Smartjac Industries Inc. - Kanalvägen 1A
2nd floor
SE-194 61 Upplands Väsby
Sweden
www.smartjac.com / www.smartjac.biz

Phone: +46(8)41071230 - Email: order@smartjac.com

SMARTJAC SIM Editor

Brand: Smartjac Industries Inc
Product Code: SMA1000SWS

Short Description
SIM card administration by scripting methodology or instant read and write.
Create a range of advanced scripts with the help of an easy graphical user interface and execute them quickly one-by-one within the tool to change parameters, populate files and edit settings on SIM cards.
You can create 1000 scripts in a matter of seconds, and it only takes 3-4 seconds to select and execute the script on a SIM card!

- Browse files
- Filter content *****
- Read content
- Write content
- Generate dynamic scripts
- Faster execution of scripts *****
- Calculate OPc *****
- Generate Ki/Opc lists
- USIM and ISIM support
- PIN handling
- Insert dynamic values
- APDU logs
- Interpretations
- Scan non-default SIM cards
- Export scanned cards to new card profiles *****

New in v2.8x *

Description

SMARTJAC SIM Editor software tool addresses the SIM card administration by scripting methodology. Create advanced scripts with the help of an easy graphical user interface and execute them quickly one-by-one within the tool to change parameters, populate files and edit settings. One of the main advantages of this tool is that it's a tool optimized for content management of SIM cards very quickly, thanks to the ability to create a range of scripts (with a starting IMSI and an end IMSI). You can create 1000 scripts in a couple of seconds, and it only takes 5-10 seconds to select and execute the script on a SIM card!

Using SIM Editor:

SIM Editor provides a graphical interface for you to do the following:

- Browse a specific card type's file system using the File Content table
- Filter the content of the File table
- Display the default content of data files in either an easy-to-read or in binary representation.
- Get file specific help and documentation
- Read and write new file content directly to the SIM card
- Checking of SIM card in card reader
- Import Ki/Opc lists
- Include AUTH keys in both USIM and ISIM in scripts
- Disable GPIN

- Prepare scripts by adding edited files to a script list
- Creation of unlimited scripts with dynamic / incremental values in:

- IMSI

- MSISDN

- SPN

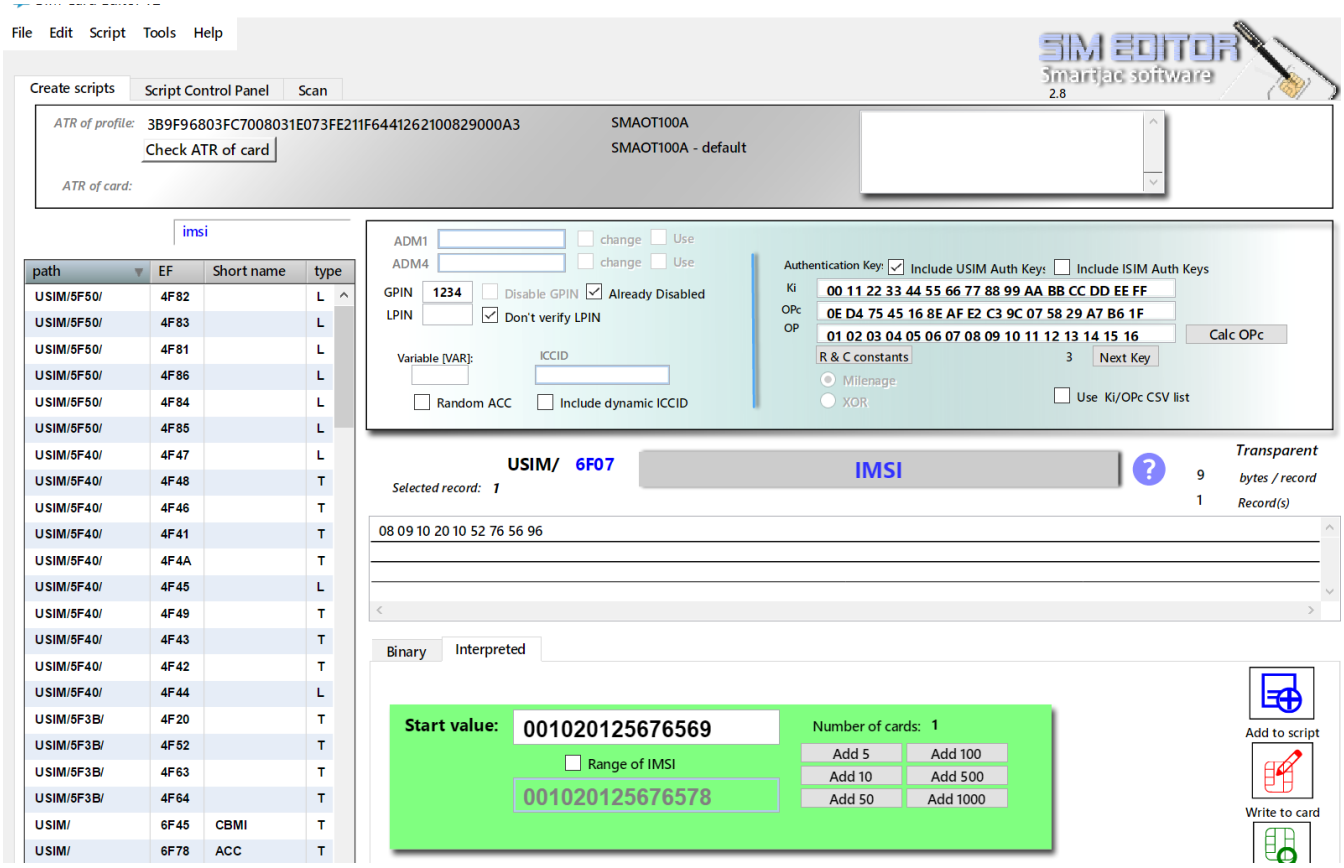
- ICCID

- ACC

- IMPU

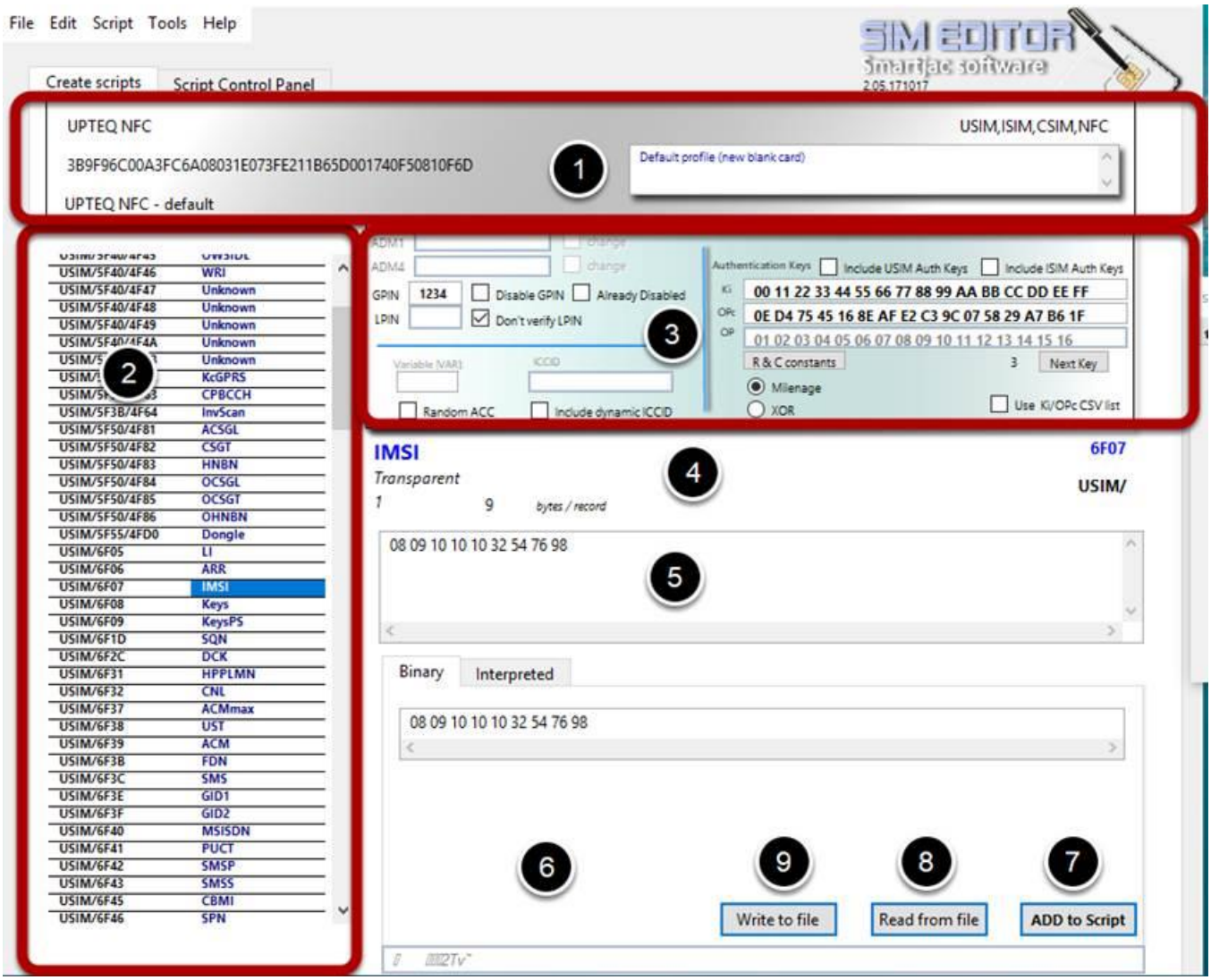
- IMPI

- Execute scripts to change contents on real SIM cards
- See APDU logs during execution
- Interpretation of errors after execution
- Direct editing and saving of scripts
- Read card contents with specific card type scripts
- Scan non-default SIM cards
- Export scanned cards to new card profiles



SIM Editor main window explained
Create Script windows – Areas

SIM Editor main window



Window areas:

1.Basic information about the card type: Name, ATR, Name of the profile,

applications on the card (USIM,ISIM, etc) and some personal notes.

2.Here we now find the files contained in this card profile. Note that this is NOT live

information from the card, just the files and default values that this card has.

3.In this area we have some options to work with before creating scripts.
For example if GPIN should be disabled, or if it is already disabled on the card (we don't

want to verify GPIN if its disabled);
Here is also where we enter or select the Authentication keys Ki / OPc, and we also have to check the box if the keys should be included in the script.
Finally there is also an option to include your own ICCID's in script.

4.This area shows File specific information about file type, record size etc.

5.File data

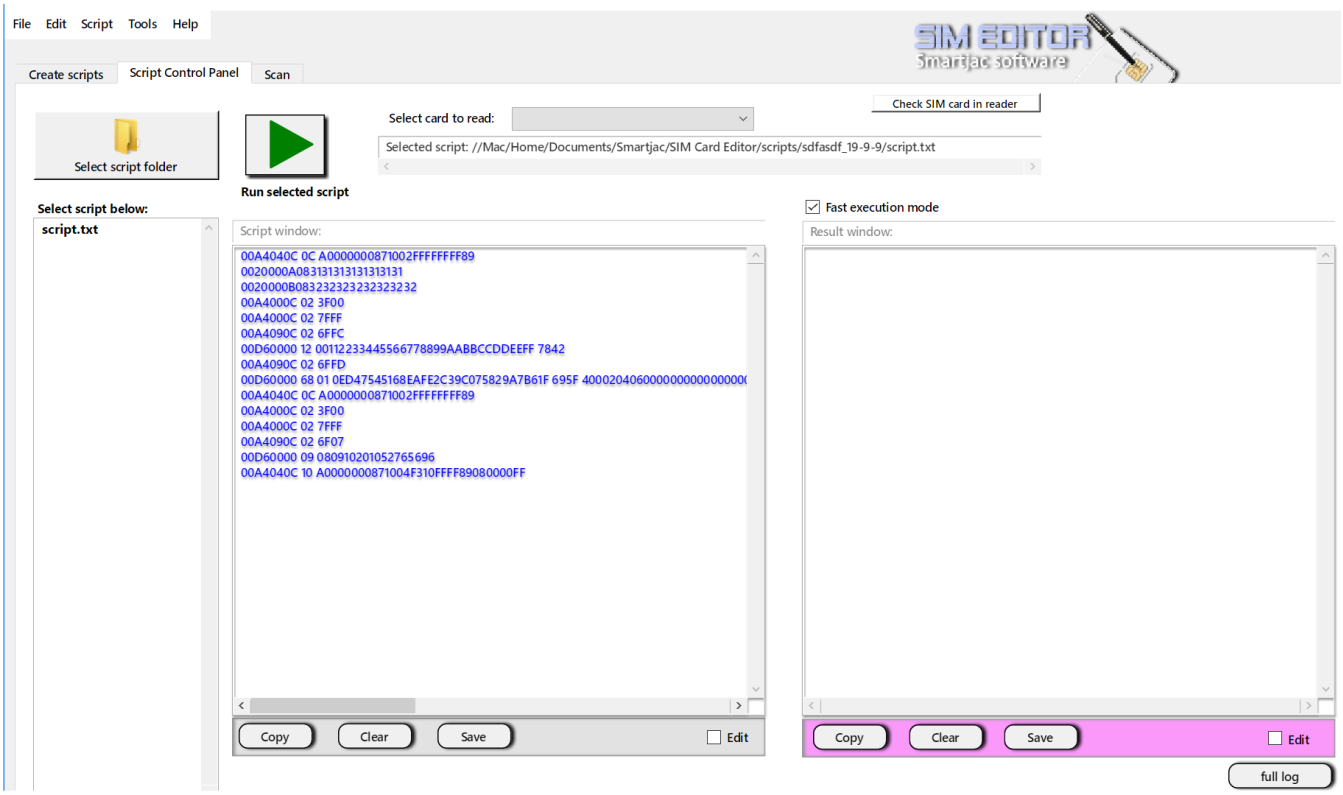
6.File data in two modes: Binary and Interpreted

7.ADD to script button - when you have entered your values click this button to add it to the script list.

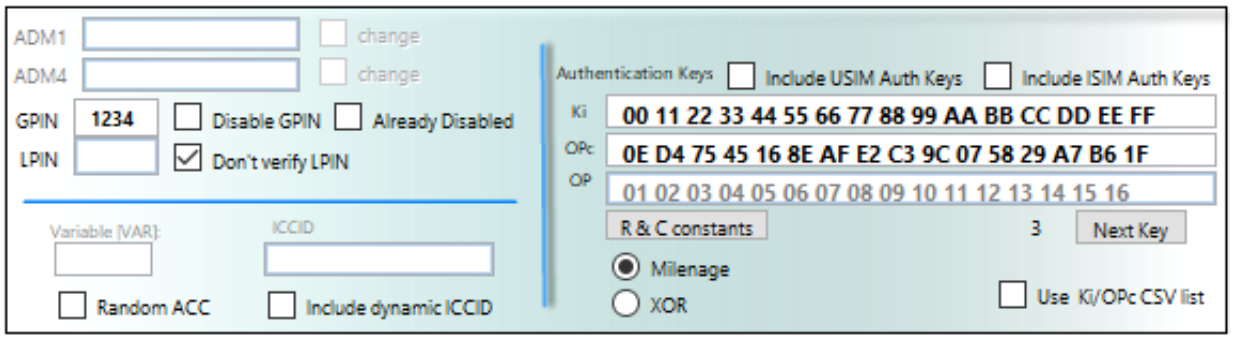
8.READ data from the SIM card (selected file)

9.WRITE the current file data (selected file and record) to the SIM card

User Interface – Script Control Panel window



PIN and Authentication Keys
SIM Editor PIN and Auth Keys



PIN's

When you open a card profile, information is automatically added to the PIN boxes. Normally correct GPIN and LPIN is entered. For this card there is actually no LPIN value so it's empty and we do not need to verify it. If you want to disable GPIN just check that box and GPIN will be disabled on that card after running the script. So next time you run a script on that same card you'll need to check the "Already Disabled" box or you will have an error.

Authentication

Authentication keys: You can enter your keys manually, and be very careful to enter the correct length (16 bytes). Or you can select any of the default keys by clicking the "Next Key" button. If you are using the card in a IMS network and edit the ISIM files on the card, you should also check the "Include ISIM Auth Keys" so that the Auth keys also are programmed for ISIM application. New in v2.8: Calculate OPc from from Ki and OP directly with “Calc OPc” button.

Algorithm
If the card supports both Milenage and XOR, then you will have the option to select which algorithm to use.
R&C constants: Only change these, Rotation and Constant constants for Milenage algorithm, if you know what you are doing. The R&C constants will be saved for all next sessions, even after restarting SIM Editor.
Use Ki/Opc CSV list: If you generate a random Ki/Opc list with Tools / Ki OPc generator you can click this checkbox, and during script generation, you will be asked to select the CSV file. If this checkbox is checked the Ki/OPc fields will not be used.

ICCID
Check the "Include dynamic ICCID" checkbox if you want to include dynamic ICCID values (increases by one). You don't enter the checksum at the end of the value as it is calculated when the tool creates the script(s).

Variable VAR
Enter a number in the VAR checkbox if you intend to use a variable in IMPI or IMPU (ISIM). (Variables are only used when generating a range of scripts)

Scanning functionality - Reading contents
This is a new addition to SIM Editors functionality that came in version 2.4x.

• EF = Elementary Files

• DF = Dedicated Files (DF can contain EF’s and DF’s)

• ADF = Application Dedicated File (ADF is selected by it’s AID. USIM, ISIM, CSIM, PKCS15 are samples of of

AID’s / ADF)

The Scan card functionality can scan any card and retrieve its file structure that it puts in

a Tree view. It scans for applications

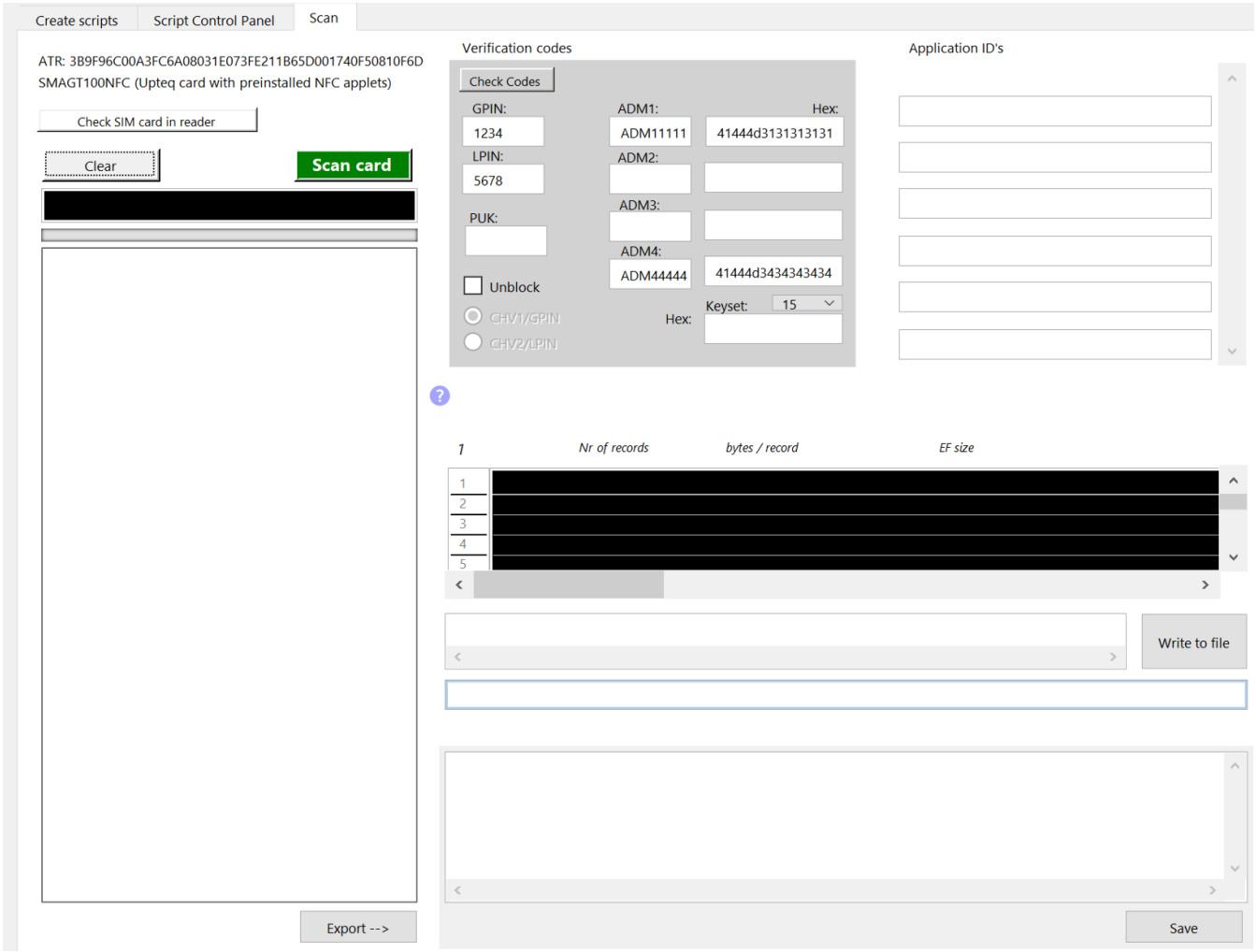
on the card (AID’s) , ADF’s, DF’s and EF’s. The EF’s are analyzed for file type, file size, number of records, record size and

access rights.

In order for the content to be read, you will need to enter the cards verification codes like GPIN, LPIN, ADM codes or

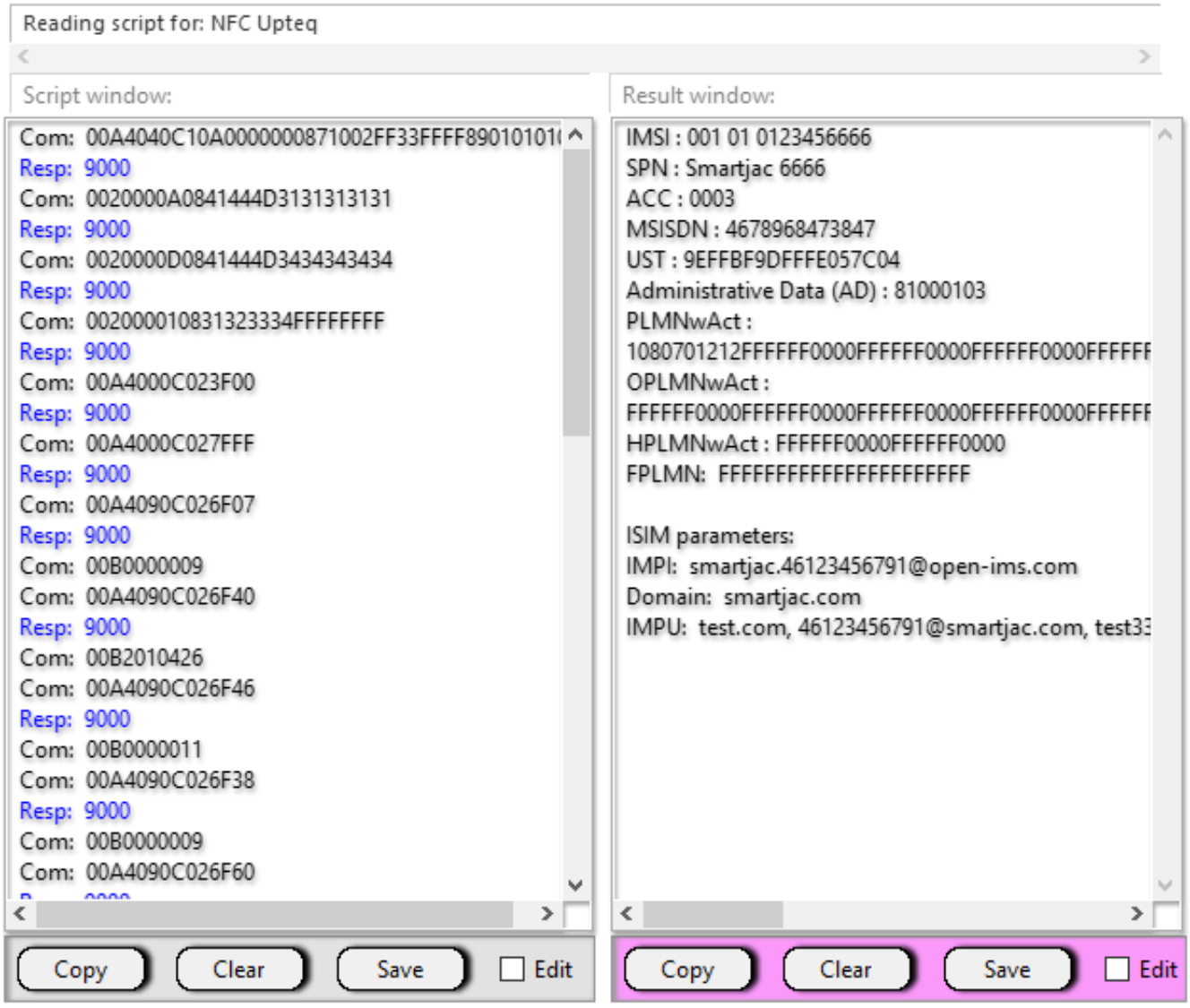
KEYSET’s, and then select / click on a file.

The Scan page:


Create scripts
Script Control Panel
Scan
ATR: 3B9F96C00A3FC6A08031E073FE211B65D001740F50810F6D
SMAGT100NFC (Upteq card with preinstalled NFC applets)
Check SIM card in reader
Clear
Scan card
Export -->
Verification codes
Check Codes
GPIN:
1234
LPIN:
5678
PUK:
Unblock
CHV1/GPIN
CHV2/LPIN
ADM1:
ADM11111
Hex:
41444d3131313131
ADM2:
ADM3:
ADM4:
ADM44444
41444d3434343434
Keyset:
15
Hex:
Application ID's
1
Nr of records
bytes / record
EF size
1
2
3
4
5
Write to file
Save

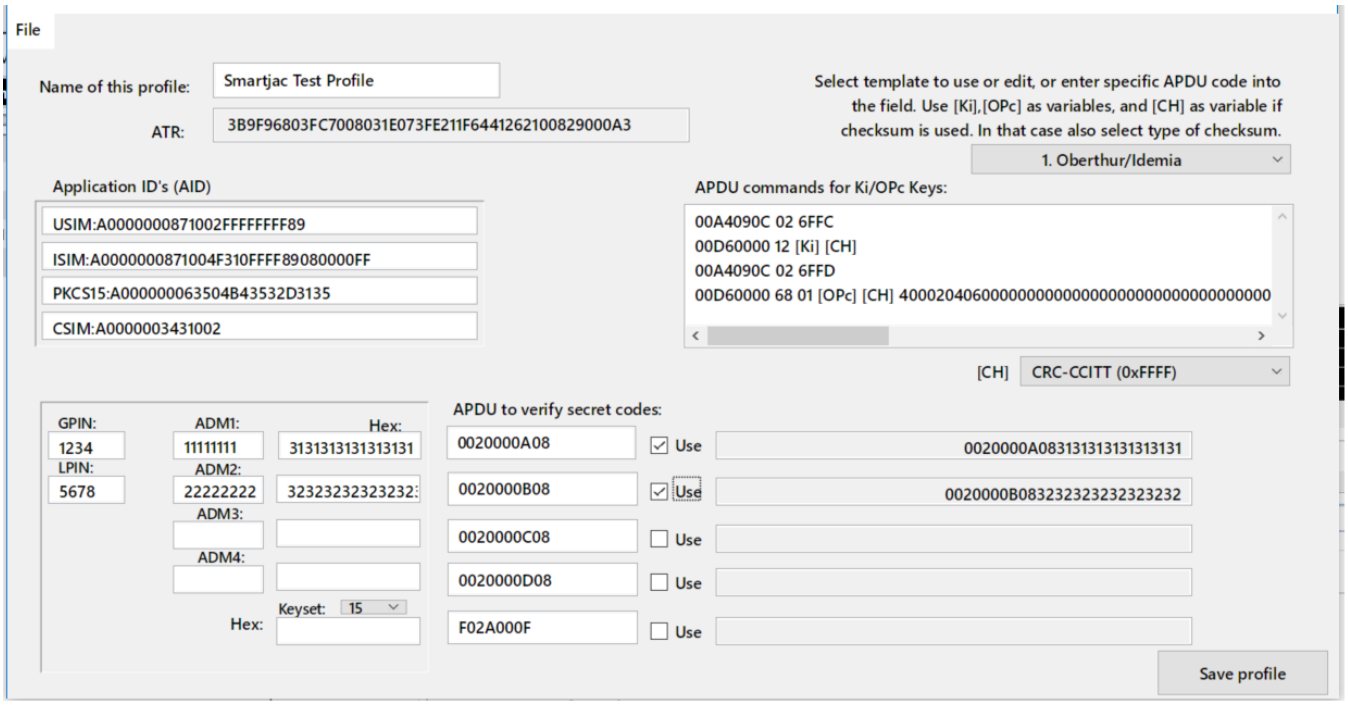
A reading script is executed and analysed and the result is presented in a readable form in the result window.

SIM Editor reading contents



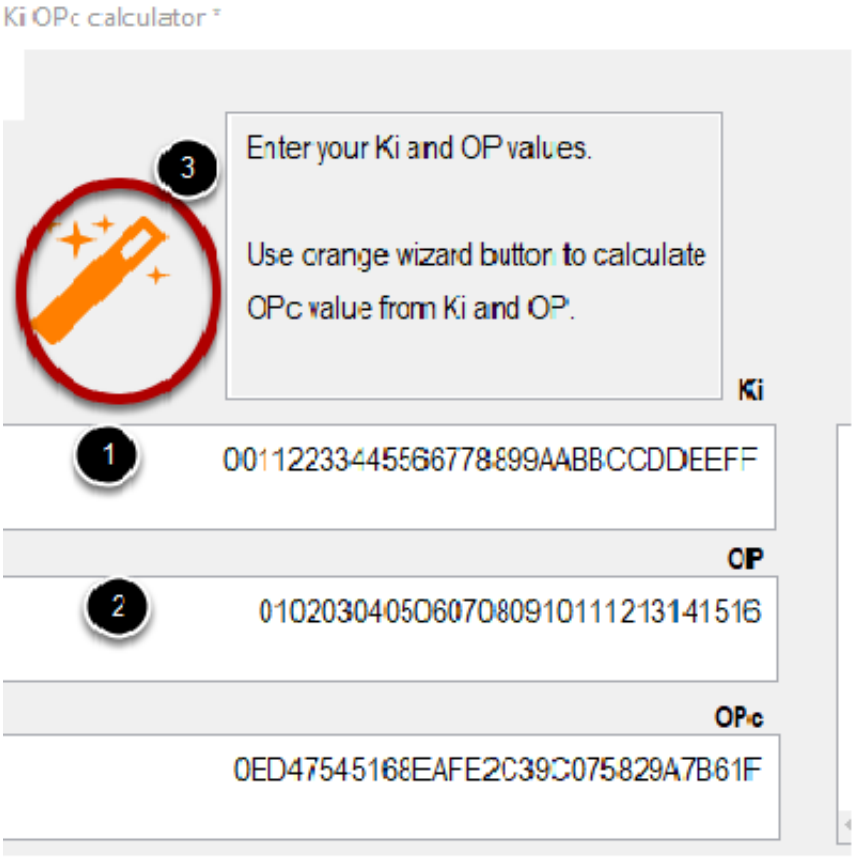
New in v2.8x:

You will now have the possibility to export the card profile of new / non-default SIM cards for use in the “card create” page
where you can work with scripting and interpretations as with our default SIM card types.



• Enter a name for your card profile
• Applications ID’s should be pre-filled. If not, exit this window and rescan your card
• Fill in GPIN, LPIN and ADM codes (or a Keyset code)
• Click the checkboxes for the ADM codes you need to use
• The tricky part is the APDU code to fill in Ki and OPc on the card. This is different for almost all SIM cards even from the same vendor! You need to get this info from your vendor, otherwise your profile will not be complete and you will NOT be able to put Ki and OPc in your SIM card. We’ve included some templates for Idemia and Gemalto/Thales SIM cards. Ki keys should be entered as parameter [Ki], OPc parameter as [OPc] and if a checksum is used, parameter [CH]. These are then replaced with your values during script generation.
• Save profile
• If you want your profile to be included in the Menu, click Yes under when the pop-up question asks you this.

Tools - Ki OPc generator - Calculating OPc
SIM Editor Ki and OPc calculator



1. Enter the Ki

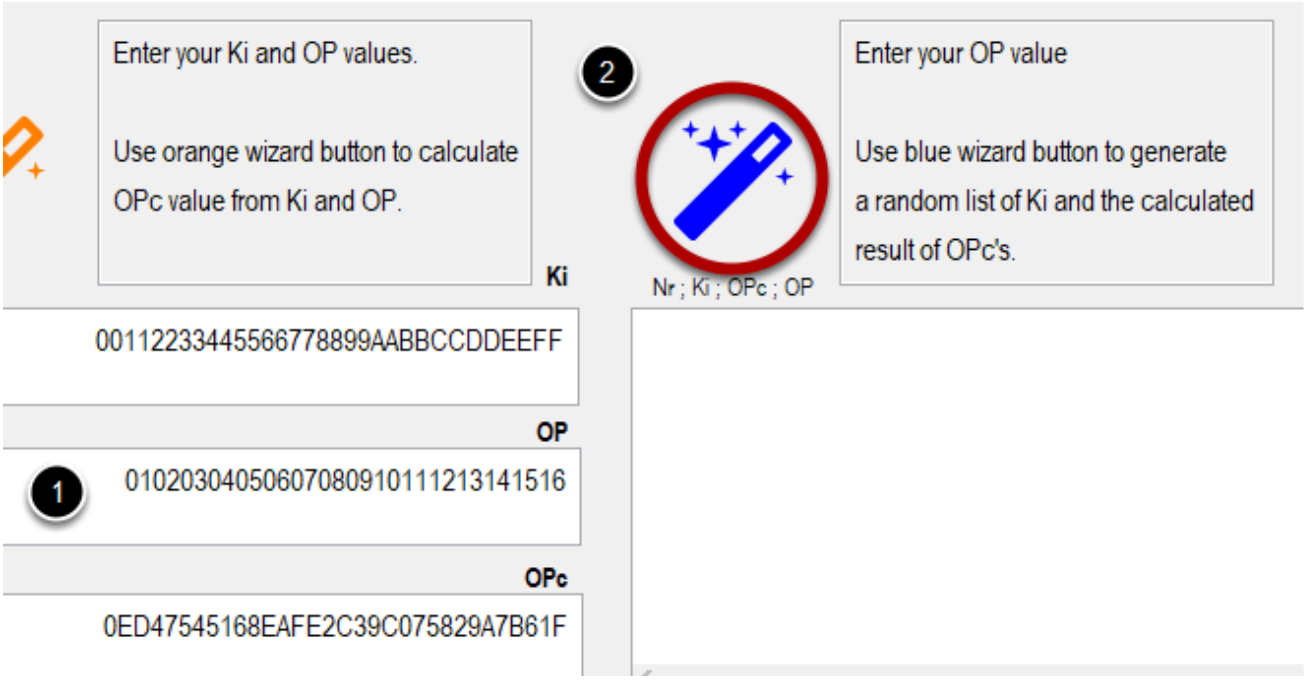
2. Enter the OP

3. Click the orange wizard button

4. If you have a connection to the Internet your OPc value is calculated

Ki OPc generator - Generating random Ki and OPc

Using the Ki OPc generator under Tools you can generate a list of random Ki's and the resuting OPc's based on the OP value.



1. Enter your networks OP value

2. Click on the blue wizard button