 24568:

1	0111	1001	0101	1111	1111	1000	0
Parity	**'7'**	**'9'**	**'5'**	**'F'**	**'F'**	**'8'**	**Parity**

T6.4 -TTL - S31 Reader - Card AND Keys

Keys and UID / Id will be sent to that following enciphered frames.

Data	Random value	CRC
12 bytes	2 bytes	2 bytes

Frame key

+

Data	Random value	CRC
12 bytes	2 bytes	2 bytes

Frame1

Data	Random value	CRC
12 bytes	2 bytes	2 bytes

Frame 2

Data	Random value	CRC
12 bytes	2 bytes	2 bytes

Frame …

T6.5 -TTL - S31 Reader - Card OR Keys

Keys enciphered frame and UID/Id enciphered frame will be sent independently. They are enciphered using «Enciphered Weigand output key».

Data	Random value	CRC
12 bytes	2 bytes	2 bytes

Enciphered frame1

Data	Random value	CRC
12 bytes	2 bytes	2 bytes

Enciphered frame2

Data	Random value	CRC
12 bytes	2 bytes	2 bytes

Lest Enciphered frame

Example for key 1 pressed

Value is coded by 4 bits which are sent within a frame according the chosen protocol.
Data (12o) = 0x10 00 00 00 00 00 00 00 00 00 00 00

Value is coded by 4 bits only which are sent according the chosen protocol
Data (12o) = 0x10 00 00 00 00 00 00 00 00 00 00 00

Value is coded by 8 bits which are sent according the chosen protocol.
Data (12o) = 0xE1 00 00 00 00 00 00 00 00 00 00 00

Example for key 1, 5, 7 pressed

4 bits keys framed – n keys within a frame according the chosen protocol.
Protocol W3i: Data (12o) = 0x00 01 57 00 00 00 00 00 00 00 00 00
Protocol W3Ca: Data (12o) = 0x00 00 01 57 00 00 00 00 00 00 00 00
Protocol ISO2B: Data (12o) = 0x00 00 00 01 57 00 00 00 00 00 00 00

T6-6 - RS232 / RS485 - R32/S32/R33/S33 Readers - Card OR Keys

No difference between hexadecimal and decimal mode.

The data are coded by 8 bits as shown below:

Value of the key MSB … LSB		
'0'	11110000	0xF0
'1'	11100001	0xE1
'2'	11010010	0xD2
'3'	11000011	0xC3
'4'	10110100	0xB4
'5'	10100101	0xA5
'6'	10010110	0x96
'7'	10000111	0x87
'8'	01111000	0x78
'9'	01101001	0x69

Mono directional mode

Refer to the chapter *T5.1 - Unidirectional communication mode* for more details about the options of the frame.

Regarding the Card OR Keys configuration, the structure of the frame is:

1 byte	***1 byte ****	***1 byte***	***1 byte***	***1 byte***	***1 byte***
STX	*Key code*	*LRC*	*0x0D*	*0x0A*	*ETX*

**Doubled if the ASCII option is activated.*

Bidirectional mode

Refer to the chapter

T5.2 - Bidirectional communication mode for more details about the bi-directional communication of the reader.

In Card OR Keys mode, the card data is sent through the ***Output_Protocol.*** The **keyboard data** are sent through the command described below:

Output_Keyboard

Description

This command is generated by the reader when you press a keyboard key in Card OR Key mode.

Reader: CTRL CommandCode AAh 55h L_{out} $Data_{out}$

CommandCode *2 bytes:* 01h 07h
L_{out} *2 bytes:* 00h 03h
$Data_{out}$ *3 bytes:* 00h 01h "Value of key pressed 8 bits format".

System: ACK L_{in} 00h 00h

ACK *2 bytes:* 01h 07h
L_{in} *2 bytes:* 00h 00h

Example for key 0 and RS485 address 0:
Reader sends: 02 00 0B 01 00 00 00 01 07 AA 55 00 03 00 01 F0 03 75.
System answers: 02 00 04 01 00 01 07 00 00 46 7C.

T6-7 - RS232 / RS485 - R32/S32/R33/S33 Readers - Keys AND Card

The encoding key is in 8bits format, number of key to press is configured by the configuration card SCB.

Mono directional mode

Refer to the chapter *T5.1 - Unidirectional communication mode* for more details about the options of the frame.

Regarding the Card AND Keys configuration, the structure of the frame is:

1 byte	***X bytes***	***X bytes***	***1 byte***	***1 byte***	***1 byte***	***1 byte***
STX	*Key code**	*Data**	*LRC*	*0x0D*	*0x0A*	*ETX*

**Doubled if the ASCII option is activated.*

Example in mode Card AND Keys:

- ✓ 3 keys: *7, 8 et 9*
- ✓ Identifier: 0x11223344 in hexadécimal and 287454020 in decimal.
- ✓ Protocol size: 5 bytes
- ✓ Output hexadecimal format: 0x*877869* 11223344
- ✓ Output decimal format: *877869*0000287454020

Bidirectional mode

Refer to the chapter

T5.2 - Bidirectional communication mode for more details about the bi directional communication of the reader

In Card AND Keys mode, the card data is sent through the ***Output_Protocol.***

T7 - Biometric data format

T7.1 - Biometric Templates format

The information which contains the fingerprints data is contained into a specific MIFARE® DESFire® EV1/2 file or in sectors 32 up to 39 for MIFARE Plus® Level 3 and defined in the "*Biometric*" part.

- ✓ When it is created, SECard defines the size according to: Number of fingers * 170 bytes.
- ✓ The biometric templates are written according to the Morpho Sagem format (PK_COMP).
- ✓ Mapping of the MIFARE® DESFire® EV1 file or MIFARE Plus® Level 3 sectors:

MSB *LSB*

[**LenTotale**] | [**Nb Template**] | [**LenTemplate$_x$** | **Template$_x$**] ^{n}

- ✓ **LenTotale** is the total lenght data to write on the chip on 2 bytes.
- ✓ **Nb Template** is the template number (max 5), on 1 byte.
- ✓ **LenTemplate$_x$** is the size of the Xth template on 1 byte.
- ✓ **Template$_x$** is the Xth template with **LenTemplate$_x$**.
- ✓ n is the number of templates.

Number of MIFARE Plus® Level 3 sectors to be written depends on the numbers of fingers to be encoded. The maximum size is: 2+5*(1+170) = 857 bytes. (cf. Sagem).

T7.2 - Biometric derogation

From version 3.1, you can activate a biometric derogation template when encoding a user card.

The user will not be asked to encode their fingerprints, a derogation template will be encoded instead.

This option allows you to set the reader whether to authorize or not the user cards using the biometric derogation.

When the biometric derogation is activated, the cards can be encoded "on-the-fly" if the system is designed to do so.

$$\text{TemplateDerogation} = \text{SHA2}(\text{salt} \,|\text{UID}, \text{UIDLen})$$

- ✓ **salt** 16 bytes private fixed value
- ✓ **UID** chip serial number
- ✓ **UIDLen** lenght of UID

T8 - Management of biometric + Keypad

Mode 1: Key **OR** (Card **AND** biometric).

The operation is identical to Card OR Key, with the addition of the reading of the fingerprint after reading the card.

Mode 2: Key **AND** (Card **AND** biometric).

The operation is identical to Card AND Key, with the addition of the reading of the fingerprint after reading the card.

Mode 3: Key **OR** (Card **AND** biometric), 26-bit Wiegand mode

The operation is identical to Card OR Key, with the addition of the reading of the fingerprint after reading the card.

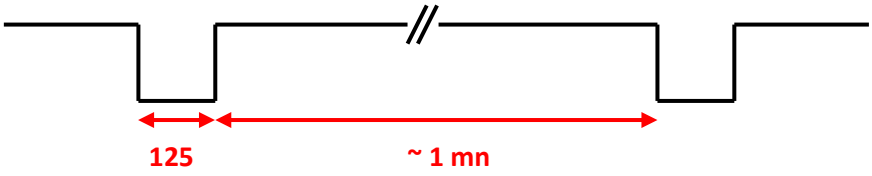
T9 - Life signal function

T9.1 - TTL- Readers

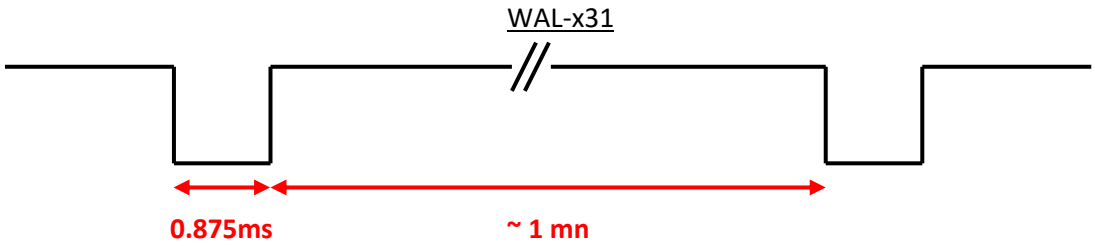
When this feature is enabled, the reader sends a signal about every minute on the Data/DATA1 lines.

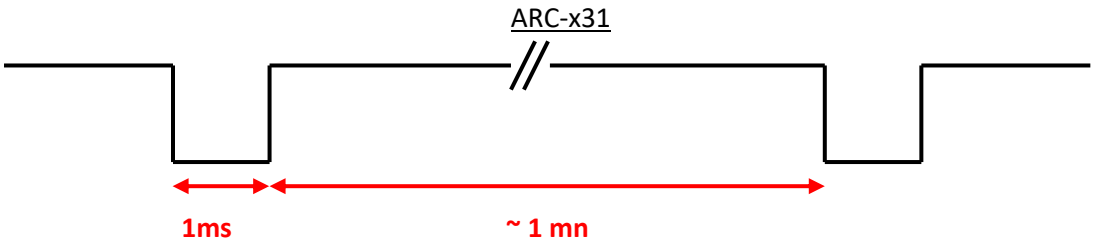
The life signal can be activated in a generic (Generic life signal - a life signal common to all readers) and (Specific life signal – life signal different for each reader).

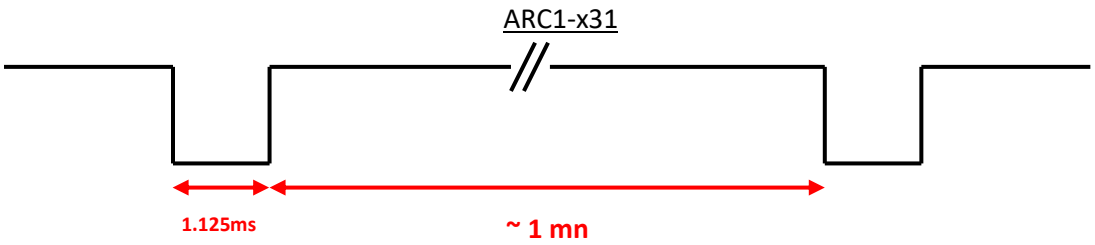
***Generic life signal**:*

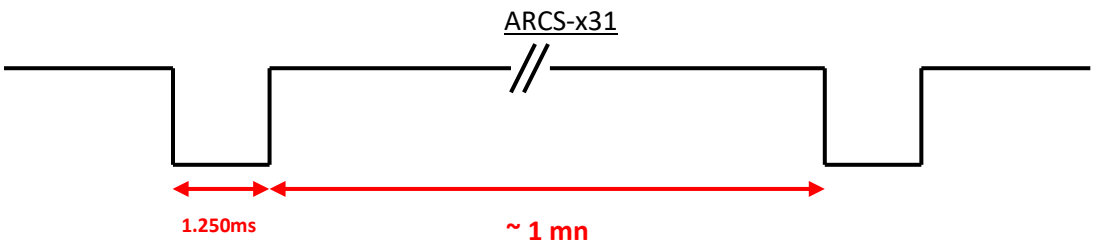


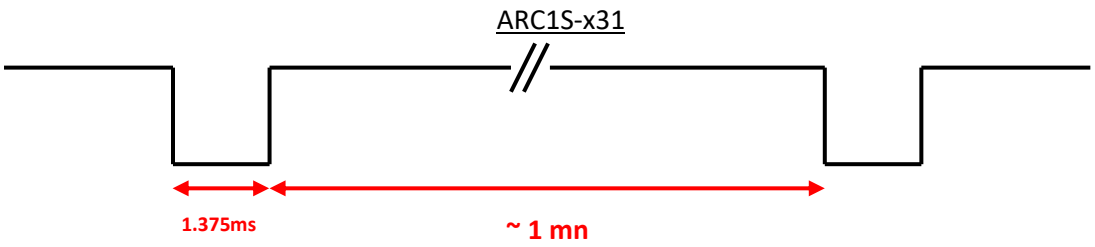
***Specific life signal**:*



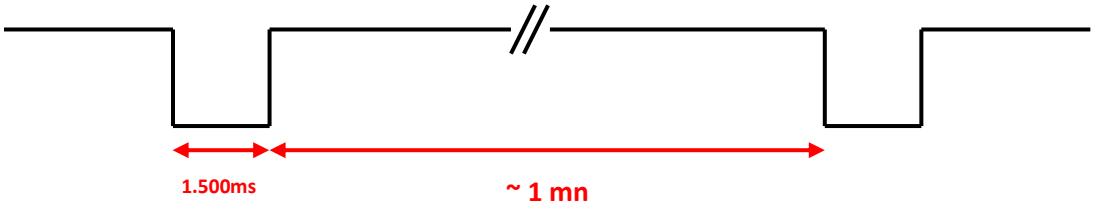




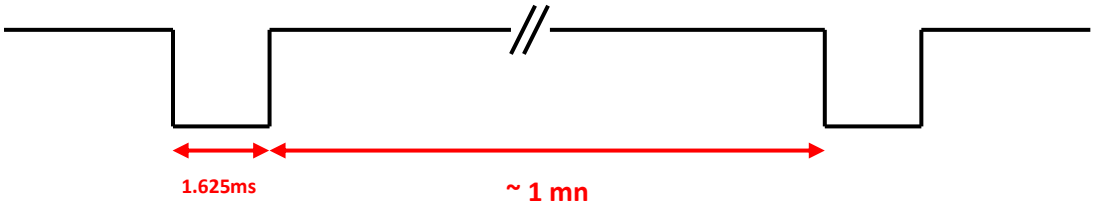




MS2-x31



MS2S-x31



T9.2 - Bidirectional serial reader

Reader send in plain on the serial link the command code 0x0102.

Data = x * 125us (example: for ARC-R32/R33, x = 8)

T9.3 - Unidirectional serial reader

Reader send on the serial kink the command code:

Generic: 0x50

Specific:

ARC-R32/R33= 0x61

ARC1-R33 = 0x62

ARCS-R33 = 0x63

ARC1S-R33 = 0x64

MS2-R31 = 0x65

MS2S-R31 = 0x66

Specific Gamme E:

LXS-R32/R33= 0x50

MS-R31 = 0x52

LXE-R32/R33 = 0x54

LXC-R32/R33 = 0x55

WAL-R32/R33 = 0x56

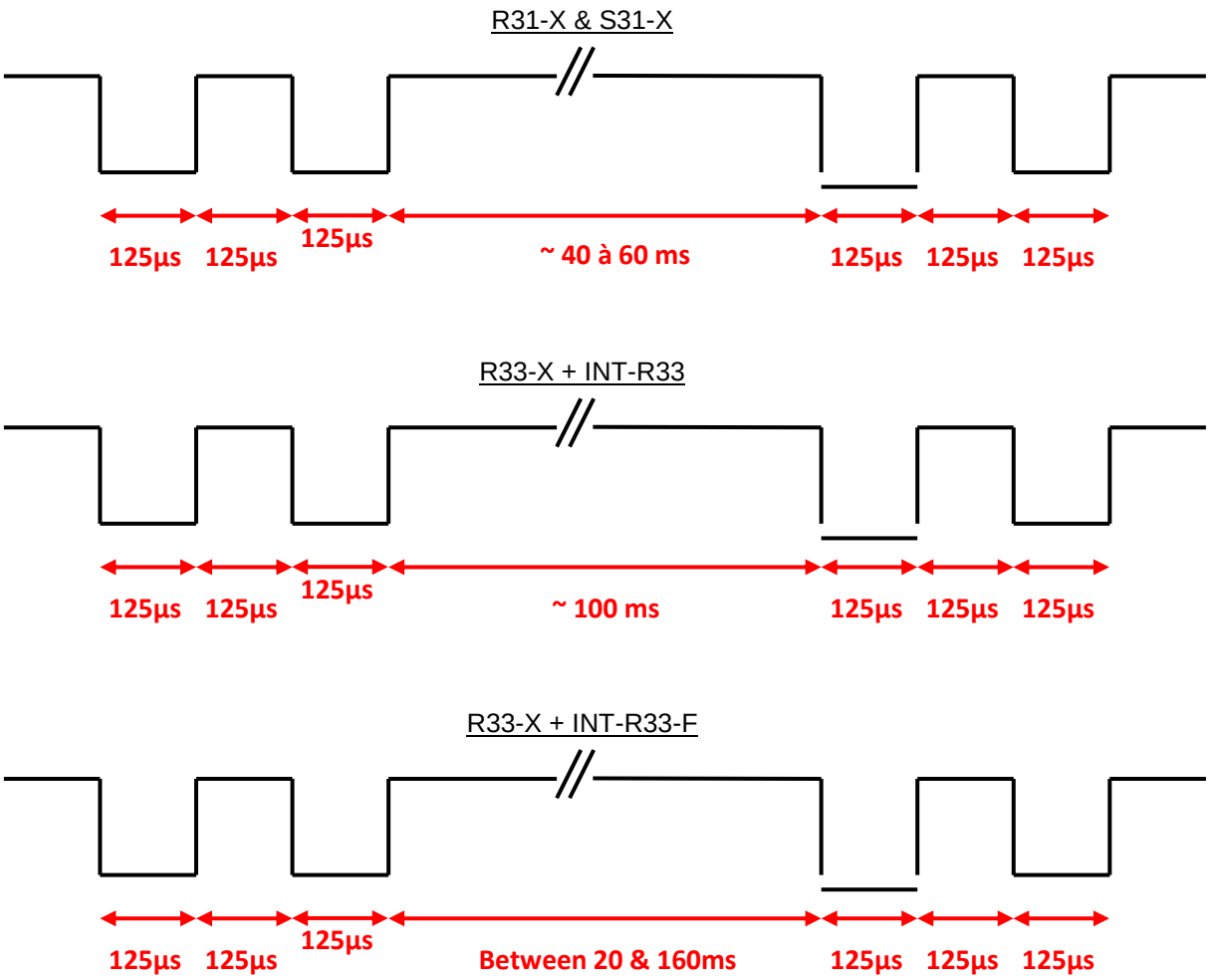
T10 - Tamper switch signal

When this feature is enabled, the reader remembers (at startup) its initial state of « ***Switch*** » input or accelerometer.

T10.1 - TTL- Readers

At each moment when that state changes, the reader sends a Tamper signal to the line « ***Data/Data 1*** ».

During the breakout, by default or if the option is enabled, the shape of the signal on the line "Data / Data 1" is as follows:



T10.2 - Bidirectional serial reader

Reader send in plain on the serial kink the command code 0x0103

T10.3 - Unidirectional serial reader

Reader send on the serial kink the command code 0xAA

T11 - Tamper switch ID

When this feature is enabled, the reader remembers (at startup) its initial state of accelerometer.

Specific ID sent when reader is wrenched, value in conformance with current protocol. This specific ID is sending only one time each time the reader is wrenched.

Value of the specific ID:

- 16 bytes max for Wiegand and serial readers
- 10 bytes max for ISO readers

Note: If the protocol size is above this value, reader padd with 0.

T12 - Mutual Life / Tamper switch Signal

Only available on R31/S31 and R33+INTR33E readers

When this option is activated, the reader emits each second a specific life signal. The format of this one depends on the current protocol.

If the "*Switch"* input or accelerometer state changes, the emitted signal changes also. The data "*Tamper*" is sent in the frame instead the "*Life*" data.

✓ *Example of a life signal (operating mode – without wrenching) emitted each second:*

- ISO2 Protocol:

  Start Sentinel + Life data byte + End Sentinel + LRC

- Wiegand :

  Life data byte + LRC

✓ *Example of a wrenching emitted each second:*

- ISO2 Protocol:

  Start Sentinel + Tamper data byte + End Sentinel + LRC

- Wiegand :

  Tamper data byte + LRC

Note:

This option is not available on the 26 bits Wiegand (3i).

If this option is activated, the delay of the led blinking cannot be more than 400 ms.

T13 - Command Line

T13.1 - Description

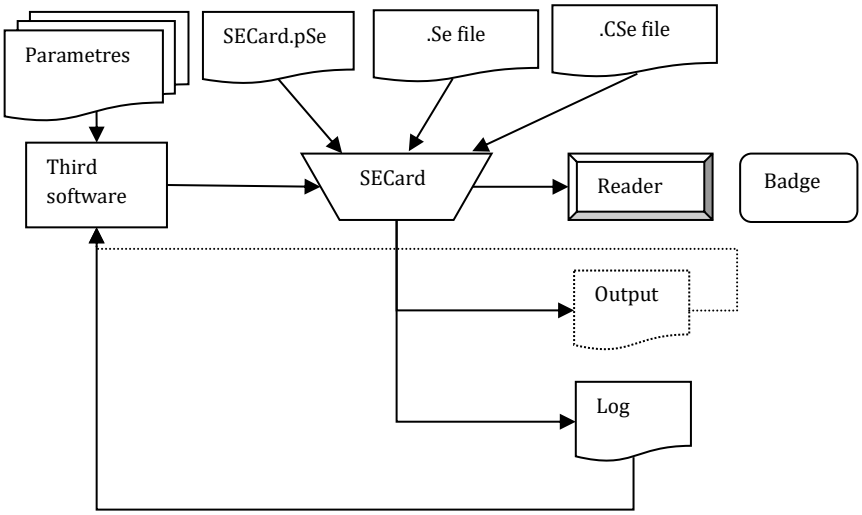
SECard includes a “command line” mode which allows work in background tasks and which allows interfacing with another application.

SECard allows to:

1. Load specific configuration.
2. Use current configuration.
3. Make tags encoding and reading.
4. Provide the results in a user file.
5. Save all operations.

“Command line” mode thus allows interfacing tags encoding/reading (or any operation that SECard known to make), with third application.
Simply configure application to launch SECard with correct parameters.

The process is summarized in the following diagram:



T13.2 - User instructions

To execute SECard in “command line” just:

- launch secard.exe in “Windows Command Line” with parameters.
- or made a batch file using secard.exe with parameters.
- or launch secard.exe via another application that allows you to enter parameters. This last method will be used in “customizing badges” software.

The command line is:

secard[.exe] -u userid -p password [-a action] [-i|I config.Se] [-q PSEPassword] [-o outputfile.txt] [-l|L logfile.log] [-d dataTOencode] [-h] -v

Parameters:

-u: specifies the user who will launch SECard, this parameter is required if not -I

1=User
2=Power user
3=Administrator

-p: specifies password used by -u, this parameter is required if not -I

-q: specifies password used for eSe file if locked

-a: specifies the action to achieve by SECard:

- UEncode encode user tag, -d required
- URead read user tag, -o required
- UID read tag UID,-o required
- KEncode encode SKB
- KRead read SKB,-o required
- CEncode encode SCB
- CRead read SCB,-o required
- CSe2PSE convert CSE file into PSE file

-b: specifies the communication baudrate of the encoder

0 : 9600 ; 1 : 19200 ; 2 : 38400 ; 3 : 57600 ; 4 : 115200

-d: specifies the user data to encode, text string representing ID (hex/dec).
Warning, this chain must be compatible with the current configuration file automatically loaded by SECard, or SE/CSE file imported.

-i|I: import a configuration file .Se in plain, and fills the corresponding parameters in SECard.
Executed before the action defined by -a.
If the parameters -I is used then the import configuration file is encrypted and contains the login and password associated (parameters -u and -p and -q are ignored).

-o: name of output file containing the operations made by –a, if the action done is CSe2PSE the output file will be PSE file creates.

-l|L: name of log file containing the status of all operations made by -a. l for display short log (OK|NOK) or L for complete log.

-v: verbose log, used with -l|L. Specifies whether the log should be in verbose mode.
The user running the command line must be logged in as an administrator or power user with reader and RFID keys management rights, otherwise the log will be classic.
Caution: verbose log generates a file (SECard_VerboseLOG.txt) that contains the keys values of RFID and readers.

-h: displays help in DOS windows if launched from DOS, in windows message if launch from windows with IHM (exclusive, the rest are ignored).

SECard command line is not blocking, it returns immediately.
So that there is no accessing problem to reader/configuration, the command line is exclusive; there can be more than one at the same time.
However, there may be another classic SECard (no command line) to run (be careful sharing the communication port).

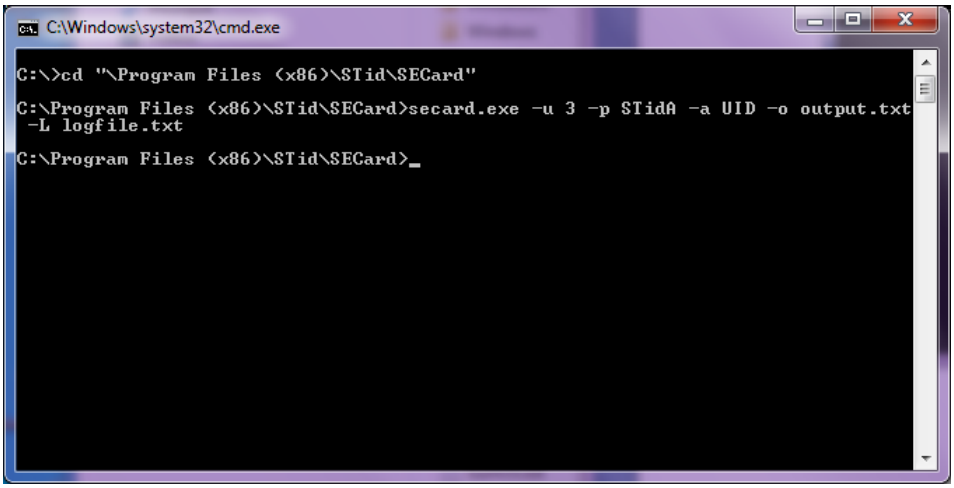
In command line mode, SECard uses automatically the default file setting or the one chosen by user.
Thus, it will suffice to define and save the user configuration by running SECard in Classic mode so that it is loaded automatically when you launch SECard.

T13.3 - Control consol

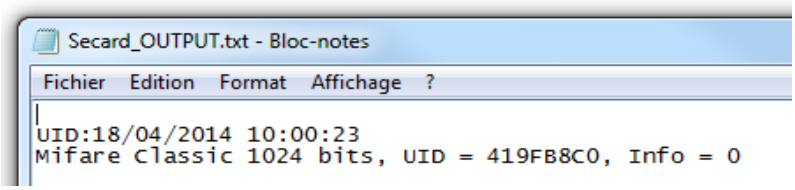
Open Windows command console: execute cmd.exe
Select the SECard install directory:

cd \Program Files\STid\Secardvxxx\ or cd \Program Files (x86)\SECardvxx\

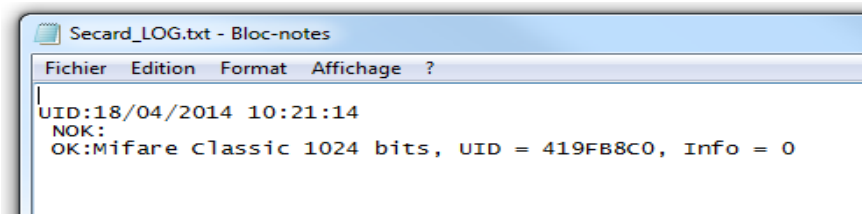
Then enter the desired command line.
For example if you want to read UID:
Put a RFID tag in front of the reader switched on and configured in SECard, then type:



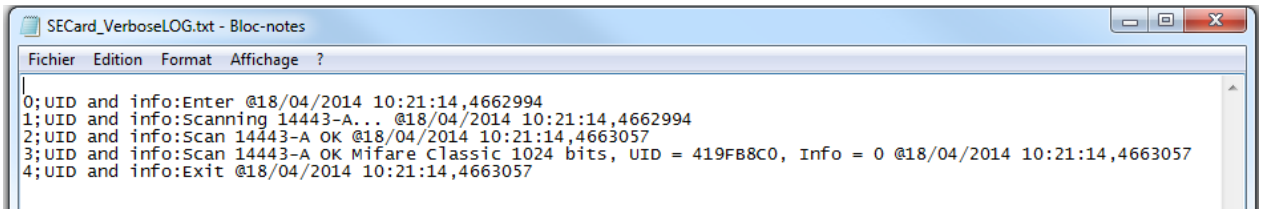
The result of the operation (so the tag UID presented to the reader) is written to the file output.txt.



If the operation it is successful, will be recorded in the log file logfile.txt.



If the log is verbose log, file log is:



T13.4 - Batch file

With batch files (executable by the command interpreter of Windows command console) and commands accepted by SECard a multitude of scenarios is possible.

For example, to retrieve the UID of ten tags, the batch file (UIDof10.cmd) is:

```
REM @echo off
for /l %%d in (1,1,10) ^
do (secard.exe -u 3 -p STidA -a UID –o output.txt –L logfile.txt)
```

The UID of ten tags will be collected and added sequentially to the file output.txt.
Be careful to be in phase with the presentation of different tag to reader. You can add a sleep for x seconds with ping command ping 127.0.0.1 –n x just after secard.exe:

```
REM @echo off
for /l %%d in (1,1,10) ^
do (secard.exe -u 3 -p STidA -a UID –o output.txt –L logfile.txt
ping 127.0.0.1 –n 5)
```

To encode IDs contained in a text file IDsList.txt (one ID per line) you can use the following batch file:

```
@echo off
for /F %%i in (IDsList.txt) ^
do (
echo Present the tag to be program with %%i
secard.exe -u 3 -p STidA -a UEncode -o output.txt -L log.txt -d %%i
echo 5 seconds to take following tag
ping 127.0.0.1 -n 5 > NUL
```

T13.5 - Third application

Setting

It is possible to use SECard with command line in third application (for example printing application).

For this, run application, create the design of the card by referring to the manual of application.
Select or activate “Smart Card” then select “Command Line”. Configure the use of RFID.
Select secard.exe it’s typically located in c:\Program Files\STid\SeCard Vx.x.x\SeCard.exe.
Set the location of the return, if this file does not exist, create the file CMDlineLOG.txt.
Then define the access to value (static value or database values).
Remains to inquire the arguments:

Note: If the parameters –o &/or –l|L used with files with long names &/or contain spaces or special characters it must be enclosed by " ".

- -u 3 -p STidA –a UEncode –o “C:\Program Files (x86)\STid\SeCard\output.txt” –l “C:\Program Files (x86)\STid\SeCard\cmdlinelog.txt”
- -d 11223344 or –d < database value >

Error handling

❖ **Third application cannot communicate with SECard**

Check that SECard was launched by the third application: open “Task manager” of Windows and check that SECard appears (at least for a moment) in the process list. If this is not the case, check your command line and the address to the file SECard.exe.

If SECard is launched but it still does not work, you must start SECard with the -L option instead of -l followed by the name of the log file. SECard then record all operations effected before the close. Retry the operation. Check the contents of the log file:

- "Data received length error (too short)": communication port is misconfigured in SECard. Open SECard classic and change the port to match it with your RFID coupler, check the seed, save the settings file before closing.

- “Bad parameter file, (.eSe) corrupt or invalid communication port”: SECard current settings file is not registered correctly for the command line. With a text editor, open the file SECard.gcf which located in the SECard installation directory. Search key “Settings” in the “File”.
  Check that the name using an absolute path, that is to say of the form « C:\Program Files(x86)\ STid\SECard\SECard.eSe » and NOT as « .\SECard.eSe »(which is the default configuration during installation).
  If this is not the case, it must be modified for these two possibilities, either directly in the file SECard.gcf or open SECard classically, go to the menu "File" and to "save" the settings file the desired location (it is possible to overwrite the default settings if this is the one used).

❖ **SECard cannot communicate with third application**

Communication between SECard and application is done through the log file, if the communication is broken is that there is a problem with the file used.
Check that the file name defined as the file back in the third-party application is the same as the name of the log file defined by the SECard command line and check that his name is well enclosed by " " if it contains spaces or special characters. Check access rights to this file.

T13.6 - Import configuration file

The following file determines all parameters compatible with the import configuration file in clear, and encrypted when launching from the SECard command line.
As it stands, this file specifies all drive parameters, SSCP® and only the DESFire® parameters.

```
;; SECard command line import configuration file
;; defines all parameters available in SECard command line mode from V3.6.0

[Login]
;Values are ONLY defined if import configuration file is Encrypted (.CSe)
;Access level : 1=User, 2=PowerUser, 3=Administrator
ACCESSLevel=3
;Password for corresponding user
Password=STidA

;If command line action is "CSe2PSE" you have to defined passwords that will be saved in PSE file
PSEUserPassword=STidU_123
PSEPowerUserPassword=STidP_123
PSEAdministratorPassword=STidA_123
;Read (Open) password is unconstrained, default is empty (no password)
PSEReadPassword=


;PowerUser Rights : 1=Enable, else disable
;Load/Save configuration file
LSconf=0
;Reset conf counters
Rcc=0
;Create/Read SKB
CRSKB=0
;Create/Read SCB
CRSCB=0
;Create/Read User cards
CRUserCards=0
;Manage Reader communication keys
MRCKeys=0
;Manage RFID keys
MRFIDKeys=0


[ReaderFamily]
;0 for LXS family
;1 for ARC family
;2 for WAL family
ReaderFamilyID=1

[CompatibilityVersion]
; Override .gcf compatibility mode

; For LXS family
; 0 = SeCard v1.1.x or Unknown;
; 1 = SeCard v1.2.x
; 2 = SeCard v1.3.x
; 3 = SeCard v1.4.x
; 4 = SeCard v1.4B.x
CompatibilityVersion= 3

; For ARC family
; 0 = SECard v2.0.0
; 1 = SECard v2.1.0
```

```
; 2 = SECard v2.2.0
; 3 = SECard v3.0.0
; 4 = SECard v3.1.0
; 5 = SECard v3.2.0
; 6 = SECard v3.3.0
; 7 = SECard v3.4.0
; 8 = SECard v3.5.0
ARCCompatibilityVersion=3

; For WAL family
; 0 = SECard v2.1.0
; 1 = SECard v2.2.0
WALCompatibilityVersion=0


[SSCP]
COMPort=COM4

;Baudrate = 9600,19200,38400,57600,115200
Baudrate=38400

;Security mode, Plain=0, Sign=1, Enc=2, SignEnc=3
SecurityMode=0

;To use SecurityMode>0 we need keys !
;WARNING: if you use SSCP keys, this file should be enciphered to CSe file
SSCPSignKey=A087754B7547481094BE
SSCPEncKey=E74A540FA07C4DB1B46421126DF7AD36



[Reader]
;SCB company key
SCBKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Change=0
SCBNewKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

;Reader reference
;0=R31E/103
;1=R31E/Ph5/Ph1
;2=S31E/Ph5
;3=R33E/Ph5 + INT-R33E
;4=R32E,R35E/Ph5
;5=S32E,S35E/Ph5
;6=R33E/Ph5
;7=S33E/Ph5
;8=S33E/Ph5+INT-E-7AA/7AB
ReaderReference=1

;BiometricActivation available for R31E/103,R31E/Ph5/Ph1 and S31E/Ph5  readers
BiometricActivation=0

;Save user keys in memory
SaveEEPROM=0

;Erase keys at tamper switch activation
EraseKeys=0

;Tamper switch signal activation
TamperSwitch=0

;On tamper activation keeps LED red as default
TamperKeepLEDRed=0
```

;Mutual life signal and Tamper switch signals available for R31E/103,R31E/Ph5/Ph1,S31E/Ph5 and R33/Ph5+INT-R33E readers
Mutual=0
;Life signal 1 byte
Life=0C
;Tamper signal 1 byte
Tamper=1C

;KeyPad activation available for R31E/103,R31E/Ph5/Ph1,S31E/Ph5,R32E,R35E/Ph5,S32E,S35E/Ph5,R33E/Ph5,S33E/Ph5
KeyPadActivation=0

;If keypad activated Badges/keys mode
;BKmode, =0 Badge OR Key, =1 Badge AND Key
;SECard v3.6.0, add BKmode=2 =W3i card OR key, see below for KeyboardSiteCode
BKmode=0

;KeypadFormat 0=4bits framed, =1 4 b, 2=8 b,3=4b Keys framed
KeypadFormat=2

;KeyPad nb keys [1..9]
KeyPadNbKeys=1

;Enable/disable Tagtype
MIFARECClassicTagEnable=0
MIFAREPlusTagEnable=0
MIFAREDESFireTagEnable=1
MIFAREUltraLightTagEnable=0
CPS3TagEnable=0
MoneoTagEnable=0
125kHzTagEnable=0
NFC_HCEEnable=0
;SECard v3.6.0, Application Multiservices Citoyenne tag type to enable/disable 1/0
AMCTagEnable=0

;V3.0.0
;TagType
BlueMobileID=1
;Blue MobileID Configuration Activation
BlueMobileIDActivation=1
;DESFire Configuration Activation
DESFireConfigurationActivation=1

;PUPI ISO14443-3B
PUPIEnable=0
PUPIMSB=1
PUPISign=0
PUPISignKey=FFFFFFFFFFFFFFFFFFFF

;UID/ID range, From=To=RandgeFrom=00000000=Disabled
RandgeFrom=00000000
RandgeTo=00000000

;SiteCode
ReaderSiteCode=10BF

;Protocol data size
ProtocolSize=5

;For R31/S31/INT-R33E
;ProtocolID 0=W3i (24bits),1=Iso 2H (32bits),2=Iso 2S (32bits),3=Iso 2B (40bits),4=W3Ca (32bits),5=W3Cb (40bits),6=W3La (32bits),7=W3Lb (40bits),8=W3T (64bits),9=Iso custom size,10=Wiegand LRC custom size,11=Wiegand custom size,12=Wiegand 34 bits - 3Eb,13=Wiegand 35 bits - 3W,14=Wiegand 37 bits - 3V,

```
;+V3.3.0 16=PAC 32bits-5Pa, 17=PAC 64bits-5Pb
;+V3.6.0 18=W3Y Wiegand 38bits, 19=W3Z Wiegand 72bits
ProtocolID=5

;For R32/S32/R33/S33
;SerialConfiguration
;Baudrate : 0=9600,1=19200,2=38400,3=57600,4=115200
SCBaudrate=0
SCRS485Adr=0
SCBidirectionnal=0
;Radix : 0=Hexa, 1=Decimal
SCBase=0

SCNoLeadingZeros=1
SCASCII=1
SCLRC=0
SCCRLF=1
SCSTXETX=0

;Security mode (SSCP bidirectional) Plain=0, Sign=1, Enc=2, SignEnc=3
SCSecurityMode=0
SCSignKey=FFFFFFFFFFFFFFFFFFFF
SCChangeSignKey=0
SCNewSignKey=FFFFFFFFFFFFFFFFFFFF
SCEncKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
SCChangeEncKey=0
SCNewEncKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

;Life signal :0=Disabled, 1=Generic,2=Specific
LifeSignal=0

;Output encipherment AES key for S31 reader
OutEncKey=000102030405060708090A0B0C0D0E0F
OutEncChange=0
OutNewEncKey=000102030405060708090A0B0C0D0E0F

;;For LXS Family
;Default LED action Color: Off=0, Green=1,Red=2,Orange=3
DefActLED=3
DefActLEDBlink=0
DefActLEDBlinkDuration=4
;Card detection action LEd Color: Off=0, Green=1,Red=2,Orange=3
DetActLED=3
;For WAL reader, used only if WALDetectionLEDBlinkTimes=0
DetActLEDDuration=4
DetActBuzzDuration=4

;;For WAL Family, LED Color in RGB, allowed values are only 00 or FF for each byte
;Yellow,use DefActLEDBlink and DefActLEDBlinkDuration to select blinking
WALDefaultLEDColor=FFFF00

;Yellow
WALDetectionLEDColor=FFFF00
; Nb of LED blink at badge detection, cannot be used if DetActLEDDuration >0
; so to use it set DetActLEDDuration to 0 and set blink times here
WALDetectionLEDBlinkTimes=0


;;For ARC Family
;;use SECard selection color window to get RGB code of a color
;Default LED action Color: RGB 3 bytes hexa
;orange
ARCDefLEDColor=FF6400
;0=Off,1=Fixed,2=Blinking,3=Pulse,4=Rainbow
```

```
ARCDefLEDMode=1
;Blink duration [1..31] x100ms
ARCDefLEDBlinkDuration=4
;Pulse speed
;Slow=0, Medium=1, Fast=2
ARCPulseSpeed=1
;Card detection action LED Color: RGB 3 bytes hexa
;Green
ARCDetectionLEDColor=00FF00
;BlinkTimes [0..5]
ARCDetectionBlinkTimes=0
;ARCDetection LED duration x100ms
ARCDetectionLEDduration=4
;ARCDetection Buzzer duration x100ms
ARCDetectionBuzzerduration=4

;Added in V3.0.0 For ARC-S ARC1-S and ARC1 v2, user can select buzzer sound level
;0=Low, 1=Medium, 2=Loud
BuzzerSoundLevel=2

;;External control LED Color available for ARC and WAL series
;For ARC : RGB 3 bytes hexa
;For WAL : RGB 3 bytes hexa, allowed values = FF or 00
;Blue
ExtLED1Color=0000FF
;Yellow
ExtLED2Color=FFFF00
;Pink
ExtLED1LED2Color=FF00FF


;;For ARC and WAL Families AccelerometerSensitivity defines accelerometer sensibility
;0=Low,1=Normal,2=High
AccelerometerSensitivity=1

;Direct buzzer
DirectBuzzer=0
;Enable external LED/Buzzer control
EnableExtBuzzLED=0
;Polling period x100ms
ExtPolPeriod=1


;Biometric settings
; Security level [1..3] 3 is highest security
BioSecurityLevel=1
; Threshold level [0..10]
BioThreshold=5
; Nb of finger to enroll [1..5]
BioNb2Enroll=1
; Nb of finger to check [1..5] <= BioNb2Enroll
BioNb2Check=1
; Minutiae capture consolidation
BioConsolidation=0

; V3.3.0
; Duress biometric, 0 = disabled, 1 = enabled
BioDuress=0
; Auto change serial communication key 0 = disabled, 1 = enabled. For serial bidirectional readers or INTx
AutoChangeSerialCommKey=1

;ARC Enable Eco mode
ARCEco=0
;ARC DENY UHF configuration
```

```
ARCDenyUHF=0

;;Authenticated Encryption, available for ARC from firmware version Z02
;and WAL from firmware version Z18
;EnableAE = 1 to Enable AuthenticateEncryption and 0 to disable
EnableAE=0
;If AE enabled, enter User key 16bytes
AEKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

;;Touch Screen enable=1, disable=0, available for ARC-C/F with Screen
EnableTS=0
;;ARC with screen defines actions and associates texts, images can only be load with SECard in normal mode
(no CMDline)
;Enable(1) disable(0) Events
ARCTS_BadgeDetectionEvent=0
ARCTS_TamperingEvent=0
ARCTS_ExtLED1Event=0
ARCTS_ExtLED2Event=0
ARCTS_ExtLED1and2Event=0
;Default Text
;Text colors are in Red/Green/Blue 3 bytes hexa
ARC_TSTextColor0=0000FF
ARC_TSText1_0=Present your
ARC_TSText2_0=credential
ARC_TSText3_0=
;Badge detection text
ARC_TSTextColor1=00FF00
ARC_TSText1_1=Authorized card
ARC_TSText2_1=
ARC_TSText3_1=
;Tamper switch activation text
ARC_TSTextColor2=FF0000
ARC_TSText1_2=Alert
ARC_TSText2_2=Attempted tampering
ARC_TSText3_2=
;Biometric template
;NO TEXT for bio, hard coded in reader
ARC_TSTextColor3=000000
ARC_TSText1_3=Place your finger
ARC_TSText2_3=on the sensor
ARC_TSText3_3=
;External LED1 action text
ARC_TSTextColor4=FF0000
ARC_TSText1_4=Authorized access
ARC_TSText2_4=
ARC_TSText3_4=
;External LED2 action text
ARC_TSTextColor5=FF0000
ARC_TSText1_5=Access denied
ARC_TSText2_5=
ARC_TSText3_5=
;External LED1+LED2 action text
ARC_TSTextColor6=FF0000
ARC_TSText1_6=Free access
ARC_TSText2_6=
ARC_TSText3_6=
;ARC Reader with TS default Language
;0 for French, 1=for English
ReaderLANG=1
;ARC Reader with TS, display Ring
;1 to display
ARCTS_DisplayRing=0
;If keypad is active, you can choose to enable ScramblePad (set to 1)
ARCTS_ScramblePad=0
```

```
;Encoding type, used with UEncode command line parameter
; 0 = PId, 1 = PId AND Biometric template, 2 = Only Biometric
; See DESFire settings for Biometric template location and security
EncodingType=0


;ARC TouchScreen Display Option
;Keypad=0, DefaultImage=1
DisplayOption=0

;Blue Mobile ID Reader Configuration
;Configuration name, max 14 chars
BlueMobileIDReaderConfigurationName=AyConfigNameB
;Configuration Site Code 2 hexdecimal bytes
BlueMobileIDReaderConfigurationSiteCode=92AD
;Identification modes, disable=0, enable=1
IdModeBadge=1
IdModeSlide=0
IdModeTapTap=0
IdModeHandsFree=0
IdModeRemote=0
;Identification mode distances
;0=Contact, 1=0.2m, 2=0.3m, 3=0.5m
IdModeBadgeDistance=0
;0=Very Low, 1=Low, 2=Medium, 3=High, 4=Very high distance
IdModeSlideDistance=0
;Less than 3m=0, less than 5m=1, less than 10m=2, less than 15m=3
IdModeTapTapDistance=0
;Less than 3m=0, less than 5m=1, less than 10m=2
IdModeHandsFreeDistance=0
;Less than 3m=0, less than 10m=1, less than 15m=2, less than 20m=3
IdModeRemoteDistance=0
;Remote options =0 for Remote 1, =1 for Remote 2
IdModeRemoteOptions=0
;Requires smartphone unlocking to authenticated
;NOT required=0, required=1
BlueMobileIDReaderConfigurationRequiresUnlocking=0
;STid Mobile ID CSN configuration activation, 0 =disable, 1=enable
STidMobileIDCSN=0


;;Added in SECard V3.1.0, begin

;TamperSwitchAsProtocol define the tamper signal a the protocol, 1 to enable
;Can be selected only if Classic Tamper switch is NOT selected and if Common frame for Tamper and Life signal is NOT selected
TamperSwitchAsProtocol=0

;If TamperSwitchAsProtocol=1, the TamperSignalValue must be set
;1 to 16 hexa bytes or 1 to 10 digits decimal, radix is defined by the current Reader's protocol
TamperSignalValue=0A0B0C0D0E

;Rotation of the screen of the ARC with Touchscreen, set to 1 to enable
ARCTS_Rotation=0

;ARC keypad backlight, set to 1 to enable
ARCKeypadBacklight=0
;ARC on keypad pressed Buzzer, set to 1 to enable
ARCOnKeypadPressedBuzz=0
;ARC on keypad pressed flicker, set to 1 to enable
ARCOnKeypadPressedFlicker=0

;ARC Bluetooth LED flashes at BT connection, set to 1 to enable
```

```
ARCBlueLightAtBTConnection=0
;If ARCBlueLightAtBTConnection=1, change the LED color, RGB 3 bytes hexa, default=FFFFFF=White
ARCBlueBTConnectionColor=FFFFFF
;ARC Bluetooth Mode/Algo, 0=STid Mobile ID, 1=Orange PackID, 2=STid Open API
ARCBlueMode=0

;;Added in SECard V3.1.0, end


;;Added in SECard V3.2.0, begin
;Affect the LED brightness, 0=Normal brightness, 1=subdued light
ARCSubduedLED=0
;;Added in SECard V3.2.0, end


;;Added in SECard V3.4.0, begin
;Biometric FakeFinger Detection (MorphoSagemIdemiaDevice/SupremaDevice), 0=Disabled, 1 =Low/Weak,
2=Medium/Normal, 3=High/Strong,4 Critical
BioFFD=0

;Mute all reader sound, to mute set to 1
MuteAll=0

;CardDetectionCloseRelay close relay @ card detection during a delay, duration is in second from 1 to 20
CardDetectionCloseRelay=0
CardDetectionCloseRelayDuration=1

;BlueTooth External Hand, hand detection managed by external
BTExternalHand=0
;Manage additionnal SAK and ATQA for specific smartphone, up to 3 new ATQASAK (hex value), 000000
means not used, 4578A9 means new SAK=45 and new ATQA=78A9
ATQASAK1=000000
ATQASAK2=000000
ATQASAK3=000000

;;Added in SECard V3.4.0, end


;;Added in SECard V3.5.0, begin
; Reader Matrix Code settings  : disable=0, enable=1
DataMatrix=1
QRCode=1
AztecCode=1
Code128=1

;0=hex , 1=dev, 2=ASCII
MaxtrixCodeFormat=1

;DataMatrix Lightning Brightness  0/1
DataMatrixLB=1
;DataMatrix Lightning Target/aim  0,1,2
DataMatrixLT=2
;DataMatrix Detection sensitivity 0,1,2
DataMatrixDS=1
;DataMatrix Ambien light 0,1,2
DataMatrixAL=1
;;Added in SECard V3.5.0, end


;;Added in SECard V3.6.0, begin
;;Reader Prefix Suffix , max 5 bytes hexa string, ex Prefix=0A0102040F
Prefix=
Suffix=
```

```
;Reader adds IDLen, boolean value 1/0 to enable/disable
IDLen=0
;Reader adds IDTag, boolean value 1/0 to enable/disable
IDTag=0
;Command line Se import will use IDTagList defined in PSE

;W3i keyboard mode, site code value, one byte 0..255
KeyboardSiteCode=0

;Matrix code 39, boolean value  11/0 to enable/disable
Code39=1

;Keyboard backlight duration enable/diablen 1/0, and value in second
TimedBacklight=0
BacklightDuration=6

;;Added in SECard V3.6.0, end


[DESFire]
;Detection type: 0=UID, 1=PrivateID, 2=Private ID but UID
DetectionType=1

;Key mode: 0=One key per file (RW), 1=Two keys per file (R and W)
KeyMode=0

;Crypto mode: 0=3DES, 1=AES, 2=AES but 3DES
CryptoMode=0

;Card Master Key
;change : 0=No change, 1=Change with NewCMK
CMK=00000000000000000000000000000000
ChangeCMK=0
NewCMK=00000000000000000000000000000000

;Application Master Key
;change : 0=No change, 1=Change with NewAMK
AMK=00000000000000000000000000000000
ChangeAMK=0
NewAMK=00000000000000000000000000000000

;Diversification
;3DES diversification key
;Enablediv=0 NO div , = 1 div enabled
;alsoCMK also diversify CMK , =0 No, =1 Enable
;NXP diversification 32 bytes padding, =0 No NXP, =1 NXP enable

Enablediv=0
3DESdivK=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
alsoCMK=0
NXP=0

;Added in SECard V2.2.0
;NXP Padding, active if NXP=1, 20 bytes of padding data
;If you want to read/encode French CIMS card your have to set to 80000000000000000000000000000000000000000000
NXPPadding=0000000000000000000000000000000000000000

;Added in SECard V2.2.0
;If NXP diversification is selected you can also modify the MSB/LSB read direction of AID to compute diversified key
;If you want to read/encode French CIMS card your have to set to 1
AIDreversed=0
```

```
;Added in SECard V2.2.0
;FID1 Data type 0=RAW classical type and can be encoded, 1=ASCII Decimal value cannot be encoded
FID1DataType=0

;Added in SECard V3.0.0
;For NXP diversification (NXP=1), consider data as input or padding, and determine to use K1 or K2 of CMAC sub keys
;0 for padding (K2), 1 for input (K1)
InputPadd=0

;Added in SECard V3.0.0
;In case of RandomID DESFire, allow user to specify a key nb/value to get the real UID using the GetUID DESFire function
;GetUIDKeyNb=0 means AMK
GetUIDKeyNb=0
GetUIDCurrentKeyValue=00000000000000000000000000000000
ChangeGetUIDKeyValue=0
GetUIDNewKeyValue=00000000000000000000000000000000

;Format DESFire card before encoding, need CMK
;=1 Format , =0 NOT format
Format=0

;RandomID, =0 no RandomID, =1 Configure DEFire to RandomID
RandomID=0

;MSB first, =0 No, =1 Yes, Most Significant Byte First
MSBFirst=0

;Free Application Directory allowed=1 (No authentication required), no=0 (need authentication)
FreeAppDir=0

;Added in SECard V3.0.0
;Free Creation/deletion of AID's files
FreeCD=0
;DESFire Communication mode, 0=Plain, 1=MACed and 2=FullyEncphered (default value)
CommMode=2

;AID 3 bytes application identifier
AID=F51BC0

;Authenticate with Key Itself before Change Key value
;0=Use AMK
;1=Use KeyItself
DESFireChangeKeyKeyIDItself=0

;FID1 settings
FID1ID=0
FID1KeyID=0
;AsFID2: to encode FID1 with FID2 settings (keys)
AsFID2=0

;Keys used in KeyMode=0 (One RW key)
FID1RWKey=00000000000000000000000000000000
FID1ChangeRWKey=0
FID1NewRWKey=00000000000000000000000000000000
;+keys used in KeyMode=1 (Two keys R and W)
FID1WKeyID=2
FID1WKey=00000000000000000000000000000000
FID1ChangeWKey=0
FID1NewWKey=00000000000000000000000000000000

;Private ID/UID to encode/read
FID1size=5
```

```
FID1offset=0

;FID2 settings
FID2Enabled=0
FID2ID=0
FID2KeyID=3
;Concatenate=1: to encode/read FID1 data+FID2
;First= not Concatenate; to encode/read First FID read (authenticated)
Concatenate=0

;Write =0 NOT write FID2, =1 WRITE FID2 after (but in the same process) FID1
WriteFID2=0

;Keys used in KeyMode=0 (One RW key)
FID2RWKey=00000000000000000000000000000000
FID2ChangeRWKey=0
FID2NewRWKey=00000000000000000000000000000000
;+keys used in KeyMode=1 (Two keys R and W)
FID2WKeyID=4
FID2WKey=00000000000000000000000000000000
FID2ChangeWKey=0
FID2NewWKey=00000000000000000000000000000000

;Private ID/UID to encode/read
FID2size=5
FID2offset=0

;Biometric template location and security
;Biometric template location is forced into PId AID, and the security used is the same crypto as the PId
BioFIDId=2

;BioFIDId Read/Write keys (One key mode)
BioFIDRWKeyId=1
BioFIDRWKey=00000000000000000000000000000000
ChangeBioFIDRWKey=0
BioFIDRWNewKey=00000000000000000000000000000000

;BioFIDId Write keys (Two keys mode)
BioFIDWKeyId=2
BioFIDWKey=00000000000000000000000000000000
ChangeBioFIDWKey=0
BioFIDWNewKey=00000000000000000000000000000000

;Added in SECard V3.1.0, Biometric exemption : 0=Disable, 1=Enable exemption
DESFireBioExemption=0

;Added in SECard V3.1.0, Diversification for ID¨Prime MD3811, only used for SCB and NOT for DESFire emulation PrivateID encoding
DESFireIDPrimeDiversification=0


;;Added in SECard V3.2.0, begin
; DESFire EV mode : 0=EV1 mode  only, 1=EV2 else EV1 mode, 2=EV2 mode only
DESFireEVMode=0

; If card and selected EV mode is EV2 then user can choose to lock card in EV2 mode only by setting
DESFireLockEV2Mode=1
DESFireLockEV2Mode=0

; If card is an EV2 then user can choose to use DESFire EV2 Proximity Check by setting
DESFireEV2ProxCheck=1
DESFireEV2ProxCheck=0
; and defines max time to get a response from the chip, in multiple of 100 µs
DESFireEV2ProxCheckRespTime=20
```

```
;;Added in SECard V3.2.0, end

;; SECard v3.5.0
; UID MSB First ofr DESFire UID read mode, 0=disabled, 1=enabled
DESFireUIDMSBFirst=0
; If selected crypto is 3DES user can select divAV1 diversification; set to 1 to enable
DESFiredivAV1=0

[BlueMobileID]
;Added in SECard V3.0.0
;Virtual access card name max 14 characters
BMIDVCardName=AyVCardNamB

;Blue Mobile ID Read mode, 0 = PrivateID, 1=From DESFire configuration
;if From DESFire configuration is selected, all BlueMobileID settings will be ignored and replaced by DESFire
configuration
BMIDReadMode=0

;Keytype, 0=one key, 1=two keys
BMIDKeyType=0

;KeyValues, all key are 16 hexa bytes, *Change* = 0 for non change, =1 for changing
BMIDCurrentRWK=00000000000000000000000000000000
BMIDChangeRWK=0
BMIDNewRWK=00000000000000000000000000000000
;Write keys are only used if Keytype=1
BMIDCurrentWriteK=00000000000000000000000000000000
BMIDChangeWriteK=0
BMIDNewWriteK=00000000000000000000000000000000

;Data size/offset/reverse
BMIDDataSize=5
BMIDDataOffset=0
BMIDDataReverse=0

;Display options , 0=disable, 1=enable
BMIDDisplayConfName=1
BMIDDisplaySiteCode=1
BMIDDisplayDisplayID=1
BMIDDisplayDisplayRemote1=1
BMIDDisplayDisplayRemote2=0
;Added in SECard v3.2.1, ask user to first unlock (=1) his smartphone before authentication
BMIDLockVCard=0
;Added in SECard v3.3.0, forbid user (=1) to delete VCard from the mobile app
BMIDProhibitVCardDeletion=0



;;Added in SECard V3.1.0, begin
; If ARCBlueMode=1=OrangePackID, CompanyId = 2 hexa bytes, ServiceId = 4 hexa bytes, AccessId = 6
hexa bytes, TX power integer value
BTS_OrangePackID_CompanyId=0000
BTS_OrangePackID_ServiceId=00000000
BTS_OrangePackID_AccessId=000000000000
;BTS TXPower in dbm : 0=-16, 1=-12, 2=-8, 3=-4, 4=0, 5=4
BTS_OrangePackID_TXPower=2
;;Added in SECard V3.1.0, end


;;Added in SECard V3.2.0, begin
;If ARCBlueMode=2=Open Mobile Protocol
;Complete local name, max 5 char
OMP_CLN=ARCoa
```

```
;Site Code two hexa bytes
OMP_SiteCode=51BC
;3 General purpose bytes
OMP_GPBS=000000
;To enable secure communication set to 1
OMP_SecureComm=0
;To set TX power dbm : 0=-16, 1=-12,2=-8,3=-4,4=0,5=4
OMP_TXPower=5
;To set CompanyID : two hexadecimal bytes, STid ID by default
OMP_CompanyId=51BC

;;Added in SECard V3.2.0, end

;;Added in SECard v3.4.0
;Request user for biometric smartphone unlock before any authentication
BMIDBioLockVCard=0
```

T13.7 - Securing the command line mode

To secure the command line operation, it must be secure:

- The import configuration file, loaded with -i parameters
- The login by securing the parameters –u et –p that appear in plain

Note: If the import configuration file is used in encrypted then just put the parameters –u et –p as data in this file.

Changes to the files .gcf

The addition of the security in command line mode involves modifications of the data (for illustrative purposes) in SeCard.gcf file.

```
[Login]
ACCESSLevel=2

[File]
Settings=.\SeCard.pSe
Location=0

[Serial Number]
SN=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
PN=xxx……

[Lang]
;1033=Us
;1036=Fr
LangID=1036


[CompatibilityVersion]
eSe_SCB=1

[CommandLineRSA]
; This section ONLY exhibits values integrated in SeCard, none of them is used.
; This is just to remind the values defined in Manual/Specifications.

; RSA decryption for command line configuration file import
; fixed public exponent e = 010001(hex)
; keyLen : 1=1024bits, 2=2048bits, 4=4096 bits

; Key for RSA 1024 bits
;RSA_pub1=3CA377661F13DE29E51E9C2B94CBB7F58EEE4B40377FA3FE22A0EC37F965E7D810E64CC01F3
3391B7FB6A85AC13CEC7D16EA07B07ACA67934A39C79985D13FC0B1599FEB435721CA4192A31AB805D82
39DC52D1F7F55DED1452DC2309824AB655E719371BD9A103D6AC0308EEEDEAE57E0B14B978DA47A2DBE
73377471132D05
;RSA_priv1=PRIVATE

; Key for RSA 2048 bits
```

;RSA_pub2=E511A50D7CE6C94D37B99EA0206F5CBDB1402C5D20BA92CEFDF29C1D553A645BCAD3C2D118
068F7AF1EB49D577C76E170993291ABA56E1E4DC1119539D8EBA635140DCD51B6F36A949FA7E88594683
8796FFC09DC57CD1B1B0649F9B15B5610934EAF62DD0B51BA327F7C65E28EC400D6380E9F9CA0C3D6C4F
AEBB1F6CCA2FFBDB4199A6DDF2E43A761AEA83DFF176909AE772DC453CFA9D54C24600E3B2B8ABB2574
9D610B5DC85E9146E59AB46AB07A87B6C1F813A53DDCB5C6119BB6ABAEAB3788B0F2B23382A6FB8B617
77AF67C4F1606AC199A0BDB40A4B0BE5C104D773293790D64743028C79C88C61E76C90460696D8CD42AA
E7718246DC1B1B38F329
;RSA_priv2=PRIVATE

; Key for RSA 4096 bits
;RSA_pub4=5EE503A29011327ECC85F50144CEB2009663DCE96A1EE2C20E065067DCF5D2585FB4ECA532E
DB213A7859F32398958C37088563A0795E482DFD67929EF5C6195DECE80B9D55E54F0644C3A90DFEBDCE
01D84255B3BA4A4B4499D409F00C82065645D1096B07C0466C8BF52C037CD360FB068895D5787825F50FC
A1307058087D7BA045517F7BA4C9B4A9357A1C409ED2FB2C3425FE8F6FCAD6344CF8E798BFB87A417A83
27BC443E8D6F32211758F50A74AC56B2E3EFFBA38AE087E3844AA742864F3C64AB182E6D4A5F2346648F3
1796146B705A2B5B02EA867247258560DAC206F4CE9040C458B81197E051A1EB7A40C81A6D3A39A4CCB6
EC1667CDCC77F2C0C4D74CE98D9BC0DA4C3088E7348F4E1B20AC13B9D099ACEF1A720C2CF41B06E7B316
DBCBE167A2F0CC69FABED315C308307CF8AD7BC2FCA14861E92CC51DD0654A66639766BC2BF42F5D39A7
2FBB1594CBC20073AFDEE531226024DF3CAF4790BA147FE71315672751AED93833EFC915B7B8A9DF9387
6C53B466B72553F8C7B84B32CD19C00BAF61F9902A346D2F1ABF0223CC21C1EEFC5838B7B4859F983A530
14693838B45B08CF65F1E9BFB8B5AC420F595ADAEE893F854174D51749F31C074E61A9806080A0184F1C2
C0D11AA82367C8C9B1299D4FB7F3A271BDF5811C8B9A17843288CA390ADCFBD28E7DDD0C8611B02F959
AAB9703BF595FA1B46CF77

;RSA_priv4=PRIVATE

Encryption of .Se file in .CSe

To encrypt the import configuration file use the DLL CmdLineLib.dll.

The DLL, its user manual and two sample applications are available in the folder SECard

T14 - Recommendation to save the configuration files PSE

T14.1- Definition

Configuration files .pse are the files created by SECard. They contain all the configuration settings of the readers, RFID chips setting and **login** SECard passwords.

These files are encrypted with AES-CBC using user key (k). This key is generated from the user login password and uses PBKDF2.

These files are therefore unusable without SECard. Of over .pse files can be locked by a read password, one will be asked to open. This password uses a hash key.

T14.2 - Use

The default .pse configuration file (comes with SECard) is file Secard.pSe, that is located in the SECard installation directory.

At the first opening of SECard it is necessary to fill in the fields on the communication with the RFID encoder (STR-xx).

It's possible to save these settings (and all other) in another file. PSe using a file name and a directory different from the default. The last file PSe used will be automatically loaded to open SECard.

T14.3 - Recommendations

.pse files contain sensitive data, it is therefore necessary to consider, backup and archiving. It is therefore advised to follow the recommendations:

- Use pse locked files with different login password.
- Limit the diffusion of these files
- Save files pSe on a computer other than the one used to encode
- Archive pSe files on a media unmodifiable (CD / DVD)
- In the last option the user can retrieve the current settings and save the list of parameters in a text file, which is protected by a third method (eg rtf file product can be zipped, encrypted and backed up by the entity in charge security).

Users who have access to SECard and can open files pSe have access to the data they contain therefore the values of security settings (key values, cryptography used ...), so be careful that these people are trained to using SECard and that they are of confidence (authorized..).

T15 - Glossary

- ✓ **AES:** *Advanced Encryption Standard*. Encryption algorithm using a public key of 128, 192 or 256 bits. SECard uses 128 bits keys.
- ✓ **AES-CBC:** *Advanced Encryption Standard* with Cipher Block Chaining
- ✓ **ADF:** Application Dedicated File.
- ✓ **APK:** Android Package file.
- ✓ **Application:** Application contains data files.
- ✓ **Application Master Key:** Application master key of MIFARE® DESFire® and MIFARE® DESFire® EV1 RFId chips.
- ✓ **Authentication:** Security mechanism based on an algorithm (AES, Crypto1 etc. ...) using a key.
- ✓ **BCC:** Check Byte of CSN. Used by MIFARE Ultralight® and MIFARE Ultralight® C.
- ✓ **Card Master Key:** Card master key MIFARE® DESFire® and MIFARE® DESFire® EV1.
- ✓ **Company key:** Protecting key of « *SCB* » badge and reader it configure.
- ✓ **Crypto1:** Private Encryption Algorithm (*NXP*) based on 48 bits key. Used by MIFARE® Classic and MIFARE Plus® Level 1.
- ✓ **CSN:** Chip Serial Number
- ✓ **DF:** Dedicated File
- ✓ **EF:** Elementary file
- ✓ **Encoding:** User code in chip memory writing.
- ✓ **FCP:** File Control Parameter
- ✓ **FID:** *File Identifier*. File number.
- ✓ **Format:** MIFARE® DESFire® and MIFARE® DESFire® EV1 chips format.
- ✓ **HCE:** Host Card Emulation.
- ✓ **Lock Bytes:** Used by MIFARE Ultralight® and MIFARE Ultralight® C chips.
- ✓ **MAD:** Mifare® Application Directory. For more details, please refer to the *NXP* documentation AN10787 MIFARE® Application Directory (MAD).pdf.
- ✓ **Mifare Plus Levels:** Security levels of MIFARE Plus® chip.
  - ➢ **Level 0:** MIFARE Plus® configuration security level
  - ➢ **Level 1:** MIFARE® Classic Compatibility level. Use *Crypto1*algorithm.
  - ➢ **Level 2:** Not used by SECard. Intermediate level.
  - ➢ **Level 3:** Strong security level. Use *AES* encryption algorithm.
- ✓ **NFC: Near Field Communication**
- ✓ **OCB:** Configuration Badge for OSDP readers.
- ✓ **OTP:** *One Time Programming*.
- ✓ **PBKDF2:** key derivation function **(Password-Based Key Derivation Function 2)**
- ✓ **Private ID:** Private (user) Code.
- ✓ **PUPI:** 14443-B chip serial number.
- ✓ **SCB:** Secured Configuration Badge for TTL readers.
- ✓ **SCB-R/W:** Secured Configuration Badge for Read/Write readers.
- ✓ **SSCP®:** STid Secure Common Protocol.
- ✓ **SKB:** Secured Key Bundle contains AES-3DES-Crypto1 keys, it is used by RS232 RS485 and USB readers to deal with indexed security keys.
- ✓ **UID:** Unique ID, unique chip identification number.
- ✓ **3DES:** *Triple Data Encryption Standard.* DES variant, the algorithm is based on two keys of 56 bits.
- ✓ **Diversification keys -** For more details, please refer to the following *NXP* documents:
  MIFARE® DESFire® EV1 and MIFARE Plus®:AN-165310.pdf MEthode NXP MIFARE® SAM
  MIFARE® Classic: P5DF072EV2.pdf §8.6.1
  MIFARE Ultralight® C: P5DF072EV2.pdf §8.6.2

SECard V3.6 evolution – Firmware version Z17 / osdp-Z11

Date	Description
08/07/2021	**Added:** - Compatibility badges AMC. - Add ID-Tag, ID-Len, Prefix and suffix for serial (R32/R33) and ospd reader. - Compatibility for Screen readers with characters Ð Þ ð þ and German Ü, ü, ß, ° and §. - QR Code: Compatibility with code 39. - QR Code: Prefix and Suffix management. - Keypad: specific mode 26-bit Wiegand. - Keypad**:** backlight with timing. - Protocols: Wiegand 38 bits (W3Y) and Wiegand 72 bits (W3Z) - osdp: Creation of the configuration file for the FileTransfer command. - osdp: Compatibility with STid Settings for reader configuration. - osdp: Modification of the IEEE number + legacy management
	Modification: - Use only of DESFire EV2 / 3 8 kb badge for the creation of SCB / OCB - CPS3: modification timeout RF
	Suppression - Mode “Bio Hors CNIL” (biometry into the reader)

REVISION

Date	Version	Description
25/03/2014	*5.0*	*Creation.*
18/04/2014	*5.1*	*Changing screen printed following the removal of the question mark "About"* *"Mutual Life and Wrenching signal" added for R33+INTR33E (p25, 37, 128)* *Verbose mode added in command line (p130-132)*
03/12/2014	*5.2*	*Reference ARC USB reader added / Security certificate installation added / Compatibility table modified / Warning on administrator rights added /Step by step for "Save as" added / Wizard SCB WAL print screen added / Table of chip available to create SCB / Wizard SCB WAL added / Authenticate encryption for ARC added / Red LED on tearing added / Scramble option added / Step 7 in wizard SCB ARC added / Authenticated encryption key added / Note about formatting DESfire added / ARC-F added / File Se modified / All print screen changed.*
02/03/2015	*5.3*	*Security certificate delivered by a trusted certificate authority instead of the certificate STid/ Chip activation added in settings file for command line*
14/12/2015	*5.4*	*Part1:New compatibility version added (p9) / Modification of the passwords (p17-19) / ARC1 added (p50) / Biometric data into reader added in Wizard ARC (p58-59) / Data type to read added for DESFire FID ID1 (p69) / Diversification NXP with AID reversed and padding added (p72) / NFC-HCE setting sand keys added in Wizard LXS, WAL & ARC (p86-89) / "Key Ceremony creation mode" added for SKB(p96-99) / Creation of Biometric Configuration Card BCC added (p100-103) /* *Part2: ARC1 added (p126-p131) / Chip type HCE added in Wiegand 3T (p143) / Biometric Data into reader added (p162-164) / File Se modified/* *All print screen changed.*
19/12/2016	*6.0*	*Part 1: I.4 Windows installation location of user files added // I.6 Compatibility modified // II.2 Blue Mobile ID encoding added // II.4 Credit Request added // III.5 SCB ARC wizard: Blue Mobile ID options added // III.7 Mifare DESFire settings: configuration Blue mobile, communication mode added // III.8 Mifare DESFire keys: NXP diversification data, Diversified Key Random added // III.11 Mifare Classic settings: Biometric template sector added // III.15 Blue Mobile ID settings added // III.15 Blue Mobile IDkeys added // VI.1 Data: Random list added // VI.2:Encode Blue Mobile ID added // VI.3 STid Mobile ID+ added // VII.9 Update: example added.* *Part 2: T2.1: Powering up modified // T4.2: Protocol 3T BLE added // T5.2.2 Message structure modified // T10 Life signal function: specific signal added// T11 Tamper switch: specific signal added // T13.6 Import configuration file: new reader parameters added // SECard Evolution added.*
04/08/2017	*6.1*	*Part 1 : I.5 Compatibility modified // III Upload SCB via serial added // III.5 LED light at Bluetooth® connection // Keypad Options // Screen Rotation // Orange™ Pack ID // III.7 /9/11 derogation biometrics // III.8 IDPrime diversification //III.12 MAD key A // III.15 Read mode Blue // III.17 Orange™ Pack ID added // IV.3 Index keys assignation // VI.2 bio Derogation // VII.5 delete DESFire file*
23/10/2017	*6.2*	*Tools DESFire Delete Application and File for IDPrime added // -b to specify the Baudrate in command line*
19/03/2018	*6.3*	*Part 1 : I.5 Compatibility modified // II-2 user rights Use tools added for power user // II-3 File: Password generator added // II-4 Credits: Delete VCard and dynamic credit counter // III IHM modification // Step 6 of the configuration wizard : option to attenuate the LEDs added // Step 8 of the configuration wizard : Open Mobile Protocol added // In STidMobileID 2 new thresholds in card mode added // III-7 Predefined configurations DESFire & mode EV2 added // III-15- Add print Open Mobile Protocol // VII-5 DESFire tools lock EV2 added* *Part 2: T4.2 Protocol 3Eb 3V 3W added// T13.6 Modified configuration import file*
09/07/2018	*6.4*	*Addition: NFC Mobile ID*
11/12/2018	*7.0*	*Addition: OCB // R/W SCB // serial configuration RW reader/ / PAC &PAC64 protocol // Duress biometric // Deletion of all pages related to standard readers*
03/01/2020	*7.1*	*Addition related SECard v3.4 release.*
01/10/2020	*7.2*	*Addition related SECard v3.5 release.*
08/07/2021	*7.3*	*Addition related SECard v3.6 release.*