STid
Electronic Identification

SECARD

Designed in France
Made in France

www.stid.com

Contenu

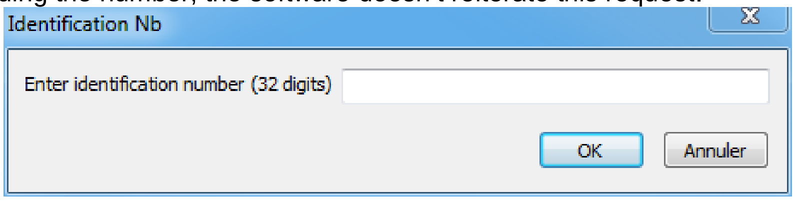
I. ARCS-R31-X-BT1-xx configuration

I-1. SECard settings

Step 1: Connect STid ARC-W35-G/BT1-5AA encoder to a com port of the computer.

Step 2: Launch SECard.exe ≥ V3.0

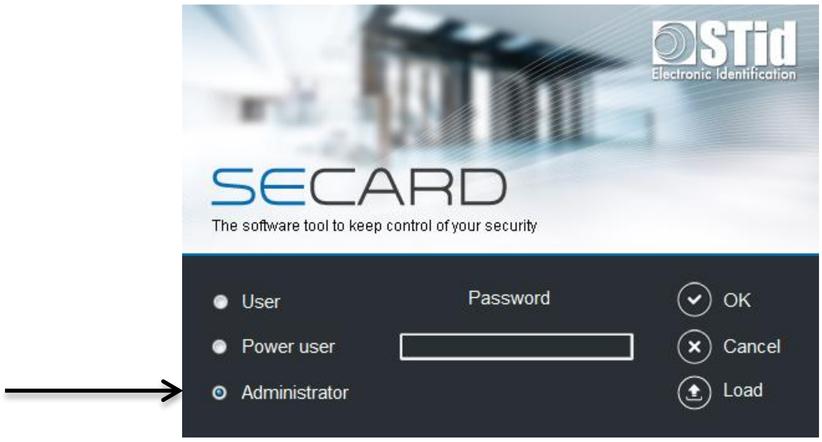
Step 3: At first use, the software opens a window to enter the serial number of 32 characters located at the back of the encoder. After recording the number, the software doesn't reiterate this request.



Identification Nb

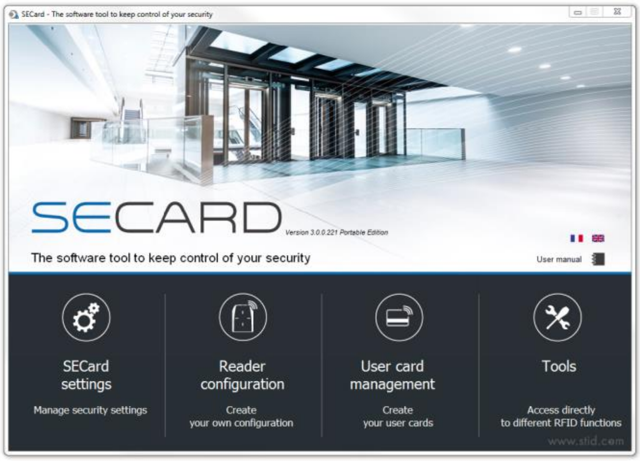
Enter identification number (32 digits)

Step 4: Select the Access level « Administrator » and the password: **STidA**

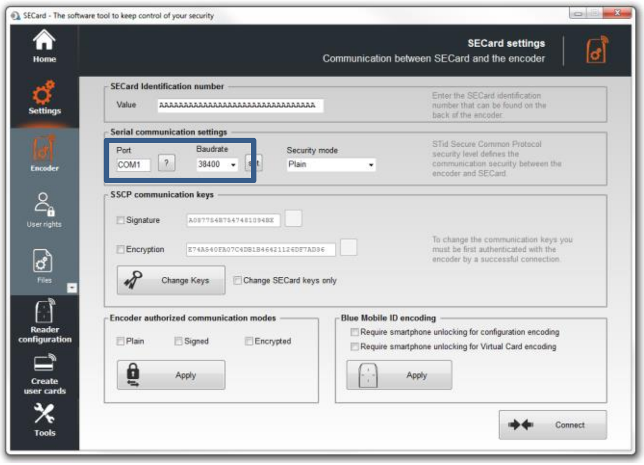


STid
Electronic Identification
SECARD
The software tool to keep control of your security
○ User
○ Power user
● Administrator
Password
OK
Cancel
Load

Step 5: In SECard settings, select the COM port on which the encoder has been connected, if you do not know the number click on the interrogation point.



SECard - The software tool to keep control of your security
SECARD
Version 3.0.0.221 Portable Edition
The software tool to keep control of your security
User manual
SECard settings
Manage security settings
Reader configuration
Create your own configuration
User card management
Create your user cards
Tools
Access directly to different RFID functions
www.stid.com



SECard - The software tool to keep control of your security
Home
Settings
Encoder
User rights
Files
Reader configuration
Create user cards
Tools
SECard settings
Communication between SECard and the encoder

SECard Identification number

Value: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Enter the SECard identification number that can be found on the back of the encoder.

Serial communication settings

Port: COM1 ?

Baudrate: 38400

Security mode: Plain

STid Secure Common Protocol security level defines the communication security between the encoder and SECard.

SSCP communication keys

□ Signature A08775487547481094BX

□ Encryption E74A640FA07C4DB1B46421126DF7AD36

Change Keys □ Change SECard keys only

To change the communication keys you must be first authenticated with the encoder by a successful connection.

Encoder authorized communication modes

□ Plain □ Signed □ Encrypted

Apply

Blue Mobile ID encoding

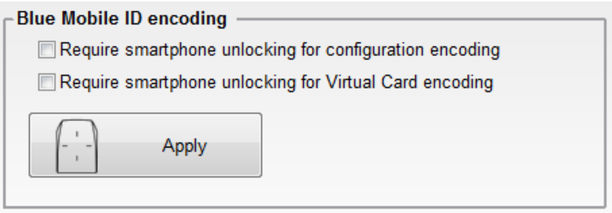
□ Require smartphone unlocking for configuration encoding

□ Require smartphone unlocking for Virtual Card encoding

Apply

Connect

Step 6: Define permission to encode in smartphone

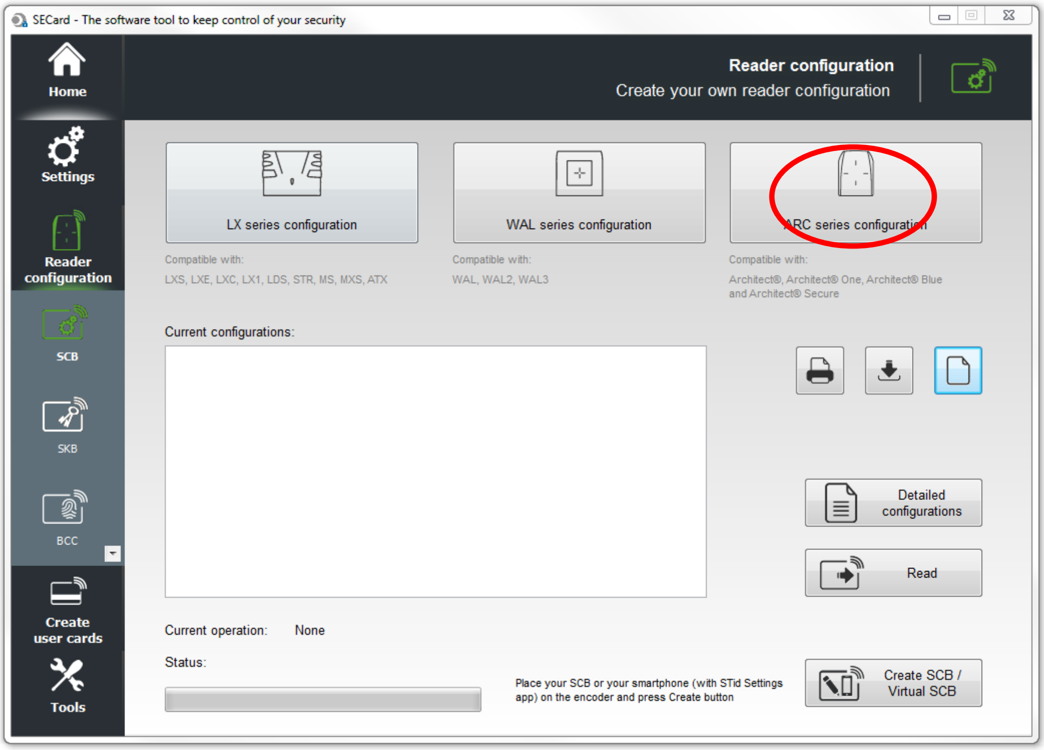


Blue Mobile ID encoding

□ Require smartphone unlocking for configuration encoding

□ Require smartphone unlocking for Virtual Card encoding

I-2. Select ARC series configuration wizard



SECard - The software tool to keep control of your security

Reader configuration

Create your own reader configuration

Compatible with: LXS, LXE, LXC, LX1, LDS, STR, MS, MXS, ATX

Compatible with: WAL, WAL2, WAL3

Compatible with: Architect®, Architect® One, Architect® Blue and Architect® Secure

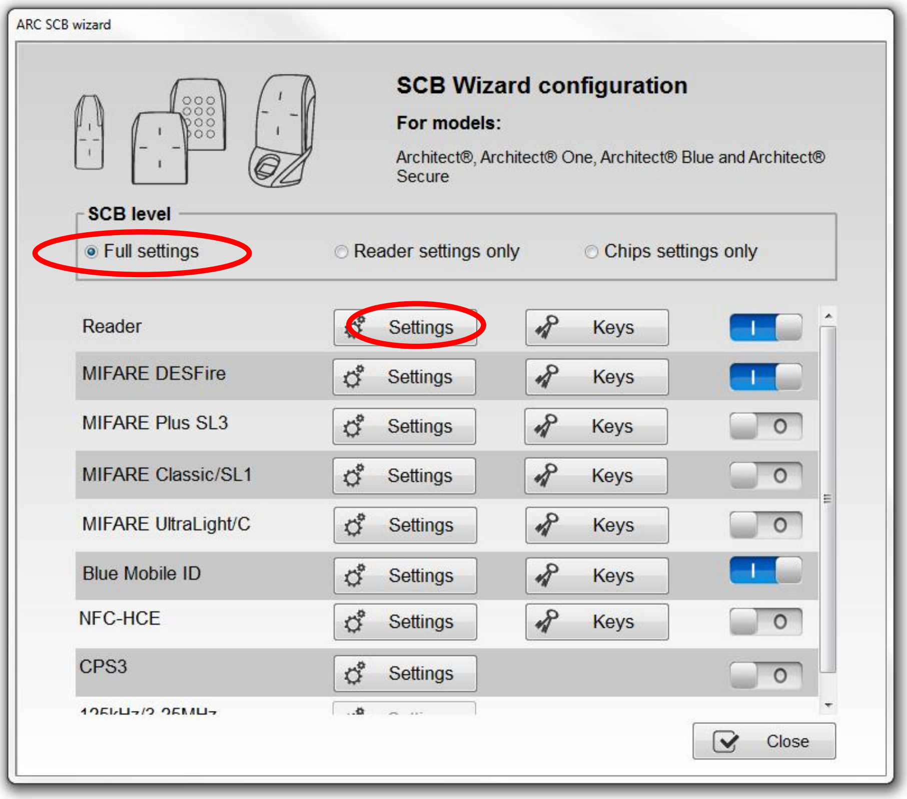
Current configurations:

Current operation: None

Status:

Place your SCB or your smartphone (with STid Settings app) on the encoder and press Create button

I-3. Reader: Setting



ARC SCB wizard

SCB Wizard configuration

For models:

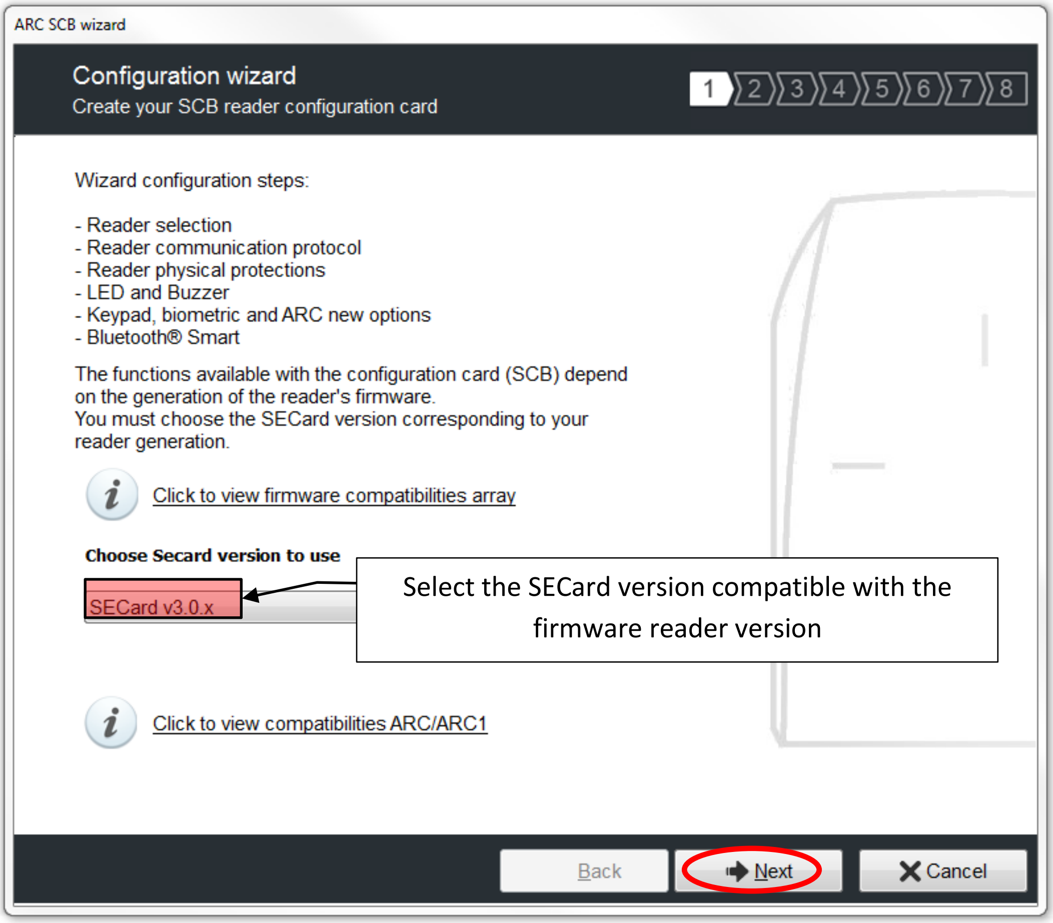
Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	I
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	I
NFC-HCE	Settings	Keys	O
CPS3	Settings		O
125kHz/3.25MHz	Settings		

Follow the 8 steps of the wizard:



Configuration wizard

Create your SCB reader configuration card

Wizard configuration steps:

- Reader selection
- Reader communication protocol
- Reader physical protections
- LED and Buzzer
- Keypad, biometric and ARC new options
- Bluetooth® Smart

The functions available with the configuration card (SCB) depend on the generation of the reader's firmware. You must choose the SECard version corresponding to your reader generation.

Click to view firmware compatibilities array

Choose Secard version to use

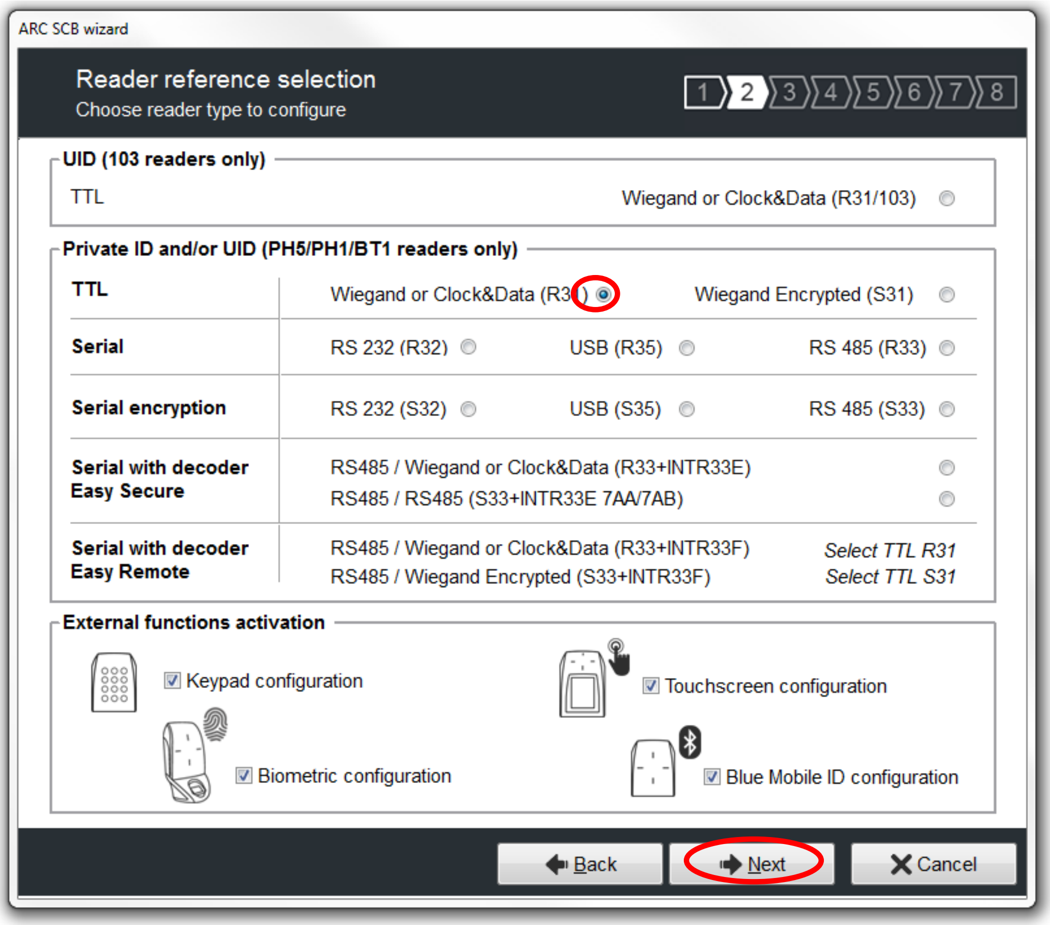
SECard v3.0.x

Select the SECard version compatible with the firmware reader version

Click to view compatibilities ARC/ARC1

The firmware version is located on the label of the reader and is indicated after the initialization phase of the reader by a color code:

Red	**= +10**
Orange	**= +5**
Green	**= +1**



ARC SCB wizard

Reader reference selection

Choose reader type to configure

UID (103 readers only)

TTL — Wiegand or Clock&Data (R31/103) ○

Private ID and/or UID (PH5/PH1/BT1 readers only)

TTL	Wiegand or Clock&Data (R31) ●	Wiegand Encrypted (S31) ○	
Serial	RS 232 (R32) ○	USB (R35) ○	RS 485 (R33) ○
Serial encryption	RS 232 (S32) ○	USB (S35) ○	RS 485 (S33) ○
Serial with decoder Easy Secure	RS485 / Wiegand or Clock&Data (R33+INTR33E) ○ RS485 / RS485 (S33+INTR33E 7AA/7AB) ○		
Serial with decoder Easy Remote	RS485 / Wiegand or Clock&Data (R33+INTR33F) RS485 / Wiegand Encrypted (S33+INTR33F)		*Select TTL R31* *Select TTL S31*

External functions activation

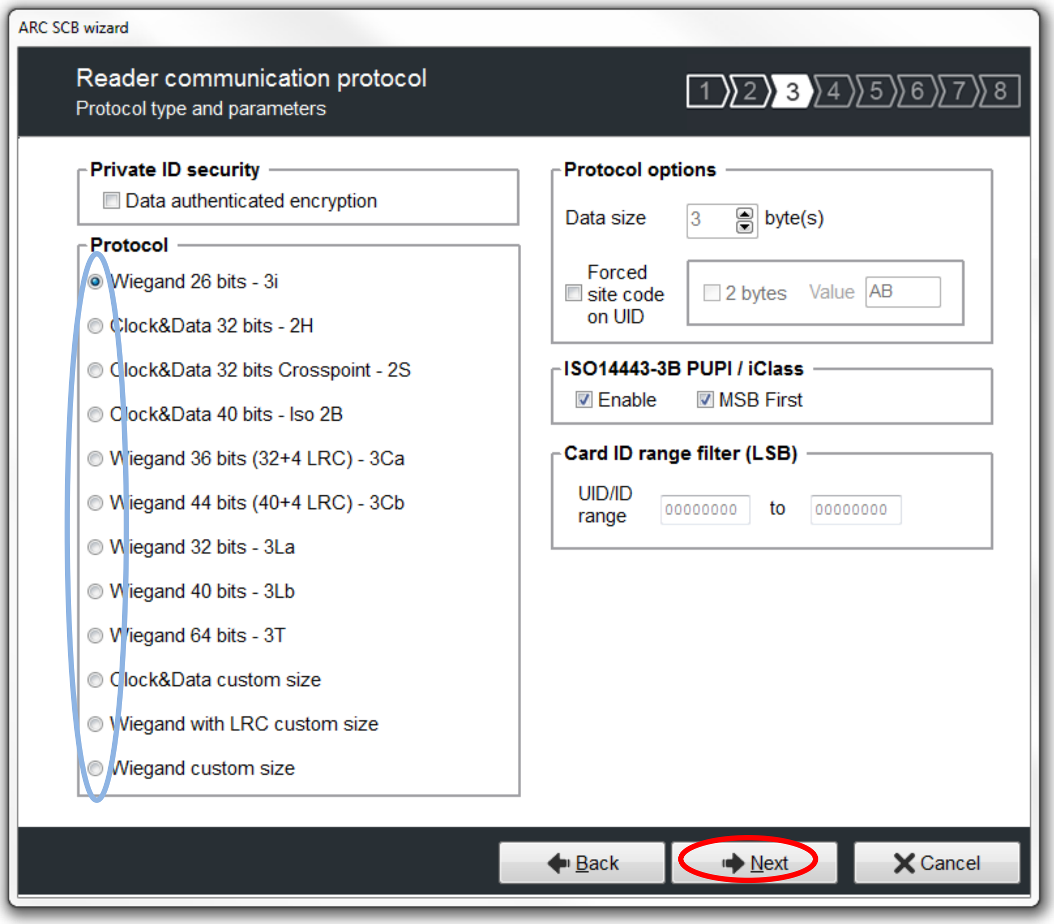
☑ Keypad configuration

☑ Touchscreen configuration

☑ Biometric configuration

☑ Blue Mobile ID configuration

All the options are activated in this guide (Keyboard, Biometry and touch screen) if one of the options is not used, deactivate it by unchecking the corresponding box.


ARC SCB wizard

Reader communication protocol

Protocol type and parameters

Private ID security

□ Data authenticated encryption

Protocol

● Wiegand 26 bits - 3i

○ Clock&Data 32 bits - 2H

○ Clock&Data 32 bits Crosspoint - 2S

○ Clock&Data 40 bits - Iso 2B

○ Wiegand 36 bits (32+4 LRC) - 3Ca

○ Wiegand 44 bits (40+4 LRC) - 3Cb

○ Wiegand 32 bits - 3La

○ Wiegand 40 bits - 3Lb

○ Wiegand 64 bits - 3T

○ Clock&Data custom size

○ Wiegand with LRC custom size

○ Wiegand custom size

Protocol options

Data size 3 byte(s)

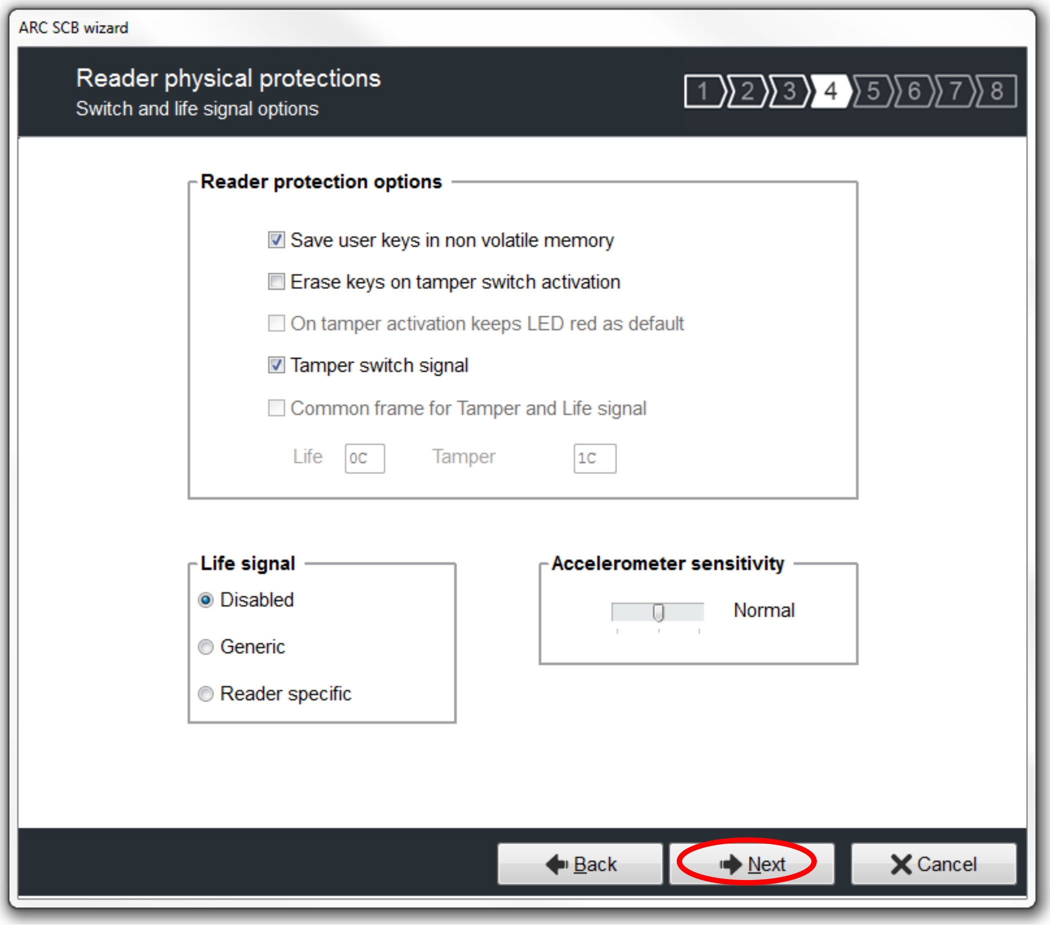
□ Forced site code on UID □ 2 bytes Value AB

ISO14443-3B PUPI / iClass

☑ Enable ☑ MSB First

Card ID range filter (LSB)

UID/ID range 00000000 to 00000000


ARC SCB wizard

Reader physical protections

Switch and life signal options

Reader protection options

☑ Save user keys in non volatile memory

□ Erase keys on tamper switch activation

□ On tamper activation keeps LED red as default

☑ Tamper switch signal

□ Common frame for Tamper and Life signal

Life 0C Tamper 1C

Life signal

● Disabled

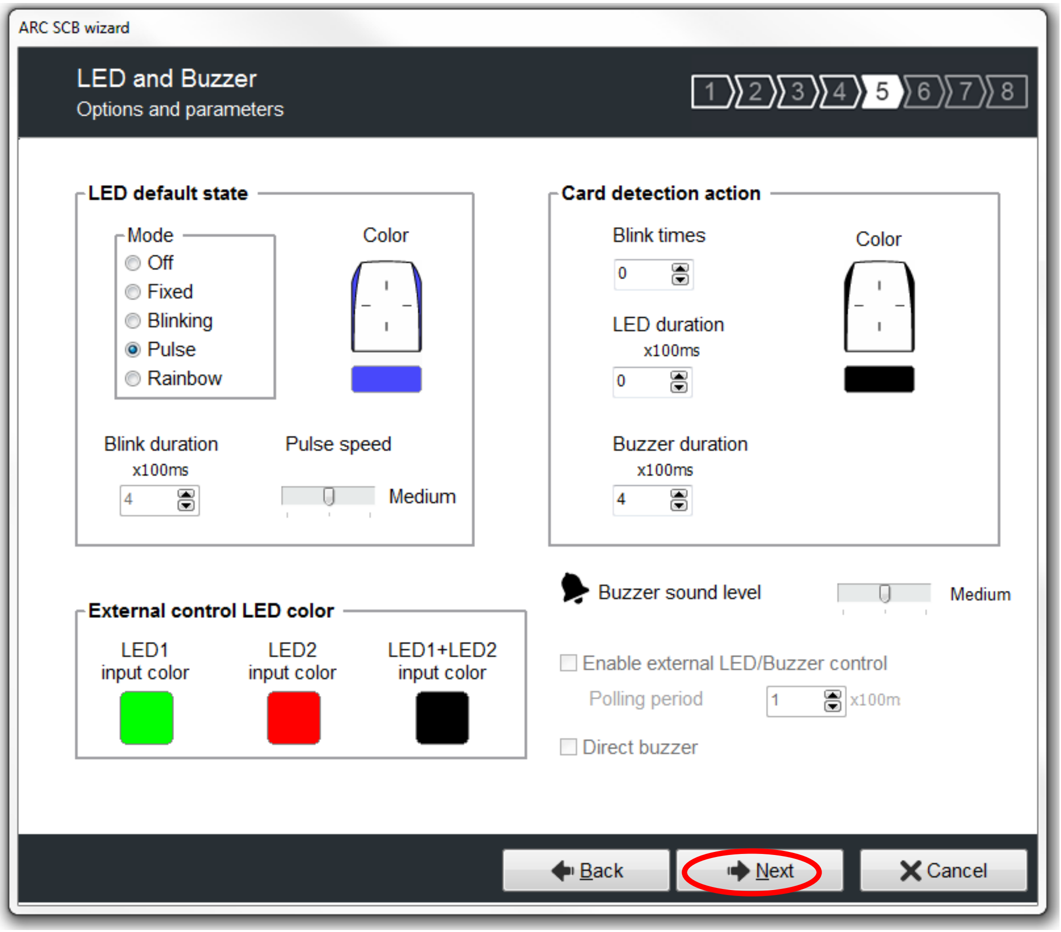
○ Generic

○ Reader specific

Accelerometer sensitivity

Normal

Are checked the most commonly used options, it is possible to activate or deactivate these options according to your specifications.



ARC SCB wizard

LED and Buzzer

Options and parameters

LED default state

Mode
○ Off
○ Fixed
○ Blinking
● Pulse
○ Rainbow

Color

Blink duration x100ms: 4

Pulse speed: Medium

Card detection action

Blink times: 0

LED duration x100ms: 0

Buzzer duration x100ms: 4

Color

External control LED color

LED1 input color: 🟩

LED2 input color: 🟥

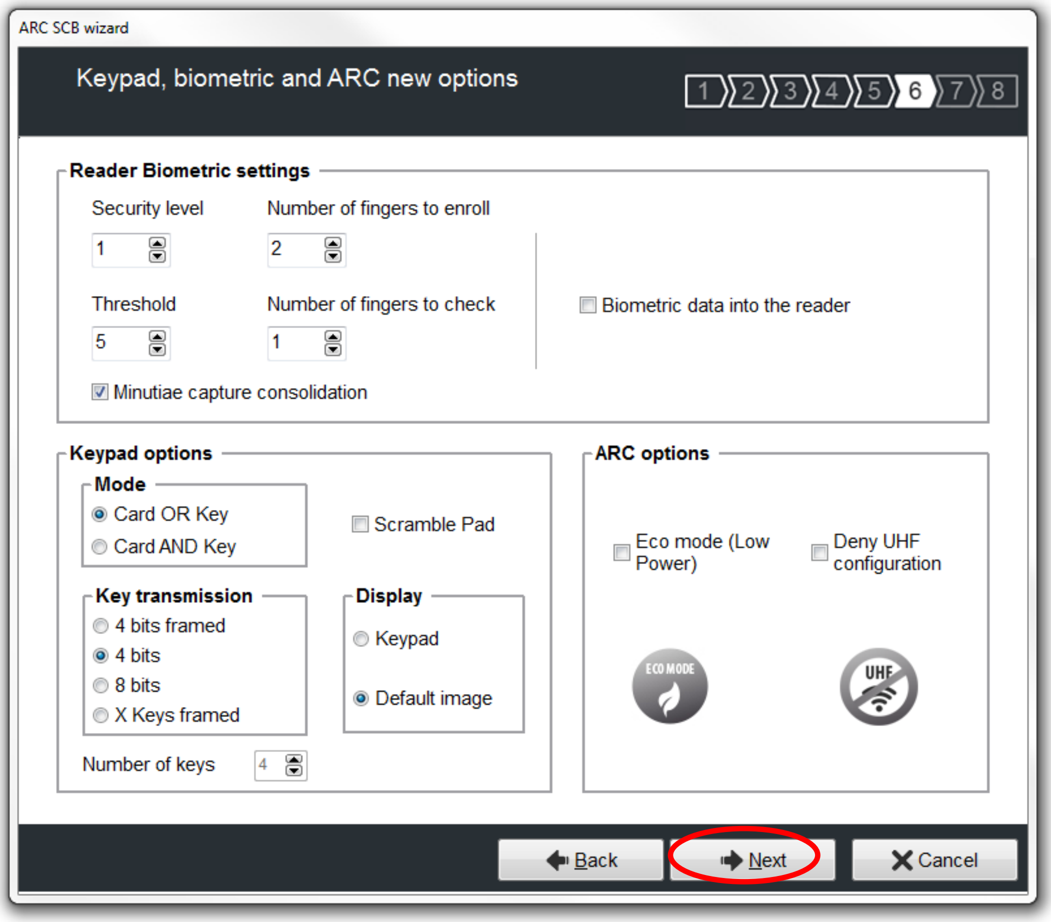
LED1+LED2 input color: ⬛

Buzzer sound level: Medium

□ Enable external LED/Buzzer control

Polling period: 1 x100m

□ Direct buzzer



ARC SCB wizard

Keypad, biometric and ARC new options

Reader Biometric settings

Security level: 1

Number of fingers to enroll: 2

Threshold: 5

Number of fingers to check: 1

□ Biometric data into the reader

☑ Minutiae capture consolidation

Keypad options

Mode
● Card OR Key
○ Card AND Key

□ Scramble Pad

Key transmission
○ 4 bits framed
● 4 bits
○ 8 bits
○ X Keys framed

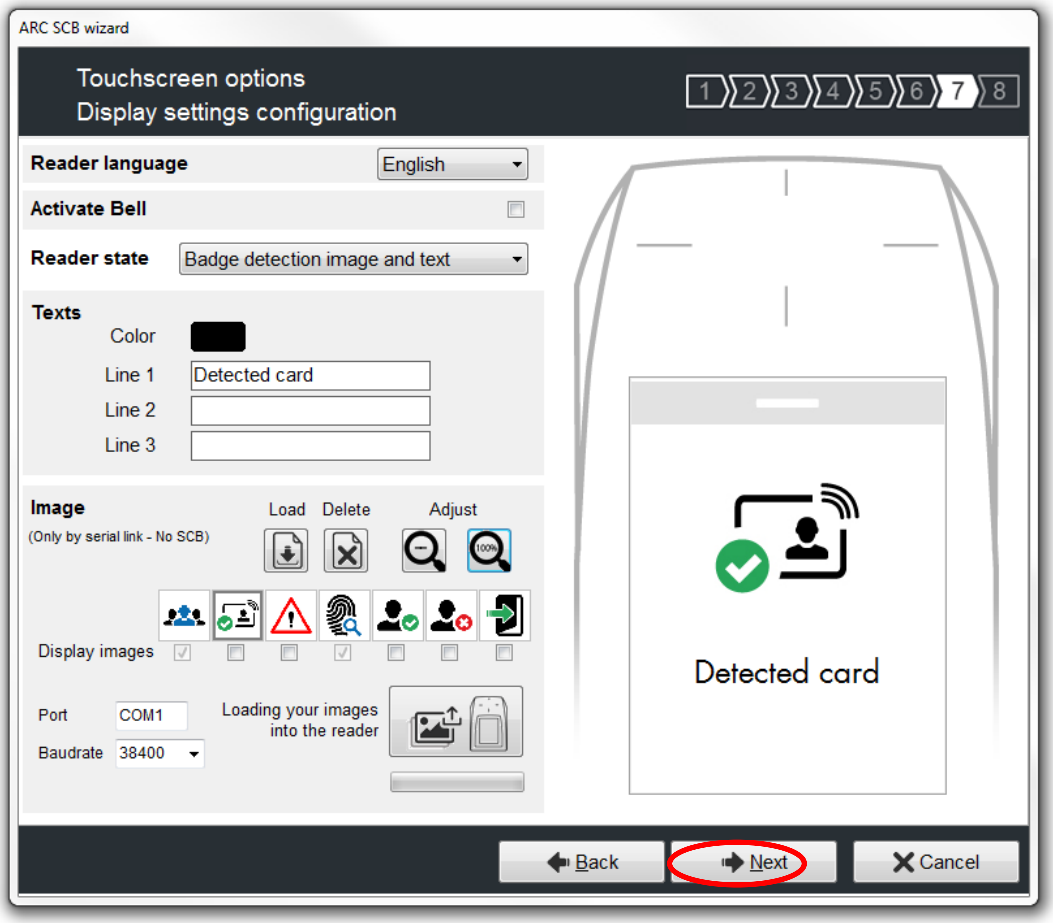
Display
○ Keypad
● Default image

Number of keys: 4

ARC options

□ Eco mode (Low Power)

□ Deny UHF configuration



ARC SCB wizard

Touchscreen options
Display settings configuration

Reader language: English

Activate Bell ☐

Reader state: Badge detection image and text

Texts
Color ■
Line 1: Detected card
Line 2:
Line 3:

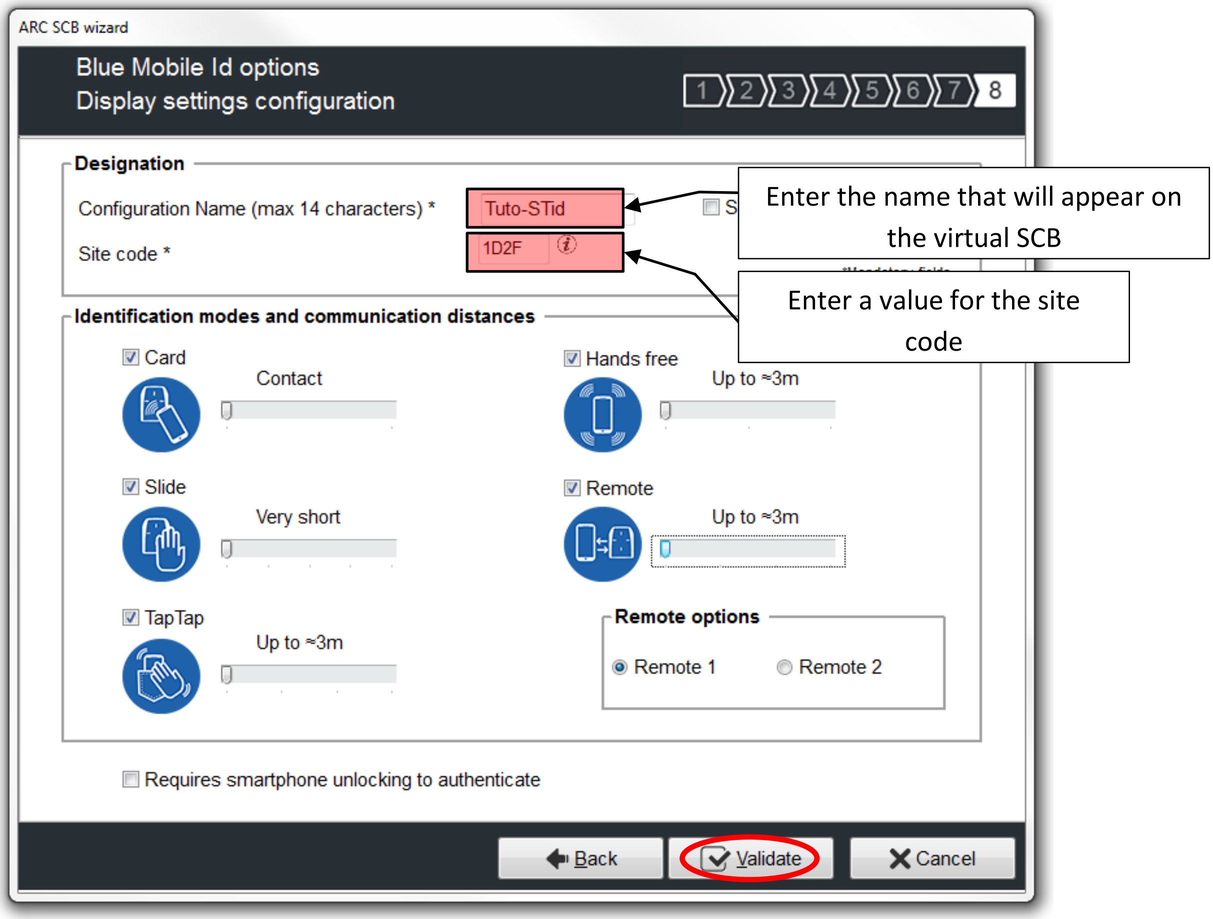
Image
(Only by serial link - No SCB)

Display images ☑ ☐ ☐ ☑ ☐ ☐ ☐

Port: COM1
Baudrate: 38400

Loading your images into the reader

You can choose new images or keep the default image as shown in the example.



ARC SCB wizard

Blue Mobile Id options
Display settings configuration

Designation

Configuration Name (max 14 characters) *: Tuto-STid

Site code *: 1D2F

Enter the name that will appear on the virtual SCB

Enter a value for the site code

Identification modes and communication distances

☑ Card — Contact

☑ Hands free — Up to ≈3m

☑ Slide — Very short

☑ Remote — Up to ≈3m

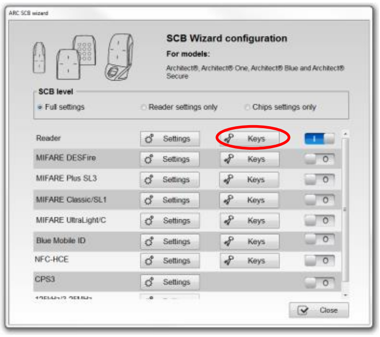
☑ TapTap — Up to ≈3m

Remote options: ● Remote 1 ○ Remote 2

☐ Requires smartphone unlocking to authenticate

Define the identification modes and the desired communication distances according to your installation. Note: If the hands free mode is activated, due to the Bluetooth technology it will take control of the other modes.

I-4. Reader: Keys



ARC SCB wizard

SCB Wizard configuration

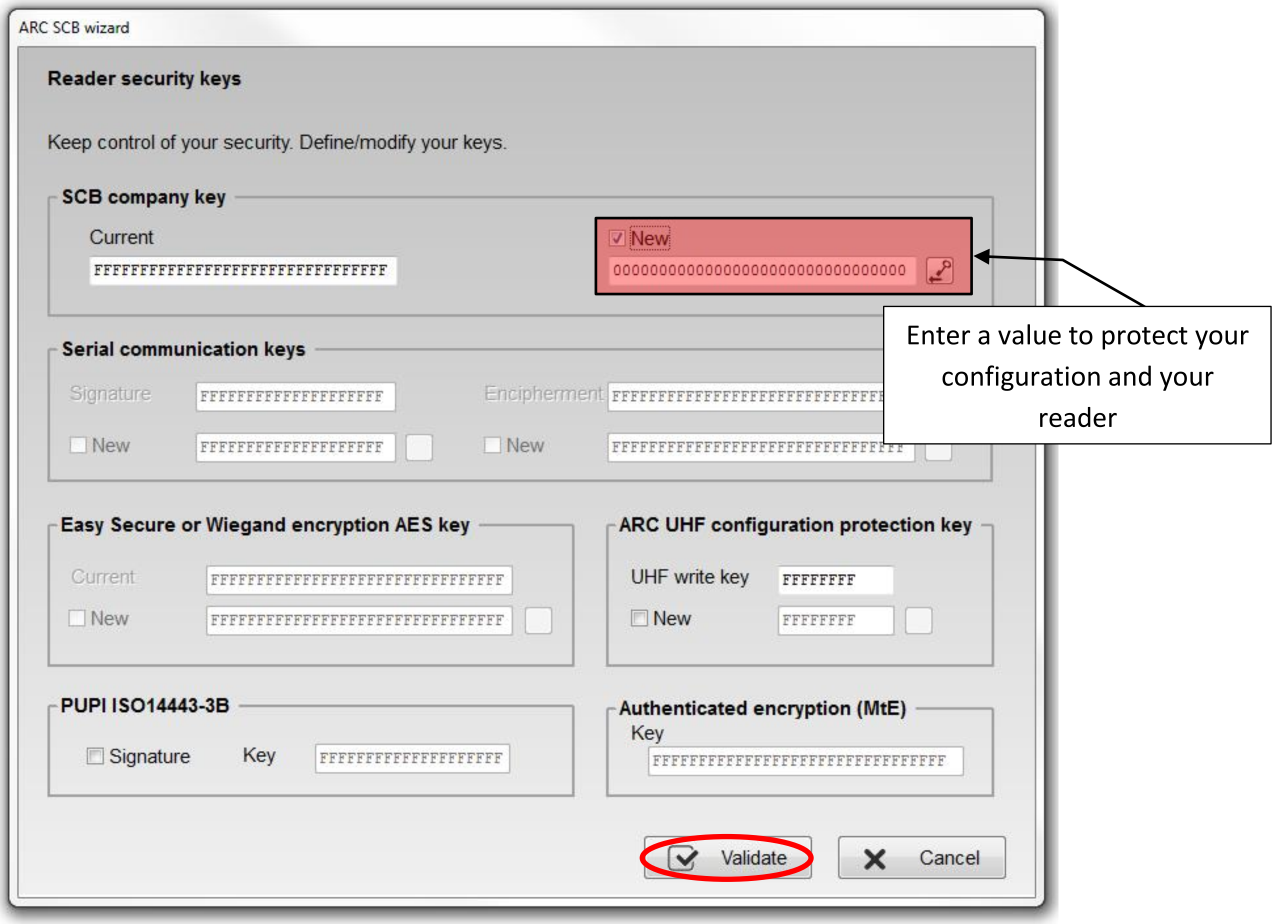
For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	O
NFC-HCE	Settings	Keys	O
CPS3	Settings		O



ARC SCB wizard

Reader security keys

Keep control of your security. Define/modify your keys.

SCB company key

Current: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

☑ New: 00000000000000000000000000000000

Enter a value to protect your configuration and your reader

Serial communication keys

Signature: FFFFFFFFFFFFFFFFFFFF

□ New: FFFFFFFFFFFFFFFFFFFF

Encipherment: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

□ New: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Easy Secure or Wiegand encryption AES key

Current: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

□ New: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

ARC UHF configuration protection key

UHF write key: FFFFFFFF

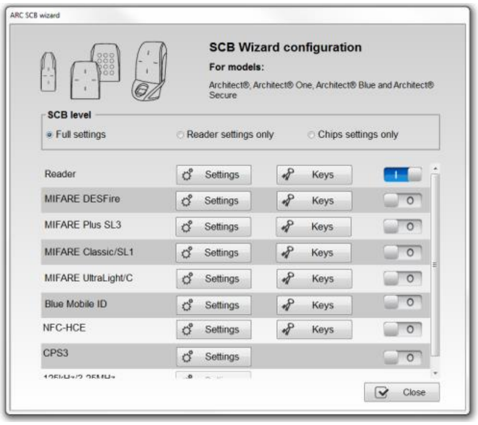
□ New: FFFFFFFF

PUPI ISO14443-3B

□ Signature Key: FFFFFFFFFFFFFFFFFFFF

Authenticated encryption (MtE)

Key: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF



ARC SCB wizard

SCB Wizard configuration

For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

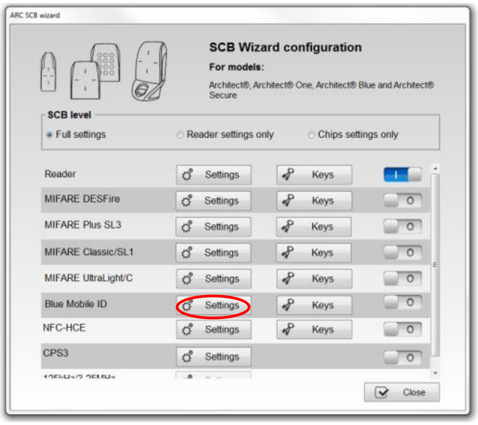
● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	O
NFC-HCE	Settings	Keys	O
CPS3	Settings		O

Close

The configuration of the settings and keys reader is complete. You can use the typical sample configuration below to configure chip.

I-5. Blue Mobile ID: Settings



ARC SCB wizard

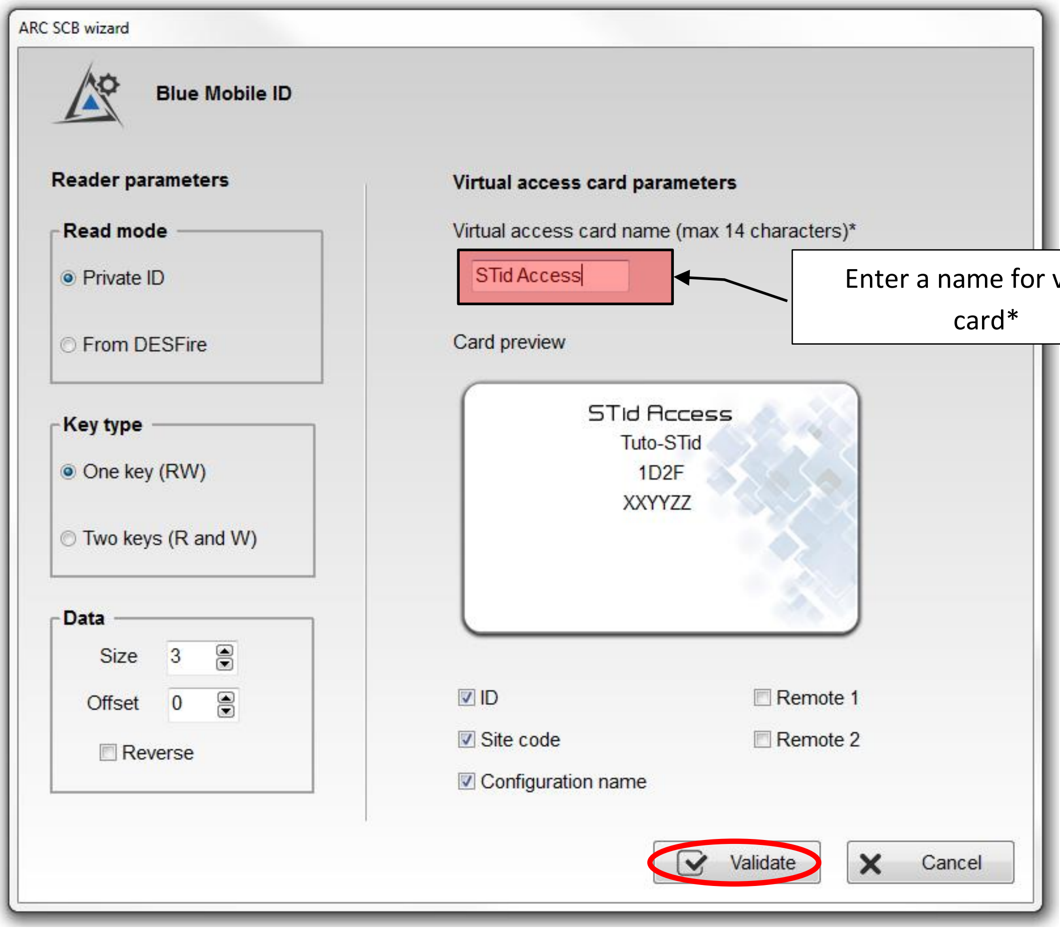
SCB Wizard configuration

For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only



ARC SCB wizard

Blue Mobile ID

Reader parameters

Read mode

● Private ID

○ From DESFire

Key type

● One key (RW)

○ Two keys (R and W)

Data

Size 3

Offset 0

□ Reverse

Virtual access card parameters

Virtual access card name (max 14 characters)*

STid Access

Card preview

STId Access
Tuto-STid
1D2F
XXYYZZ

☑ ID

☑ Site code

☑ Configuration name

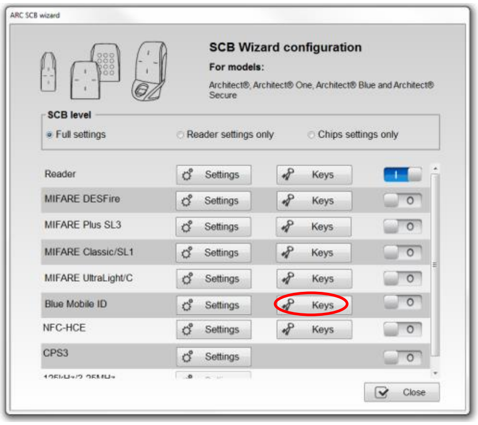
□ Remote 1

□ Remote 2

Enter a name for virtual card*

* Choose a significant name in relation to the access for which this card is created.

I-6. Blue Mobile ID: Keys



ARC SCB wizard

SCB Wizard configuration

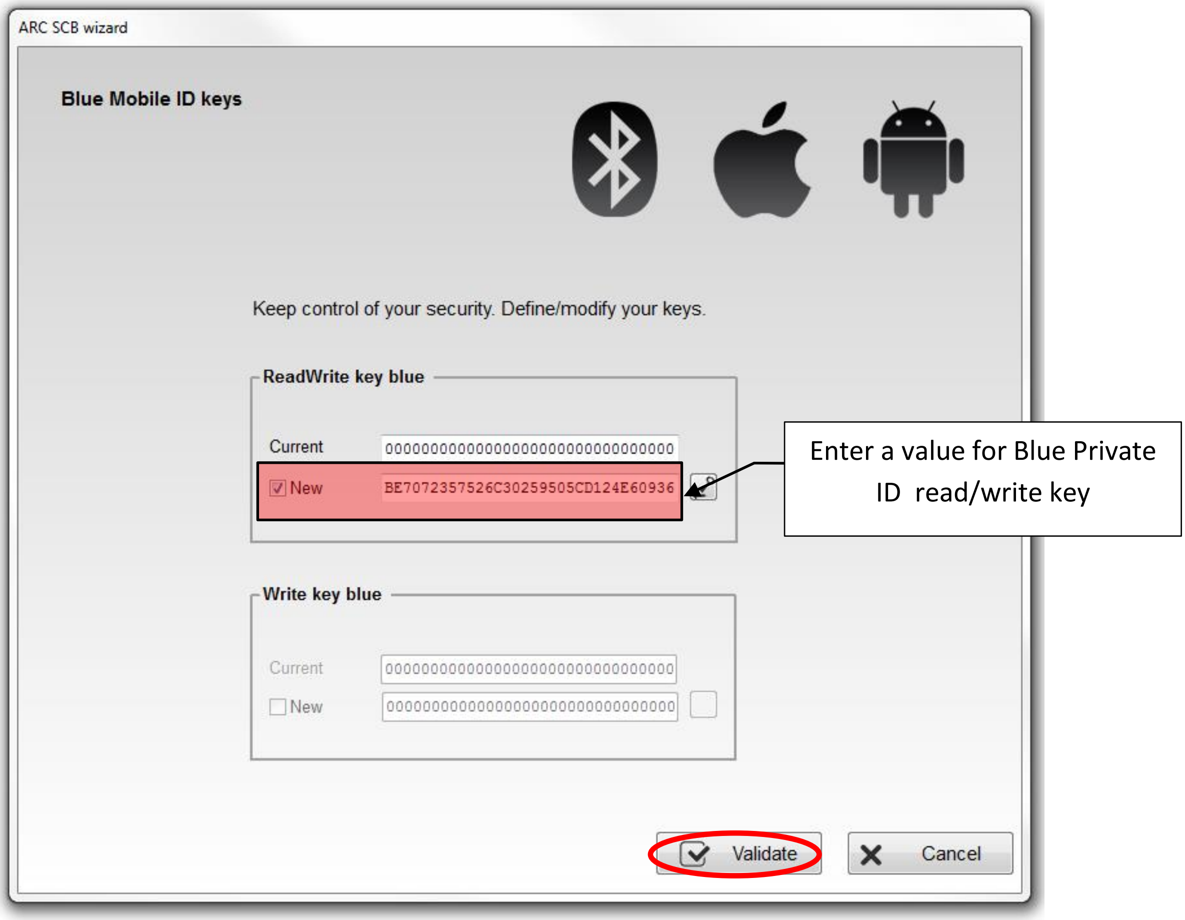
For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	O
NFC-HCE	Settings	Keys	O
CPS3	Settings		O



ARC SCB wizard

Blue Mobile ID keys

Keep control of your security. Define/modify your keys.

ReadWrite key blue

Current 00000000000000000000000000000000

☑ New BE7072357526C30259505CD124E60936

Write key blue

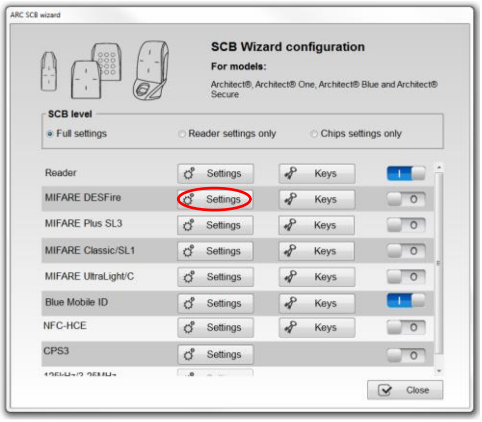
Current 00000000000000000000000000000000

□ New 00000000000000000000000000000000

Enter a value for Blue Private ID read/write key

In case you want to use the same identifier in Virtual Access Card and on physical card DESFire® follow the two steps below, if not go to I-8 Creation of the virtual configuration card.

I-7. DESFire® settings



ARC SCB wizard

SCB Wizard configuration

For models:

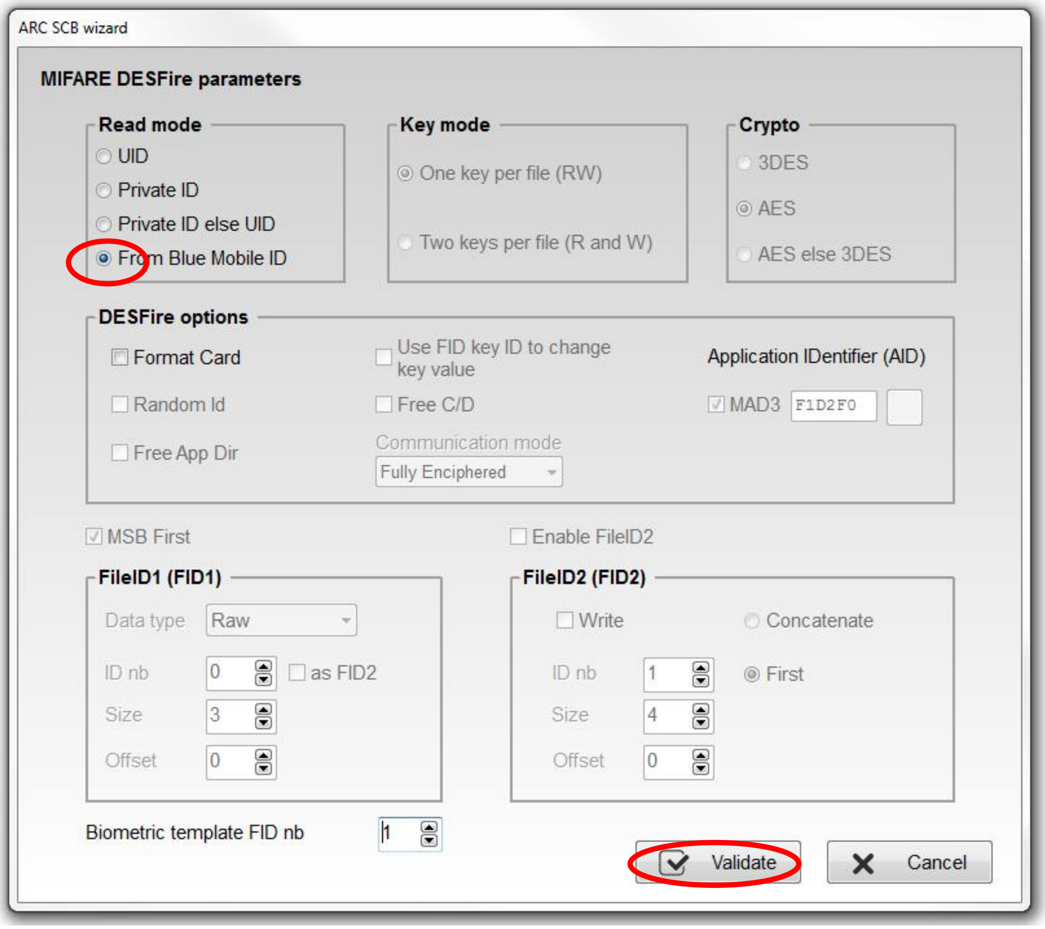
Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	I
NFC-HCE	Settings	Keys	O
CPS3	Settings		O

Select the Read mode « From Blue Mobile ID », all the settings and keys DESFire are inherited from the Blue Mobile ID configuration and appear grayed out in the wizard.



ARC SCB wizard

MIFARE DESFire parameters

Read mode

○ UID
○ Private ID
○ Private ID else UID
● From Blue Mobile ID

Key mode

● One key per file (RW)
○ Two keys per file (R and W)

Crypto

○ 3DES
● AES
○ AES else 3DES

DESFire options

□ Format Card
□ Random Id
□ Free App Dir
□ Use FID key ID to change key value
□ Free C/D

Communication mode: Fully Enciphered

Application IDentifier (AID)

☑ MAD3 F1D2F0

☑ MSB First

□ Enable FileID2

FileID1 (FID1)

Data type: Raw
ID nb: 0 □ as FID2
Size: 3
Offset: 0

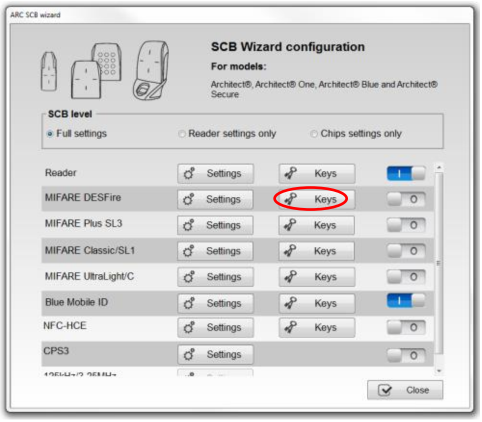
FileID2 (FID2)

□ Write
○ Concatenate
● First
ID nb: 1
Size: 4
Offset: 0

Biometric template FID nb: 1

Settings are:

User key type	Inherited from Blue
Authentication	AES
AID	0xF” site code BLE”0 (MAD3 active)
MSB First	Activated
Random Id	Non Activated
Enable File 2	Non Activated
Data type	Brut
Size	Inherited from Blue
Offset	Inherited from Blue



ARC SCB wizard

SCB Wizard configuration

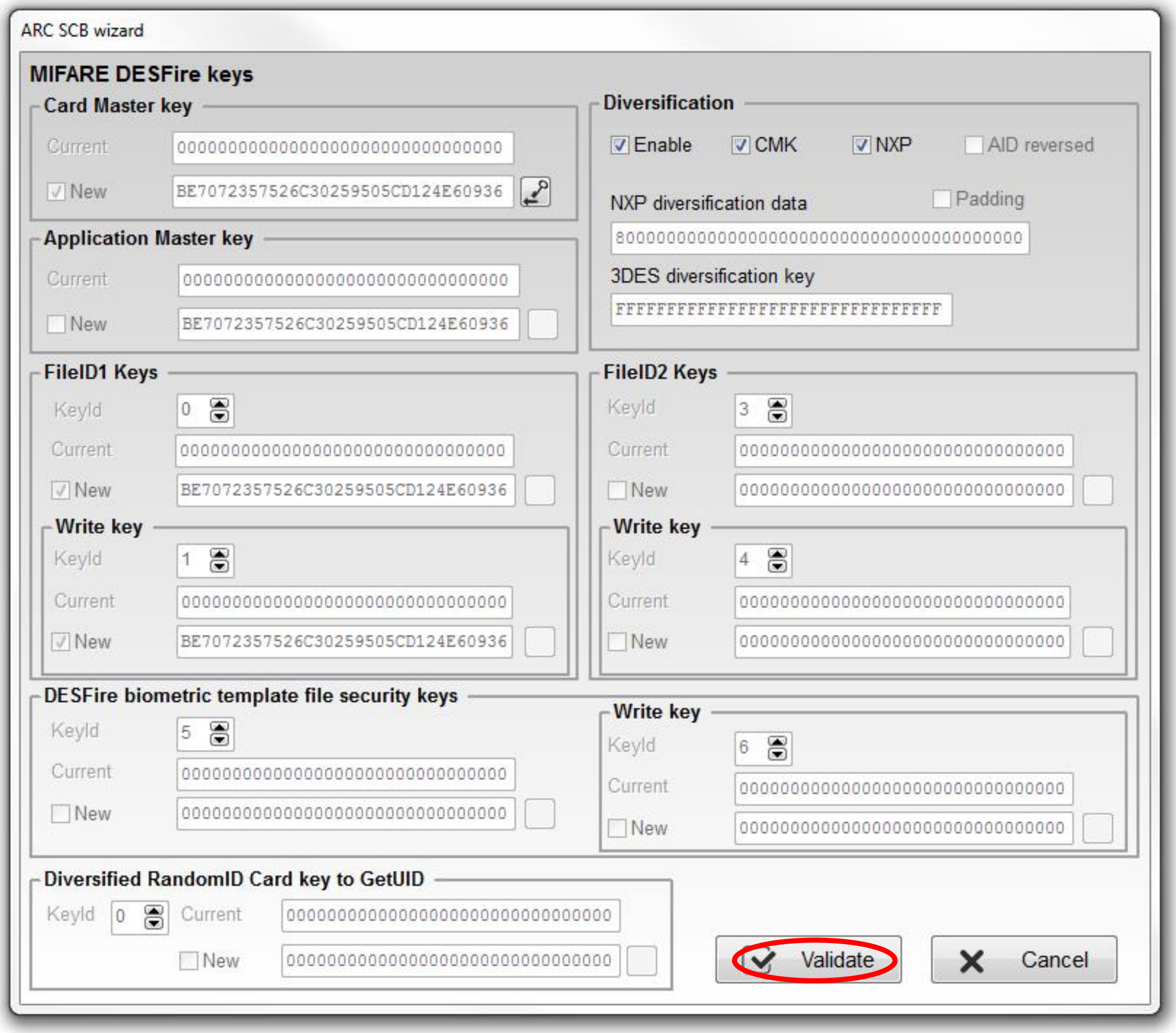
For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	I
NFC-HCE	Settings	Keys	O
CPS3	Settings		O



ARC SCB wizard

MIFARE DESFire keys

Card Master key
Current 00000000000000000000000000000000
☑ New BE7072357526C30259505CD124E60936

Application Master key
Current 00000000000000000000000000000000
□ New BE7072357526C30259505CD124E60936

Diversification
☑ Enable ☑ CMK ☑ NXP □ AID reversed
NXP diversification data □ Padding
8000000000000000000000000000000000000000
3DES diversification key
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

FileID1 Keys
KeyId 0
Current 00000000000000000000000000000000
☑ New BE7072357526C30259505CD124E60936
Write key
KeyId 1
Current 00000000000000000000000000000000
☑ New BE7072357526C30259505CD124E60936

FileID2 Keys
KeyId 3
Current 00000000000000000000000000000000
□ New 00000000000000000000000000000000
Write key
KeyId 4
Current 00000000000000000000000000000000
□ New 00000000000000000000000000000000

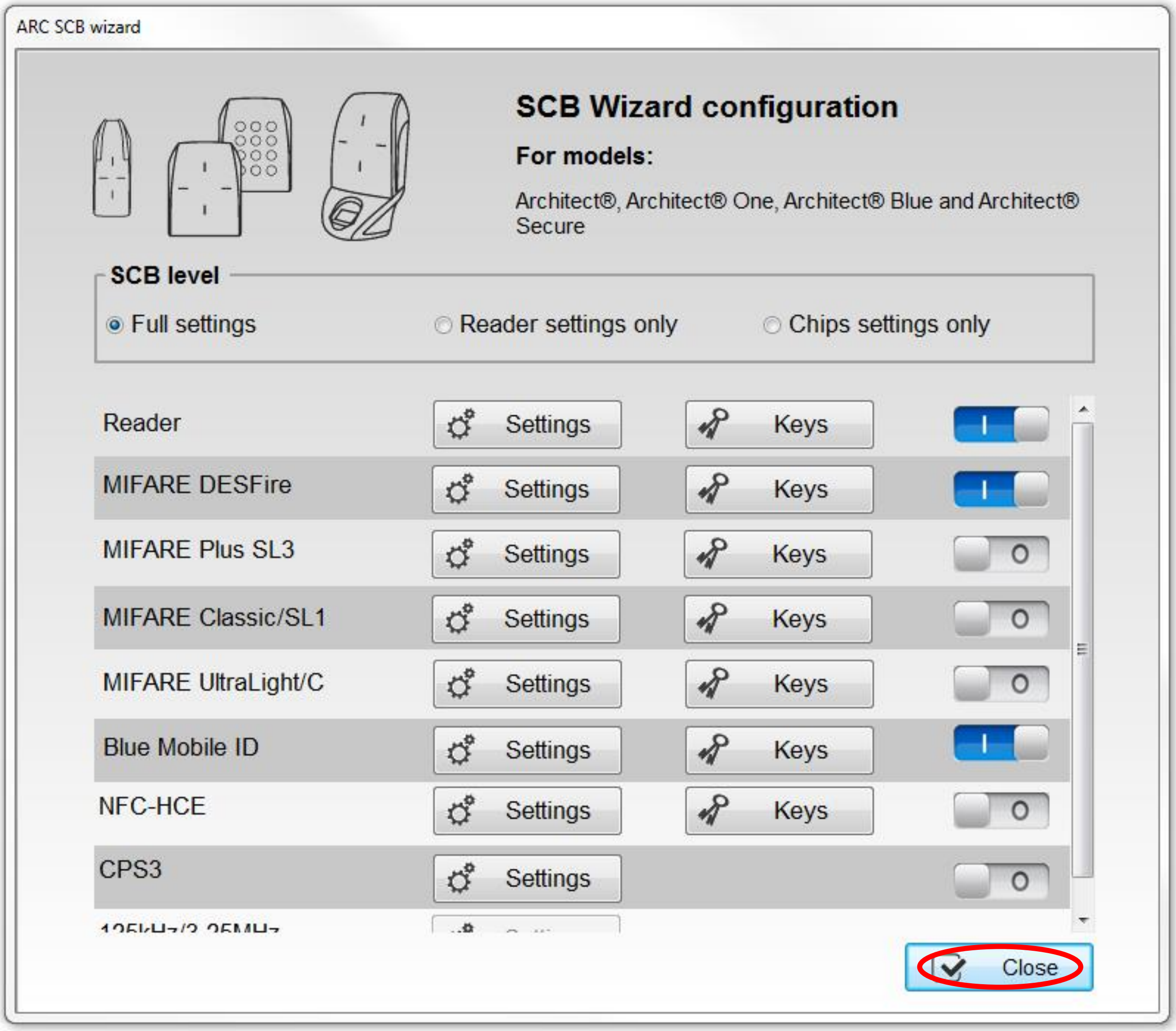
DESFire biometric template file security keys
KeyId 5
Current 00000000000000000000000000000000
□ New 00000000000000000000000000000000
Write key
KeyId 6
Current 00000000000000000000000000000000
□ New 00000000000000000000000000000000

Diversified RandomID Card key to GetUID
KeyId 0 Current 00000000000000000000000000000000
□ New 00000000000000000000000000000000

Keys settings are:

Card Master key	Value of Blue’s reading key
Application Master key	Value of Blue’s reading key
Diversification	Enable, on CMK according to AN10922
NXP diversification data	0x 8000…00
FileID1 key number	0
FileID 1 key value	Value of Blue’s reading key

Note: in case of two keys mode for Blue Configuration, the write key number will be 1.



ARC SCB wizard

SCB Wizard configuration

For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

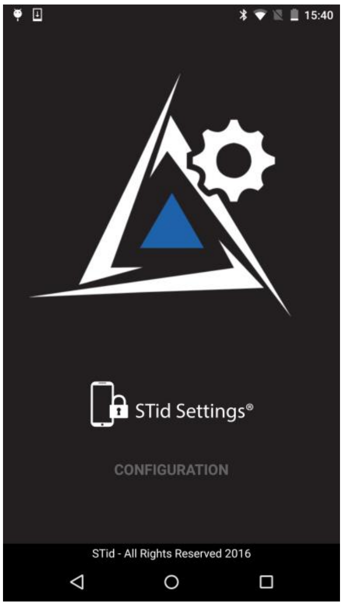
● Full settings ○ Reader settings only ○ Chips settings only

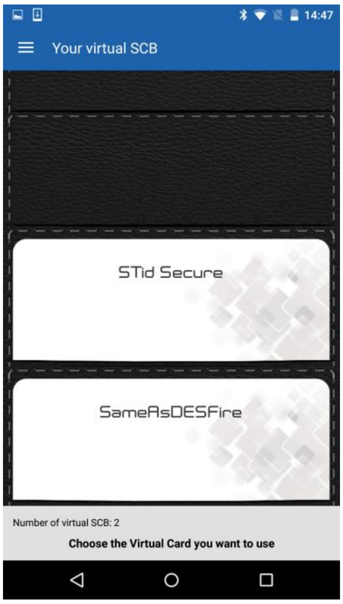
Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	I
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	I
NFC-HCE	Settings	Keys	O
CPS3	Settings		O
125kHz/3.25MHz	Settings		

I-8. Creation of the virtual configuration card

STid Settings application required

Open the application STid Settings on the smartphone.

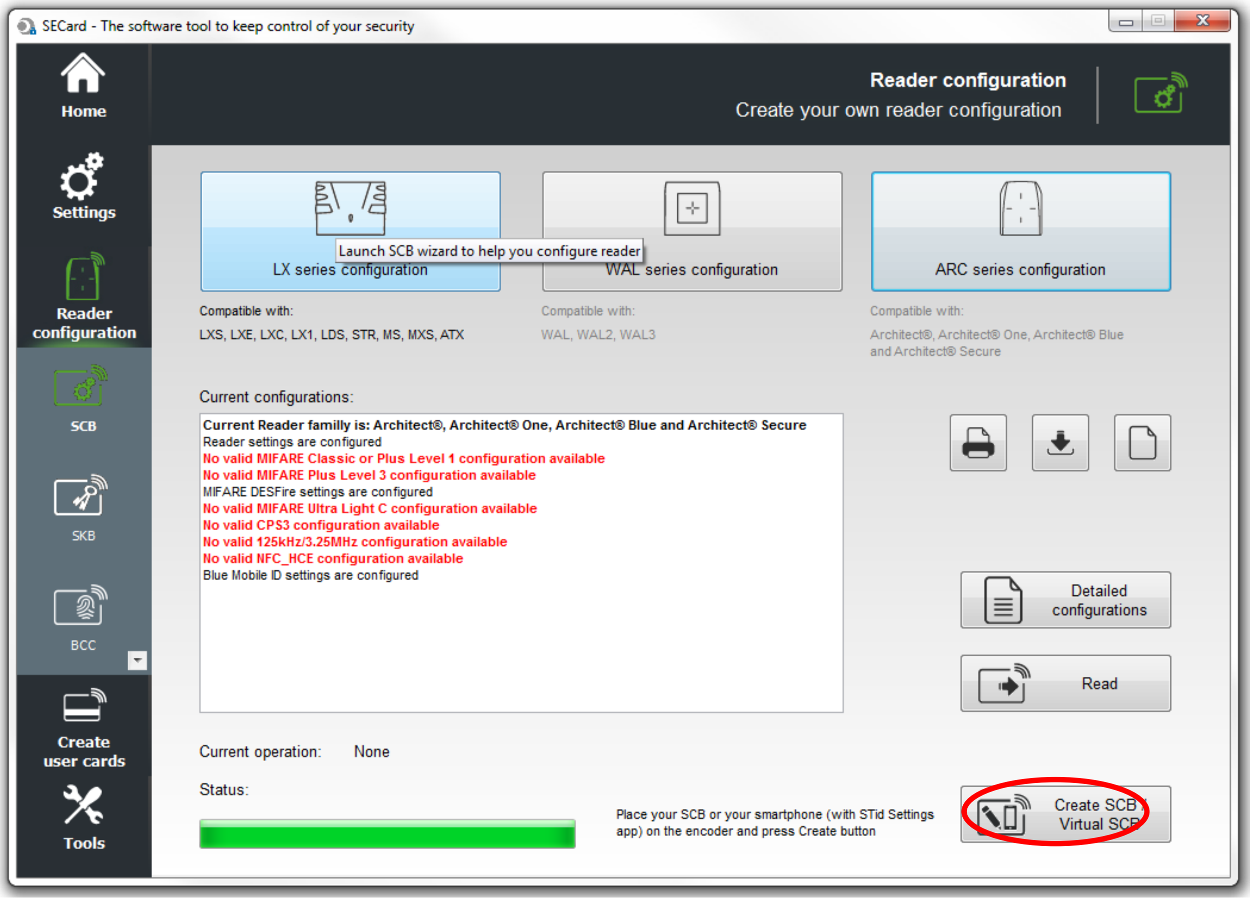




Number of virtual SCB: 2

Choose the Virtual Card you want to use

Place the smartphone on the encoder and click Create SCB / Virtual SCB



Compatible with:
LXS, LXE, LXC, LX1, LDS, STR, MS, MXS, ATX

Compatible with:
WAL, WAL2, WAL3

Compatible with:
Architect®, Architect® One, Architect® Blue and Architect® Secure

Current configurations:

```
Current Reader familly is: Architect®, Architect® One, Architect® Blue and Architect® Secure
Reader settings are configured
No valid MIFARE Classic or Plus Level 1 configuration available
No valid MIFARE Plus Level 3 configuration available
MIFARE DESFire settings are configured
No valid MIFARE Ultra Light C configuration available
No valid CPS3 configuration available
No valid 125kHz/3.25MHz configuration available
No valid NFC_HCE configuration available
Blue Mobile ID settings are configured
```

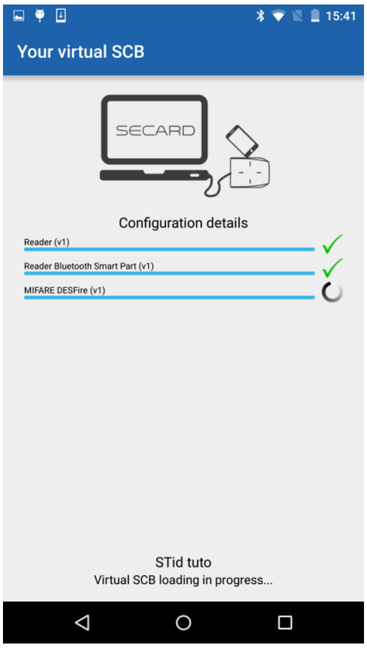
Current operation: None

Status:

Place your SCB or your smartphone (with STid Settings app) on the encoder and press Create button

Note: virtual SCB is free, no debit credit.

You can follow the progress of loading the configuration on the smartphone screen.



Configuration details

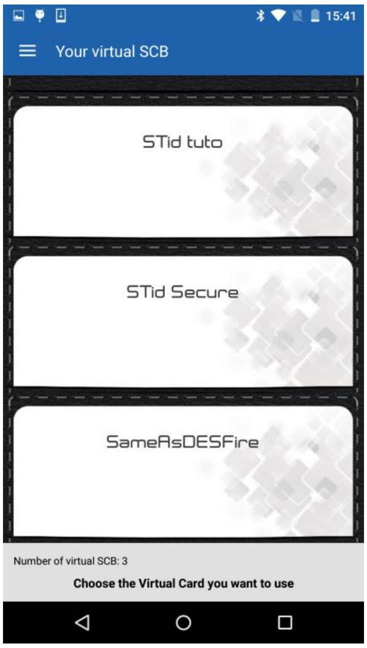
Reader (v1) ✓

Reader Bluetooth Smart Part (v1) ✓

MIFARE DESFire (v1)

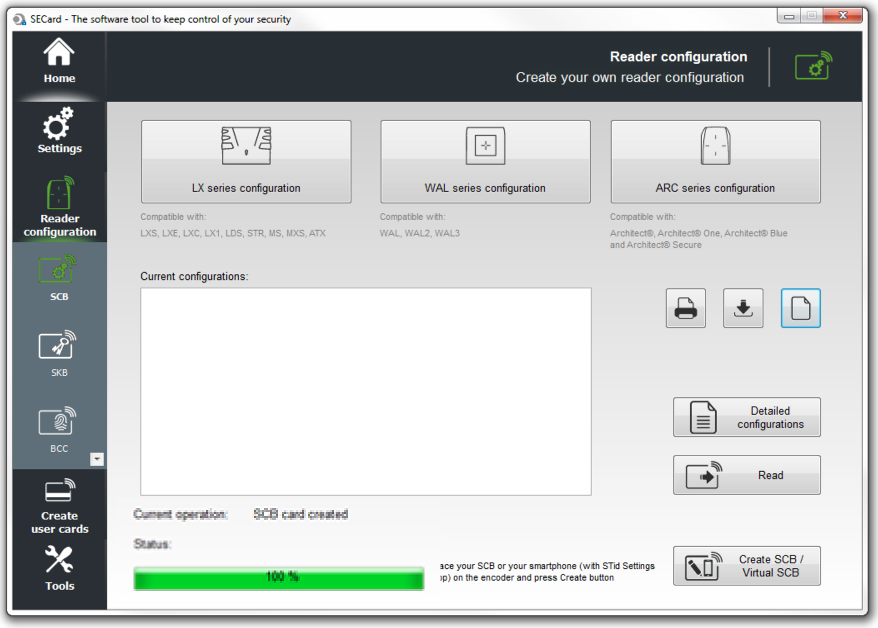
STid tuto
Virtual SCB loading in progress...

After the creation you can see the virtual card STid tuto on the screen and the message in SECard:



Number of virtual SCB: 3

Choose the Virtual Card you want to use



Compatible with:
LXS, LXE, LXC, LX1, LDS, STR, MS, MXS, ATX

Compatible with:
WAL, WAL2, WAL3

Compatible with:
Architect®, Architect® One, Architect® Blue and Architect® Secure

Current configurations:

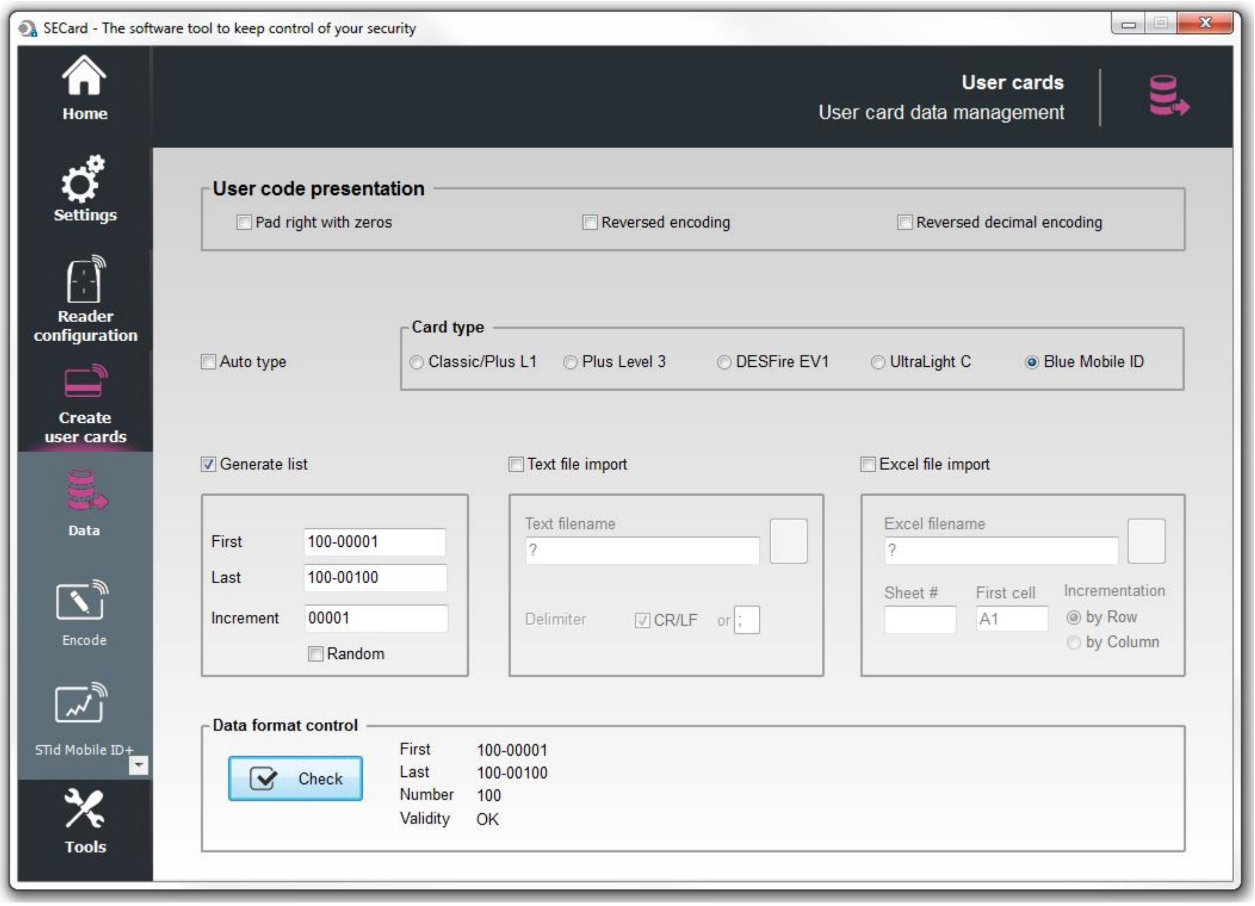
Current operation: SCB card created

Status:

ace your SCB or your smartphone (with STid Settings
ɔp) on the encoder and press Create button

You can create a physical SCB card using a MIFARE® DESFire® EV1 4Kb minimum. Place the card on the encoder and click Create SCB / Virtual SCB.

I-9. Encoding the private ID



User code presentation
□ Pad right with zeros □ Reversed encoding □ Reversed decimal encoding

□ Auto type

Card type
○ Classic/Plus L1 ○ Plus Level 3 ○ DESFire EV1 ○ UltraLight C ● Blue Mobile ID

☑ Generate list

First 100-00001
Last 100-00100
Increment 00001
□ Random

□ Text file import

Text filename ?
Delimiter ☑ CR/LF or ;

□ Excel file import

Excel filename ?
Sheet # First cell A1 Incrementation ● by Row ○ by Column

Data format control
Check
First 100-00001
Last 100-00100
Number 100
Validity OK

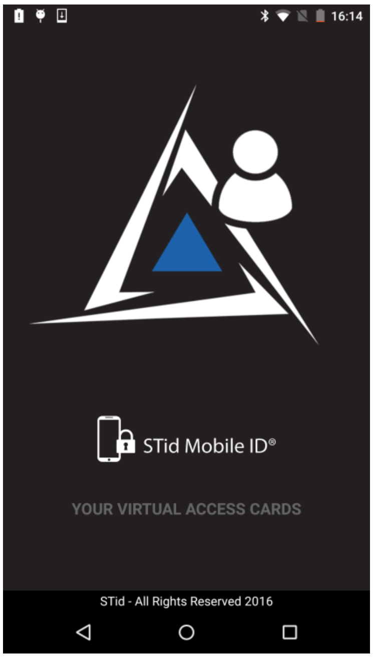
There are three possibilities:

Generate a list
Import a Text file
Import an Excel file (if for example the database already exists).

See the manual for explanations of imports.

If you want to make a single card for test pass directly on "Encode".

STid Mobile ID application is required to encode the private ID on the smartphone

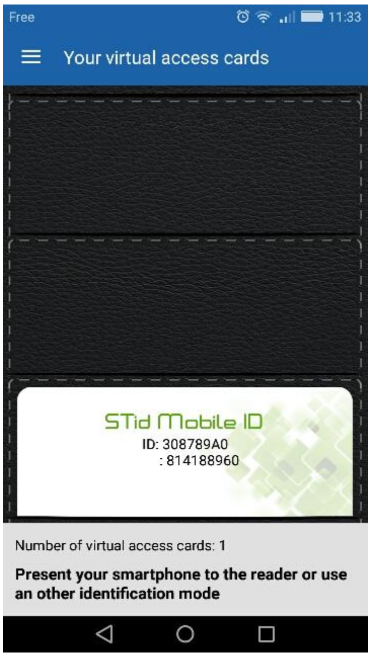


16:14

STid Mobile ID®

YOUR VIRTUAL ACCESS CARDS

STid - All Rights Reserved 2016



Free 11:33

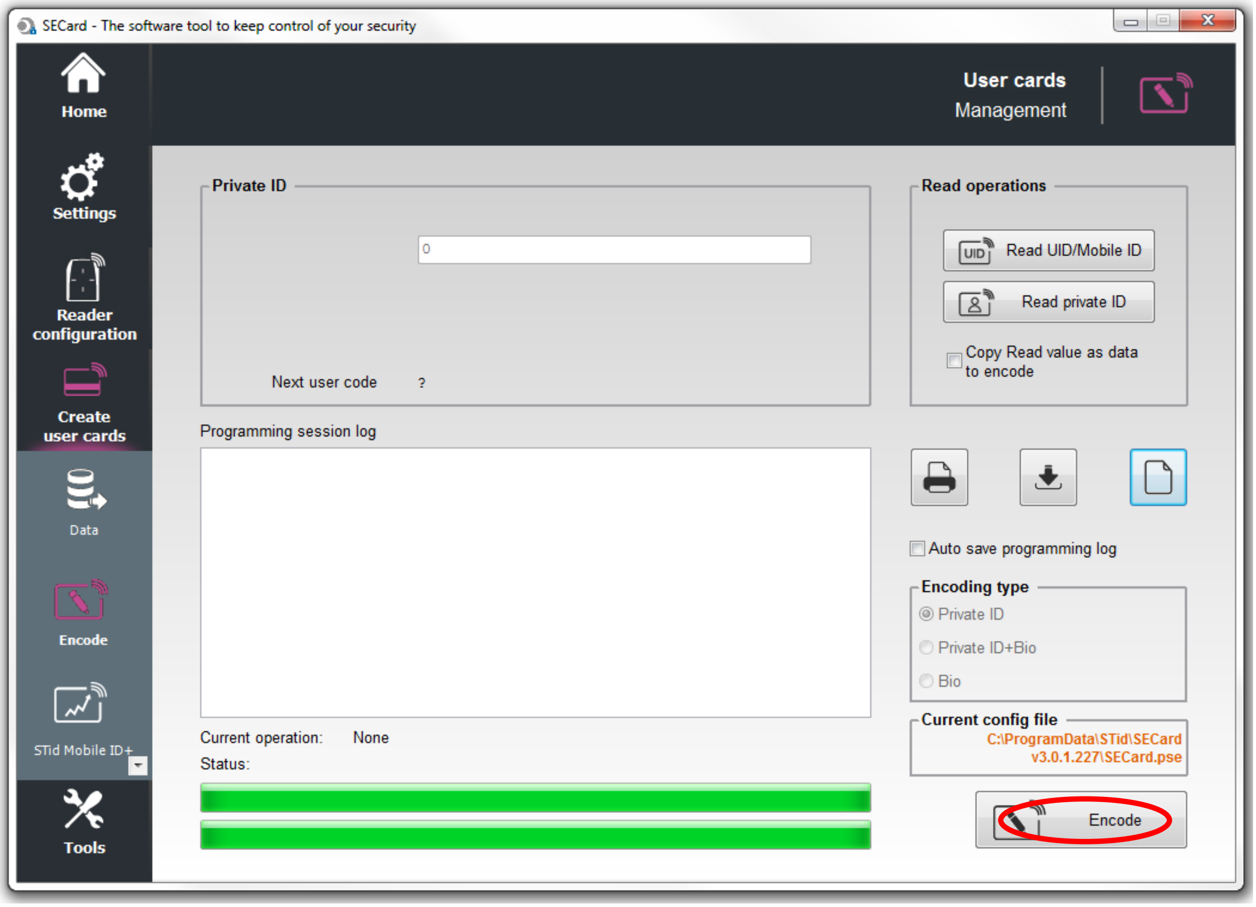
Your virtual access cards

STid Mobile ID
ID: 308789A0
: 814188960

Number of virtual access cards: 1

Present your smartphone to the reader or use an other identification mode

Place the smartphone on the encoder and click on Encode



SECard - The software tool to keep control of your security

Private ID: 0

Next user code ?

Read operations

□ Copy Read value as data to encode

Programming session log

□ Auto save programming log

Encoding type

● Private ID

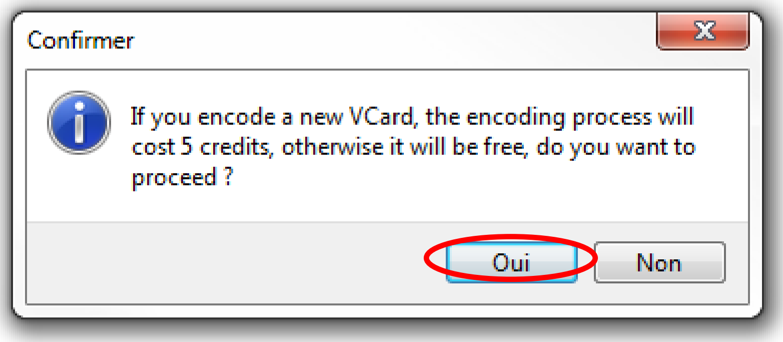
○ Private ID+Bio

○ Bio

Current config file: C:\ProgramData\STid\SECard v3.0.1.227\SECard.pse

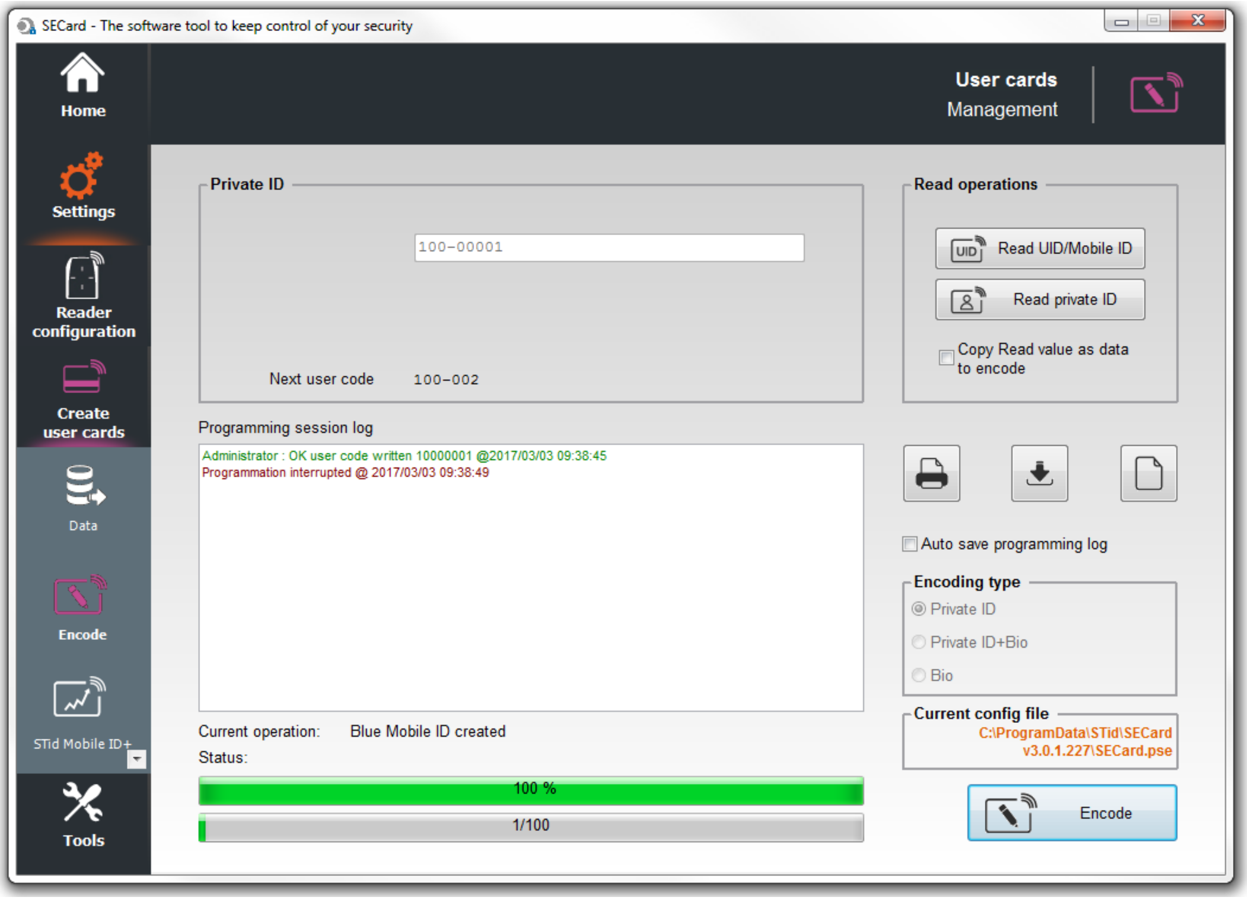
Current operation: None

Status:



Confirmer

If you encode a new VCard, the encoding process will cost 5 credits, otherwise it will be free, do you want to proceed ?



SECard - The software tool to keep control of your security

Private ID

100-00001

Next user code 100-002

Read operations

□ Copy Read value as data to encode

Programming session log

```
Administrator : OK user code written 10000001 @2017/03/03 09:38:45
Programmation interrupted @ 2017/03/03 09:38:49
```

□ Auto save programming log

Encoding type

● Private ID
○ Private ID+Bio
○ Bio

Current config file

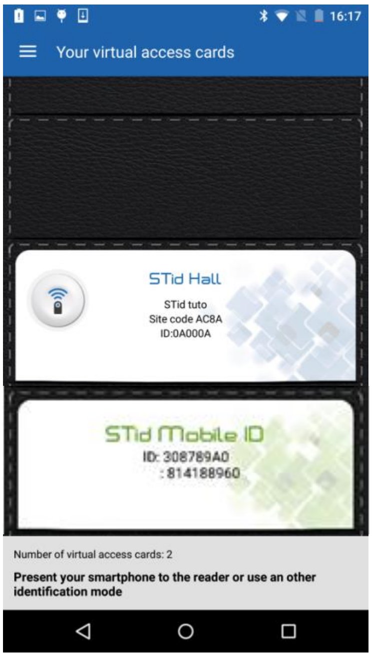
C:\ProgramData\STid\SECard v3.0.1.227\SECard.pse

Current operation: Blue Mobile ID created

Status:

100 %

1/100



Your virtual access cards

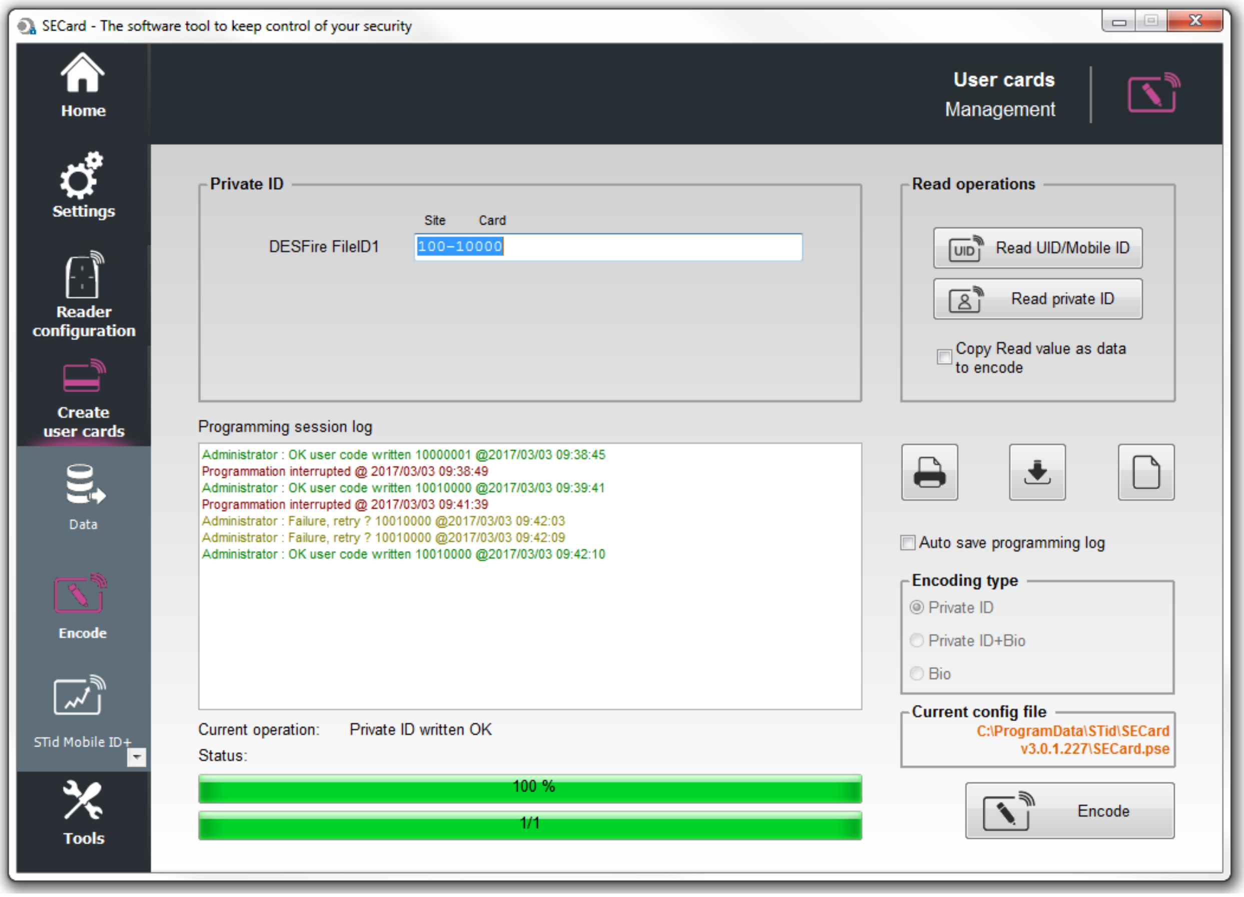
STid Hall
STid tuto
Site code AC8A
ID:0A000A

STid Mobile ID
ID: 308789A0
: 814188960

Number of virtual access cards: 2

Present your smartphone to the reader or use an other identification mode

Place the MIFARE® DESFire® EV1 on the encoder and click on Encode



Private ID

	Site	Card
DESFire FileID1	100-10000	

□ Copy Read value as data to encode

Programming session log

```
Administrator : OK user code written 10000001 @2017/03/03 09:38:45
Programmation interrupted @ 2017/03/03 09:38:49
Administrator : OK user code written 10010000 @2017/03/03 09:39:41
Programmation interrupted @ 2017/03/03 09:41:39
Administrator : Failure, retry ? 10010000 @2017/03/03 09:42:03
Administrator : Failure, retry ? 10010000 @2017/03/03 09:42:09
Administrator : OK user code written 10010000 @2017/03/03 09:42:10
```

□ Auto save programming log

Encoding type
● Private ID
○ Private ID+Bio
○ Bio

Current config file: C:\ProgramData\STid\SECard v3.0.1.227\SECard.pse

Current operation: Private ID written OK

Status:

100 %

1/1

Configuration is complete, go to the step: *VI-Save the configuration file*

II. Use a setting file (.pse) created with SECard < 3.0.0

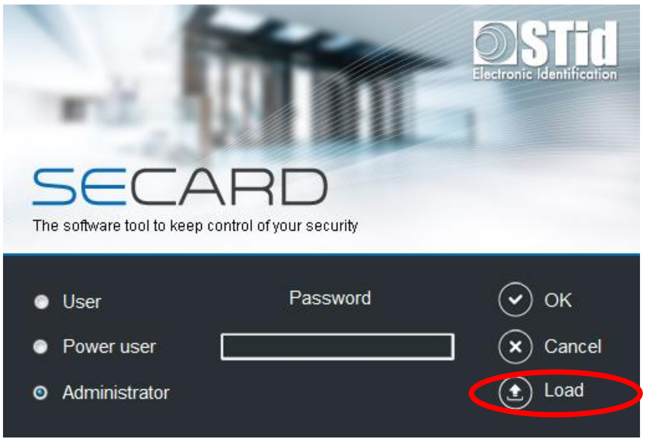
You have an existing MIFARE® DESFire® installation and want to add and / or change readers for Architect® Blue readers and use the smartphone to identify yourself while keeping your DESFire® cards.

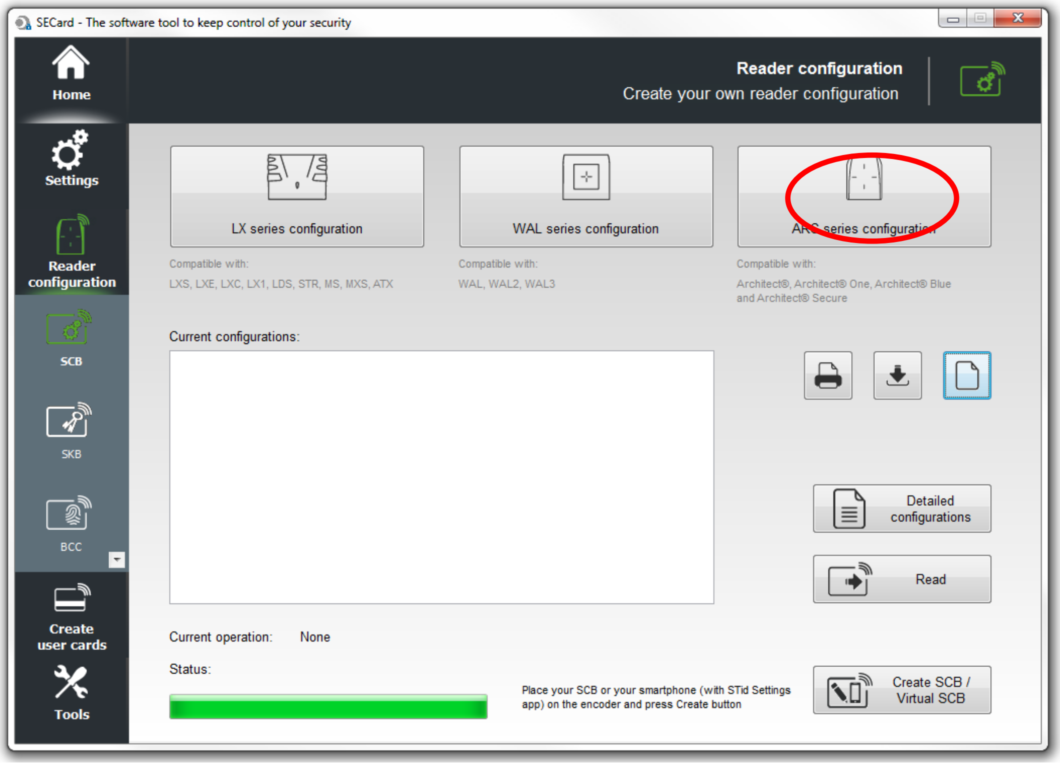
It is not necessary to recreate a new configuration card the current SCB will be used to configure the Blue readers.
In this case, a configuration inherited from the existing DESFire® parameters will be loaded into the readers.
Follow the steps below to encode the smartphones

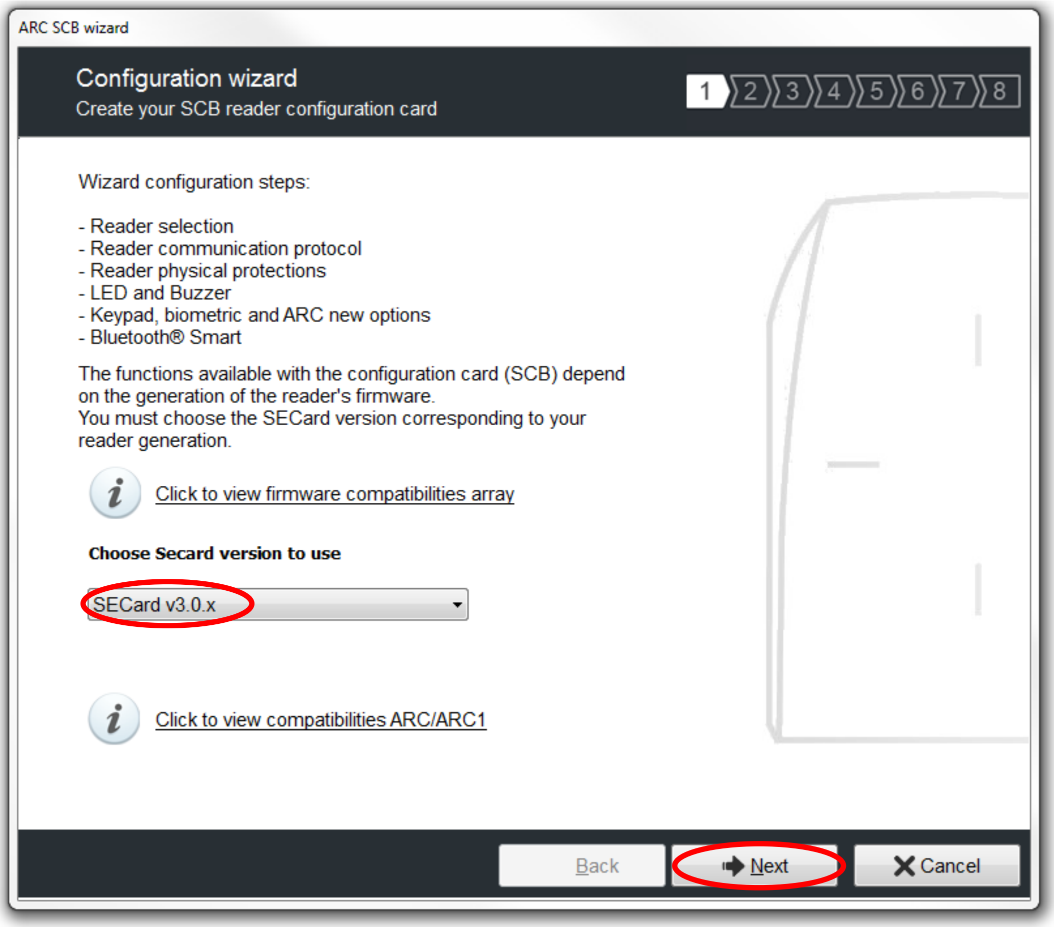
Warning: Only works if the old configuration meets the following conditions:

- Read mode: Private ID
- Enable FileID2: not used
- Biometric: not used
- Data type: Brut.

Load the configuration file into SECardV3.0 and enter the associated Administrator password:


STid
Electronic Identification
SECARD
The software tool to keep control of your security
○ User
○ Power user
● Administrator
Password
OK
Cancel
Load





ARC SCB wizard

Configuration wizard

Create your SCB reader configuration card

Wizard configuration steps:

- Reader selection
- Reader communication protocol
- Reader physical protections
- LED and Buzzer
- Keypad, biometric and ARC new options
- Bluetooth® Smart

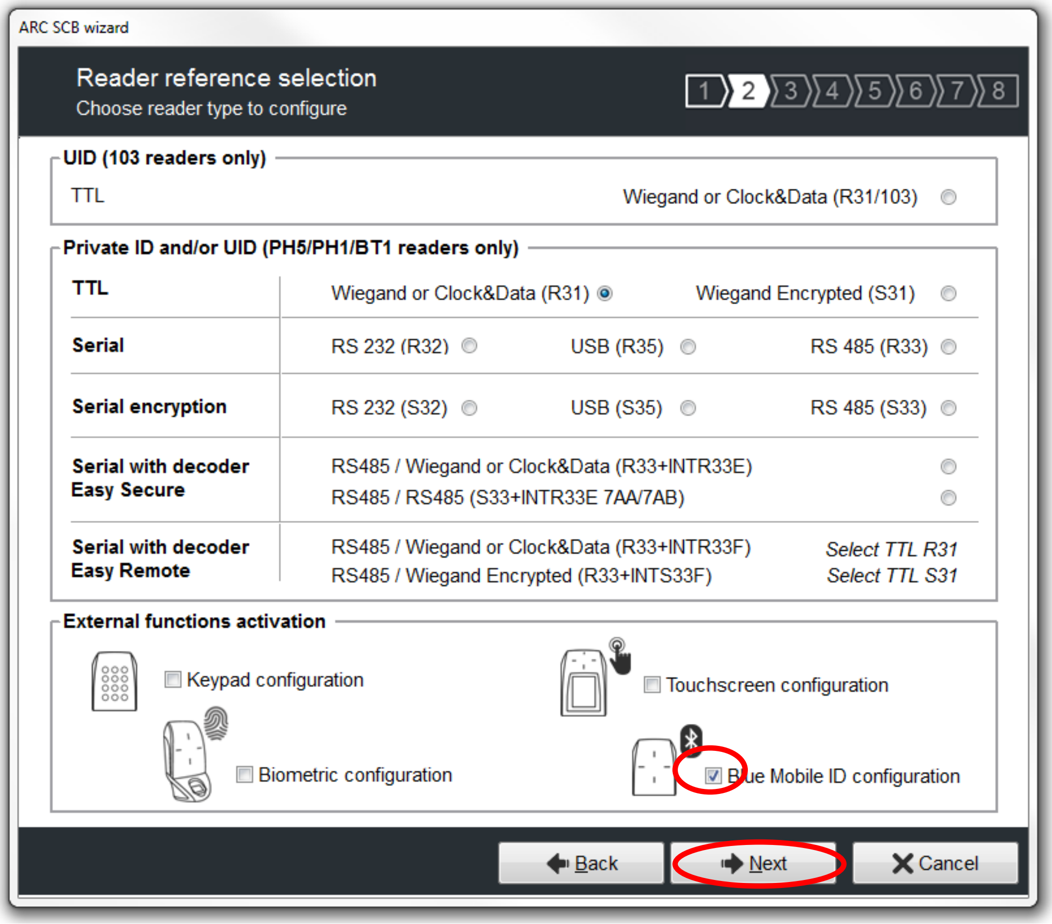
The functions available with the configuration card (SCB) depend on the generation of the reader's firmware.
You must choose the SECard version corresponding to your reader generation.

Click to view firmware compatibilities array

Choose Secard version to use

SECard v3.0.x

Click to view compatibilities ARC/ARC1



ARC SCB wizard

Reader reference selection

Choose reader type to configure

UID (103 readers only)

TTL — Wiegand or Clock&Data (R31/103) ○

Private ID and/or UID (PH5/PH1/BT1 readers only)

TTL	Wiegand or Clock&Data (R31) ●		Wiegand Encrypted (S31) ○
Serial	RS 232 (R32) ○	USB (R35) ○	RS 485 (R33) ○
Serial encryption	RS 232 (S32) ○	USB (S35) ○	RS 485 (S33) ○
Serial with decoder Easy Secure	RS485 / Wiegand or Clock&Data (R33+INTR33E) RS485 / RS485 (S33+INTR33E 7AA/7AB)		○ ○
Serial with decoder Easy Remote	RS485 / Wiegand or Clock&Data (R33+INTR33F) RS485 / Wiegand Encrypted (R33+INTS33F)		*Select TTL R31* *Select TTL S31*

External functions activation

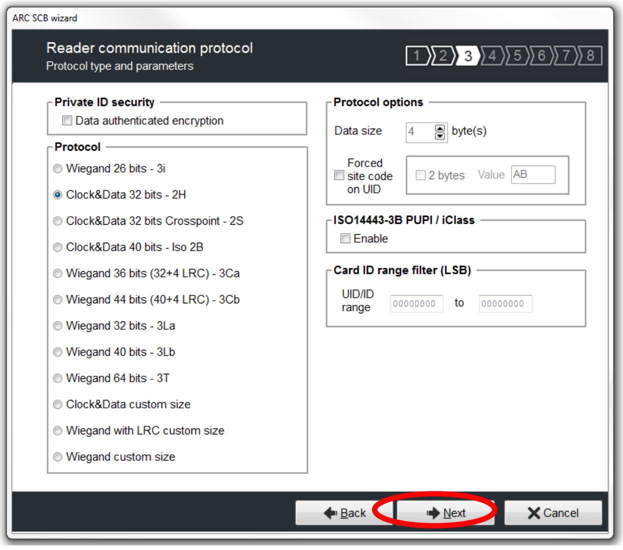
□ Keypad configuration

□ Touchscreen configuration

□ Biometric configuration

☑ Blue Mobile ID configuration

Click “Next” for all other steps without making any changes in the wizard:


ARC SCB wizard

Reader communication protocol
Protocol type and parameters

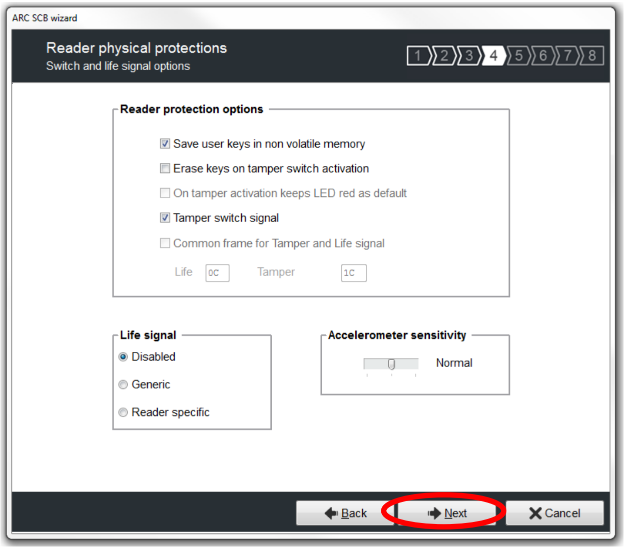
Private ID security
□ Data authenticated encryption

Protocol
○ Wiegand 26 bits - 3i
● Clock&Data 32 bits - 2H
○ Clock&Data 32 bits Crosspoint - 2S
○ Clock&Data 40 bits - Iso 2B
○ Wiegand 36 bits (32+4 LRC) - 3Ca
○ Wiegand 44 bits (40+4 LRC) - 3Cb
○ Wiegand 32 bits - 3La
○ Wiegand 40 bits - 3Lb
○ Wiegand 64 bits - 3T
○ Clock&Data custom size
○ Wiegand with LRC custom size
○ Wiegand custom size

Protocol options
Data size 4 byte(s)
□ Forced site code on UID □ 2 bytes Value AB

ISO14443-3B PUPI / iClass
□ Enable

Card ID range filter (LSB)
UID/ID range 00000000 to 00000000

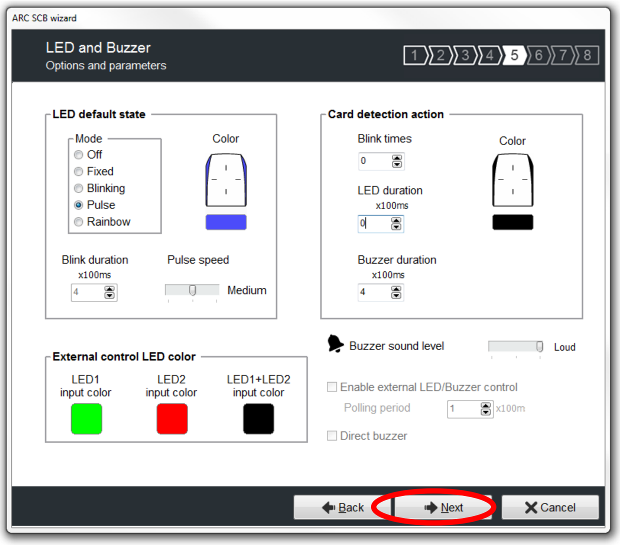

ARC SCB wizard

Reader physical protections
Switch and life signal options

Reader protection options
☑ Save user keys in non volatile memory
□ Erase keys on tamper switch activation
□ On tamper activation keeps LED red as default
☑ Tamper switch signal
□ Common frame for Tamper and Life signal
Life 0C Tamper 1C

Life signal
● Disabled
○ Generic
○ Reader specific

Accelerometer sensitivity
Normal


ARC SCB wizard

LED and Buzzer
Options and parameters

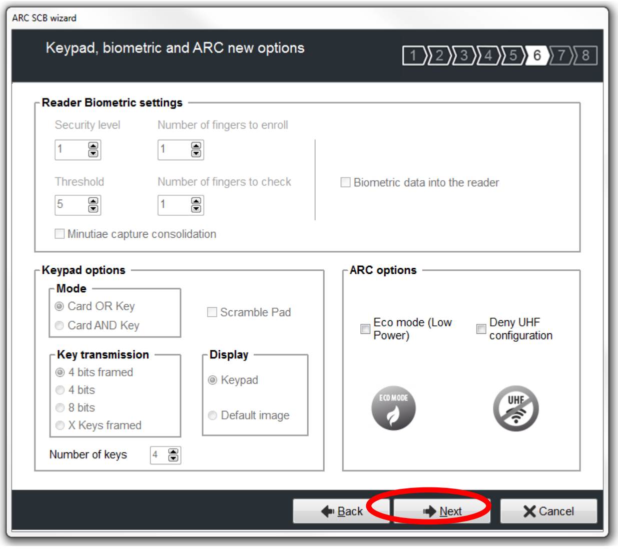
LED default state
Mode
○ Off
○ Fixed
○ Blinking
● Pulse
○ Rainbow
Color
Blink duration x100ms 4
Pulse speed Medium

Card detection action
Blink times 0
Color
LED duration x100ms 0
Buzzer duration x100ms 4

Buzzer sound level Loud

External control LED color
LED1 input color 🟩
LED2 input color 🟥
LED1+LED2 input color ■

□ Enable external LED/Buzzer control
Polling period 1 x100m
□ Direct buzzer

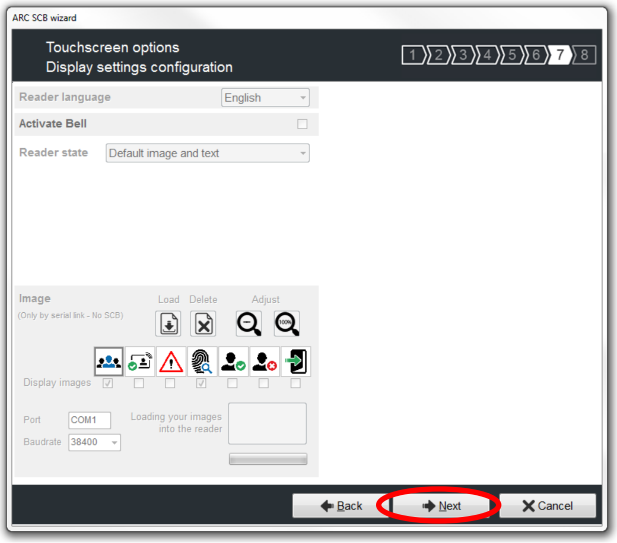

ARC SCB wizard

Keypad, biometric and ARC new options

Reader Biometric settings
Security level 1
Number of fingers to enroll 1
Threshold 5
Number of fingers to check 1
□ Biometric data into the reader
□ Minutiae capture consolidation

Keypad options
Mode
● Card OR Key
○ Card AND Key
□ Scramble Pad
Key transmission
● 4 bits framed
○ 4 bits
○ 8 bits
○ X Keys framed
Display
● Keypad
○ Default image
Number of keys 4

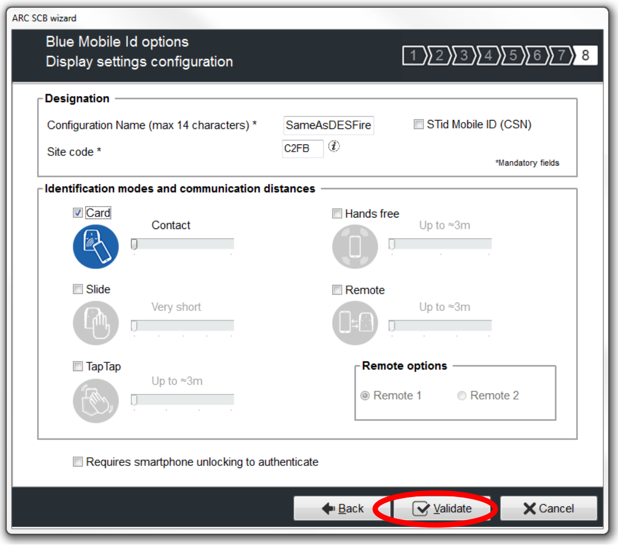
ARC options
□ Eco mode (Low Power)
□ Deny UHF configuration


ARC SCB wizard

Touchscreen options
Display settings configuration

Reader language English
Activate Bell □
Reader state Default image and text

Image
(Only by serial link - No SCB)
Load Delete Adjust
Display images ☑ □ □ ☑ □ □ □
Port COM1
Baudrate 38400
Loading your images into the reader


ARC SCB wizard

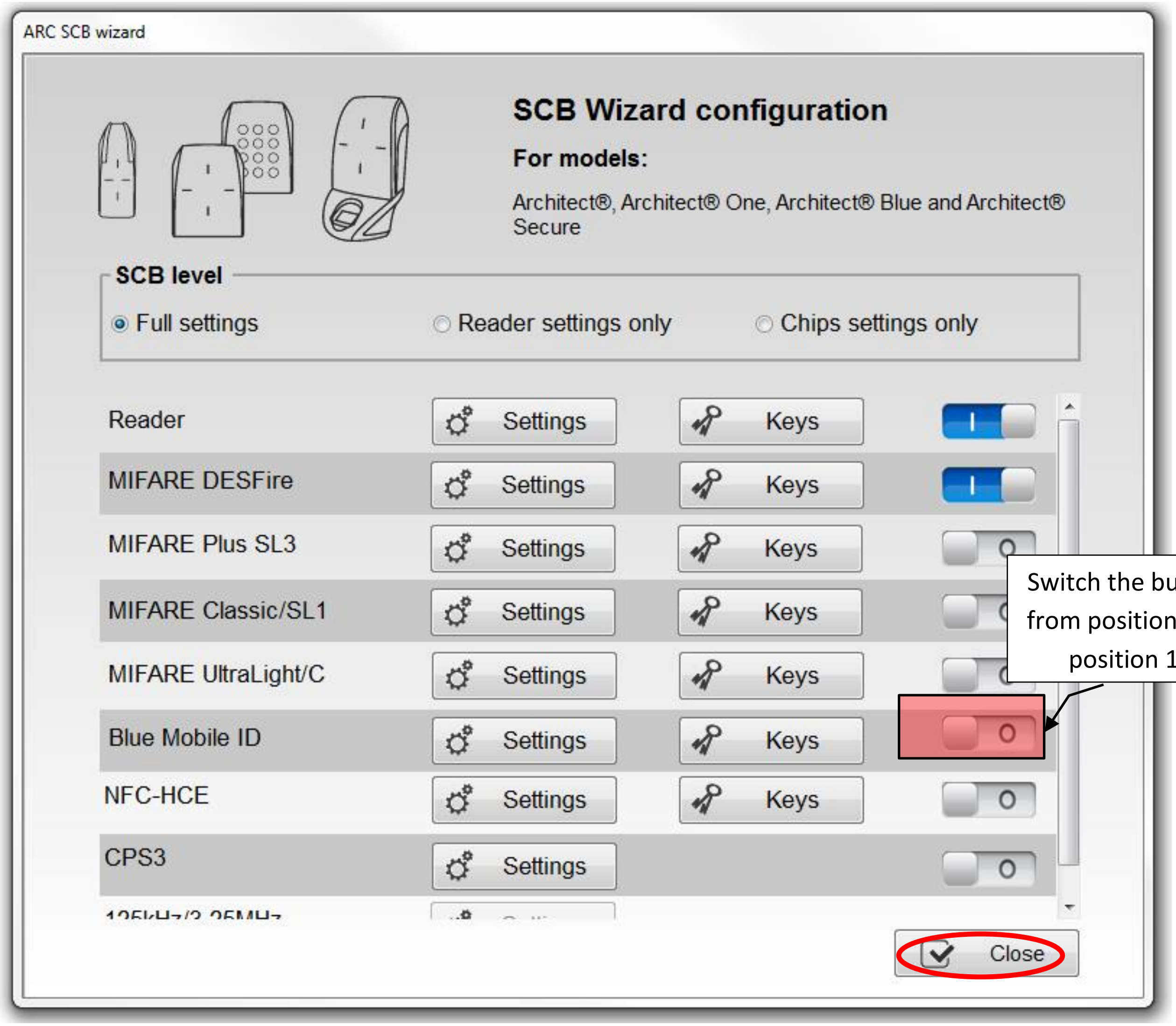
Blue Mobile Id options
Display settings configuration

Designation
Configuration Name (max 14 characters) * SameAsDESFire
Site code * C2FB
□ STid Mobile ID (CSN)
*Mandatory fields

Identification modes and communication distances
☑ Card Contact
□ Hands free Up to ~3m
□ Slide Very short
□ Remote Up to ~3m
□ TapTap Up to ~3m

Remote options
● Remote 1 ○ Remote 2

□ Requires smartphone unlocking to authenticate



ARC SCB wizard

SCB Wizard configuration

For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	I
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	O
NFC-HCE	Settings	Keys	O
CPS3	Settings		O
125kHz/3.25MHz	Settings		

Switch the button from position 0 to position 1.

Note: You do not have to enter in the Blue Mobile settings, all parameters have been automatically entered according to the parameters of your DESFire® configuration.

Go to step *I-9 Encoding the private ID*

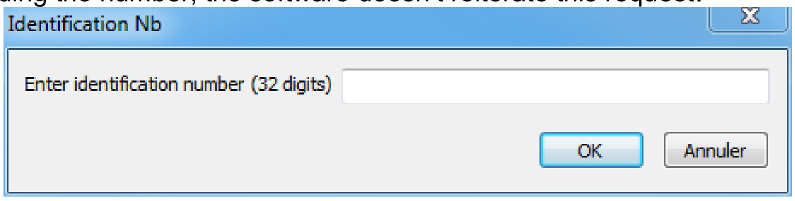
III. ARCS-R31-X-PH5-xx configuration

III-1. SECard settings

Step 1: Connect STid ARC-W35-G/BT1-5AA or ARC-W35-G/PH5-5AA encoder to a com port of the computer.

Step 2: Launch SECard.exe

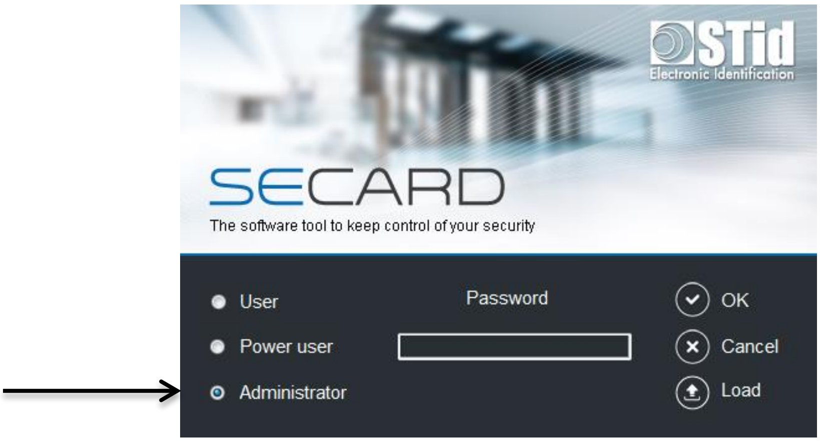
Step 3: At first use, the software opens a window to enter the serial number of 32 characters located at the back of the encoder. After recording the number, the software doesn't reiterate this request.



Identification Nb

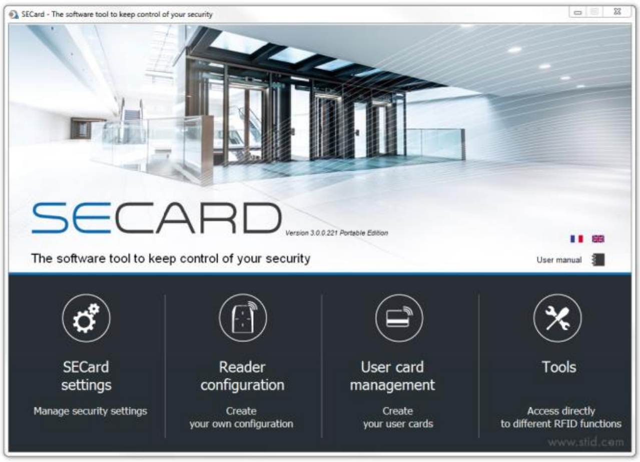
Enter identification number (32 digits)

Step 4: Select the Access level « Administrator » and the password: **STidA**

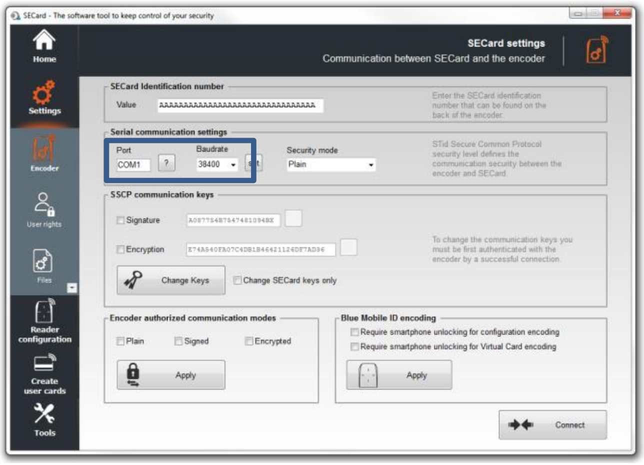


STid
Electronic Identification
SECARD
The software tool to keep control of your security
○ User
○ Power user
◉ Administrator
Password
OK
Cancel
Load

Step 5: In SECard settings, select the COM port on which the encoder has been connected, if you do not know the number click on the interrogation point.



SECard - The software tool to keep control of your security
SECARD
Version 3.0.0.221 Portable Edition
The software tool to keep control of your security
User manual
SECard settings
Manage security settings
Reader configuration
Create your own configuration
User card management
Create your user cards
Tools
Access directly to different RFID functions
www.stid.com



SECard - The software tool to keep control of your security

SECard settings
Communication between SECard and the encoder

SECard Identification number
Value: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Enter the SECard identification number that can be found on the back of the encoder.

Serial communication settings
Port: COM1 ?
Baudrate: 38400
Security mode: Plain
STid Secure Common Protocol security level defines the communication security between the encoder and SECard.

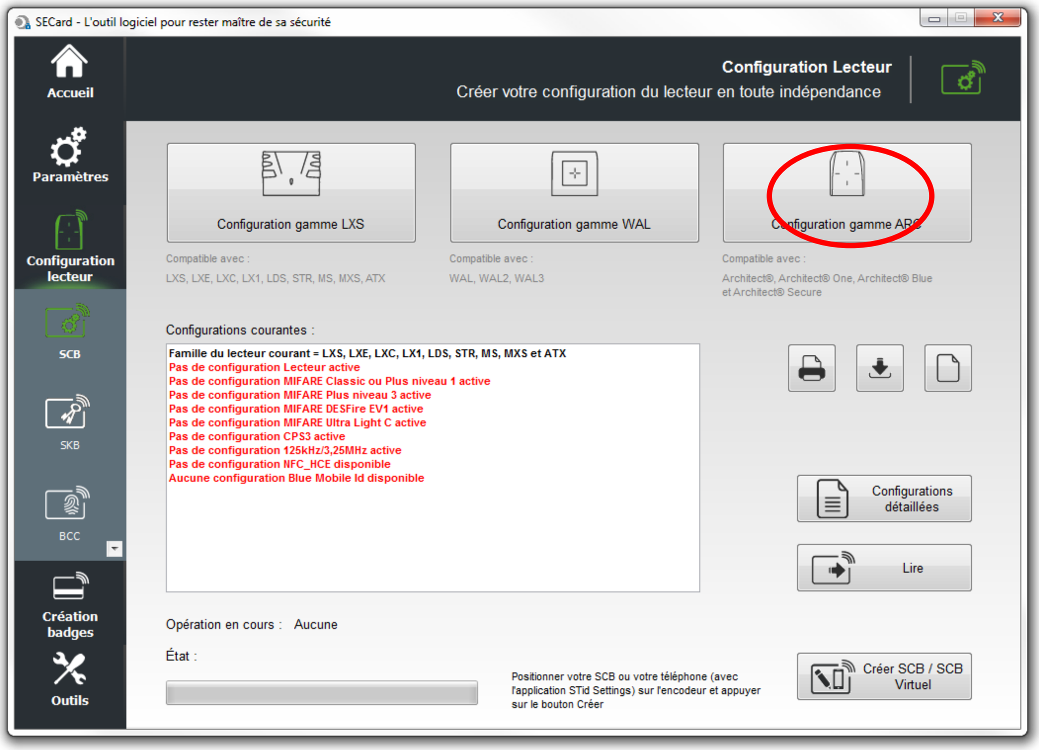
SSCP communication keys
□ Signature A08775487547481094BX
□ Encryption E74A640FA07C4DB1B46421126DF7AD96
Change Keys
□ Change SECard keys only
To change the communication keys you must be first authenticated with the encoder by a successful connection.

Encoder authorized communication modes
□ Plain □ Signed □ Encrypted
Apply

Blue Mobile ID encoding
□ Require smartphone unlocking for configuration encoding
□ Require smartphone unlocking for Virtual Card encoding
Apply

Connect

III-2. Select ARC series configuration wizard



SECard - L'outil logiciel pour rester maître de sa sécurité

Configuration Lecteur

Créer votre configuration du lecteur en toute indépendance

Compatible avec : LXS, LXE, LXC, LX1, LDS, STR, MS, MXS, ATX

Compatible avec : WAL, WAL2, WAL3

Compatible avec : Architect®, Architect® One, Architect® Blue et Architect® Secure

Configurations courantes :

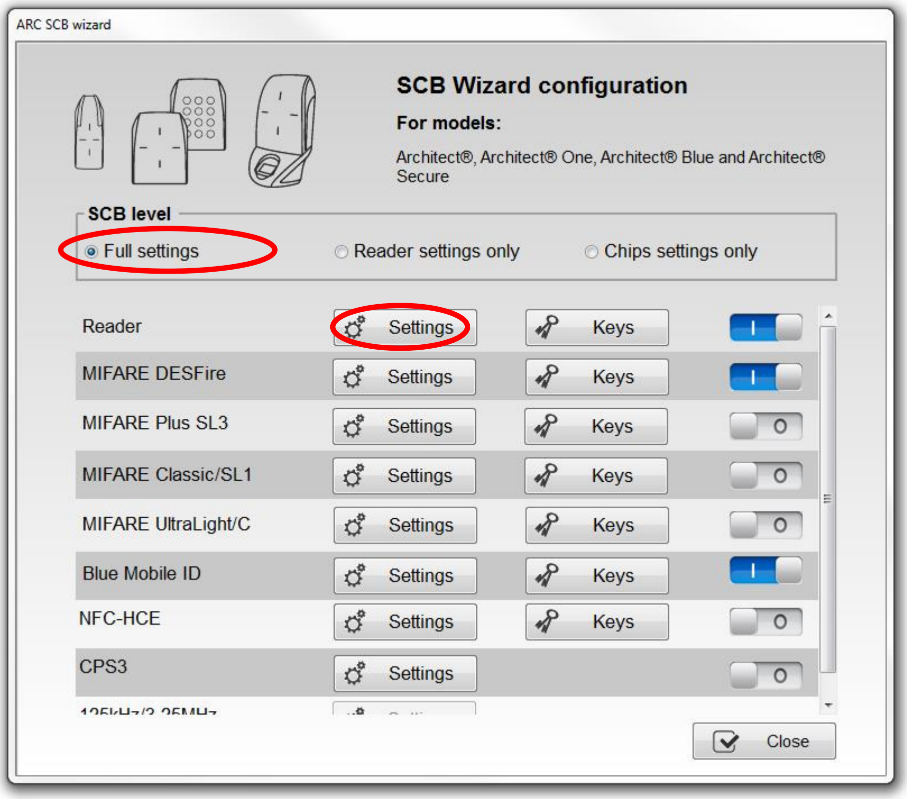
Famille du lecteur courant = LXS, LXE, LXC, LX1, LDS, STR, MS, MXS et ATX
Pas de configuration Lecteur active
Pas de configuration MIFARE Classic ou Plus niveau 1 active
Pas de configuration MIFARE Plus niveau 3 active
Pas de configuration MIFARE DESFire EV1 active
Pas de configuration MIFARE Ultra Light C active
Pas de configuration CPS3 active
Pas de configuration 125kHz/3,25MHz active
Pas de configuration NFC_HCE disponible
Aucune configuration Blue Mobile Id disponible

Opération en cours : Aucune

État :

Positionner votre SCB ou votre téléphone (avec l'application STid Settings) sur l'encodeur et appuyer sur le bouton Créer

III-3. Reader: Settings



ARC SCB wizard

SCB Wizard configuration

For models:

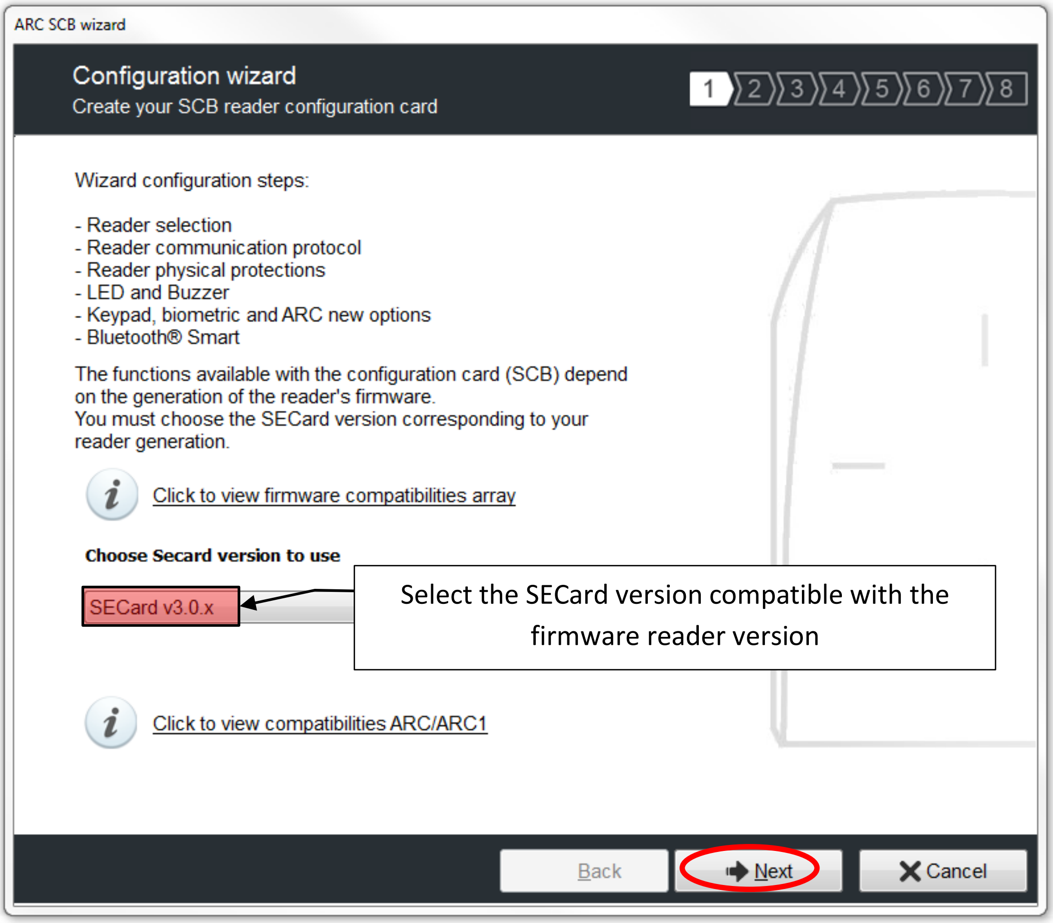
Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	I
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	I
NFC-HCE	Settings	Keys	O
CPS3	Settings		O
125kHz/3,25MHz	Settings		

Follow the 8 steps of the wizard:



ARC SCB wizard

Configuration wizard

Create your SCB reader configuration card

Wizard configuration steps:

- Reader selection
- Reader communication protocol
- Reader physical protections
- LED and Buzzer
- Keypad, biometric and ARC new options
- Bluetooth® Smart

The functions available with the configuration card (SCB) depend on the generation of the reader's firmware.
You must choose the SECard version corresponding to your reader generation.

Click to view firmware compatibilities array

Choose Secard version to use

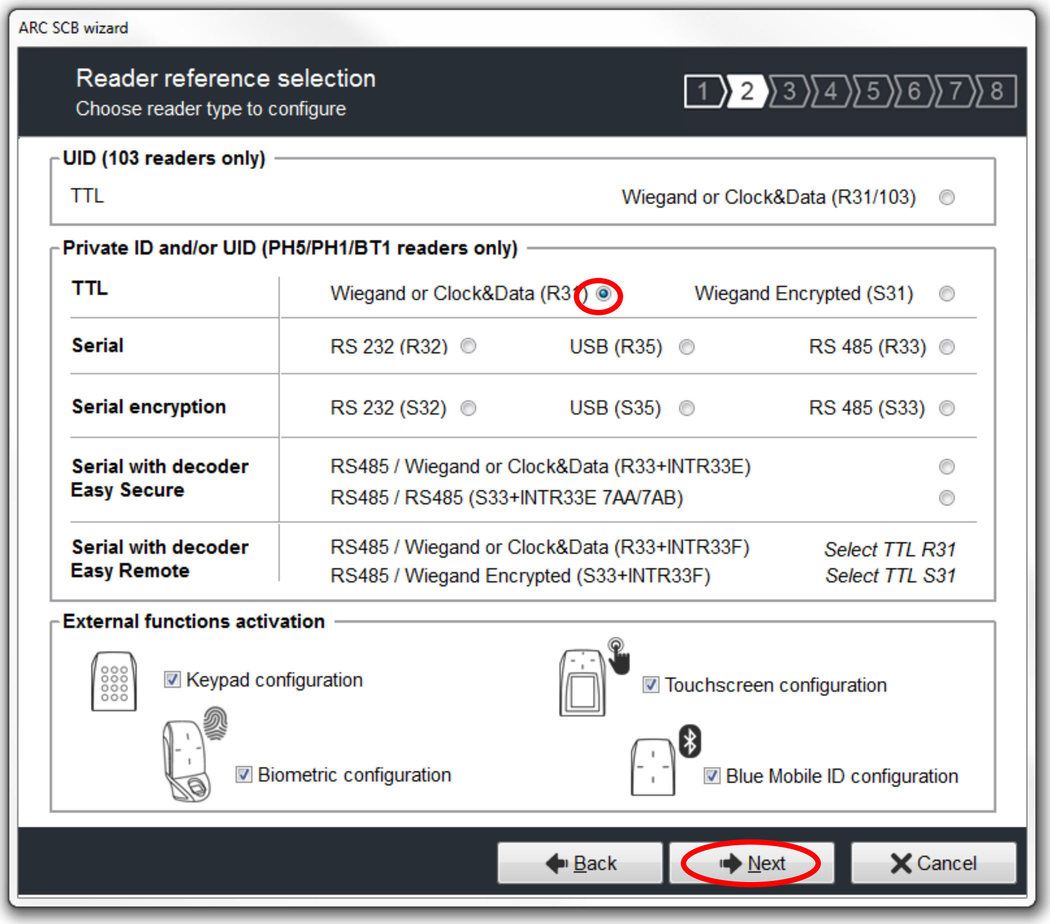
SECard v3.0.x

Select the SECard version compatible with the firmware reader version

Click to view compatibilities ARC/ARC1

The firmware version is located on the label of the reader and is indicated after the initialization phase of the reader by a color code:

Red	**= +10**
Orange	**= +5**
Green	**= +1**



ARC SCB wizard

Reader reference selection

Choose reader type to configure

UID (103 readers only)

TTL	Wiegand or Clock&Data (R31/103) ○

Private ID and/or UID (PH5/PH1/BT1 readers only)

TTL	Wiegand or Clock&Data (R31) ●	Wiegand Encrypted (S31) ○	
Serial	RS 232 (R32) ○	USB (R35) ○	RS 485 (R33) ○
Serial encryption	RS 232 (S32) ○	USB (S35) ○	RS 485 (S33) ○
Serial with decoder Easy Secure	RS485 / Wiegand or Clock&Data (R33+INTR33E) ○ RS485 / RS485 (S33+INTR33E 7AA/7AB) ○		
Serial with decoder Easy Remote	RS485 / Wiegand or Clock&Data (R33+INTR33F) *Select TTL R31* RS485 / Wiegand Encrypted (S33+INTR33F) *Select TTL S31*		

External functions activation

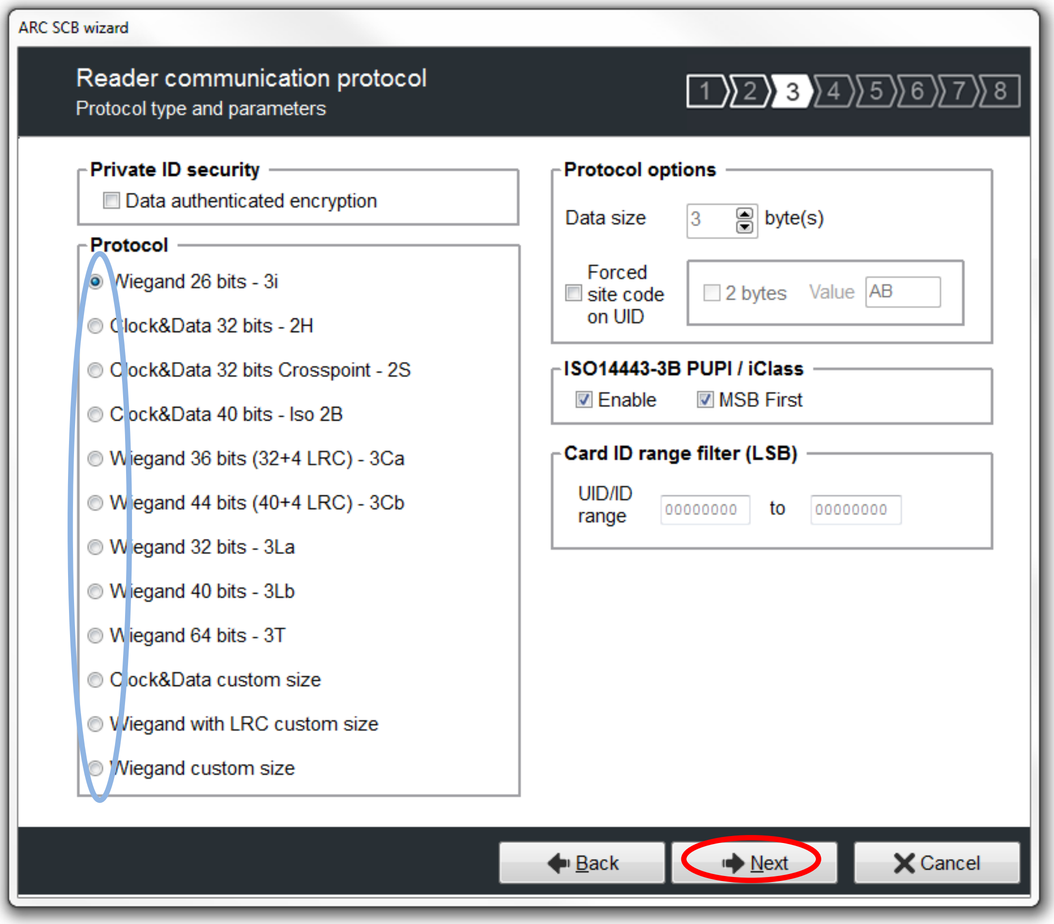
☑ Keypad configuration

☑ Touchscreen configuration

☑ Biometric configuration

☑ Blue Mobile ID configuration

All the options are activated in this guide (Keyboard, Biometry and touch screen) if one of the options is not used, deactivate it by unchecking the corresponding box.



ARC SCB wizard

Reader communication protocol

Protocol type and parameters

Private ID security

□ Data authenticated encryption

Protocol

- ● Wiegand 26 bits - 3i
- ○ Clock&Data 32 bits - 2H
- ○ Clock&Data 32 bits Crosspoint - 2S
- ○ Clock&Data 40 bits - Iso 2B
- ○ Wiegand 36 bits (32+4 LRC) - 3Ca
- ○ Wiegand 44 bits (40+4 LRC) - 3Cb
- ○ Wiegand 32 bits - 3La
- ○ Wiegand 40 bits - 3Lb
- ○ Wiegand 64 bits - 3T
- ○ Clock&Data custom size
- ○ Wiegand with LRC custom size
- ○ Wiegand custom size

Protocol options

Data size 3 byte(s)

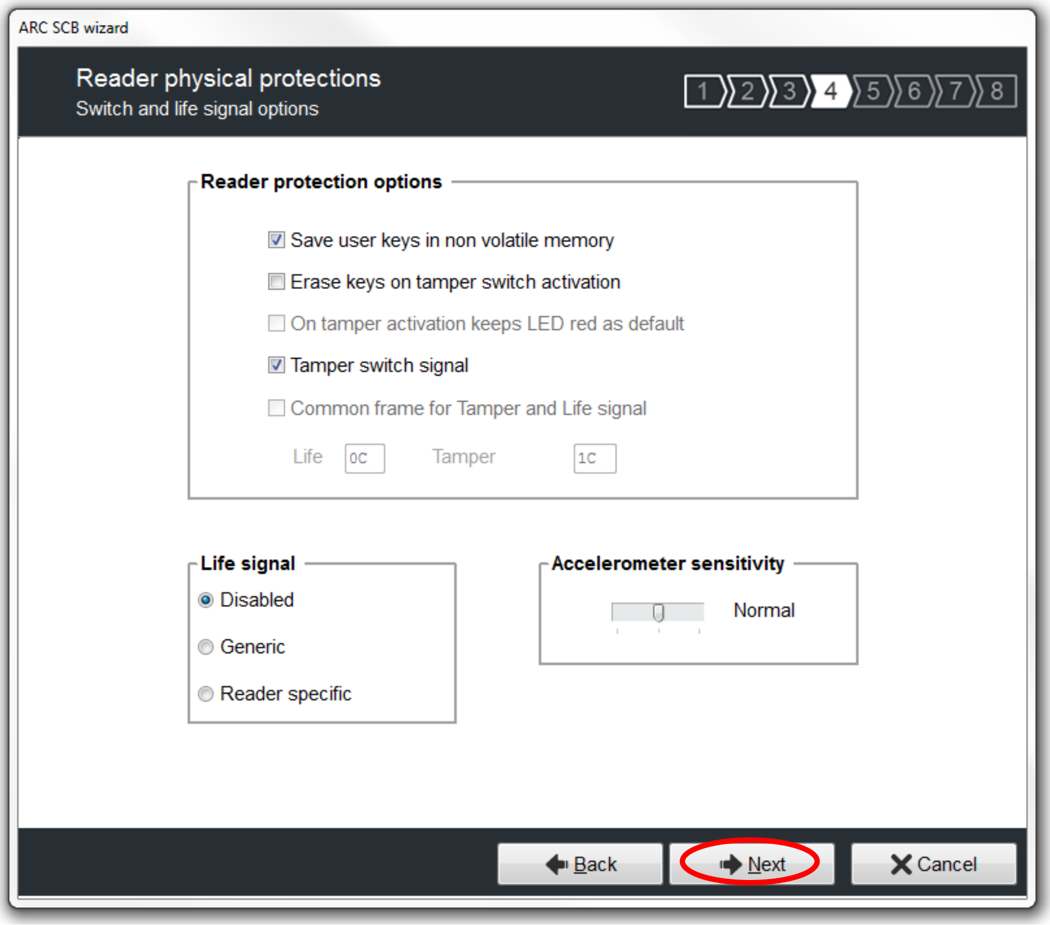
□ Forced site code on UID □ 2 bytes Value AB

ISO14443-3B PUPI / iClass

☑ Enable ☑ MSB First

Card ID range filter (LSB)

UID/ID range 00000000 to 00000000



ARC SCB wizard

Reader physical protections

Switch and life signal options

Reader protection options

☑ Save user keys in non volatile memory

□ Erase keys on tamper switch activation

□ On tamper activation keeps LED red as default

☑ Tamper switch signal

□ Common frame for Tamper and Life signal

Life: 0C Tamper: 1C

Life signal

● Disabled

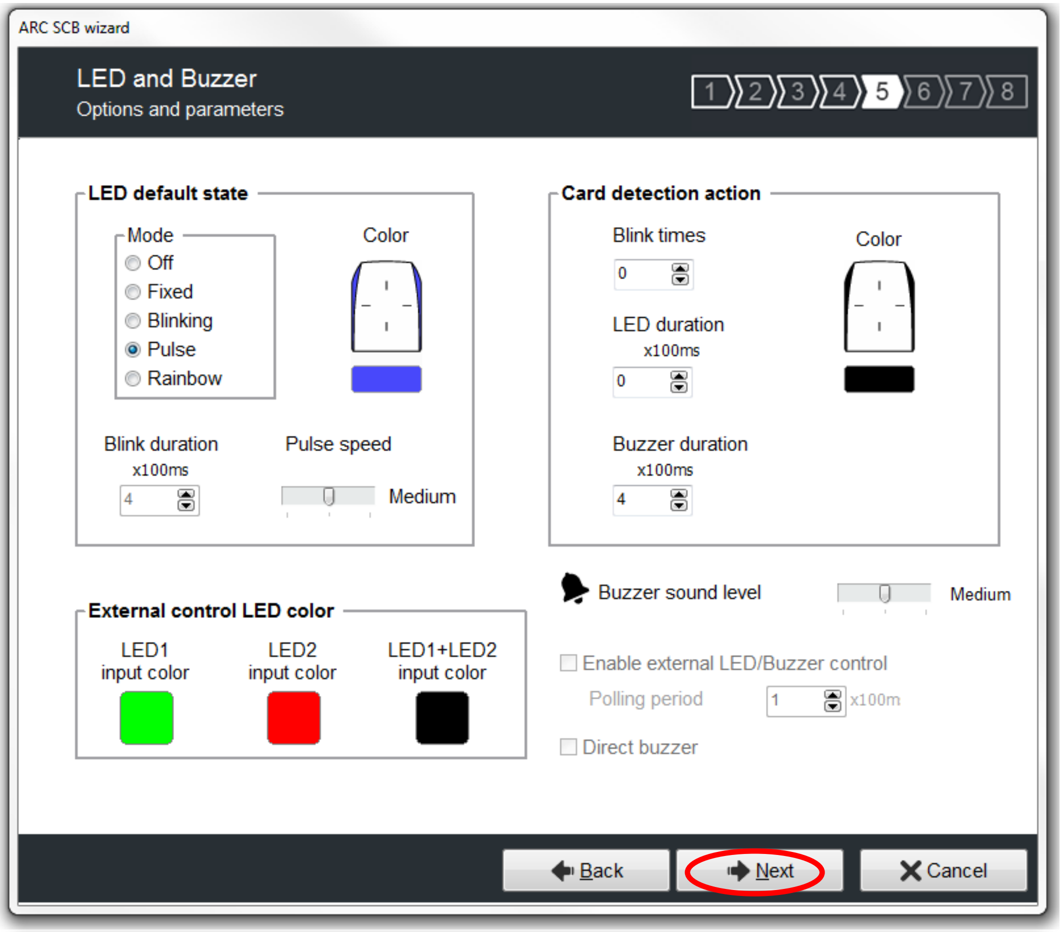
○ Generic

○ Reader specific

Accelerometer sensitivity

Normal

Are checked the most commonly used options, it is possible to activate or deactivate these options according to your specifications.



ARC SCB wizard

LED and Buzzer
Options and parameters

LED default state

Mode
- ○ Off
- ○ Fixed
- ○ Blinking
- ● Pulse
- ○ Rainbow

Color 🟦

Blink duration x100ms: 4

Pulse speed: Medium

Card detection action

Blink times: 0

LED duration x100ms: 0

Color ⬛

Buzzer duration x100ms: 4

Buzzer sound level: Medium

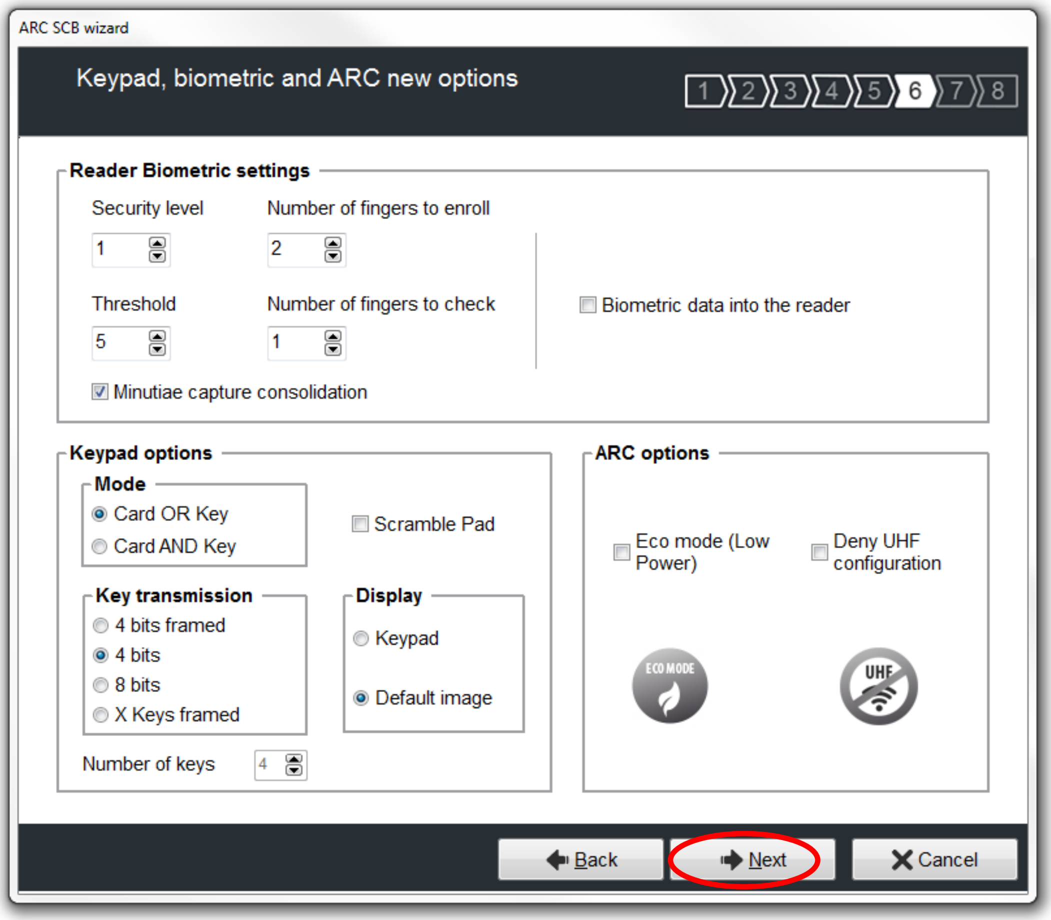
□ Enable external LED/Buzzer control

Polling period: 1 x100m

□ Direct buzzer

External control LED color

LED1 input color	LED2 input color	LED1+LED2 input color
🟩	🟥	⬛



ARC SCB wizard

Keypad, biometric and ARC new options

Reader Biometric settings

Security level: 1

Number of fingers to enroll: 2

Threshold: 5

Number of fingers to check: 1

□ Biometric data into the reader

☑ Minutiae capture consolidation

Keypad options

Mode
- ● Card OR Key
- ○ Card AND Key

□ Scramble Pad

Key transmission
- ○ 4 bits framed
- ● 4 bits
- ○ 8 bits
- ○ X Keys framed

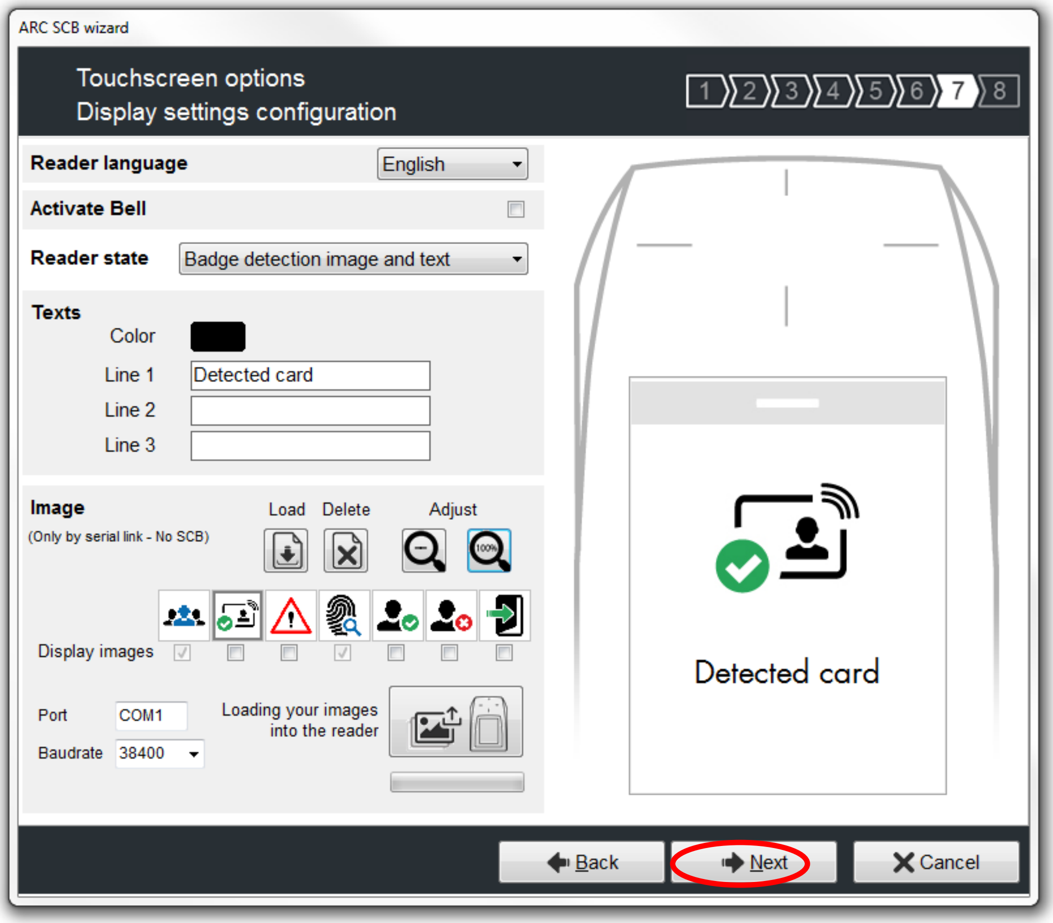
Display
- ○ Keypad
- ● Default image

Number of keys: 4

ARC options

□ Eco mode (Low Power)

□ Deny UHF configuration



ARC SCB wizard

Touchscreen options
Display settings configuration

1 2 3 4 5 6 7 8

Reader language: English

Activate Bell □

Reader state: Badge detection image and text

Texts
Color: ■
Line 1: Detected card
Line 2:
Line 3:

Image
(Only by serial link - No SCB)
Load Delete Adjust

Display images ☑ □ □ ☑ □ □ □

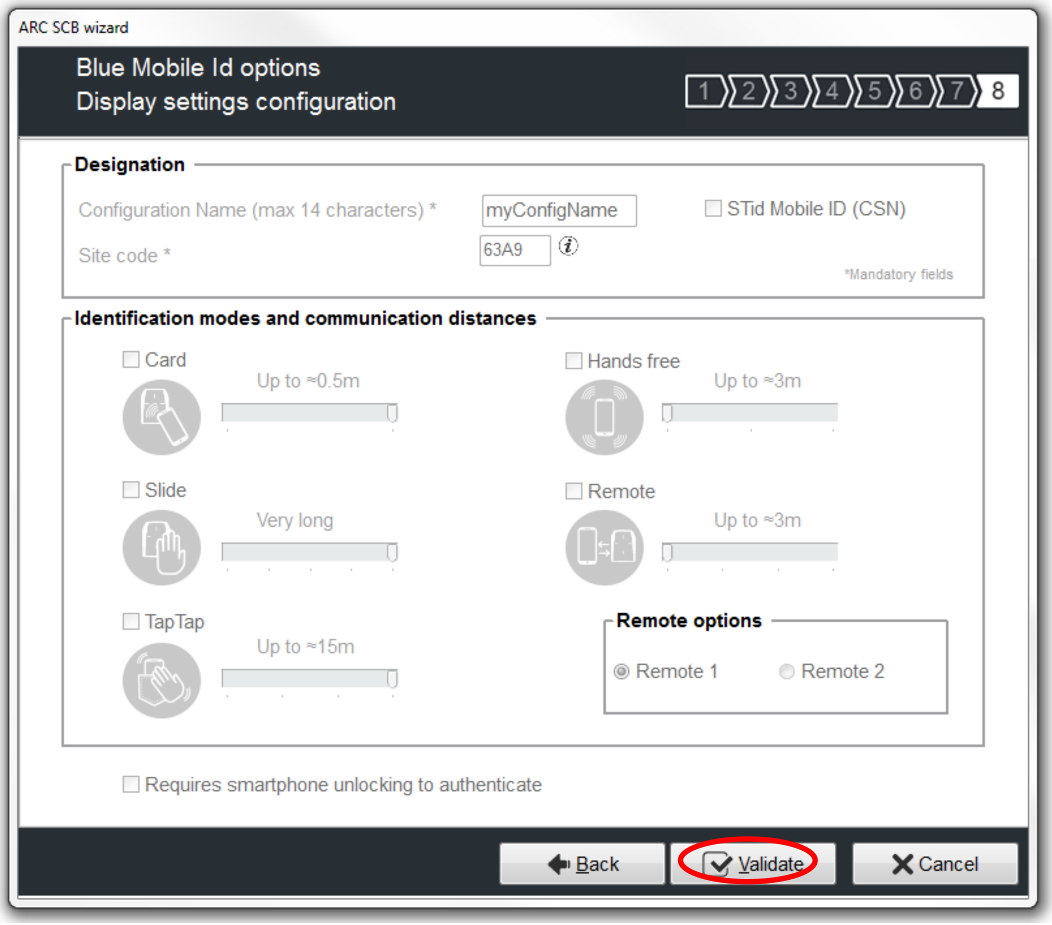
Port: COM1
Baudrate: 38400

Loading your images into the reader

Detected card

Back | Next | Cancel

You can choose new images or keep the default image as shown in the example.



ARC SCB wizard

Blue Mobile Id options
Display settings configuration

1 2 3 4 5 6 7 8

Designation

Configuration Name (max 14 characters) *: myConfigName

□ STid Mobile ID (CSN)

Site code *: 63A9

*Mandatory fields

Identification modes and communication distances

□ Card — Up to ≈0.5m

□ Hands free — Up to ≈3m

□ Slide — Very long

□ Remote — Up to ≈3m

□ TapTap — Up to ≈15m

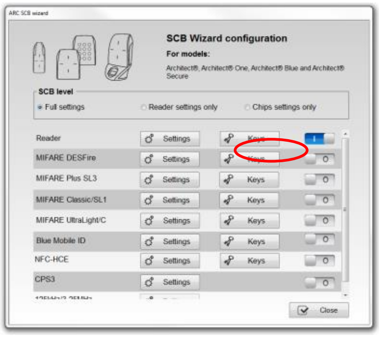
Remote options

● Remote 1 ○ Remote 2

□ Requires smartphone unlocking to authenticate

Back | Validate | Cancel

III-4. Readers: Keys



ARC SCB wizard

SCB Wizard configuration

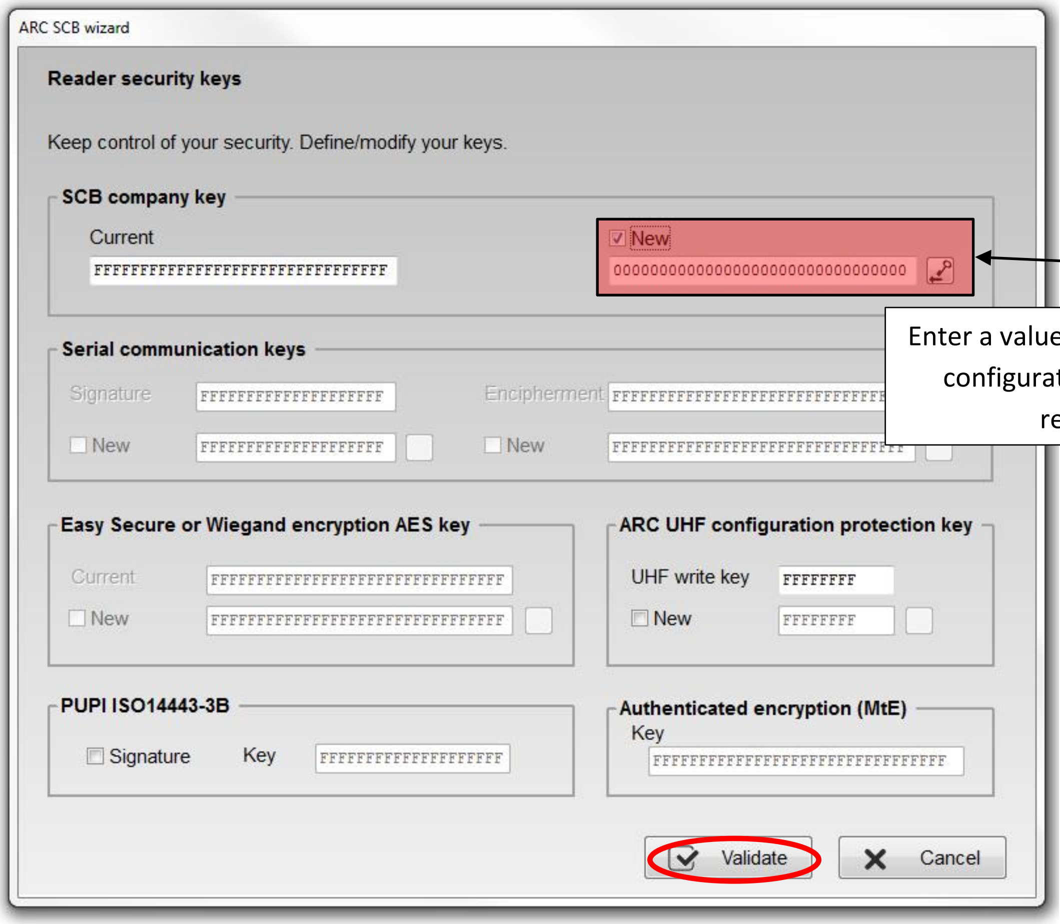
For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	O
NFC-HCE	Settings	Keys	O
CPS3	Settings		O



ARC SCB wizard

Reader security keys

Keep control of your security. Define/modify your keys.

SCB company key

Current: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

☑ New: 00000000000000000000000000000000

Serial communication keys

Signature: FFFFFFFFFFFFFFFFFFFF

□ New: FFFFFFFFFFFFFFFFFFFF

Encipherment: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

□ New: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Easy Secure or Wiegand encryption AES key

Current: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

□ New: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

ARC UHF configuration protection key

UHF write key: FFFFFFFF

□ New: FFFFFFFF

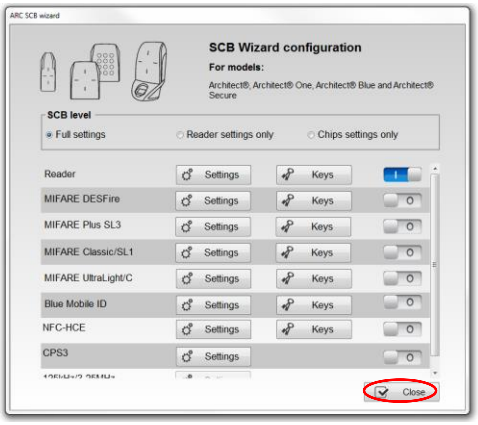
PUPI ISO14443-3B

□ Signature Key: FFFFFFFFFFFFFFFFFFFF

Authenticated encryption (MtE)

Key: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Enter a value to protect your configuration and your reader



ARC SCB wizard

SCB Wizard configuration

For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	O
NFC-HCE	Settings	Keys	O
CPS3	Settings		O

The configuration of the settings and keys reader is complete. You can use the typical sample configuration below to configure DESFire® chip *V- DESFire® EV1 configuration*

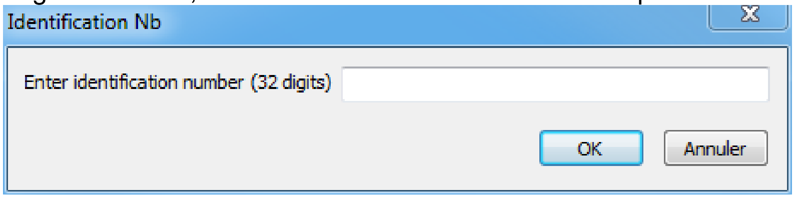
IV. ARC-R33+INTR33E (Easy Secure) configuration

IV-1. SECard settings

Step 1: Connect STid ARC-W35-G/BT1-5AA or ARC-W35-G/PH5-5AA encoder to a com port of the computer.

Step 2: Launch SECard.exe

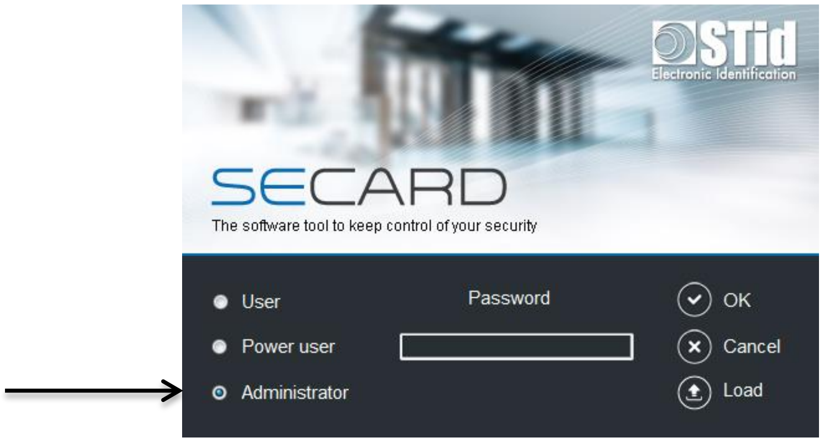
Step 3: At first use, the software opens a window to enter the serial number of 32 characters located at the back of the encoder. After recording the number, the software doesn't reiterate this request.



Identification Nb

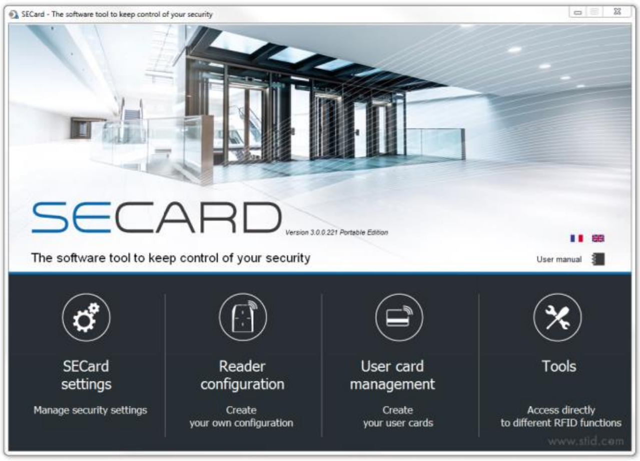
Enter identification number (32 digits)

Step 4: Select the Access level « Administrator » and the password: **STidA**

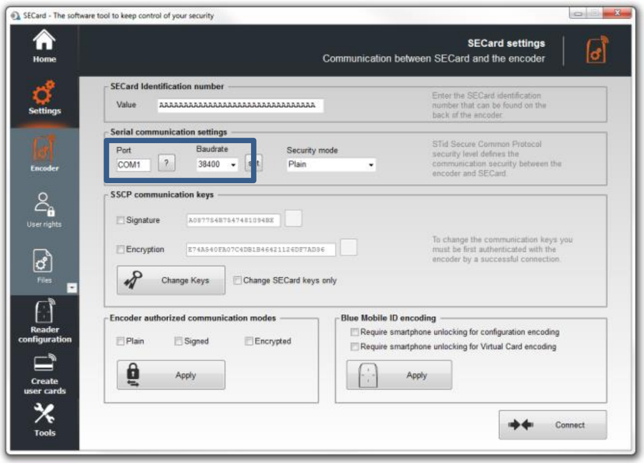


STid
Electronic Identification
SECARD
The software tool to keep control of your security
User
Power user
Administrator
Password
OK
Cancel
Load

Step 5: In SECard settings, select the COM port on which the encoder has been connected, if you do not know the number click on the interrogation point.



SECard - The software tool to keep control of your security
SECARD
Version 3.0.0.221 Portable Edition
The software tool to keep control of your security
User manual
SECard settings
Manage security settings
Reader configuration
Create your own configuration
User card management
Create your user cards
Tools
Access directly to different RFID functions
www.stid.com



SECard - The software tool to keep control of your security

SECard settings
Communication between SECard and the encoder

SECard Identification number
Value: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Enter the SECard identification number that can be found on the back of the encoder.

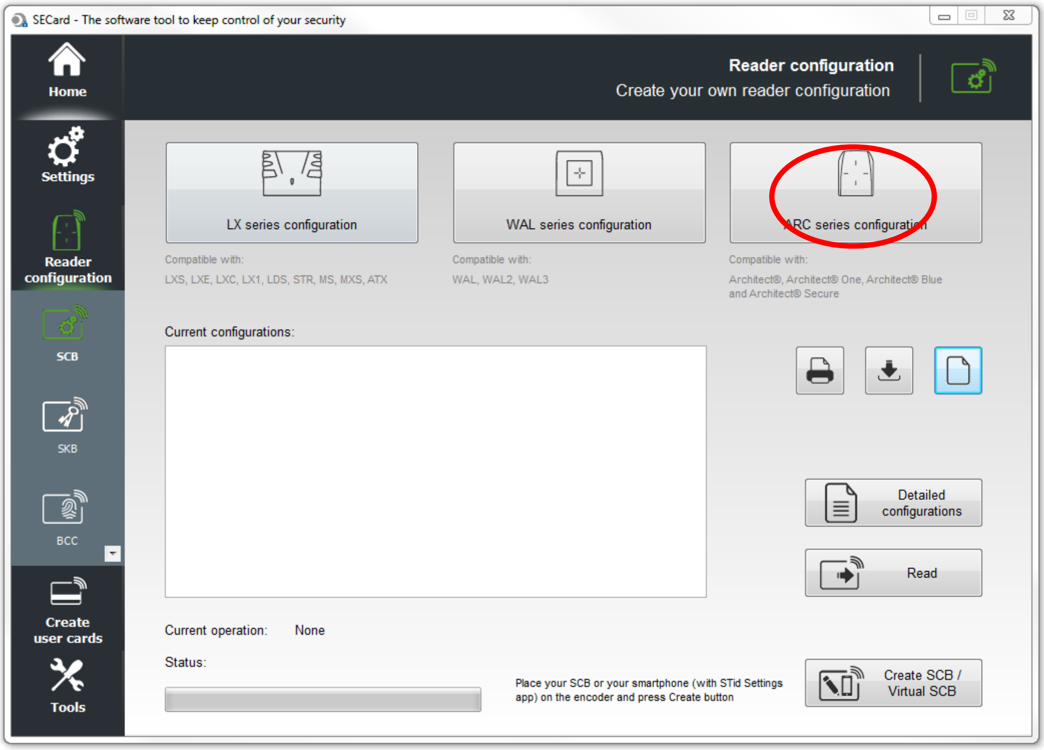
Serial communication settings
Port: COM1 ?
Baudrate: 38400
Security mode: Plain
STid Secure Common Protocol security level defines the communication security between the encoder and SECard.

SSCP communication keys
□ Signature: A0877S4B7S474810948X
□ Encryption: E74A640FA07C4DB1B46421126DF7AD86
□ Change SECard keys only
To change the communication keys you must be first authenticated with the encoder by a successful connection.

Encoder authorized communication modes
□ Plain □ Signed □ Encrypted

Blue Mobile ID encoding
□ Require smartphone unlocking for configuration encoding
□ Require smartphone unlocking for Virtual Card encoding

IV-2. Select ARC series configuration wizard



Compatible with: LXS, LXE, LXC, LX1, LDS, STR, MS, MXS, ATX

Compatible with: WAL, WAL2, WAL3

Compatible with: Architect®, Architect® One, Architect® Blue and Architect® Secure

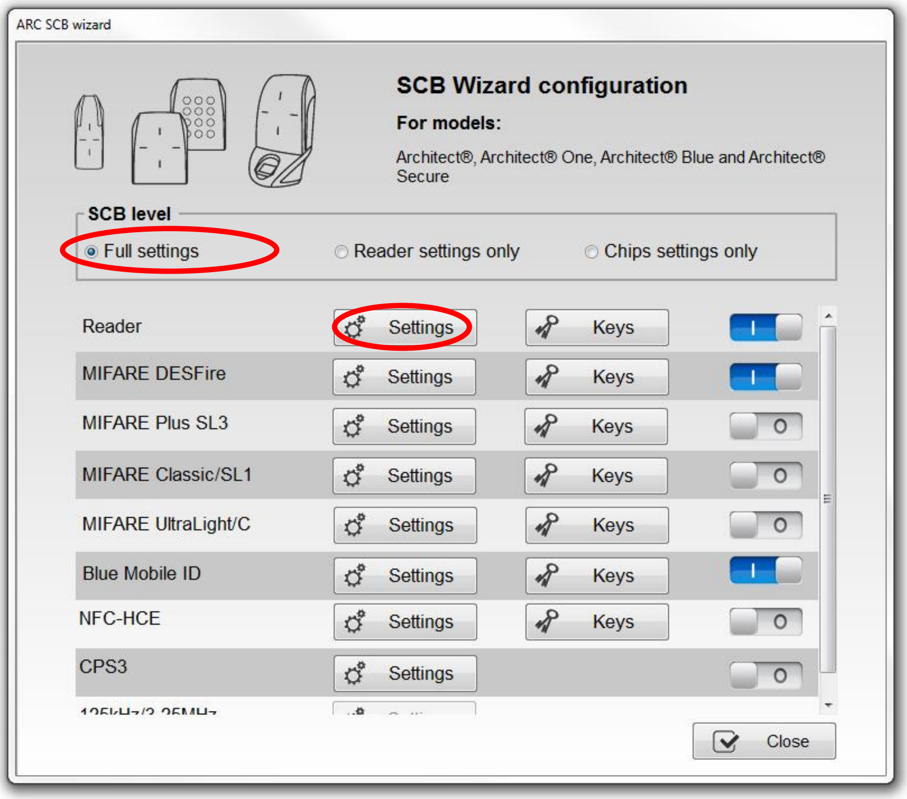
Current configurations:

Current operation: None

Status:

Place your SCB or your smartphone (with STid Settings app) on the encoder and press Create button

IV-3. Reader: Settings



SCB Wizard configuration

For models:

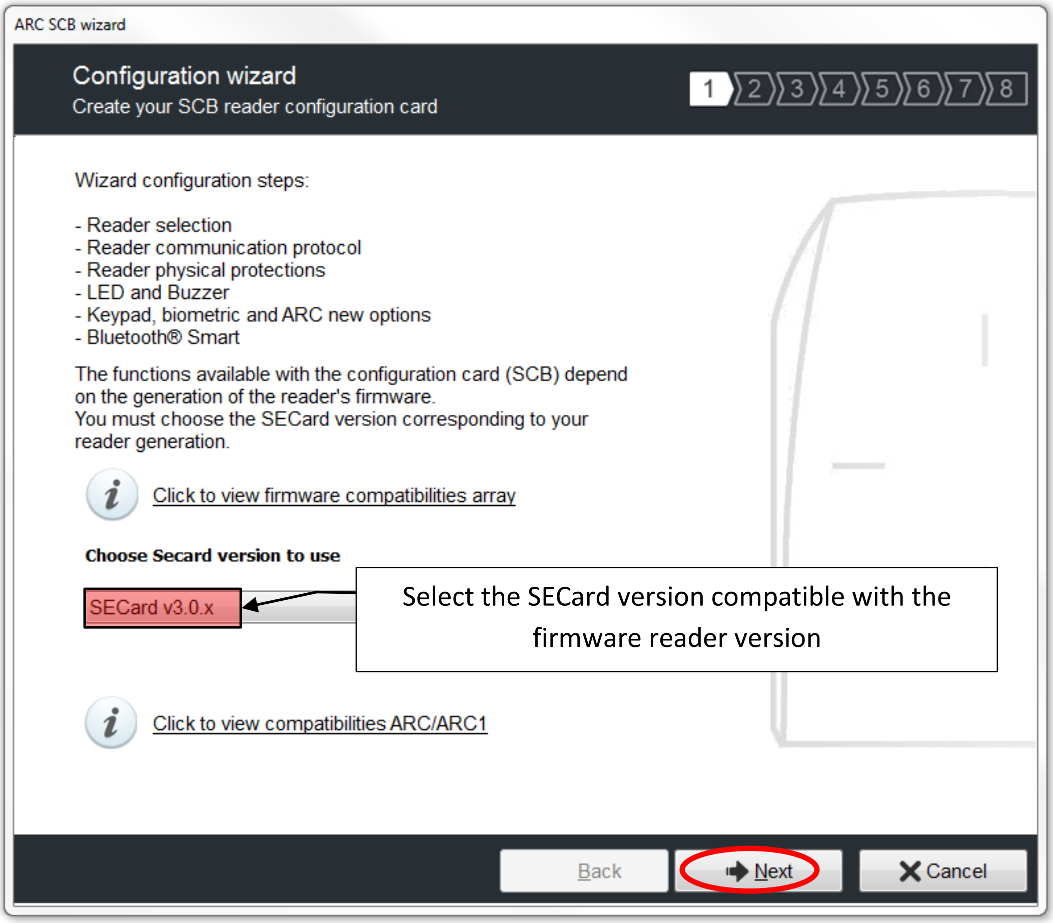
Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	I
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	I
NFC-HCE	Settings	Keys	O
CPS3	Settings		O
125kHz/3.25MHz			

Follow the 8 steps of the wizard:



Wizard configuration steps:

- Reader selection
- Reader communication protocol
- Reader physical protections
- LED and Buzzer
- Keypad, biometric and ARC new options
- Bluetooth® Smart

The functions available with the configuration card (SCB) depend on the generation of the reader's firmware.
You must choose the SECard version corresponding to your reader generation.

Click to view firmware compatibilities array

Choose Secard version to use

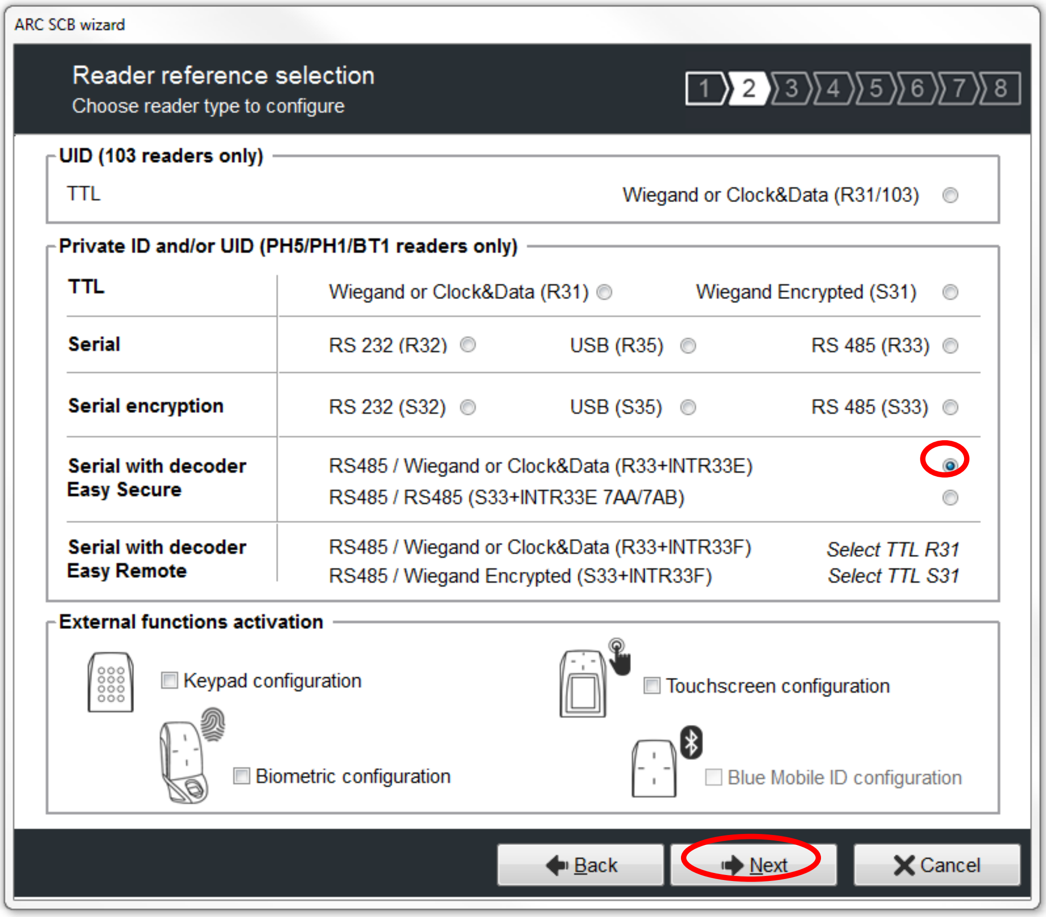
SECard v3.0.x

Select the SECard version compatible with the firmware reader version

Click to view compatibilities ARC/ARC1

The firmware version is located on the label of the reader and is indicated after the initialization phase of the reader by a color code:

Red	**= +10**
Orange	**= +5**
Green	**= +1**



ARC SCB wizard

Reader reference selection

Choose reader type to configure

UID (103 readers only)

TTL — Wiegand or Clock&Data (R31/103) ○

Private ID and/or UID (PH5/PH1/BT1 readers only)

TTL	Wiegand or Clock&Data (R31) ○	Wiegand Encrypted (S31) ○	
Serial	RS 232 (R32) ○	USB (R35) ○	RS 485 (R33) ○
Serial encryption	RS 232 (S32) ○	USB (S35) ○	RS 485 (S33) ○
Serial with decoder Easy Secure	RS485 / Wiegand or Clock&Data (R33+INTR33E) ● RS485 / RS485 (S33+INTR33E 7AA/7AB) ○		
Serial with decoder Easy Remote	RS485 / Wiegand or Clock&Data (R33+INTR33F) RS485 / Wiegand Encrypted (S33+INTR33F)	*Select TTL R31* *Select TTL S31*	

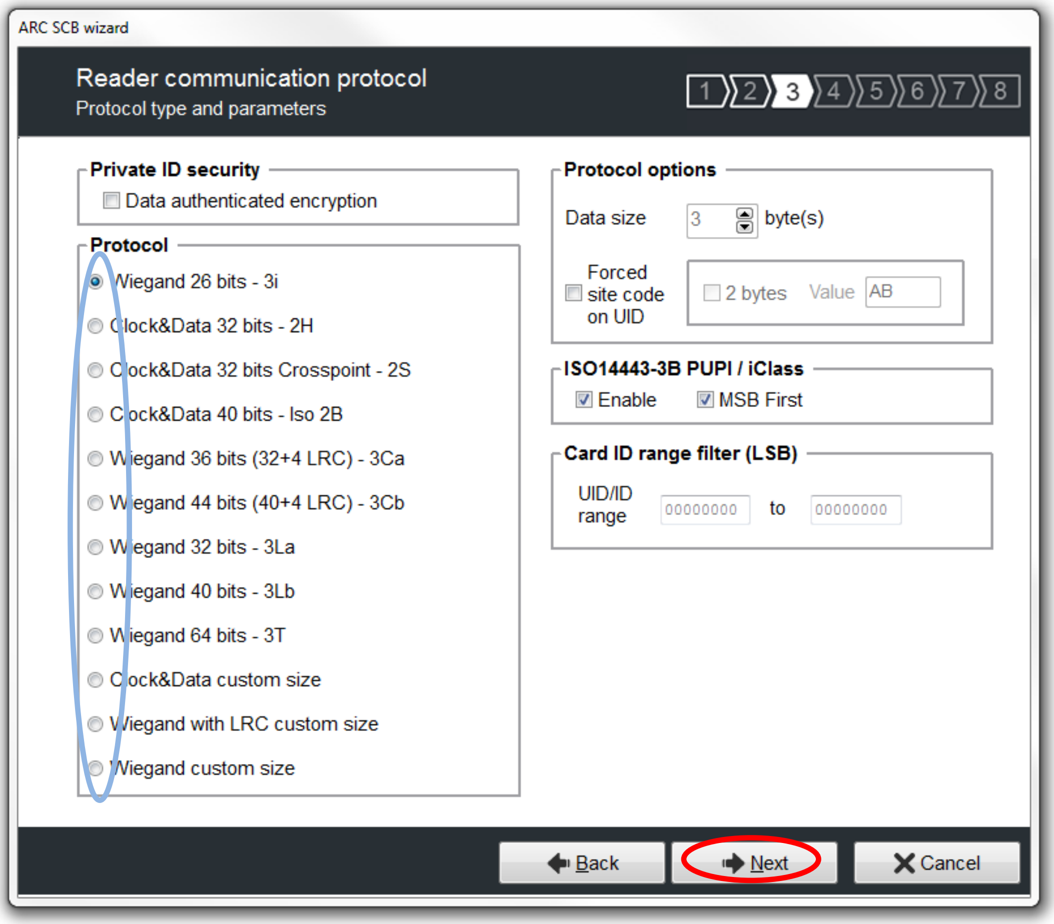
External functions activation

□ Keypad configuration

□ Touchscreen configuration

□ Biometric configuration

□ Blue Mobile ID configuration



ARC SCB wizard

Reader communication protocol

Protocol type and parameters

Private ID security

□ Data authenticated encryption

Protocol

- ● Wiegand 26 bits - 3i
- ○ Clock&Data 32 bits - 2H
- ○ Clock&Data 32 bits Crosspoint - 2S
- ○ Clock&Data 40 bits - Iso 2B
- ○ Wiegand 36 bits (32+4 LRC) - 3Ca
- ○ Wiegand 44 bits (40+4 LRC) - 3Cb
- ○ Wiegand 32 bits - 3La
- ○ Wiegand 40 bits - 3Lb
- ○ Wiegand 64 bits - 3T
- ○ Clock&Data custom size
- ○ Wiegand with LRC custom size
- ○ Wiegand custom size

Protocol options

Data size: 3 byte(s)

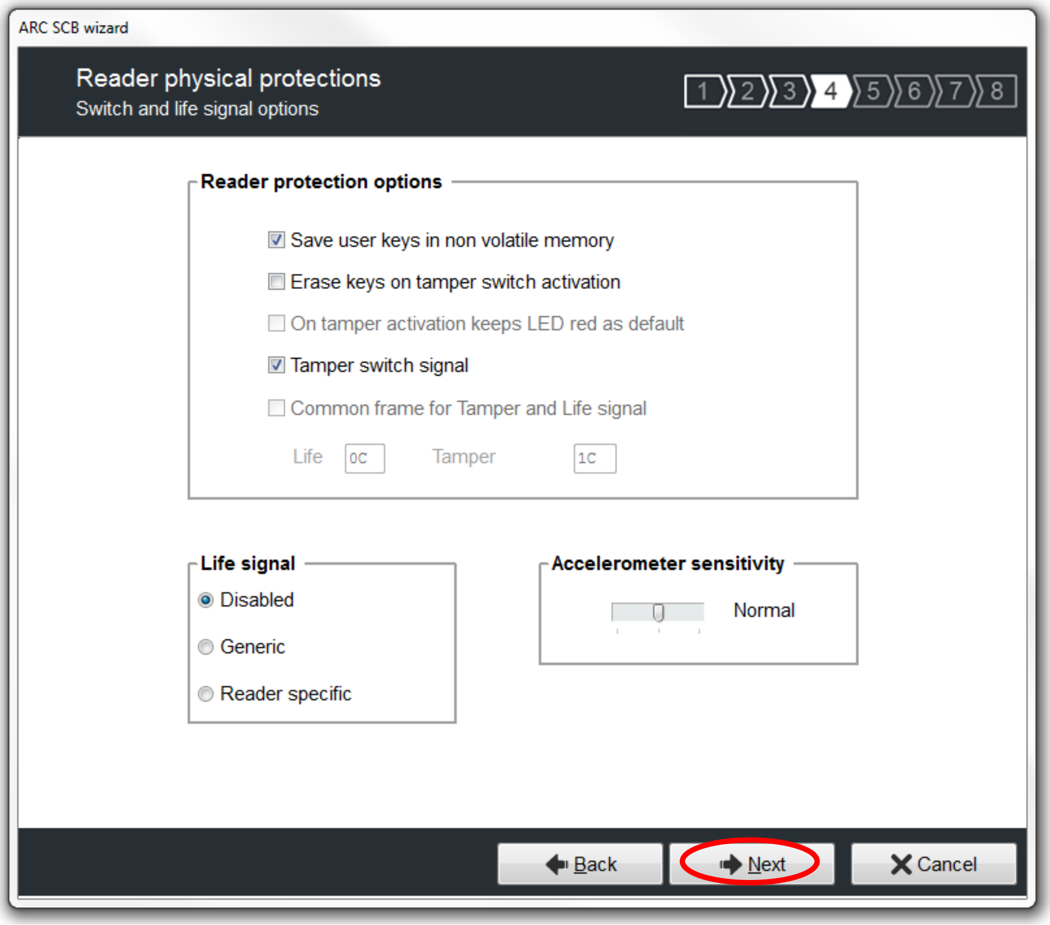
□ Forced site code on UID — □ 2 bytes Value AB

ISO14443-3B PUPI / iClass

☑ Enable ☑ MSB First

Card ID range filter (LSB)

UID/ID range 00000000 to 00000000



ARC SCB wizard

Reader physical protections

Switch and life signal options

Reader protection options

☑ Save user keys in non volatile memory

☐ Erase keys on tamper switch activation

☐ On tamper activation keeps LED red as default

☑ Tamper switch signal

☐ Common frame for Tamper and Life signal

Life 0C Tamper 1C

Life signal

● Disabled

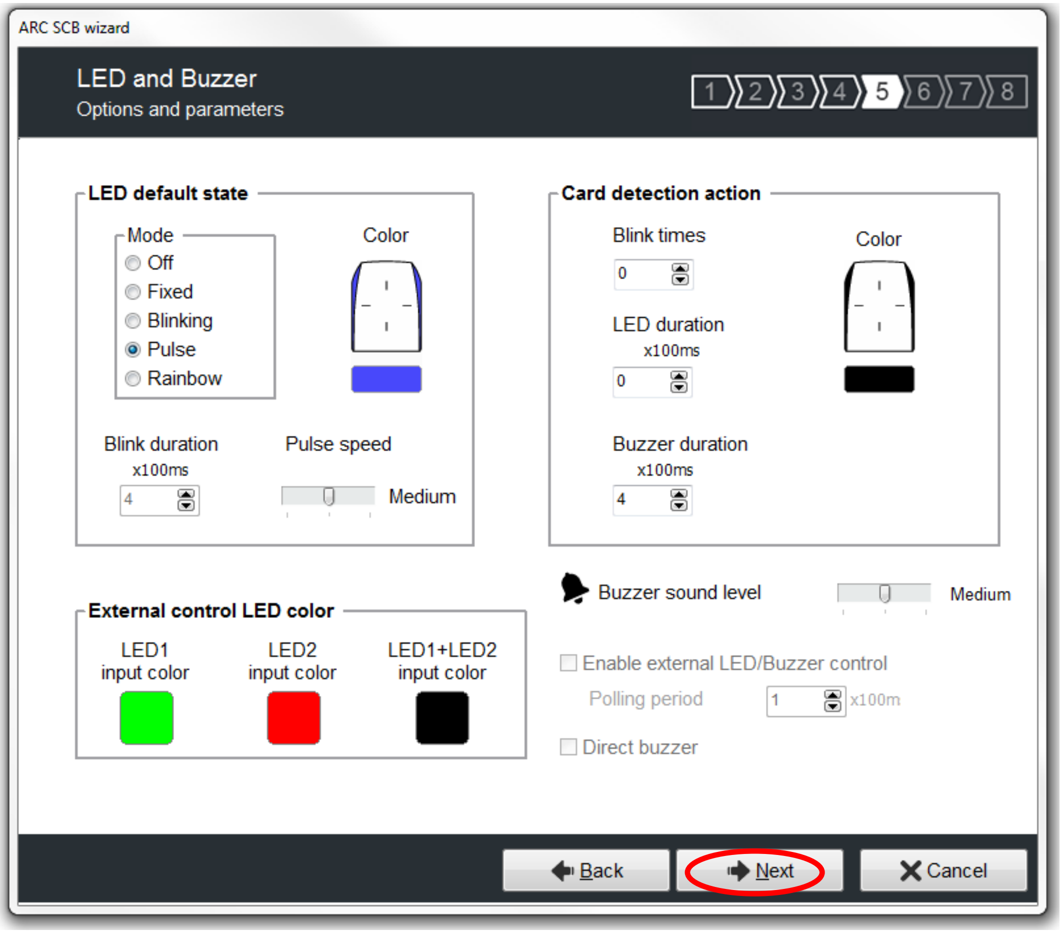
○ Generic

○ Reader specific

Accelerometer sensitivity

Normal

Are checked the most commonly used options, it is possible to activate or deactivate these options according to your specifications.


ARC SCB wizard

LED and Buzzer

Options and parameters

LED default state

Mode
○ Off
○ Fixed
○ Blinking
● Pulse
○ Rainbow

Color

Blink duration x100ms: 4

Pulse speed: Medium

Card detection action

Blink times: 0

LED duration x100ms: 0

Buzzer duration x100ms: 4

Color

Buzzer sound level: Medium

External control LED color

LED1 input color: 🟩

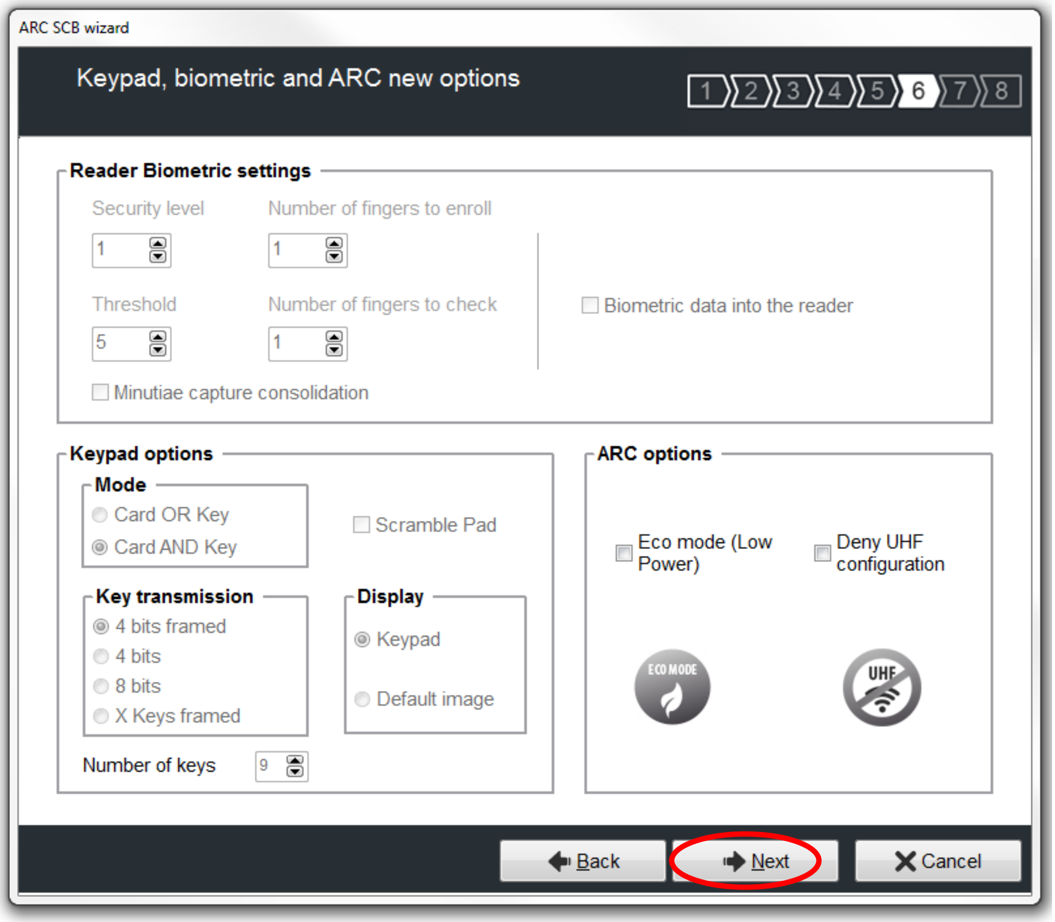
LED2 input color: 🟥

LED1+LED2 input color: ■

□ Enable external LED/Buzzer control

Polling period: 1 x100m

□ Direct buzzer


ARC SCB wizard

Keypad, biometric and ARC new options

Reader Biometric settings

Security level: 1

Number of fingers to enroll: 1

Threshold: 5

Number of fingers to check: 1

□ Minutiae capture consolidation

□ Biometric data into the reader

Keypad options

Mode
○ Card OR Key
● Card AND Key

□ Scramble Pad

Key transmission
● 4 bits framed
○ 4 bits
○ 8 bits
○ X Keys framed

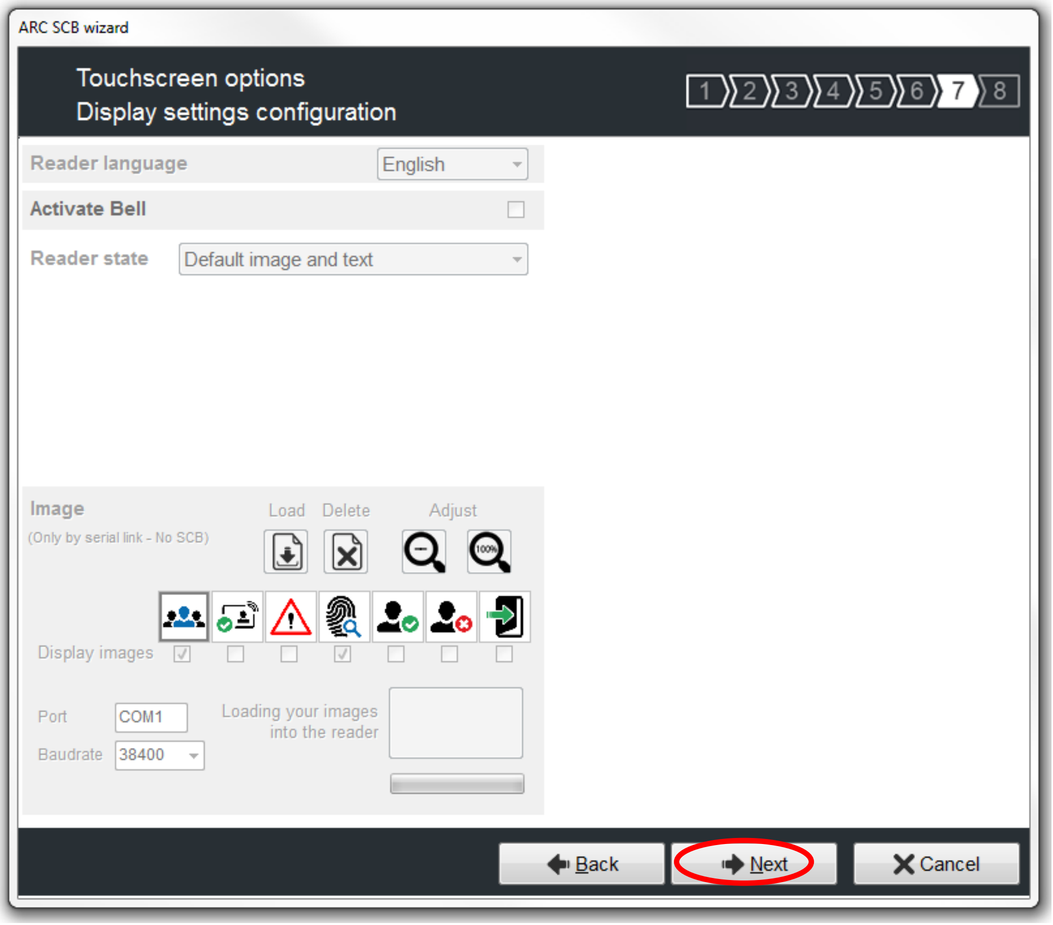
Display
● Keypad
○ Default image

Number of keys: 9

ARC options

□ Eco mode (Low Power)

□ Deny UHF configuration


ARC SCB wizard

Touchscreen options
Display settings configuration

Reader language: English

Activate Bell □

Reader state: Default image and text

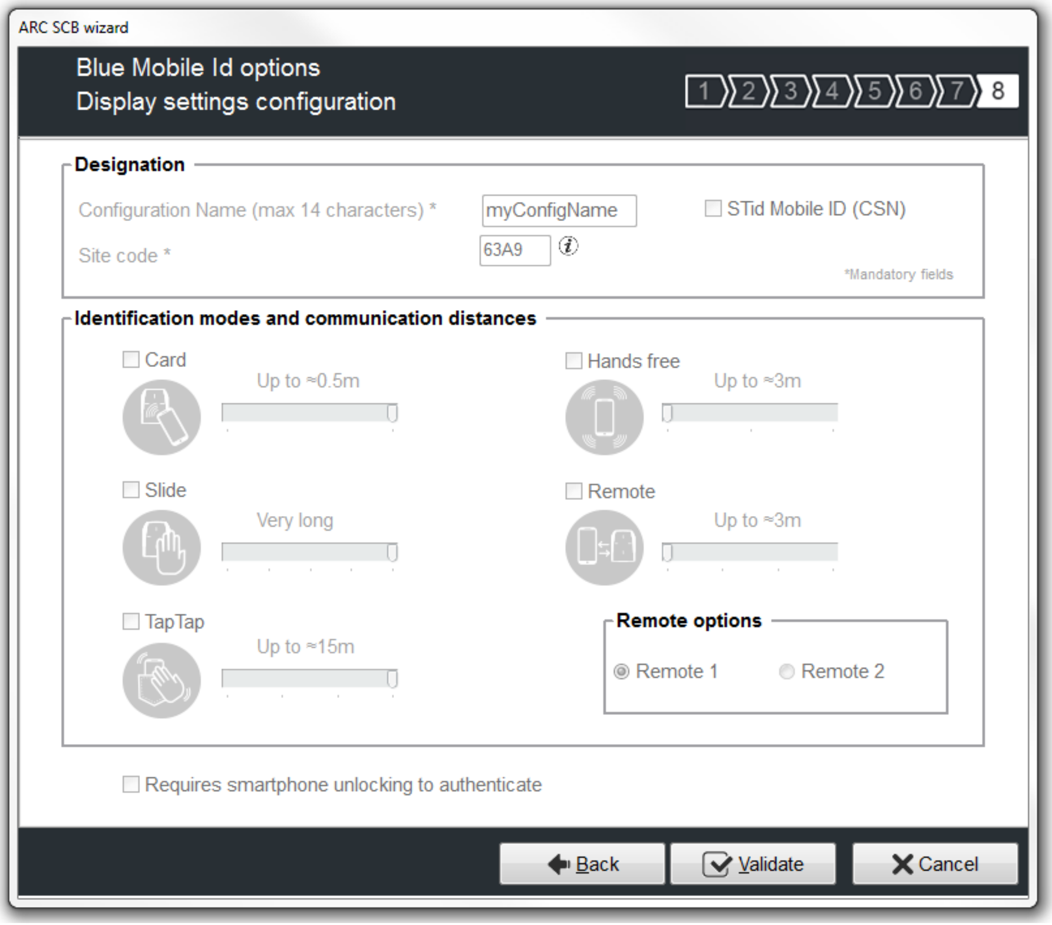
Image
(Only by serial link - No SCB)

Display images ☑ □ □ ☑ □ □ □

Port: COM1

Baudrate: 38400

Loading your images into the reader


ARC SCB wizard

Blue Mobile Id options
Display settings configuration

Designation

Configuration Name (max 14 characters) *: myConfigName

□ STid Mobile ID (CSN)

Site code *: 63A9

*Mandatory fields

Identification modes and communication distances

□ Card — Up to ≈0.5m

□ Hands free — Up to ≈3m

□ Slide — Very long

□ Remote — Up to ≈3m

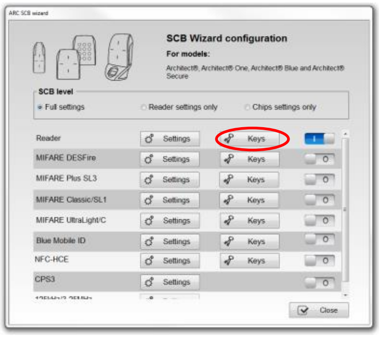
□ TapTap — Up to ≈15m

Remote options

● Remote 1 ○ Remote 2

□ Requires smartphone unlocking to authenticate

IV-4. Reader: Keys



ARC SCB wizard

SCB Wizard configuration

For models:

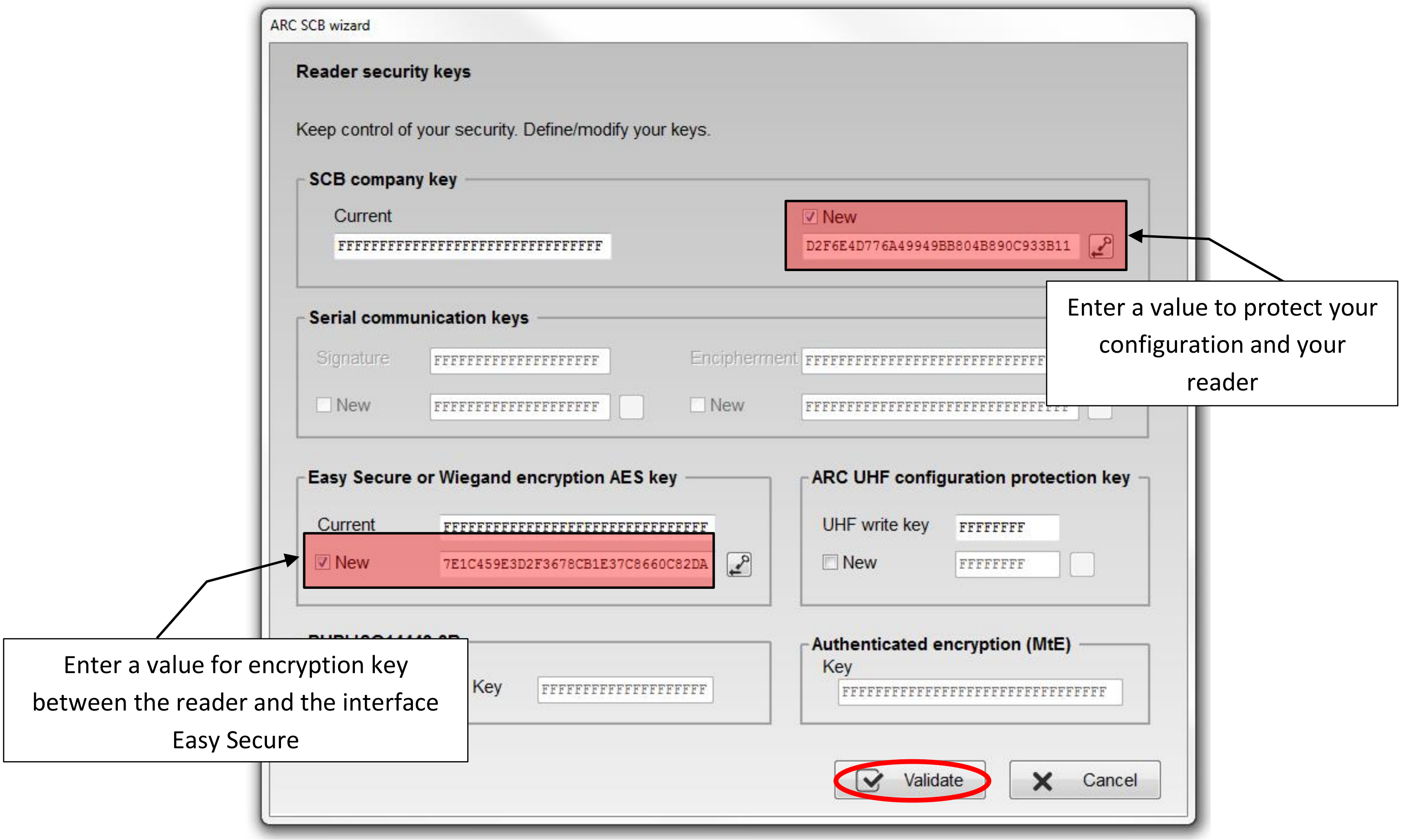
Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	O
NFC-HCE	Settings	Keys	O
CPS3	Settings		O

Close



ARC SCB wizard

Reader security keys

Keep control of your security. Define/modify your keys.

SCB company key

Current: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

☑ New: D2F6E4D776A49949BB804B890C933B11

Serial communication keys

Signature: FFFFFFFFFFFFFFFFFFF

□ New: FFFFFFFFFFFFFFFFFFF

Encipherment: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

□ New: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Easy Secure or Wiegand encryption AES key

Current: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

☑ New: 7E1C459E3D2F3678CB1E37C8660C82DA

ARC UHF configuration protection key

UHF write key: FFFFFFFF

□ New: FFFFFFFF

Key: FFFFFFFFFFFFFFFFFFFF

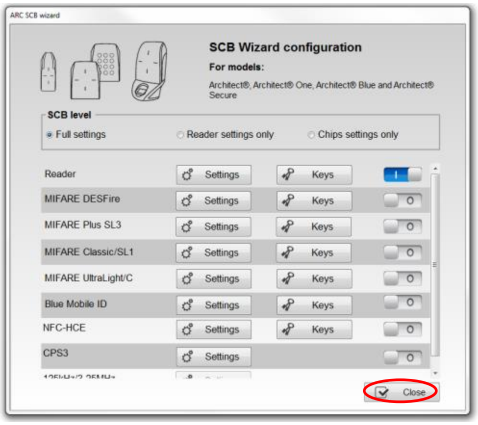
Authenticated encryption (MtE)

Key: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Validate   Cancel

Enter a value to protect your configuration and your reader

Enter a value for encryption key between the reader and the interface Easy Secure



ARC SCB wizard

SCB Wizard configuration

For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

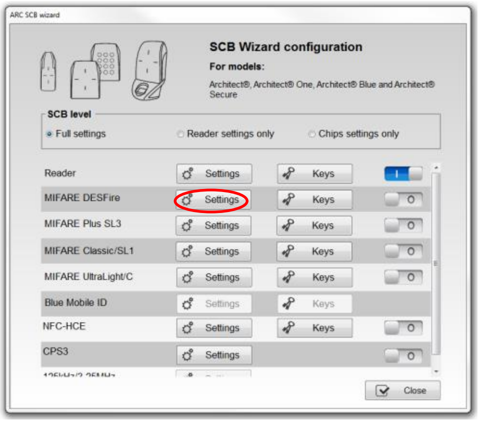
Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	O
NFC-HCE	Settings	Keys	O
CPS3	Settings		O

Close

The configuration of the settings and keys reader is complete. You can use the typical sample configuration below to configure chip. You can used example for DESFire® *V- DESFire® EV1 configuration*.

V. DESFire® EV1 configuration

This configuration is an example; the settings are the most currently used for access control.



ARC SCB wizard

SCB Wizard configuration

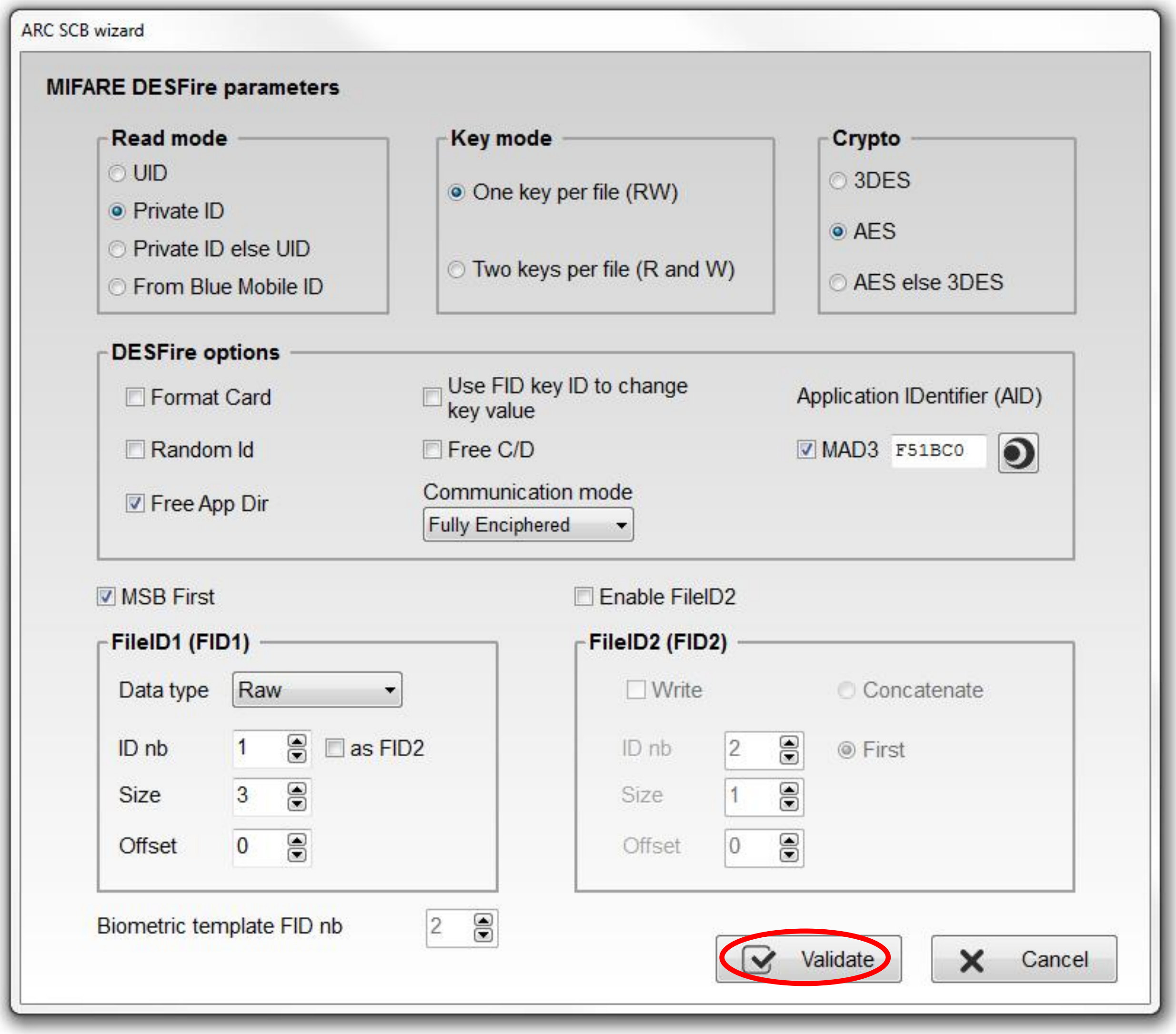
For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	O
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	
NFC-HCE	Settings	Keys	O
CPS3	Settings		O



ARC SCB wizard

MIFARE DESFire parameters

Read mode
- ○ UID
- ● Private ID
- ○ Private ID else UID
- ○ From Blue Mobile ID

Key mode
- ● One key per file (RW)
- ○ Two keys per file (R and W)

Crypto
- ○ 3DES
- ● AES
- ○ AES else 3DES

DESFire options
- □ Format Card
- □ Random Id
- ☑ Free App Dir
- □ Use FID key ID to change key value
- □ Free C/D
- Communication mode: Fully Enciphered
- Application IDentifier (AID): ☑ MAD3 F51BC0

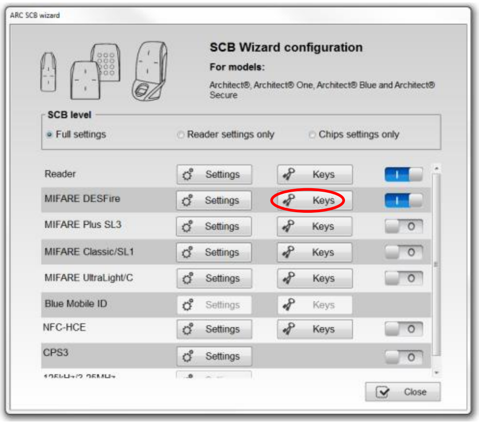
☑ MSB First

□ Enable FileID2

FileID1 (FID1)
- Data type: Raw
- ID nb: 1 □ as FID2
- Size: 3
- Offset: 0

FileID2 (FID2)
- □ Write ○ Concatenate
- ID nb: 2 ● First
- Size: 1
- Offset: 0

Biometric template FID nb: 2



ARC SCB wizard

SCB Wizard configuration

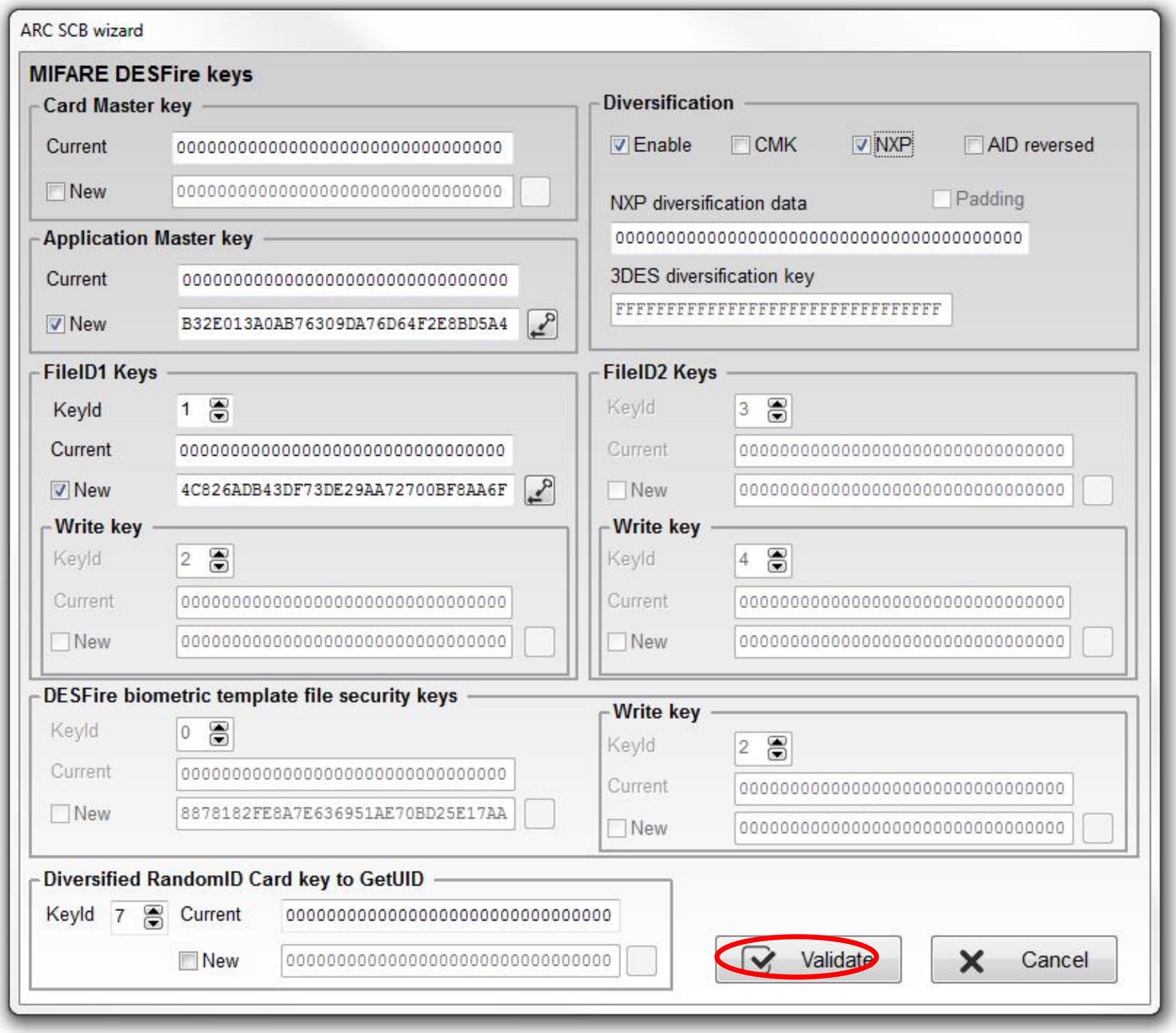
For models:

Architect®, Architect® One, Architect® Blue and Architect® Secure

SCB level

● Full settings ○ Reader settings only ○ Chips settings only

Reader	Settings	Keys	I
MIFARE DESFire	Settings	Keys	I
MIFARE Plus SL3	Settings	Keys	O
MIFARE Classic/SL1	Settings	Keys	O
MIFARE UltraLight/C	Settings	Keys	O
Blue Mobile ID	Settings	Keys	
NFC-HCE	Settings	Keys	O
CPS3	Settings		O
125kHz/3.25MHz			



ARC SCB wizard

MIFARE DESFire keys

Card Master key

Current 00000000000000000000000000000000

□ New 00000000000000000000000000000000

Application Master key

Current 00000000000000000000000000000000

☑ New B32E013A0AB76309DA76D64F2E8BD5A4

FileID1 Keys

KeyId 1

Current 00000000000000000000000000000000

☑ New 4C826ADB43DF73DE29AA72700BF8AA6F

Write key

KeyId 2

Current 00000000000000000000000000000000

□ New 00000000000000000000000000000000

DESFire biometric template file security keys

KeyId 0

Current 00000000000000000000000000000000

□ New 8878182FE8A7E636951AE70BD25E17AA

Diversified RandomID Card key to GetUID

KeyId 7 Current 00000000000000000000000000000000

□ New 00000000000000000000000000000000

Diversification

☑ Enable □ CMK ☑ NXP □ AID reversed

NXP diversification data □ Padding

0000000000000000000000000000000000000000

3DES diversification key

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

FileID2 Keys

KeyId 3

Current 00000000000000000000000000000000

□ New 00000000000000000000000000000000

Write key

KeyId 4

Current 00000000000000000000000000000000

□ New 00000000000000000000000000000000

Write key

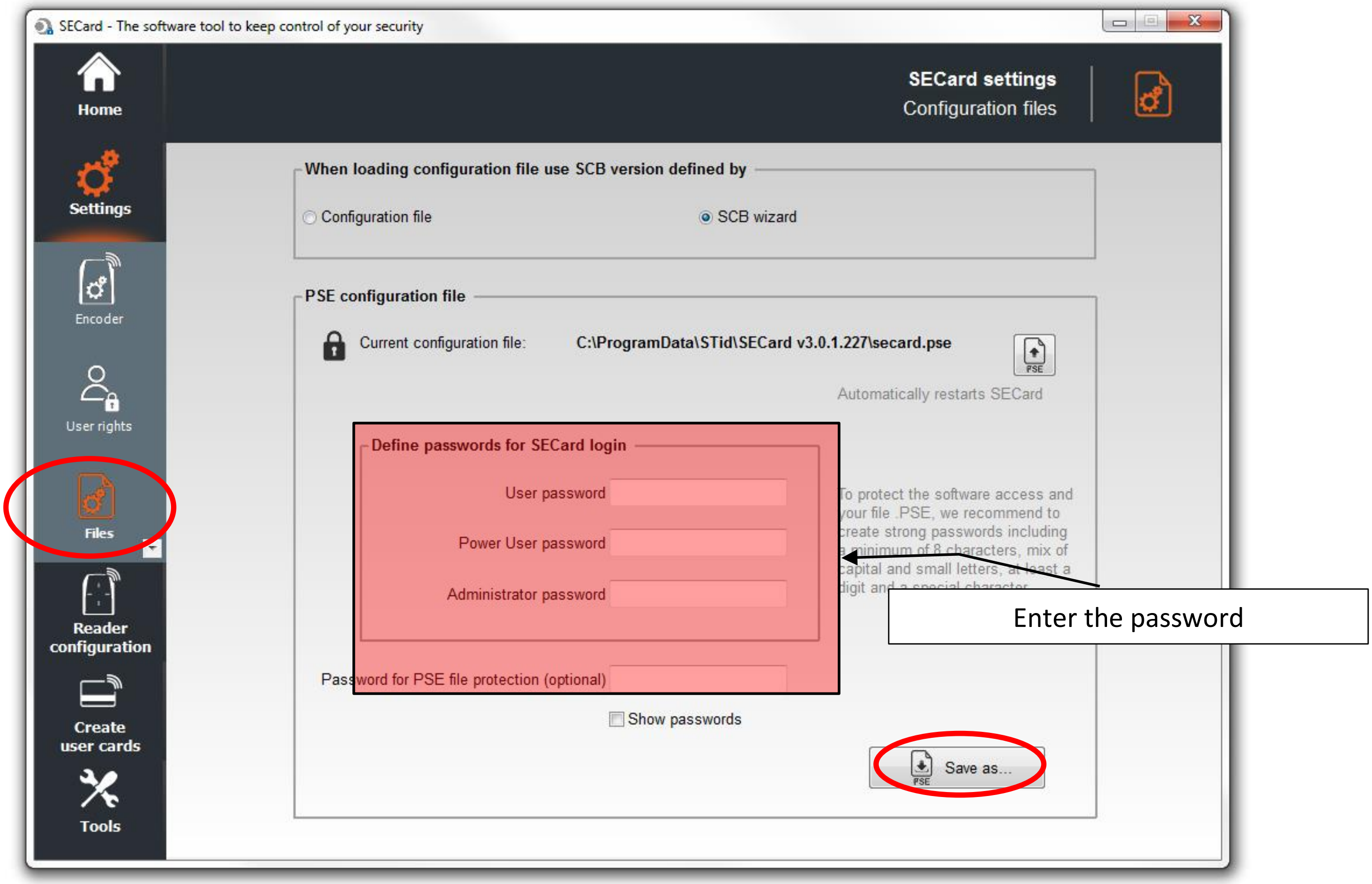
KeyId 2

Current 00000000000000000000000000000000

□ New 00000000000000000000000000000000

Note: Diversification is recommended but not required.

VI. Save the configuration file



SECard - The software tool to keep control of your security

SECard settings
Configuration files

When loading configuration file use SCB version defined by

○ Configuration file ● SCB wizard

PSE configuration file

Current configuration file: **C:\ProgramData\STid\SECard v3.0.1.227\secard.pse**

Automatically restarts SECard

Define passwords for SECard login

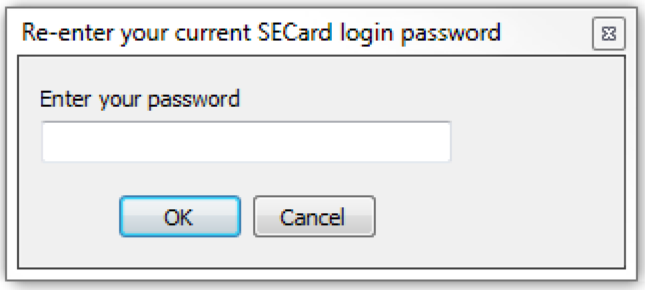
User password
Power User password
Administrator password

To protect the software access and your file .PSE, we recommend to create strong passwords including a minimum of 8 characters, mix of capital and small letters, at least a digit and a special character.

Password for PSE file protection (optional)

□ Show passwords

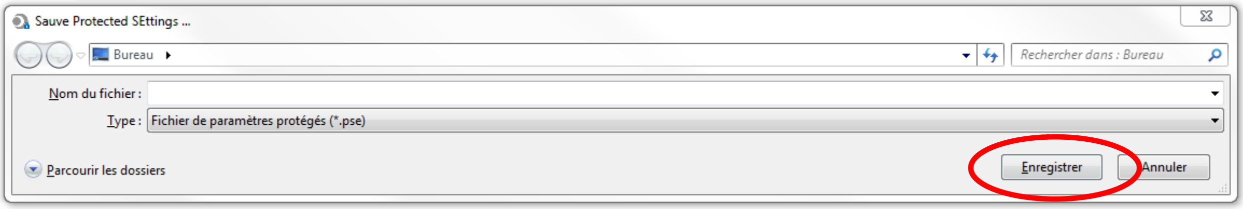
Enter the password



Re-enter your current SECard login password

Enter your password

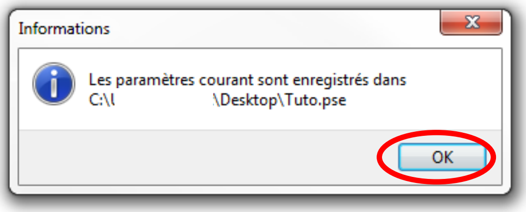
Enter the current session Administrator password (default is STidA)



Sauve Protected SEttings ...

Nom du fichier :

Type : Fichier de paramètres protégés (*.pse)

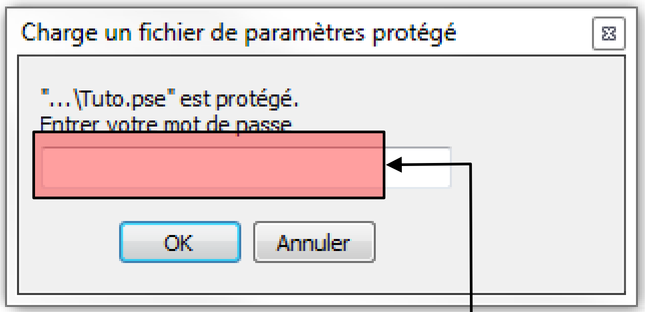


Informations

Les paramètres courant sont enregistrés dans
C:\ \Desktop\Tuto.pse

VII. Load a configuration file

If your SECard opens on this window:

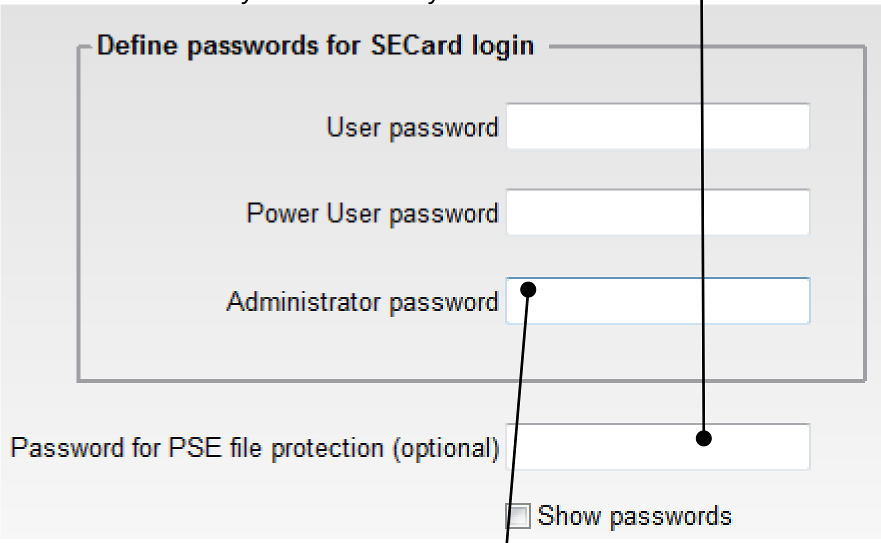


Charge un fichier de paramètres protégé

"...\Tuto.pse" est protégé.
Entrer votre mot de passe

1- Tuto.pse is the file you want to use:

Enter the Password you used when you save the file.



Define passwords for SECard login

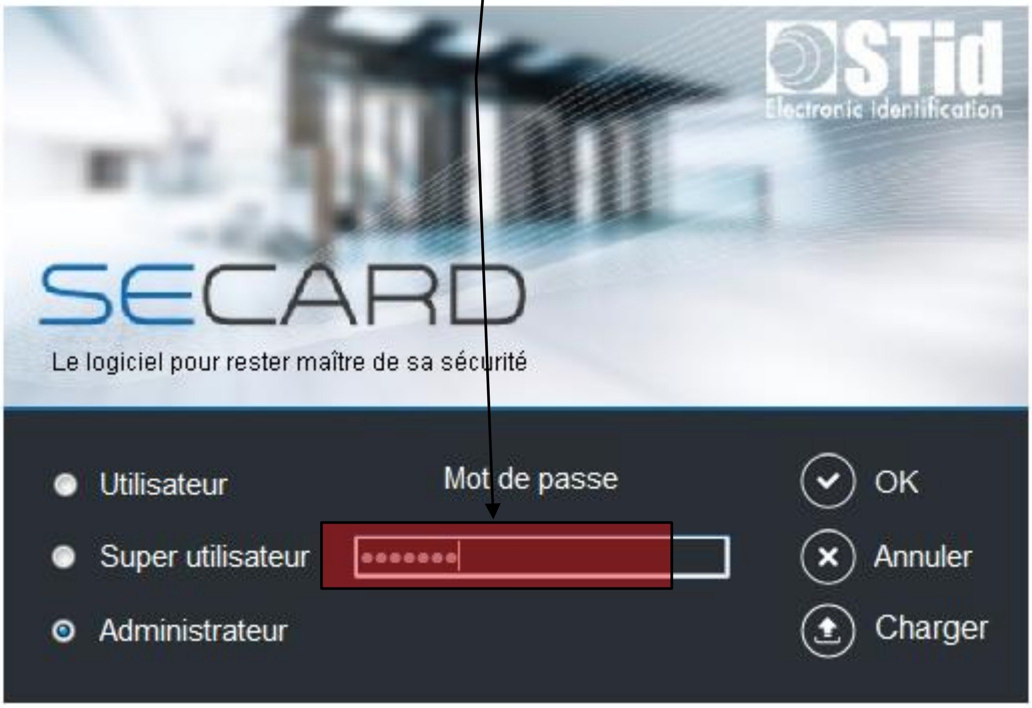
User password

Power User password

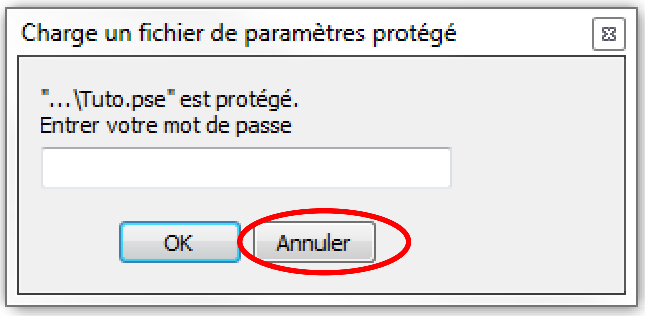
Administrator password

Password for PSE file protection (optional)

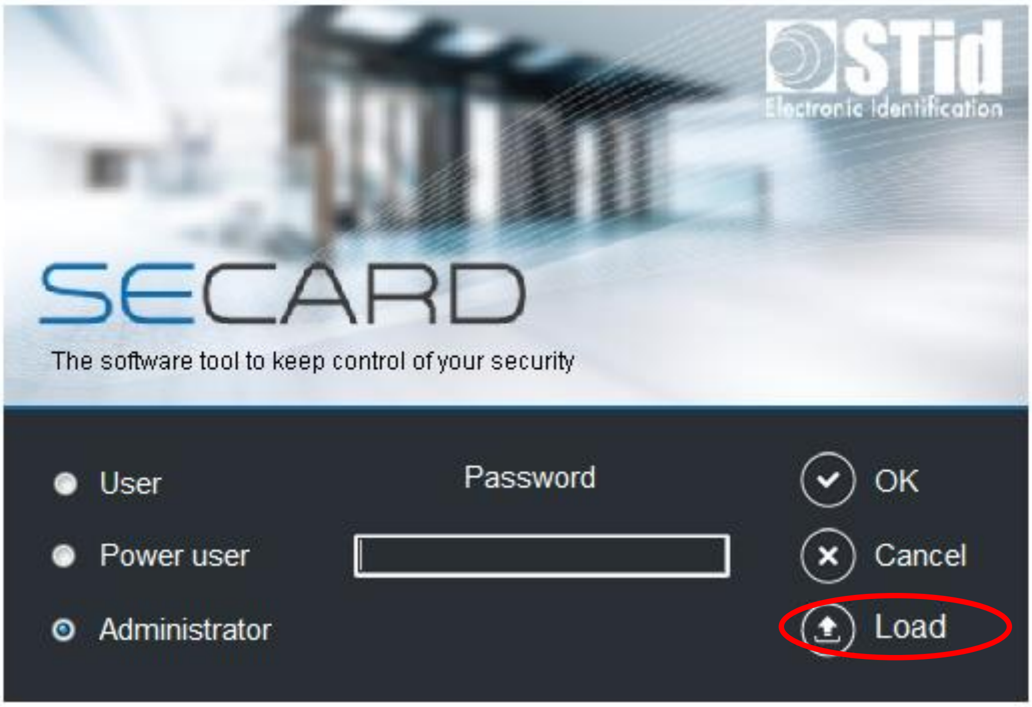
□ Show passwords



2- You want to open another file (for example, the default configuration file)


Charge un fichier de paramètres protégé

"...\Tuto.pse" est protégé.
Entrer votre mot de passe


STid
Electronic Identification
SECARD
The software tool to keep control of your security
User
Power user
Administrator
Password
OK
Cancel
Load

a- If you select Everyone during the setup: the default configuration file is located in: C:\ProgramData\STid\SECard v3.0.x

b- If you select Just me during the setup: the default configuration file is located in: C:\Users\usersXX\STid\SECard v3.0.x