



# NXP SAM AV2 Configuration Tool

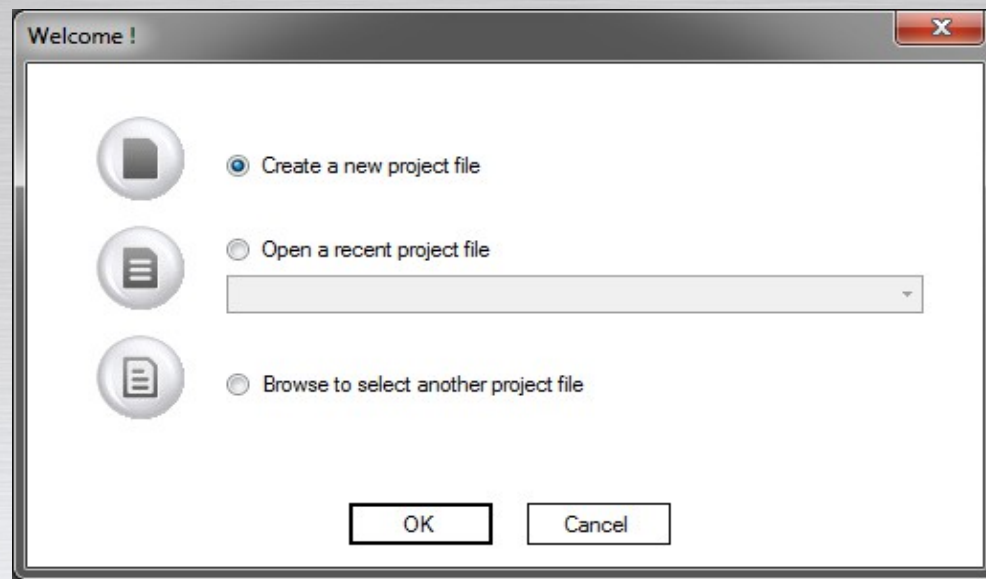
# Installation

Default directories :

- ✓ C:\Program Files\SpringCard\SAM\_AV2\_Tool\
  - contains the software : “Configuration\_SAM\_NXP\_AV2.exe”
- ✓ {user\_data}\Roaming\SpringCard\Configuration\_SAM\_NXP\_AV2\
  - contains the configuration file: “Configuration\_SAM\_NXP\_AV2.ini” (remembers directories and keys)
  - \Data: should contain all the project files created with the software
  - \Log: log files created by the software
  - It is strongly recommended to cypher the whole directory once keys are written in the SAMs, to keep them safe.

# The Welcome Form

- ✓ A quick note on project files :
  - A project file contains all the keys that will be written to a SAM (including the SAM Master Key)
  - Each type of SAM (reading SAM / writing SAM) needs a different project file
  - But the same project file can be downloaded to several SAMs.
- ✓ The first time, choose “Create a new project file”, then “OK”





Click on a Key Entry  
to expand

Scroll up  
or down

# A view on Key Entry details

SpringCard NXP SAM Tool - (New file)

File SAM Help

**SpringCard NXP SAM Tool**

00

	Vers	Value	Rand	Write to SAM	Random for every SAM				
Pos A	00	00000000000000000000000000000000	<input type="checkbox"/>	Key Type 3DES/CRC16	Key Number to Change Entry 00	DESFire Key n° 00	Diversification mandatory <input type="checkbox"/>	Keep IV <input type="checkbox"/>	
Pos B	00	00000000000000000000000000000000	<input type="checkbox"/>	Key Class Host Key	Key Vers to Change Entry 00	Host Auth. Key <input type="checkbox"/>	Disable Key Entry <input type="checkbox"/>	Disable Encipher Data <input type="checkbox"/>	
Pos C	00	00000000000000000000000000000000	<input type="checkbox"/>	DESFire Appl. ID 000000	Key Usage Counter 00	Dump Session Key <input type="checkbox"/>	SAM Lock <input type="checkbox"/>	Disable Writing to PICC <input type="checkbox"/>	

01

	Vers	Value	Rand	Write to SAM	Random for every SAM				
Pos A	00	00000000000000000000000000000000	<input type="checkbox"/>	Key Type 3DES/CRC16	Key Number to Change Entry 00	DESFire Key n° 00	Diversification mandatory <input type="checkbox"/>	Keep IV <input type="checkbox"/>	
Pos B	00	00000000000000000000000000000000	<input type="checkbox"/>	Key Class Host Key	Key Vers to Change Entry 00	Host Auth. Key <input type="checkbox"/>	Disable Key Entry <input type="checkbox"/>	Disable Encipher Data <input type="checkbox"/>	
Pos C	00	00000000000000000000000000000000	<input type="checkbox"/>	DESFire Appl. ID 000000	Key Usage Counter 00	Dump Session Key <input type="checkbox"/>	SAM Lock <input type="checkbox"/>	Disable Writing to PICC <input type="checkbox"/>	

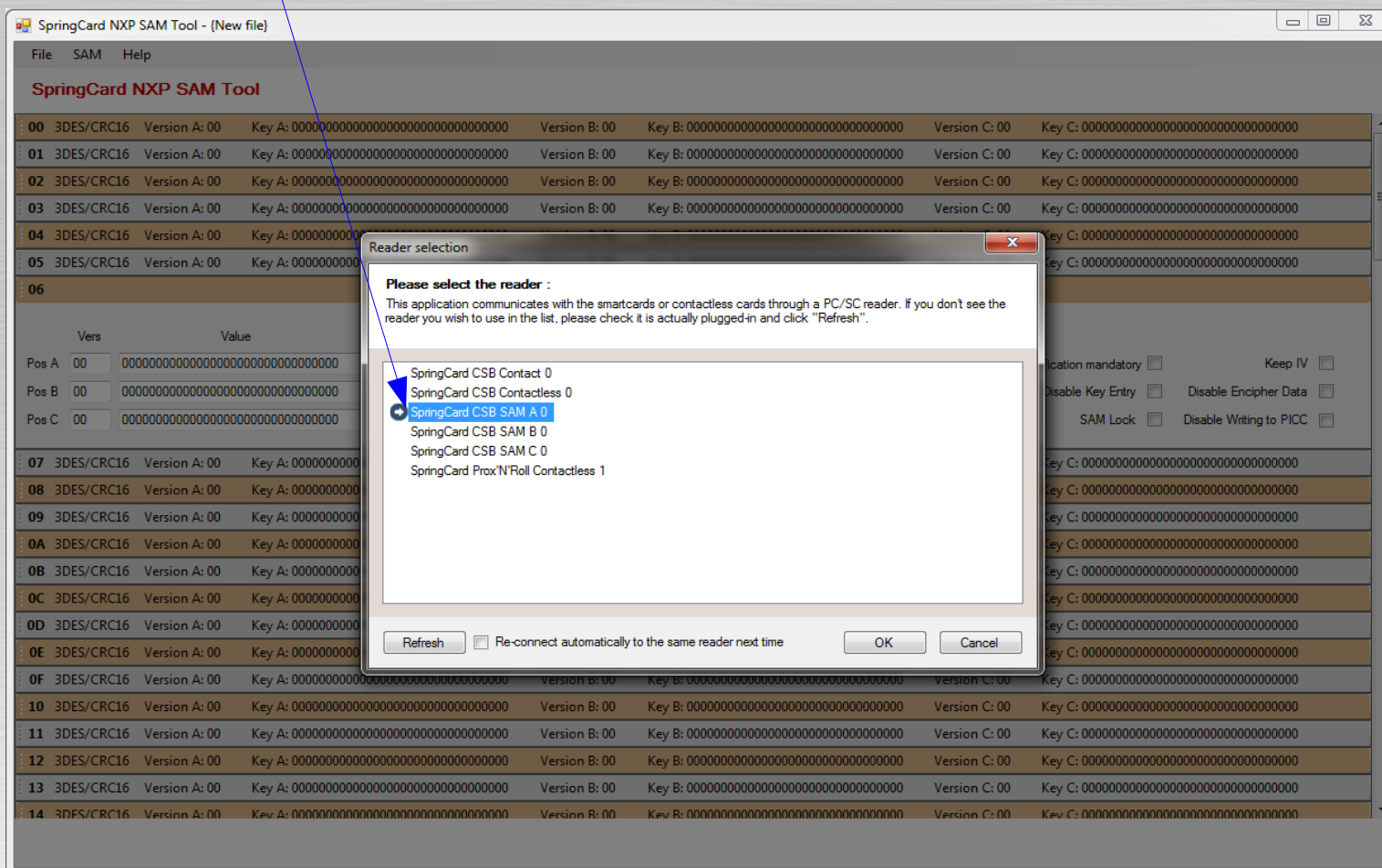
02

	Vers	Value	Rand	Write to SAM	Random for every SAM				
Pos A	00	00000000000000000000000000000000	<input type="checkbox"/>	Key Type 3DES/CRC16	Key Number to Change Entry 00	DESFire Key n° 00	Diversification mandatory <input type="checkbox"/>	Keep IV <input type="checkbox"/>	
Pos B	00	00000000000000000000000000000000	<input type="checkbox"/>	Key Class Host Key	Key Vers to Change Entry 00	Host Auth. Key <input type="checkbox"/>	Disable Key Entry <input type="checkbox"/>	Disable Encipher Data <input type="checkbox"/>	
Pos C	00	00000000000000000000000000000000	<input type="checkbox"/>	DESFire Appl. ID 000000	Key Usage Counter 00	Dump Session Key <input type="checkbox"/>	SAM Lock <input type="checkbox"/>	Disable Writing to PICC <input type="checkbox"/>	

03	3DES/CRC16	Version A: 00	Key A: 00000000000000000000000000000000	Version B: 00	Key B: 00000000000000000000000000000000	Version C: 00	Key C: 00000000000000000000000000000000
04	3DES/CRC16	Version A: 00	Key A: 00000000000000000000000000000000	Version B: 00	Key B: 00000000000000000000000000000000	Version C: 00	Key C: 00000000000000000000000000000000
05	3DES/CRC16	Version A: 00	Key A: 00000000000000000000000000000000	Version B: 00	Key B: 00000000000000000000000000000000	Version C: 00	Key C: 00000000000000000000000000000000
06	3DES/CRC16	Version A: 00	Key A: 00000000000000000000000000000000	Version B: 00	Key B: 00000000000000000000000000000000	Version C: 00	Key C: 00000000000000000000000000000000
07	3DES/CRC16	Version A: 00	Key A: 00000000000000000000000000000000	Version B: 00	Key B: 00000000000000000000000000000000	Version C: 00	Key C: 00000000000000000000000000000000
08	3DES/CRC16	Version A: 00	Key A: 00000000000000000000000000000000	Version B: 00	Key B: 00000000000000000000000000000000	Version C: 00	Key C: 00000000000000000000000000000000
09	3DES/CRC16	Version A: 00	Key A: 00000000000000000000000000000000	Version B: 00	Key B: 00000000000000000000000000000000	Version C: 00	Key C: 00000000000000000000000000000000

# Choosing the PC/SC Reader

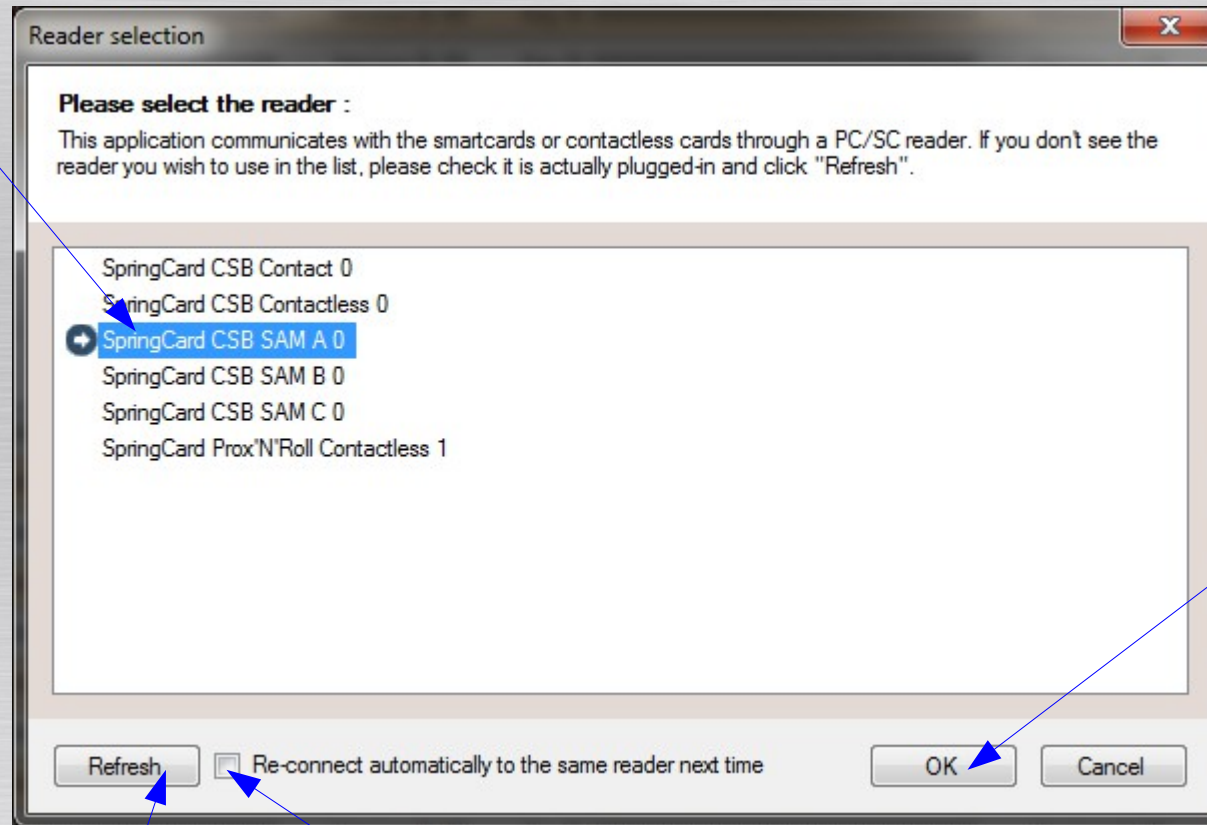
The Reader selection Form appears the first time you try to communicate with a SAM (click on “Rand” on a Key Entry, get SAM information, write to the SAM, etc ...)





# Reader Selection Form

Select the reader containing the SAM



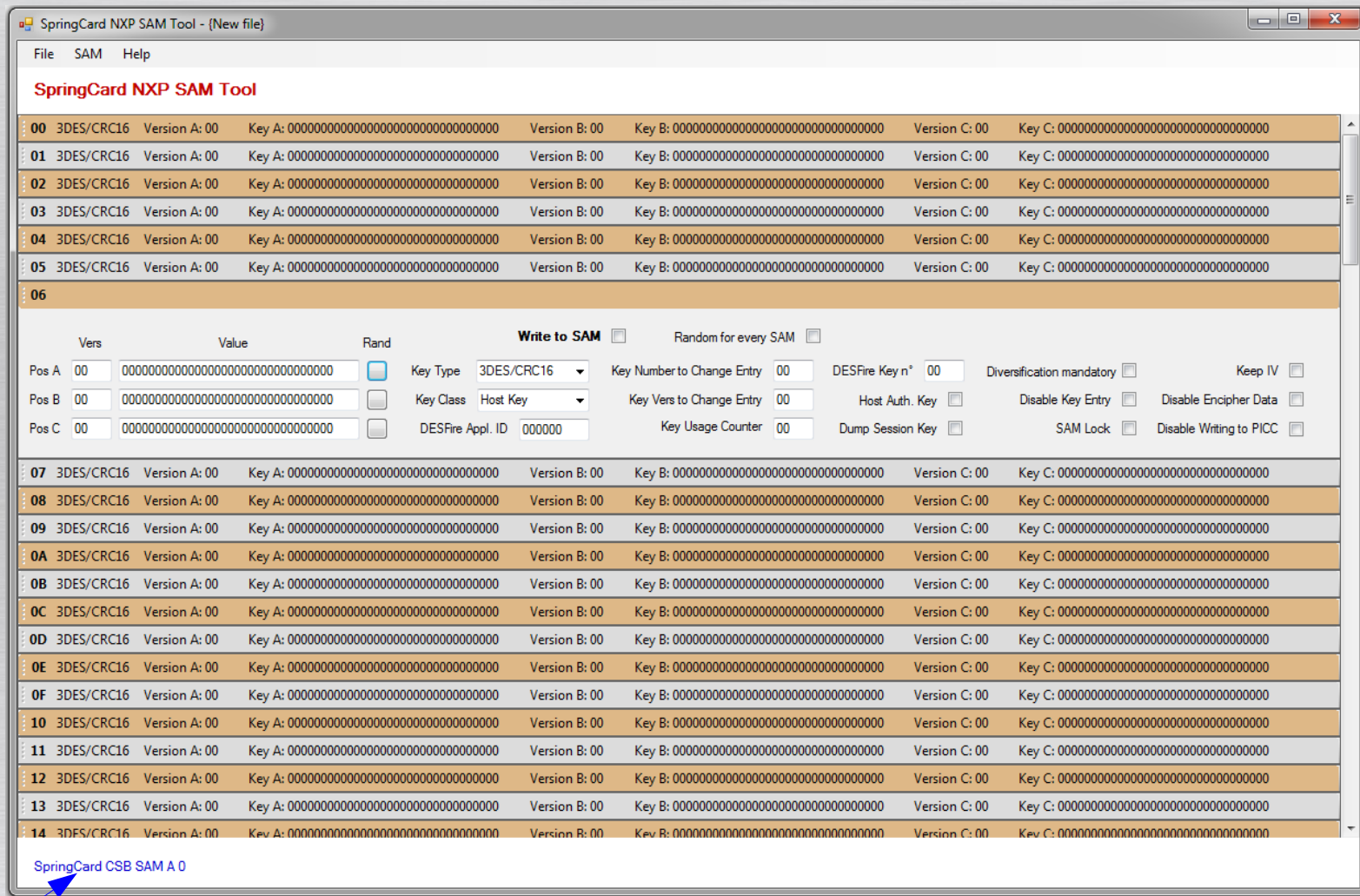
The screenshot shows a 'Reader selection' dialog box. At the top, it says 'Please select the reader :'. Below this is an instruction: 'This application communicates with the smartcards or contactless cards through a PC/SC reader. If you don't see the reader you wish to use in the list, please check it is actually plugged-in and click "Refresh".' A list of readers is shown: 'SpringCard CSB Contact 0', 'SpringCard CSB Contactless 0', 'SpringCard CSB SAM A 0' (which is highlighted with a blue selection bar and a small circular icon to its left), 'SpringCard CSB SAM B 0', 'SpringCard CSB SAM C 0', and 'SpringCard Prox'N'Roll Contactless 1'. At the bottom, there are three buttons: 'Refresh', 'OK', and 'Cancel'. There is also a checkbox labeled 'Re-connect automatically to the same reader next time' which is currently unchecked. Blue arrows point from external text labels to the 'Refresh' button, the 'SpringCard CSB SAM A 0' entry, the 'Re-connect automatically...' checkbox, and the 'OK' button.

Click "OK" when finished

Click on Refresh to list all the PC/SC readers again

Check to automatically use this PC/SC reader every time you use the software

# Switching to another reader



Click on the name of the selected  
PC/SC reader to change it



# Three different values per Key Entry

Each value must have a specific version

	Vers	Value	Rand	Key Type	Key Class	DESFire Appl. ID	Key Number to Change Entry	Key Vers to Change Entry	Key Usage Counter	DESFire Key n°	Host Auth. Key	Diversification mandatory	Keep IV	Disable Key Entry	Disable Encipher Data	SAM Lock	Disable Writing to PICC
Pos A	00	60CA85F103B1B12DFB9AAEF1788D030D		AES	Offline Crypto Ke	000000	00	00	00	00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Pos B	01	696FA9B797F82B6CC73D9DB5B530CA76									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Pos C	02	5F7B95834D2945F1DCB6DBB506407DC6									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Click here to get random numbers from the SAM (it must be inserted in a reader before), in order to generate random keys

# Global Configuration (1/3)

- ✓ Key Entry 0:
  - It should be the main key, with which authentication is mandatory, to modify the values of all the other keys
  - “Key Type” should be “AES”
  - “Key Class” should be “Host Key”
  - “Sam Lock” should be checked to ensure authentication after each reset

# Global Configuration (2/3)

- ✓ Key Entry 1:
  - Best practice: use it as the “lock/unlock” key, to access the keys in the SAM, without modifying them
  - “SAM Lock” should be checked
  - “Key Type” should be “AES”
  - “Key Class” should be “Host Key”



# Global Configuration (3/3)

## ✓ Other Keys :

- can be Mifare, AES, or 3DES keys
- can be offline crypto keys or PICC keys
- can be used to secure the content of a card (example: AES-PICC key for Mifare Plus SL3 or DESFire)
- can be used to perform offline cryptographic operations (example: make the SAM decipher data read on a card)

# Key Entry Options (1/8)

- ✓ Write to SAM
  - Must be checked if the Key has to be written to the SAM
  
- ✓ Random for every SAM
  - If checked, the key values will be different for every SAM (read the log files to know the keys) – NOT RECOMMENDED

# Key Entry Options (2/8)

## ✓ Key Type

- 3DES/CRC16 – recommended for Mifare Classic and Mifare Plus SL1 diversification keys
- 3DES/CRC32
- AES – recommended for SAM Keys, PICC Keys (DESFire, Mifare Ultralight C, Mifare Plus SL3) and Offline Crypto Keys
- Mifare Key – for Mifare Classic and Mifare PLUS SL1 sectors
- TDEA ISO 10116



# Key Entry Options (3/8)

## ✓ Key Class

- Host Key: used for Host authentication
- PICC Key: used with Mifare Cards
- Offline Change key: used for offline preparation of change key entry cryptogram
- Offline Crypto Key: used for general purpose cryptographic operations

## ✓ DESFire Appl. ID

- DESFire AID linked to this Key Entry
- Can be left to its default value (“000000”)

## ✓ DESFire Key n°

- Used to build a table of keys, linked to a DESFire AID
- Can be left to its default value (“00”)

# Key Entry Options (4/8)

- ✓ Key Number to Change Entry
  - Key entry number, with which the host must be authenticated, before changing this key value
  - We'll call it the “referenced” key entry
- ✓ Key Vers to Change Entry
  - Version of the key in the “referenced” key entry, with which the host must be authenticated, before changing this key value
- ✓ It is recommended to keep those values to “00”, so that by authenticating with the SAM Master Key (key entry 00 – version 00), all key entries can be changed
- ✓ If changes are made on those fields:
  - Changing this Key Entry will not be possible anymore with a prior authentication with the SAM Master Key
  - Prior authentication must be performed with the “referenced” key
  - “Host Auth. Key” must be checked on the “referenced” key entry

# Key Entry Options (5/8)

- ✓ Key Usage Counter
  - Reference number for a counter in the KUC table
  - Can be left to its default value (“00”)
  
- ✓ Host Auth. Key
  - For key entry 00: must not be checked
  - For another key entry: must be checked if authentication with this key entry is mandatory to change another key entry



# Key Entry Options (6/8)

- ✓ Dump Session Key
  - Must be checked if this key needs to be downloaded
  - Example: Download an AES PICC Key from the SAM and use it to personalize a Mifare Plus SL0 card
  
- ✓ Diversification mandatory
  - Must be checked if the key has to be diversified (only for PICC or Offline Crypto keys)

# Key Entry Options (7/8)

## ✓ Disable Key Entry

- Must not be checked if this key needs to be used
- There's no need to disable a key that won't be written in the SAM
- If a key is disabled, it can be re-enabled again

## ✓ SAM Lock

- For key entry 00: must be checked to ensure host authentication after each reset
- For other key entries: must be checked if this key is to be used to lock/unlock the SAM (best practice: use key entry 01 to lock/unlock the SAM)

# Key Entry Options (8/8)

## ✓ Keep IV

- Must be checked to avoid resetting the Initialization Vector at each cryptographic operation
- Check it only for DESFire cards (AES - PICC keys)

## ✓ Disable Encipher Data

- Must be checked to prevent enciphering data with this key
- Use this option only with Offline Crypto Keys, in SAMs that only need to read data from cards (and not write data to cards)

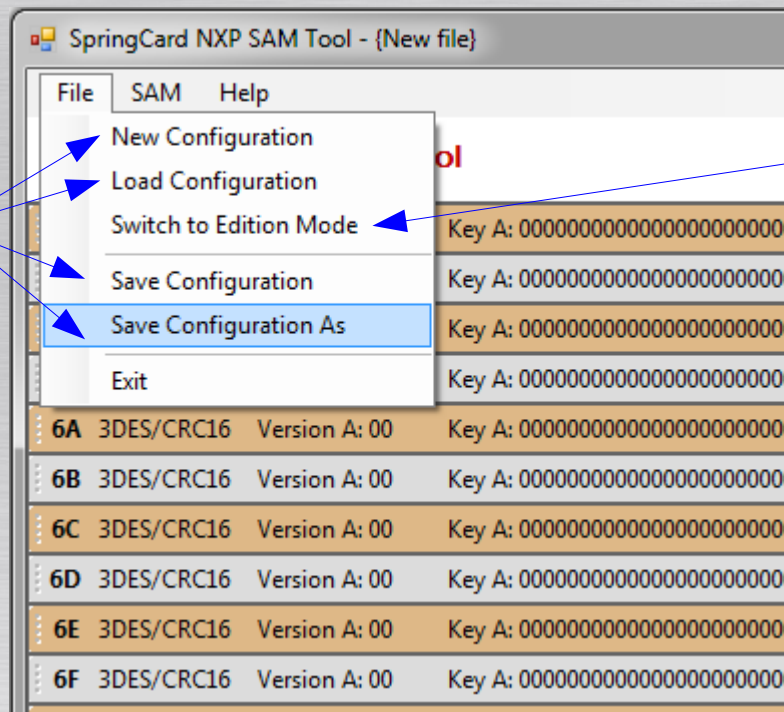
## ✓ Disable Writing to PICC

- Must be checked to prevent writing this Key to a PICC
- Use it only with DESFire AES reading keys, in SAMs that only need to read data (and not write data)



# Working with different project files (Configurations)

Use the “File” tab to save your project files, or open existing ones.



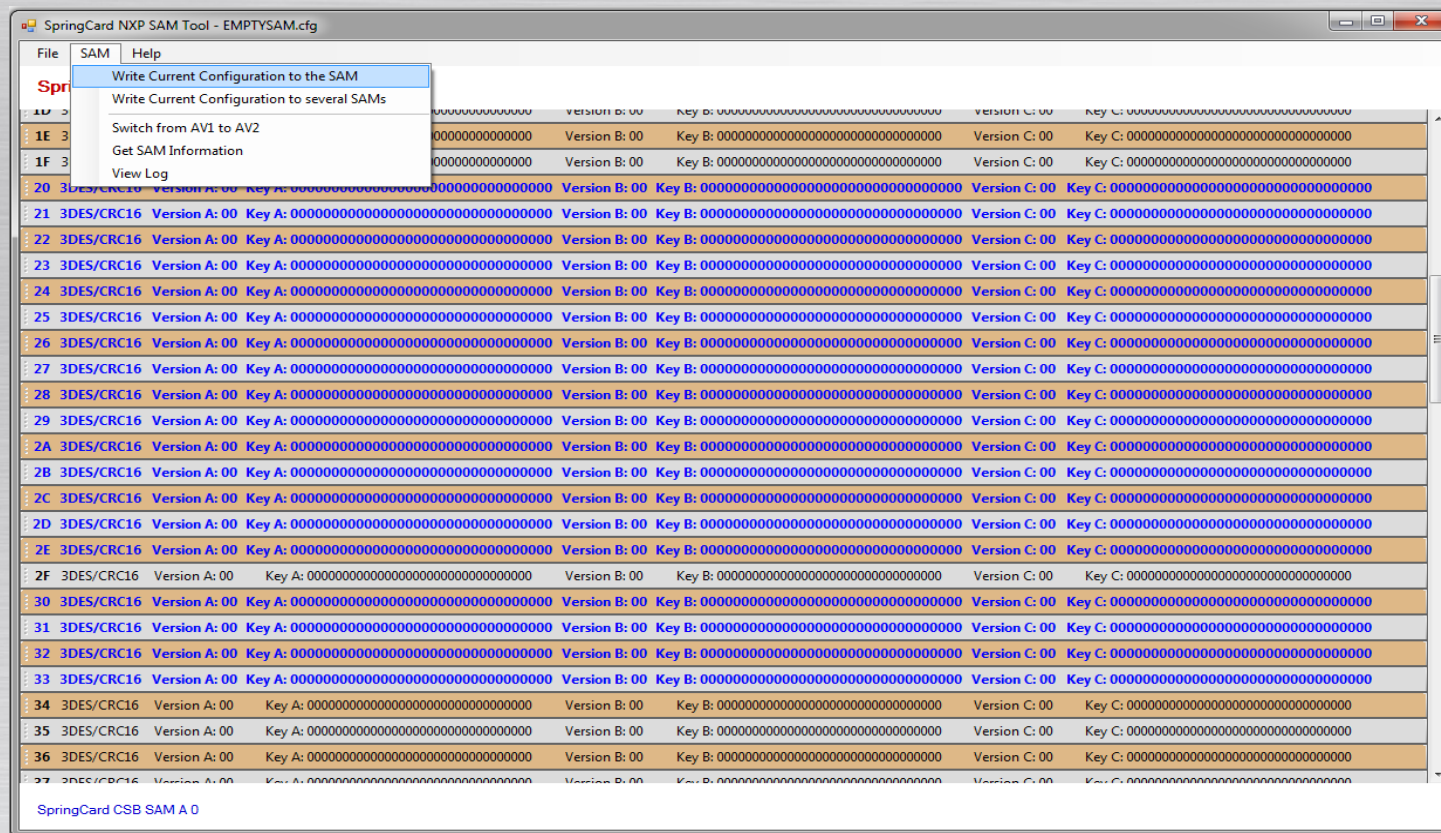
## Important note :

When opening an existing project file, click on “Switch to Edition Mode” to be able to modify it.

# Writing your keys to the SAM(s)

Choose the appropriate option (write to a SAM or several SAMs).

If the SAM is in AV1 mode, it will be switched to AV2



All keys in blue will then be written in the SAM (including the SAM Master Key, if selected)

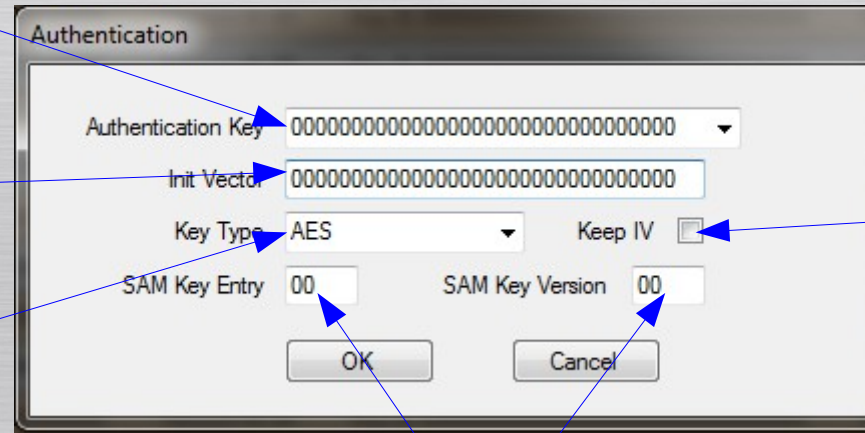


# Authenticating with Master Key before writing keys

Enter the value of the Key

Enter the Init Vector

Enter the Key Type



The screenshot shows a dialog box titled "Authentication". It contains the following fields and controls:

- Authentication Key:** A text field with a dropdown arrow, containing the value "00000000000000000000000000000000". An arrow points from the text "Enter the value of the Key" to this field.
- Init Vector:** A text field containing the value "00000000000000000000000000000000". An arrow points from the text "Enter the Init Vector" to this field.
- Key Type:** A dropdown menu currently set to "AES". An arrow points from the text "Enter the Key Type" to this dropdown.
- Keep IV:** A checkbox that is currently checked. An arrow points from the text "Check if IV must be kept" to this checkbox.
- SAM Key Entry:** A text field containing the value "00".
- SAM Key Version:** A text field containing the value "00".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

Two arrows originate from the "OK" and "Cancel" buttons and point towards the text "Enter SAM Key Entry and Version" located below the dialog box.

Check if IV must be kept

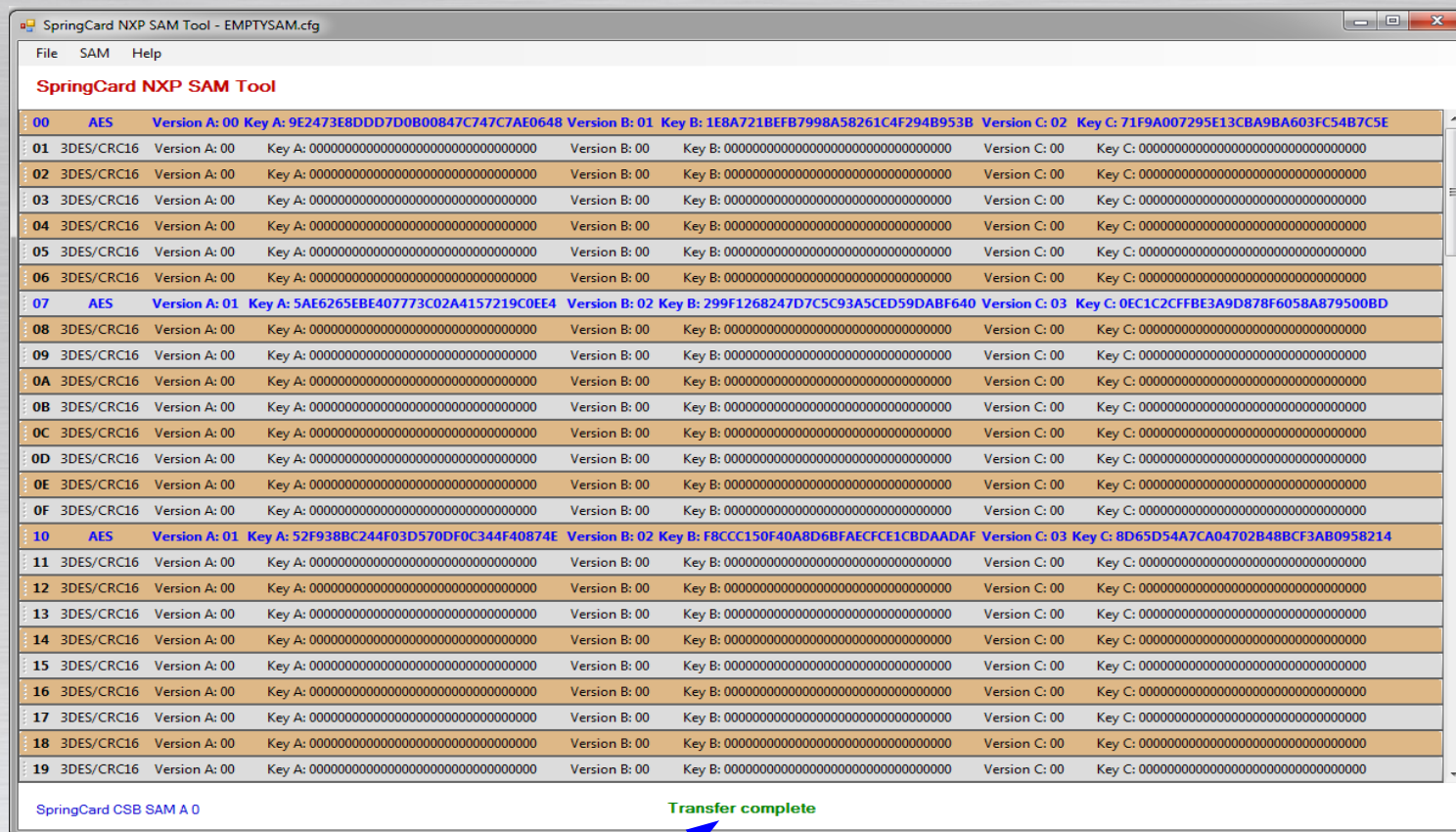
Enter SAM Key Entry and Version

- ✓ This form appears just before writing keys in a (or several) SAM(s).
- ✓ Enter the value of the SAM Master Key
  - Factory default is "00000000000000000000000000000000"
- ✓ There's no need to change the IV parameters (keep them as default)
- ✓ SAM Key Entry and SAM Key Version must match with the value which has been previously entered in the SAM



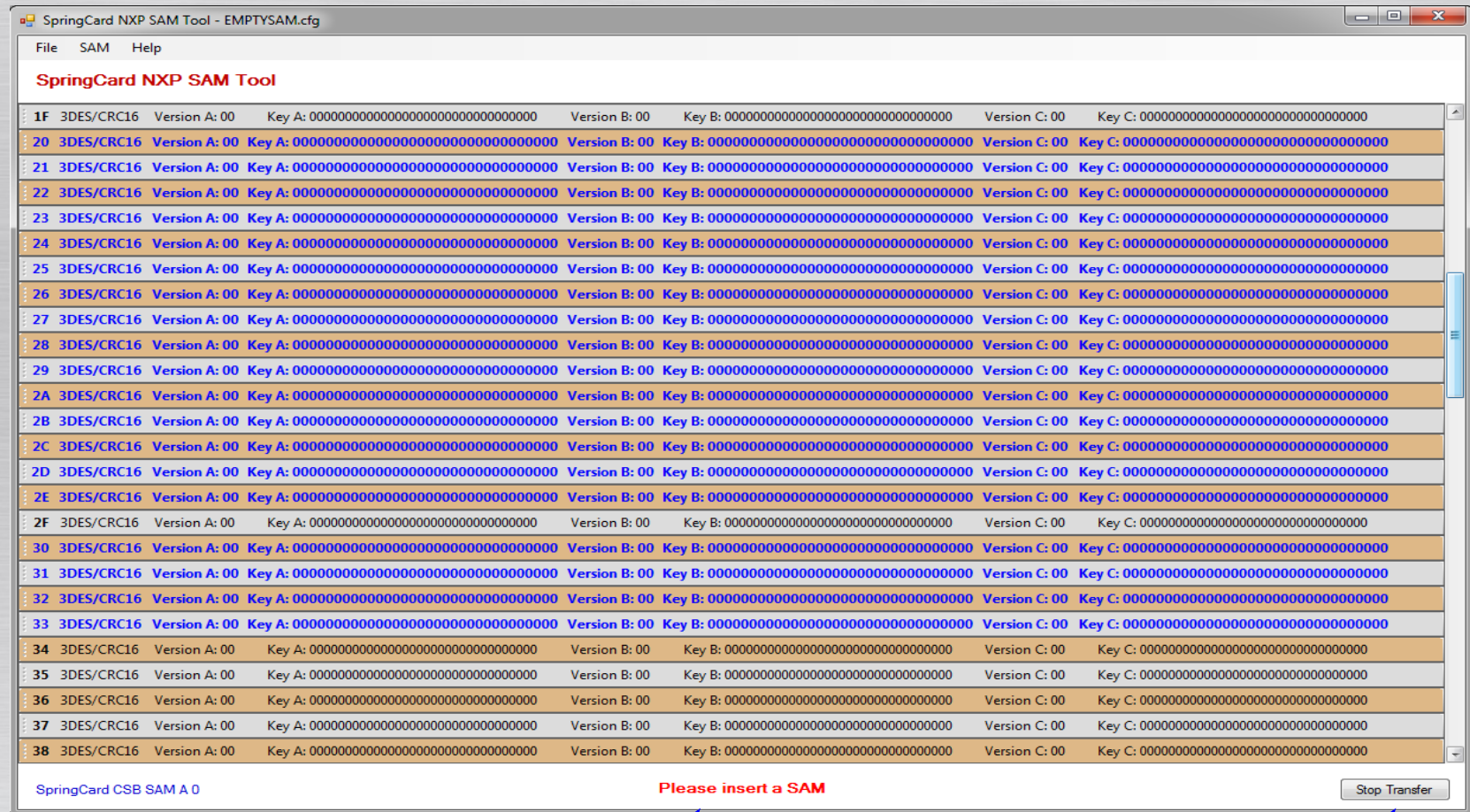
# At the end of the process

- ✓ All the “blue” keys (“Write To SAM” option checked) have been transferred
- ✓ On this example, the SAM Master Key has been changed (key entry 00)
  - => Next time, authenticate with this new key value



Click here to view the log

# When writing the keys to several SAMs



Follow the instructions

Click here to stop the transfer





[www.springcard.com](http://www.springcard.com)



#### DISCLAIMER

This document is provided for informational purposes only and shall not be construed as a commercial offer, a license, an advisory, fiduciary or professional relationship between Pro-Active and you. No information provided in this document shall be considered a substitute for your independent investigation.

The information provided in document may be related to products or services that are not available in your country.

This document is provided "as is" and without warranty of any kind to the extent allowed by the applicable law. While PRO ACTIVE will use reasonable efforts to provide reliable information, we don't warrant that this document is free of inaccuracies, errors and/or omissions, or that its content is appropriate for your particular use or up to date. PRO ACTIVE reserves the right to change the information at any time without notice.

PRO ACTIVE does not warrant any results derived from the use of the products described in this document. PRO ACTIVE will not be liable for any indirect, consequential or incidental damages, including but not limited to lost profits or revenues, business interruption, loss of data arising out of or in connection with the use, inability to use or reliance on any product (either hardware or software) described in this document.

These products are not designed for use in life support appliances, devices, or systems where malfunction of these product may result in personal injury. PRO ACTIVE customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify PRO ACTIVE for any damages resulting from such improper use or sale.

#### COPYRIGHT NOTICE

SPRINGCARD, the SPRINGCARD logo, PRO ACTIVE and the PRO ACTIVE logo are registered trademarks of PRO ACTIVE SAS.

All other trademarks are property of their respective owners.

Information in this document is subject to change without notice. Reproduction without written permission of PRO ACTIVE is forbidden.

All information in this document is either public information or is the intellectual property of PRO ACTIVE and/or its suppliers or partners.

You are free to view and print this document for your own use only. Those rights granted to you constitute a license and not a transfer of title : you may not remove this copyright notice nor the proprietary notices contained in this documents, and you are not allowed to publish or reproduce this document, either on the web or by any mean, without written permission of PRO ACTIVE.

Copyright © PRO ACTIVE SAS 2013, all rights reserved.

#### EDITOR'S INFORMATION

Published by **PRO ACTIVE SAS** company with a capital of 227 000 €

RCS EVRY B 429 665 482

NAF 722C

VAT# : FR 27 429 665 482