

# **MotoKEY User Manual**

**techgsm.com**

**© Daniel Henzulea**  
**WEB: <http://www.zulea.com>**  
**e-mail: [zulea@zulea.com](mailto:zulea@zulea.com)**

**Manual Version: 3.1**

## Table of Contents

Table of Contents.....	2
1.Introduction.....	3
2.Hardware connections.....	4
3.Direct functions.....	6
4.Flexing phone.....	7
5.Flashing phone.....	8
6.Reading Flash from phone.....	11
7.Enable/Disable menus.....	14
8.Logo Graphic read/write.....	16
9.Tamper Alert unlocking (xx.13.xx).....	18
10.Appendix 1 – EEPROM Elements.....	19
11.Appendix 2 – Language packs description.....	20

# 1. Introduction

**MotoKEY** - RoEMMI dongle adapter is a small box who transform your small RoEMMI LPT unlocking box into a powerful weapon against all Motorola Digital Phones (GSM / DCS / PCN / Dual / TriBand).

With this **MotoKEY** adapter your small RoEMMI box become more powerful than original Flashing EMMI box (known as EMMI 2D - SLN3577D).

Advantages over the clone/original Flashing EMMI 2D are:

- Flash file go directly to phone
- Faster flashing, NO more need to send flash file via COM port
- **Read the Flash contents from phone**
- Direct buttons for basic operations (SP, IMEI, Test Flag ...)
- No need in future 'memory upgrades'
- More friendly software than original MotoFlex or WinGate
- Counter for unlocked/flashed phones stored in MotoKEY
- No need external power for the adapter
- Small design (like any PKD or HASP dongle)
- **No more need ECP/EPP settings on LPT port**

This adapter (**MotoKEY**) will enable your RoEMMI (small EMMI SP unlocking box on LPT printer port) to:

- **Unlock latest versions of Motorola phones (xx.13.xx) in 4-5 seconds !!**
- **Repair "Tamper Alert" in 2-3 seconds !!**
- Repair ALL software bugs (after wrong unlocking, etc...)
- Flash phone (change Call Processor software and Language Pack)
- Read Flash from phone (really works on all models)!!
- Build your own CP and LP files from readed flash!!
- Downgrade firmware (version)
- Flex phone (change various flex parameters of phone)
- Edit EEPROM contents

## 2. Hardware connections

Plug-in the **MotoKEY** into your RoEMMI.

Plug-in your LPT cable between the **MotoKEY** and PC's Printer port (LPT1).

Plug the power supply to your RoEMMI box (battery or mains power).

### WARNING:

**Allways plug the MotoKEY DIRECTLY to your RoEMMI box!**

**Never put an 25pin-25pin cable between MotoKEY and RoEMMI!**

**You could have “data errors” or “bad flashing” if not doing this!**

Now start the program MOTOWIN.EXE

You should have this screen:



If the software say “MOTOKEY not find” check if your LPT printer port is set to address 378. If the software report “EMMI Host disconnected” checks your RoEMMI power supply or cable connection.

**WARNING:**

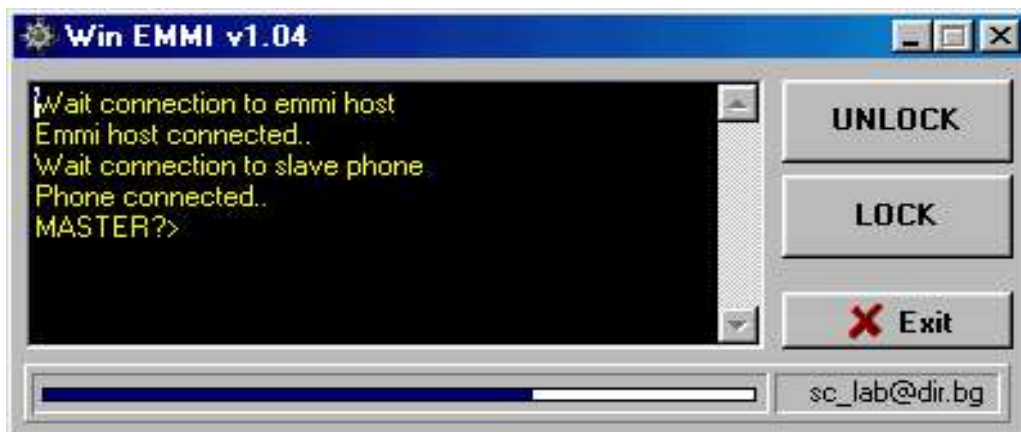
**This adapter works ONLY with RoEMMI boxes that work with software ROEMMI.EXE v2.0 (MS-DOS) or Win\_EMMI.EXE v1.04 (Windows) !!**

**This is the screenshot of ROEMMI.EXE v2.0:**

```
RoEmmi Controler v2.0.
r - read lock from slave phone
u - unlock slave phone
l - lock slave phone
f - flash slave phone
i - imei change on slave phone
q - quit EMaster

Emmi Host connected
Phone disconnected
Wait connection to emmi host
Emmi Host connected
Wait connection to slave phone
Phone connected
MASTER?>
```

**...and this is the screenshot of Win\_EMMI.EXE v1.04:**



**Please check the ROEMMI.EXE version that works with your box !**

**If your RoEMMI box work with one of this programs, all is ok, you can use [MotoKEY](#) adapter on your RoEMMI box.**

**It was on the first times on the market few RoEMMI boxes who used version 1.0 and this boxes comes each with his own 'personalized' software. On this boxes, the [MotoKEY](#) adapter NOT work.**

### 3. Direct functions

Direct Functions are most usual operations used with an original EMMI box, usually performed by editing and uploading a FLEX file.

With **MotoKEY** you DON'T need 'expert knowledge' about FLEX files and SEEM elements! The software itself for most usual functions performs this, just by checking the desired box.

This is the screen with the direct functions implemented:

The screenshot shows a list of eight direct functions. The first three are checked, and their values are entered in green input fields. The last five are unchecked.

<input checked="" type="checkbox"/>	1. Change IMEI:	12345600123456
<input checked="" type="checkbox"/>	2. Set Special Code to:	12345678
<input checked="" type="checkbox"/>	3. Lock to NET (MCC+MNC):	22601
<input type="checkbox"/>	4. Enable/Disable perm. TEST mode	
<input type="checkbox"/>	5. Reset LifeTime Count	
<input type="checkbox"/>	6. Remove network lock	
<input checked="" type="checkbox"/>	7. Set phone code to default (1234)	
<input checked="" type="checkbox"/>	8. Set sec. code to default (000000)	

The functions implemented in this software are:

- Remove network lock (clear SP lock)
- Set phone code (user code) to default: 1234
- Set security code to default: 000000
- Change IMEI to ANY 14 digits
- Lock to ANY network (MCC+MNC)
- Set special code to any 8 digits
- Enable or disable permanent TEST mode flag
- Reset life time counter

If you wish to perform any of this operations, just check the desired option and press "Make all selected jobs" button.

**To perform this operations phone must be first connected to the RoEMMI box and after that powered up! If this is not done, all these check boxes and buttons are disabled!**

## 4. Flexing phone

**FLEX** mean writing elements to phone's EEPROM memory. All Motorola phones have the EEPROM memory divided in more 'elements'. This is usually stored in Flex Definition files (\*.fdf).

Using this option, you can change Wake-up graphic, enable/disable menus, change radio parameters, etc. For performing this operation you need FDF files and some knowledge about what represent each SEEM element. Some information you can find here in Appendix 1.

For **FLEX** a phone first you have to select the right FDF file by click on the right part (small button) of the Flex file name field and select (open) the desired FDF file.



After that, just presses the "FLEX Phone" button and wait until the operation is done.

**To perform the FLEX operation phone must be first connected to the RoEMMI box and after that powered up! If this is not done, "FLEX Phone" button and "Flex file name field" are disabled!**

## 5. Flashing phone

Flashing a phone is made for firmware upgrade (change version to a newer one), firmware downgrade (change version to an older one) or to change language pack.

### **WARNING!**

**Phone MUST be with NO SIM card inside when Flashing!**

**To start Flashing, phone must be connected to RoEMMI box and powered OFF!!**

To do any of this two operations you will need a HEX file which contains the firmware or the langpack you want to upload to phone. Generally the name of the hex file should give you the idea of what it is.

There are more types of flash files.

These are:

- Main call processor file (just Firmware), this is|”CP” file
- Language pack – this is “LP” file
- All flash (Firmware+LangPack) – this is “CP-LP”

To change firmware (version up or down) you need to have ALL files (CP and LP or just “CP-LP”). To change the Language Pack, is enough to have only the “LP” file, but this MUST be from same version with the Main call processor file that is already in the phone!

All the files must be in Motorola S-HEX format (\*.HEX).

Generally the name of the hex file should give you the idea of what it is. If you have not any idea there is a tip about how to determine the contain. Usually the short files (around 200k) are only Langpack files (LP). Also you can open in a tex viewer the hex file.

**You will see something like:**

```
S00600004844521B
S3230040A000000000000DE2BEEFEA0282A0EA010A6FEA0301DEEA010A6DEA010A6CEA0174
..... many other S starting lines .....
```

**or**

```
S00600004844521B
S323004D1110BE103405004E22EC0000000004DADC80000000004D8F78004DCBC0004DD0
..... many other S starting lines .....
```

The second line is interesting. If after SXXX (four chars) you find 0040a000 or 00006000 that means that hex file is a firmware file (see first example). If the second line has other stuff than 40a000 or 6000 (like 004d1110 in second example) then it is a langpack and chars from 13 to 18 will give you the phone version which langpack applies (BE1034 in example) and chars 19-20 will give you the langpack ID (05 in our example).

For FLASH a phone first you have to select the right HEX file by click on the right part (small button) of the Flash file name field and select (open) the desired HEX file.



After that, just presses the “Write FLASH” button and wait until software ask you to power up the phone.

Now power up the phone and wait until progress bar goes to 98%. At this point, the phone will be automatic powered off and the software will ask you again to power up! Press the power key on phone, and the progress bar will goes to 99%.

**Wait until progress bar go to 100% and on Status Window is message “ALL FLASH OK”.**

The Flashing process for “CP+LP” files take 40 seconds to 3 minutes, depending on phone model (file size).

If you just want to change the Languages, is enough to flash only the LP (Language Pack) file, but this **MUST** be from the same version with the Main Call Processor (CP file) who is allready on the phone. To see the firmware version, you can enter TEST mode and press 19# or just connect the phone and power up (the version is reported by the software). To avoid uploading other LP file versions (not matching with Main CP firmware version) the function “Check LangPack version with phone” was implemented.

Check LangPack version with phone

**PLEASE check this box when you uploading just the LP file !**

The Flashing process for “LP” files take **only 30 seconds to 1 minut**, depending on phone model (file size).

If you flash Main Call Processor file (CP) or the full flash (CP+LP) must uncheck the box “Check LangPack version with phone” (as is shown bellow):

Check LangPack version with phone

## 6. Reading Flash from phone

This function is very useful when you need a specific Firmware version or a Language Pack for a specific version, and you don't have any of this file(s).

First step is to find a working phone who have inside the desired Firmware version and/or Language Pack. To check what version is it a phone, enable the Permanent Test mode Flag (with direct functions) and enter the Test Mode by keep the “#” key pressed few seconds after the phone was powered up. When you are in Test Mode, use command “19#” to see the Firmware version or command “193#” to see the Language Pack number.

The reading process is composed from 3 steps:

- Select the Flash size (end address)
- Read all flash into a binary file
- Extract CP, LP and CP+LP files from binary file

First, you have to connect the phone to the RoEMMI box and power up.

**Be sure you use a FULL charged battery !!**

The entire read process will take 1 to 3 hours, and to avoid loose your time is better to full charge the phone's battery first!

The first step is to select the Flash size. This define how many bytes will be read from the target phone.



Here is a table with Motorola phone models and size of flash for each model.

<b><i>Phone model</i></b>	<b><i>Flash size</i></b>
<b>L2000</b>	2 Mbytes
<b>L2000 Asia</b>	2 MBytes
<b>L7089</b>	2 MBytes
<b>M3188, M3288</b>	1 MByte
<b>M3588, M3688, M3788, M3888</b>	1 MByte
<b>P6088, M6088, Kool99</b>	1 MByte
<b>P7389</b>	2 MBytes
<b>P7389 Asia</b>	4 MBytes
<b>T180</b>	1 MByte
<b>T2288, V2288</b>	2 MBytes
<b>T2288 Asia, V2288 Asia</b>	4 MBytes
<b>V2088 Asia</b>	1 MByte
<b>V3688</b>	1 MByte
<b>V3688+ Asia</b>	2 MBytes
<b>V3690</b>	2 Mbytes
<b>V3690 Asia</b>	2 MBytes
<b>V50, V51</b>	2 MBytes
<b>V8088 Asia</b>	4 MBytes

If you are not sure about the Flash size, is better to select a bigger size. Usualy 4 Mbytes is working on almost all Motorola models. Also, by selecting a bigger Flash size, nothing happens wrong, just the entire read process will take a longer time.

The second step is to select or enter the **BINARY** file name by click on the right part (small button) of the Read Flash file name field and enter the name (save) of the desired BIN file.



Now, press the “Read FLASH” button and wait until the entire Flash is read into binary file. The software reports the elapsed time for this operation. Please be patient until the entire file is readed! When the entire process is done, the phone will be automatic powered off.

The third step is to convert the binary file into CP, LP and/or CP+LP files (Motorola S-Hex format). First mark the check boxes of what files you need. Better is to generate all the files, maybe will be usefull in future for you.



Now select the Binary file readed before



and press “Make HEX files button. The software will make the selected files in same directory with the Binary file.

## 7. Enable/Disable menus

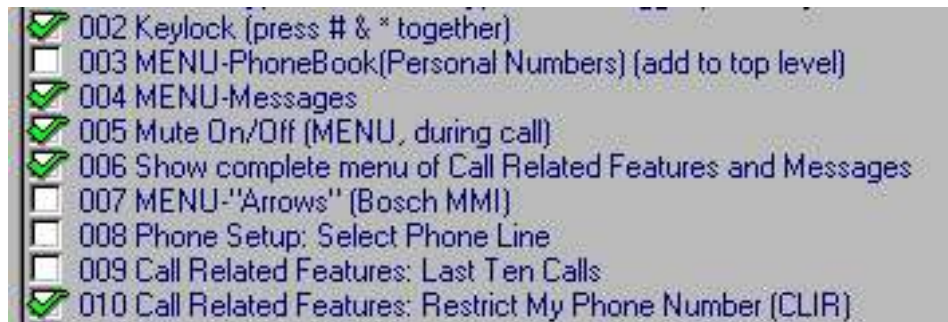
All the menus definitions in any Motorola phone is stored in EEPROM. This part is so called “Flex Definition Table” (SEEM 14). Each Menu item can be enabled/disabled by writing this part of EEPROM.

To do this, first you have to read this table stored into SEEM 14. This can be done (after the phone was connected to RoEMMI box and powered on) by pressing the button “Enable/Disable Menus”.



The SEEM 14 element (Flex Menu Table) will be read from phone. If you receive here an error, please power off and on the phone, and try again the operation.

After this, a new pop-up window will appear, with explication for each item, and also each item (Menu) will be checked/unchecked regarding his actual state in current connected phone.



Please scroll down/up on this window for view or change more items. Now, you can enable/disable any Menu item just by check/uncheck the left size checkbox. After desired changes was made, press “Write Changes” button to save the new values to phone.



**WARNING!**

**It is NOT a good idea to enable a function which is using some hardware that is not in the phone! (VoiceNotes, VibraCall, Infrared etc.) Especially: Do NOT enable/use the VoiceNotes menus on phones (e.g. T2288) which don't have the necessary chip built in! This can damage your phone!**

## 8. Logo Graphic read/write

The Logo Wake Up Graphic in any Motorola phone is stored in EEPROM. This part is so called “Graphic Logo” (SEEM 16 in Appendix 1). This graphic can be read, edited and written back by reading/writing this part of EEPROM

To do this, first you have to read this 4 fields stored into SEEM 16. This can be done (after the phone was connected to RoEMMI box and powered on) by pressing the button “Logo”.



The SEEM 16 element (Graphic Logo) will be read from phone. If you receive here an error, please power off and on the phone, and try again the operation.

After this, a new pop-up window will appear, with the readed graphic and a few buttons.



**Now you have the choice to:**

- **Load new graphic from file (Bitmap format)**
- **Save readed graphic in Bitmap format**
- **Export readed or loaded graphic to FDF Flex format**
- **Write loaded graphic to phone**
- **Exit without make changes to phone**

**If you **have more phones to change the Logo**, is better to read or load from BMP file the graphic you want to put into all this phones, and convert to Flex (FDF) format. After that, you can use this file for FLEX all the phones. Doing this operation, the Logo will be changed in all phones FLEX-ed with this file. For more information, see “Chapter 4 – Flexing phone”.**

## 9. Tamper Alert unlocking (xx.13.xx)

A new series of phones was released by Motorola. The versions of this phones are: C4\_13\_03, DB\_13\_03, F0\_13\_03 and AF\_7F\_C7. Any attempt to unlock this phones with small RoEMMI or with Full Emmi (original or clone EMMI 2D) will put the phone in 'Tamper Alert' mode.

To unlock new version of phones folow this procedure:

1. Put a simcard in phone, connect phone to box and power phone on.
2. If phone enter 'Tamper Alert' mode press “Clear TAMPER” button. The phone will power off but at next power on it will ask for 'Special Code'. If it still is in 'Tamper Alert' mode repeat step 2.
3. When phone ask for 'Special Code' press “SP Unlock xx.13.xx” and after the software say “DONE” press 00000000#. The phone will display 'Completed'. Power off phone and at next power on the phone will be no more locked. If phone displays 'Wrong Code' press again 00000000#. If phone yelds again wrong code power if off and on again and retry. If at next power up phone still ask for Special Code repeat step 3.
4. If phone displays 'Wait to Enter special Code' put it in 'Tamper Alert' mode by Flexing with TAMPER.FDF and jump to step 2.



After phone is unlocked, you can change IMEI, flash phone, etc.

### Note:

It is possible to be necessary to repeat step 2 or 3. That happens usually when phone was try to unlock by other persons with small RoEMMI or with Full EMMI 2D. Repeating step 2 or 3 will finally clear the problem. On Phones 'not touched' before, is enough to make Step 3 one time to remove Network Lock (SP Unlock).

## 10. Appendix 1 – EEPROM Elements

- \$0C (12) - IMEI (swap byte nibbles) [08 4A 74 67 09 68 89 06 80]**
- \$0D (13) - Flags, 03 33 test mode off / 13 33 test mode on**
- \$0E (14) - Keyboard and Menu Settings (122 bytes)**
- \$10 (16) - Graphic Logo (variable length)**
- \$37 (55) - Security Code (swap byte nibbles) [00 00 00]**
- \$39 (57) - Lock Code (swab byte nibbles) [21 43]**
- \$4B (75) - Phonebook (100 records)**
- \$61 (97) - SP Lock Flag (00 - not SP locked)**
- \$6D (109) - Special Code (swap byte nibbles)**

## **11. Appendix 2 – Language packs description**

### **Language Pkg\_01:**

**Danish, Dutch, Hungarian, Finnish, French, German, Greek, Italian, Norwegian, Portuguese, Spanish, Swedish, Turkish.**

### **Language Pkg\_02:**

**Bulgarian, Croatian, Czech, Estonian, Latvian, Lithuanian, Polish, Romanian, Russian, Serbian, Slovak, Slovenian, Ukrainian.**

### **Language Pkg\_03:**

**American\_English, Canadian\_French, Portuguese, American\_Spanish, German, Italian.**

### **Language Pkg\_05:**

**Dutch, French, German, Greek, Hungarian, Italian, Portuguese, Spanish, Turkish**

### **Language Pkg\_06:**

**Danish, Estonian, Finnish, Latvian, Lithuanian, Norwegian, Russian, Swedish, Ukrainian.**

### **Language Pkg\_07:**

**Bulgarian, Croatian, Czech, German, Polish, Romanian, Serbian, Slovak, Slovenian.**

### **Language Pkg\_08:**

**Arabic, Dutch, French, German, Hebrew, Russian, Turkish**

### **Language Pkg09:**

**Arabic, Dutch, French, German, Russian, Turkish**