
SMARTJAC SIM Editor

Brand: Smartjac Industries Inc
Product Code: SMA1000SWS



Short Description

SIM card administration by scripting methodology or instant read and write.

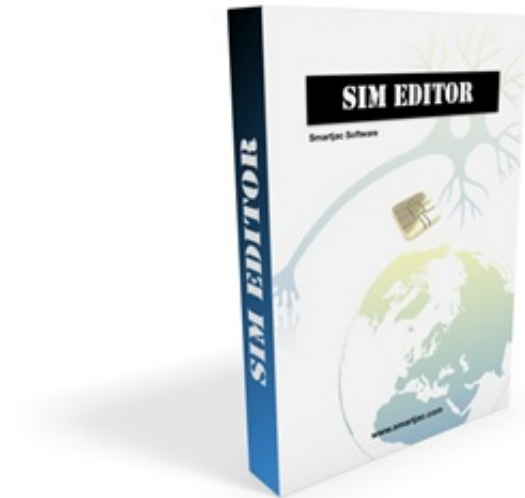
Create a range of advanced scripts with the help of an easy graphical user interface and execute them quickly one-by-one within the tool to change parameters, populate files and edit settings on SIM cards.

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

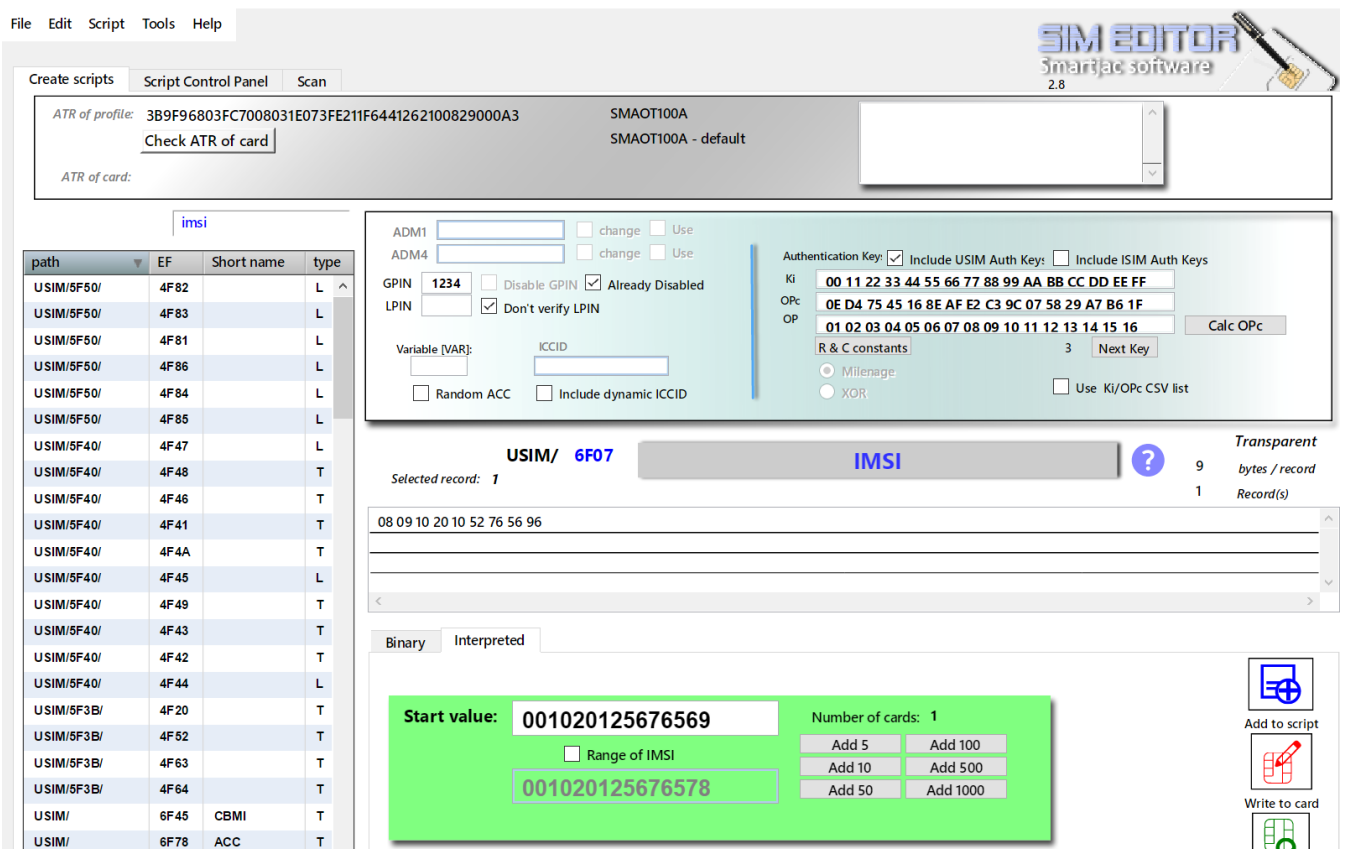
- ICCID

- 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

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

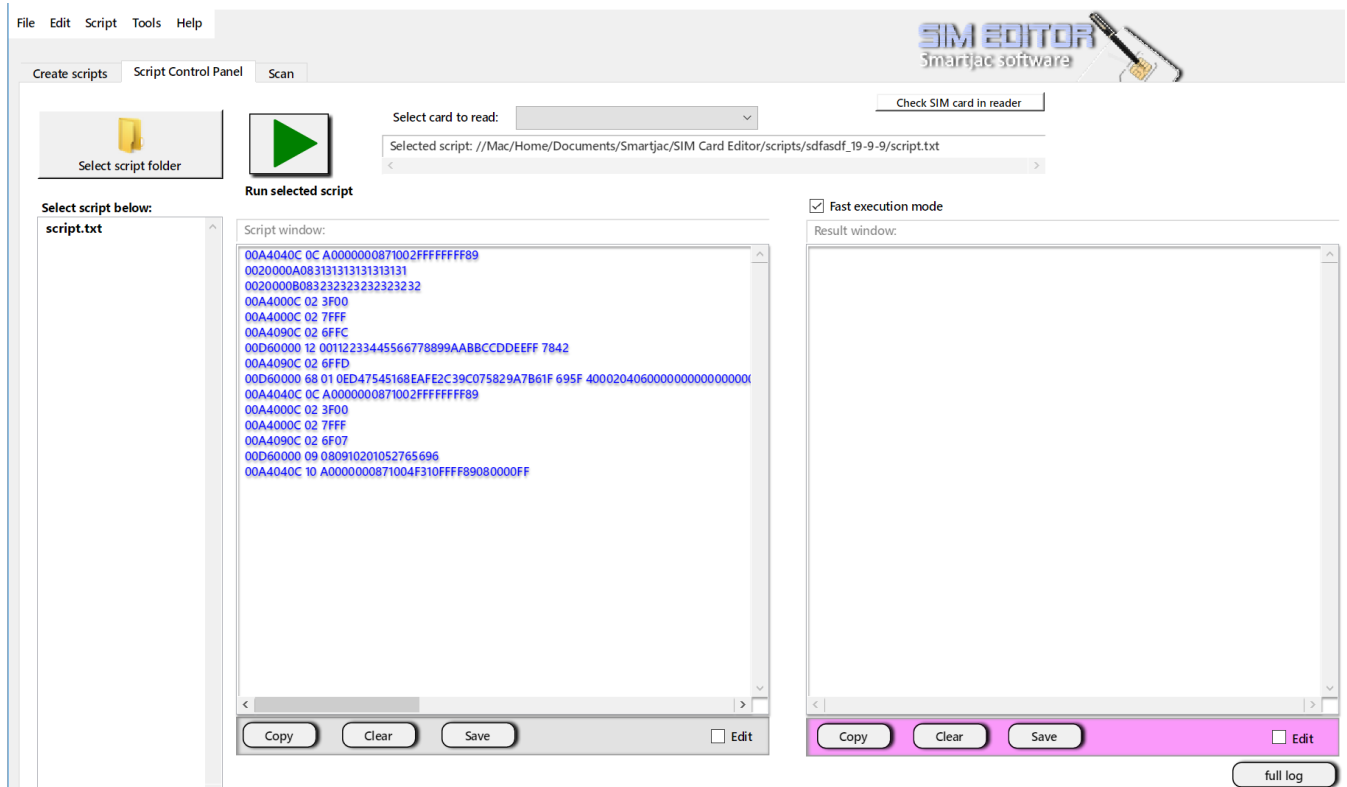
6.File data in two modes: Binary and Interpreted

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

ADM1	<input type="text"/>	<input type="checkbox"/> change	Authentication Keys <input type="checkbox"/> Include USIM Auth Keys <input type="checkbox"/> Include ISIM Auth Keys Ki <input type="text" value="00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF"/> OPc <input type="text" value="0E D4 75 45 16 8E AF E2 C3 9C 07 58 29 A7 B6 1F"/> OP <input type="text" value="01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16"/> R & C constants <input type="text" value="3"/> <input type="button" value="Next Key"/> <input checked="" type="radio"/> Milenage <input type="radio"/> XOR <input type="checkbox"/> Use Ki/OPc CSV list
ADM4	<input type="text"/>	<input type="checkbox"/> change	
GPIN	<input type="text" value="1234"/>	<input type="checkbox"/> Disable GPIN <input type="checkbox"/> Already Disabled <input checked="" type="checkbox"/> Don't verify LPIN	
LPIN	<input type="text"/>		
Variable (VAR): <input type="text"/> ICCID <input type="text"/> <input type="checkbox"/> Random ACC <input type="checkbox"/> Include dynamic ICCID			

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:

ATR: 3B9F96C00A3FC6A08031E073FE211B65D001740F50810F6D
SMAGT100NFC (Upteq card with preinstalled NFC applets)

Check SIM card in reader

Clear

Scan card

Export -->

Verification codes

Check Codes

GPIN:
1234

ADM1:
ADM11111

Hex:
41444d3131313131

LPIN:
5678

ADM2:

ADM3:

PUK:

ADM4:
ADM44444

41444d3434343434

☐ Unblock

☐ CHV1/GPIN

☐ CHV2/UPIN

Hex:

Keyset: 15

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

Reading script for: NFC Upteq

Script window:

Com: 00A4040C10A0000000871002FF33FFFF89010101
Resp: 9000
Com: 0020000A0841444D3131313131
Resp: 9000
Com: 0020000D0841444D3434343434
Resp: 9000
Com: 002000010831323334FFFFFFFF
Resp: 9000
Com: 00A4000C023F00
Resp: 9000
Com: 00A4000C027FFF
Resp: 9000
Com: 00A4090C026F07
Resp: 9000
Com: 00B0000009
Com: 00A4090C026F40
Resp: 9000
Com: 00B2010426
Com: 00A4090C026F46
Resp: 9000
Com: 00B0000011
Com: 00A4090C026F38
Resp: 9000
Com: 00B0000009
Com: 00A4090C026F60
Resp: 9000

Copy Clear Save ☐ Edit

Result window:

IMSI : 001 01 0123456666
SPN : Smartjac 6666
ACC : 0003
MSISDN : 4678968473847
UST : 9EFFBF9DFFFE057C04
Administrative Data (AD) : 81000103
PLMNwAct :
1080701212FFFFFFFF0000FFFFFFFF0000FFFFFFFF0000FFFFFFF
OPLMNwAct :
FFFFFFFF0000FFFFFFFF0000FFFFFFFF0000FFFFFFFF0000FFFFFFF
HPLMNwAct : FFFFFFFF0000FFFFFFFF0000
FPLMN: FFFFFFFFFFFFFFFFFFFFFFFF

ISIM parameters:
IMPI: smartjac.46123456791@open-ims.com
Domain: smartjac.com
IMPU: test.com, 46123456791@smartjac.com, test33

Copy Clear Save ☐ Edit

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.

File

Name of this profile: Smartjac Test Profile

ATR: 3B9F96803FC7008031E073FE211F6441262100829000A3

Select template to use or edit, or enter specific APDU code into the field. Use [Ki],[OPc] as variables, and [CH] as variable if checksum is used. In that case also select type of checksum.

1. Oberthur/Idemia

Application ID's (AID)

USIM:A0000000871002FFFFFFF89

ISIM:A0000000871004F310FFFF89080000FF

PKCS15:A000000063504B43532D3135

CSIM:A0000003431002

APDU commands for Ki/OPc Keys:

00A4090C 02 6FFC

00D60000 12 [Ki] [CH]

00A4090C 02 6FFD

00D60000 68 01 [OPc] [CH] 400020406000000000000000000000000000000000000000

[CH] CRC-CCITT (0xFFFF)

GPIN: 1234

LPIN: 5678

ADM1: 11111111

ADM2: 22222222

ADM3: 32323232323232

ADM4: 32323232323232

Hex: 3131313131313131

Keyset: 15

Hex:

APDU to verify secret codes:

0020000A08 ☒ Use 0020000A08313131313131313131

0020000B08 ☒ Use 0020000B08323232323232323232

0020000C08 ☐ Use

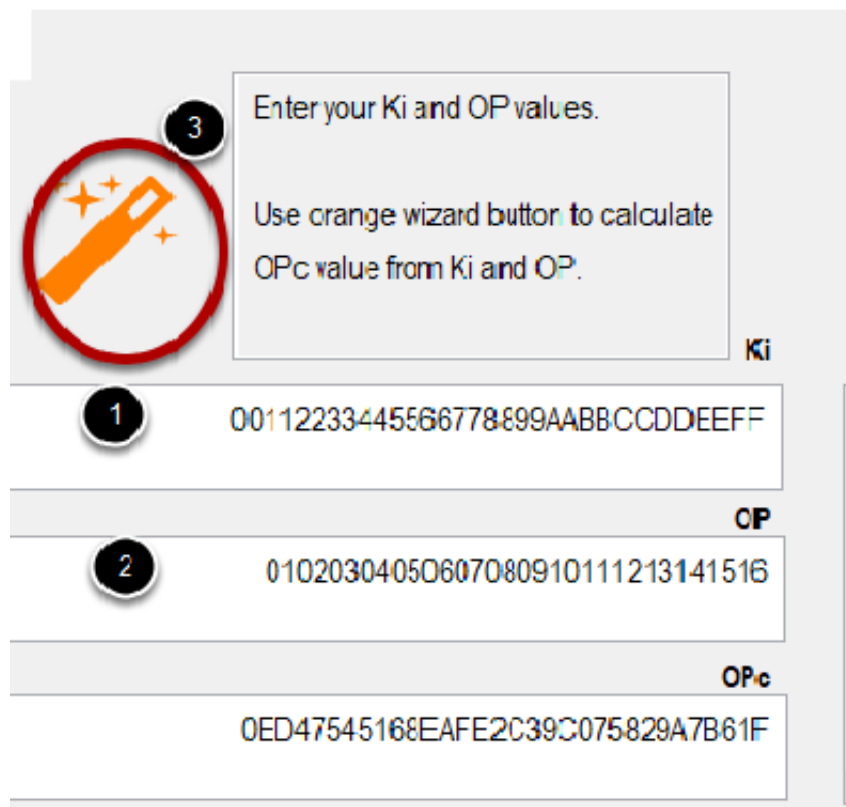
0020000D08 ☐ Use

F02A000F ☐ Use

Save profile

- 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



The image shows a web-based calculator interface for Ki and OPc values. It features three numbered instructions: 1. Enter the Ki value (00112233445566778899AABBCCDDEEFF), 2. Enter the OP value (01020304050607080910111213141516), and 3. Click the orange wizard button to calculate the OPc value (0ED47545168EAFE2C39C075829A7B61F). The interface includes input fields for Ki, OP, and OPc, and a red circle highlights the orange wizard button.

Enter your Ki and OP values.
Use orange wizard button to calculate OPc value from Ki and OP.

1 00112233445566778899AABBCCDDEEFF

2 01020304050607080910111213141516

OPc 0ED47545168EAFE2C39C075829A7B61F

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 resulting OPc's based on the OP value.

Enter your Ki and OP values.

Use orange wizard button to calculate OPc value from Ki and OP.

Ki

00112233445566778899AABBCCDDEEFF

OP

01020304050607080910111213141516

OPc

0ED47545168EAFE2C39C075829A7B61F

2

Enter your OP value

Use blue wizard button to generate a random list of Ki and the calculated result of OPc's.

Nr; Ki; OPc; OP

1. Enter your networks OP value

2. Click on the blue wizard button