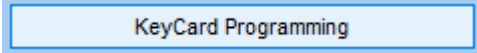
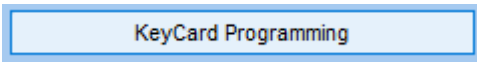
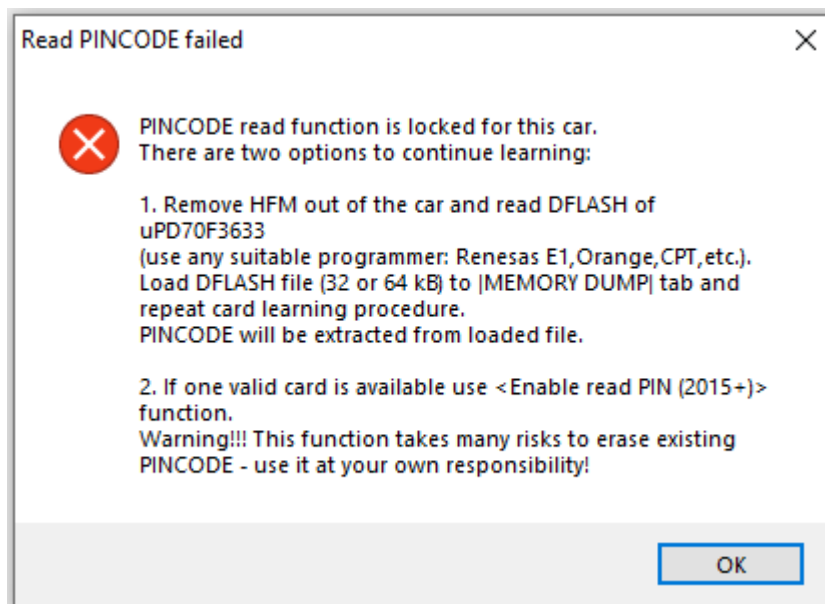


## Safe way of programming when valid card(s) present or when all keys were lost (AKL) for *Clio IV / Captur (2012-2015)*

- Connect cable of Renault ECU Tool to the OBDII port in the vehicle
- Run software of Renault ECU Tool
- Make sure the card is removed from card reader slot
- Press button  KeyCard Programming
- Software will establish a diagnostic connection to HFM module and it will read PINCODE from the car. Then it will send this PINCODE to the car to unlock card learning routine
- Follow software messages that will guide you during entire programming process
- Use a blank (unprogrammed) card if spare card should be learned or when all keys were lost. Make sure to learn all the cards that already belong to the vehicle when spare card is programmed.  
HFM module is capable to store up to 4 cards.

## Safe way of programming when valid card(s) present or when all keys were lost (AKL) for Clio IV / Captur (2015+)

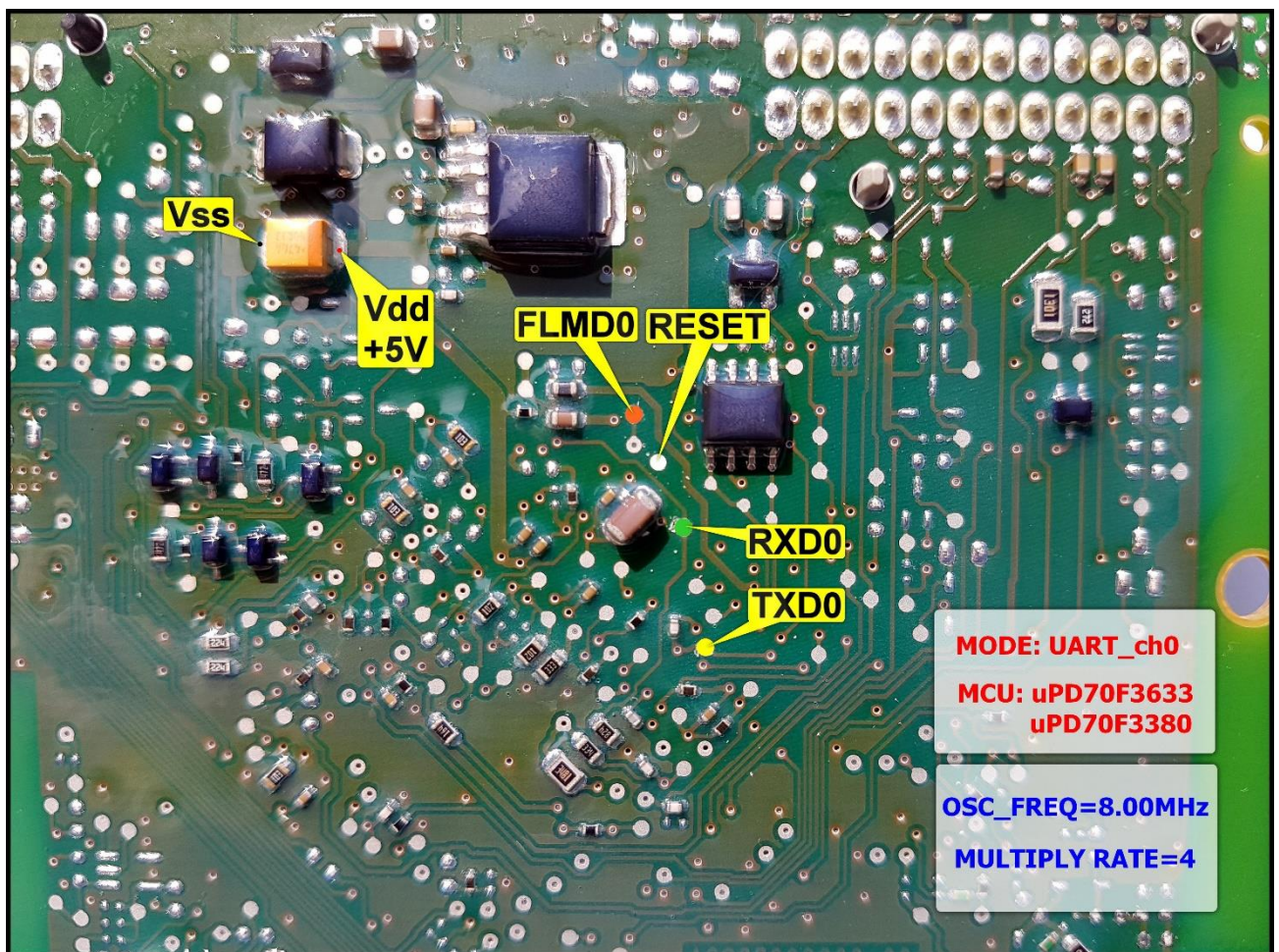
- Connect cable of Renault ECU Tool to the OBDII port in the vehicle
- Run software of Renault ECU Tool
- Make sure the card is removed from card reader slot
- Press button 
- Software will establish a diagnostic connection to HFM module and it will try to read PINCODE from the car. It will send this PINCODE to the car to unlock card learning routine if read was successful. In case of success, cards can be learned as described in the previous chapter for 2012-2015 vehicles.
- In case when PINCODE extraction is disabled in HFM module, following message will take place:



It means that PINCODE cannot be extracted by diagnostics.

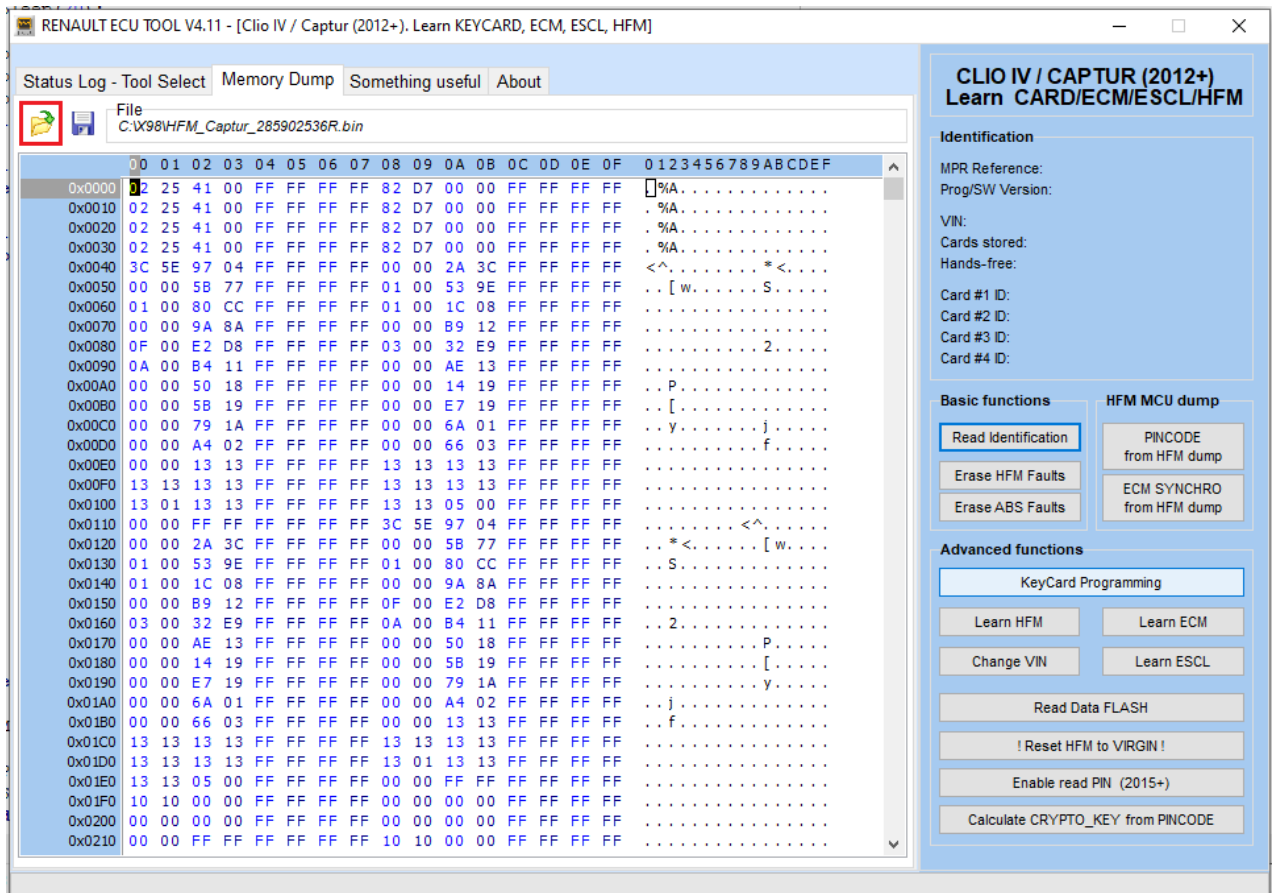
Here is described the safest way to obtain PINCODE for card learning when HFM module is locked. We recommend this way because it is risk-free to erase existing PINCODE.

1. Remove HFM module out from the car and read **Data Flash content from the NEC uPD70F3633** using any suitable MCU programmer. Connect wires from the programmer to printed circuit board of HFM module as in the picture below:



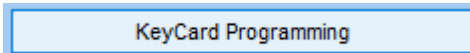
2. Install HFM module back to the car after Data Flash was read.

- Go to [**Memory Dump**] tab and load Data Flash file using yellow “Open File” icon. Software of Renault ECU Tool supports binary Data Flash files of size 32 or 64 kilobytes.



- With Data Flash file loaded, repeat card learning procedure in the exactly same way, as it was described in the chapter about card learning for 2012-2015 vehicles.

Press button



Software will try to read PINCODE from HFM module by diagnostic connection. It will fail, because HFM module is still locked. Then it will calculate PINCODE from loaded Data Flash file and it will send it to the car to unlock card learning procedure.

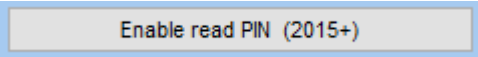
- Follow software messages that will guide you during entire card learning process.

## **(!) Enable PINCODE read for Clio IV / Captur (2015+)**

Read of PINCODE by diagnostic can be re-enabled for 2015+ Clio IV / Captur vehicles **if one valid card, that can start the vehicle, is available**. Technique to override read protection is based on the fact, that ISK code in the HFM is not erased in most cases after reset-to-virgin: data record that stores ISK code is just marked as outdated, meanwhile new record with a virgin state is created.

**Unfortunately, this method takes many risks for ISK code to be lost irreversibly. It could happen that all eight data records in Data Flash are already full and MCU must to erase whole Data Flash range to create a new virgin record. In that case ISK code is permanently erased and cannot be recovered. In the other words, this procedure is very unreliable and should be used on your own risk!!!**

**A way better choice is to use procedure that calculates PINCODE from the loaded Data Flash dump!**

If in spite of everything you decided to go on, here is explanation of what will happen when you will press the button 

It is allowed to remove read protection feature only in case when HFM module is virgin, so we need to reset HFM to virgin, disable read protection and learn back the HFM module, using a valid card. This is done by software of Renault ECU Tool in several interactive steps:

- Check if valid card is available
- Reset HFM to virgin
- Disable read protection
- Read PINCODE from unlocked HFM module
- Learn virgin HFM module using extracted PINCODE and a valid card

## (!) Card learning when all keys lost for Clio IV / Captur (2015+)

Read of PINCODE by diagnostic can be re-enabled for 2015+ Clio IV / Captur vehicles **also in case when all keys were lost**. Technique to override read protection is based on the fact, that ISK code in the HFM is not erased in most cases after reset-to-virgin: data record that stores ISK code is just marked as outdated, meanwhile new record with a virgin state is created.

**Unfortunately, this method takes many risks for ISK code to be lost irreversibly. It could happen that all eight data records in Data Flash are already full and MCU must to erase whole Data Flash range to create a new virgin record. In that case ISK code is permanently erased and cannot be recovered. In the other words, this procedure is very unreliable and should be used on your own risk!!!**

**A way better choice is to use procedure that calculates PINCODE from the loaded Data Flash dump!**

All you need is a blank **Hitag-AES** card and transponder programmer, capable to operate with **Hitag-AES** keys. Current article refers to **Master Key III (MK3)** transponder programmer, but you are free to use any other programmer with support for **Hitag-AES** transponders.

Before to proceed please check if you got latest software of Renault ECU Tool downloaded (V4.10 or higher).



Fig. 1 Transponder programmer **Master Key III**

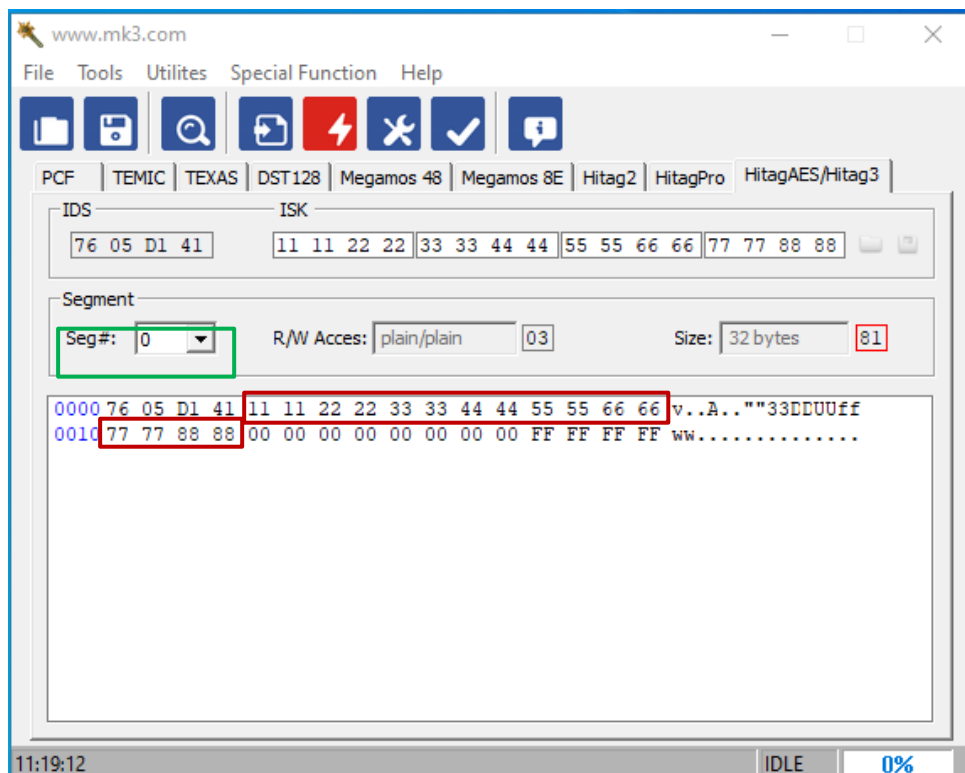
1. Connect Renault ECU Tool to the vehicle and reset HFM module to **VIRGIN**. PINCODE read protection is removed during RESET-TO-VIRGIN procedure.
2. Read **PINCODE** and **TRANSPONDER CRYPTO\_KEY**. Just press <Read Identification> button for this.

```

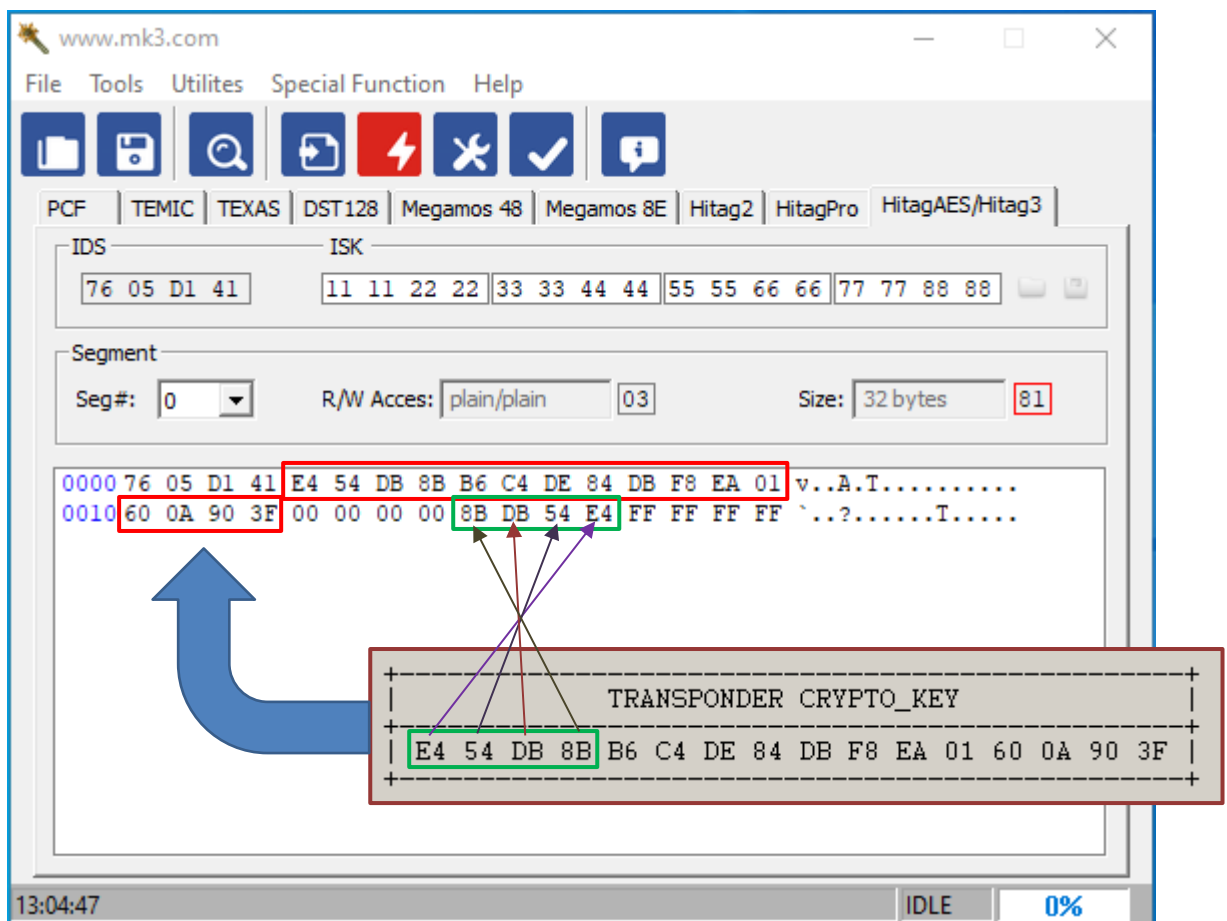
[11:09:38]
[11:09:38] Status : Reading ISK:
[11:09:48] Status : STEP_1...OK
[11:09:50] Status : STEP_2...OK
[11:09:50] Status : STEP_3...OK
[11:10:27] Status : STEP_4...OK
[11:10:28] Status : STEP_5...OK
[11:10:28] Status : STEP_6...OK
[11:10:28]
[11:10:28] ISK      : 9A 18 96 7F 9E D6 86 50 07 12 83 03 E2 2C 2C 10
[11:10:28] PINCODE: 98 09 58 1A 4C 01 FA 40 B2 23 6B FE 23 F6 30 8D
[11:10:28]
[11:10:28]      +-----+
[11:10:28]      |                                |
[11:10:28]      |          TRANSPONDER CRYPTO_KEY          |
[11:10:28]      +-----+
[11:10:28]      | E4 54 DB 8B B6 C4 DE 84 DB F8 EA 01 60 0A 90 3F |
[11:10:28]      +-----+
[11:10:28]
[11:10:28] Status : Waiting For Commands

```

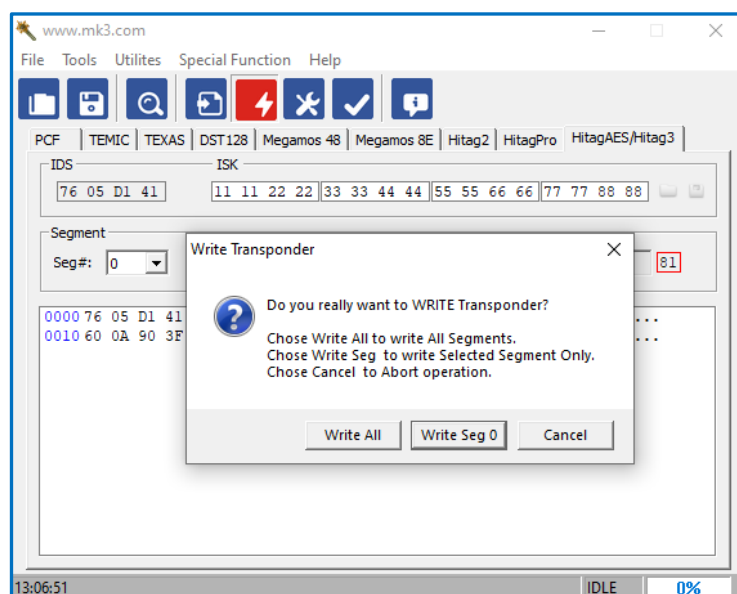
3. Read blank **Hitag-AES** card using transponder programmer. You can see factory default crypto key in **Segment 0**.



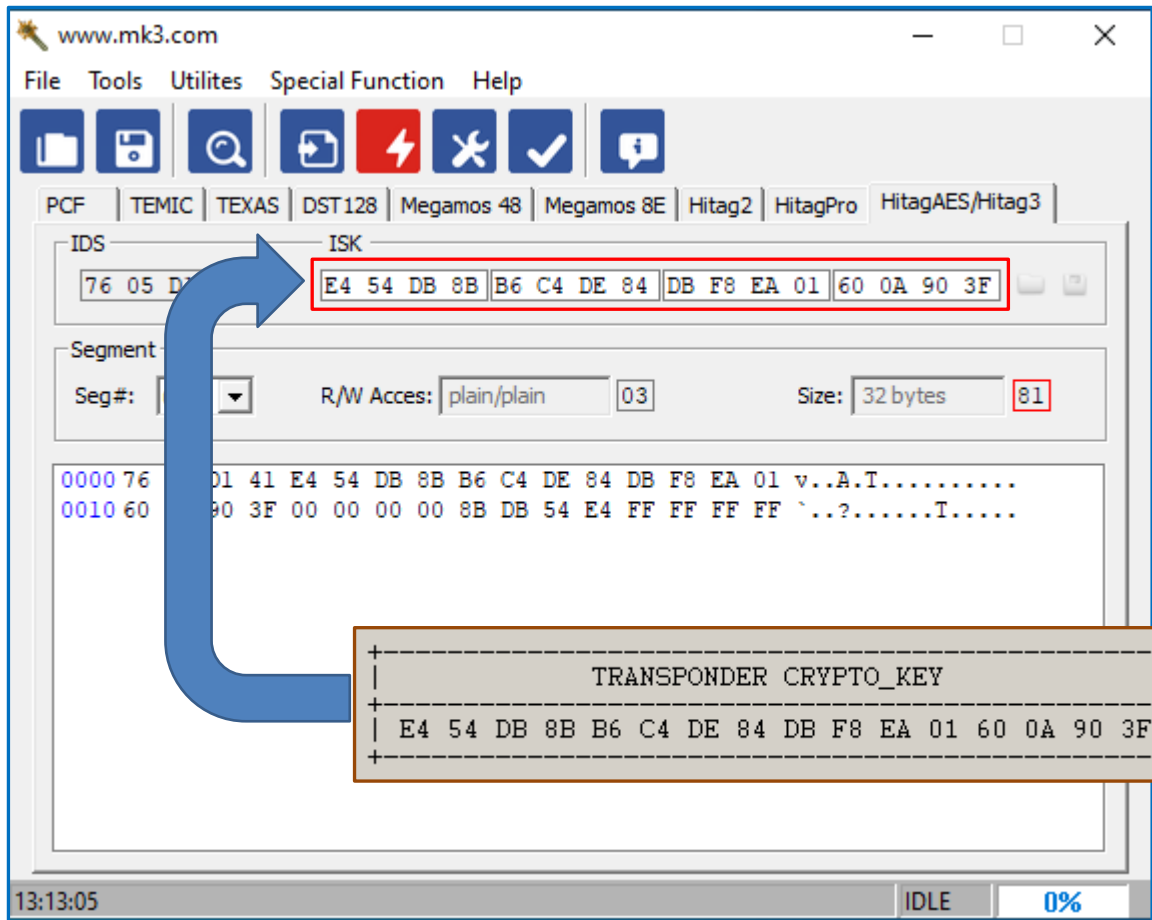
- Replace factory default key **11112222333344445555666677778888** with the one, you did read during step 2. Also replace 4 bytes in a green frame with highest four bytes of **TRANSPONDER\_CRYPTO\_KEY** in reversed order.



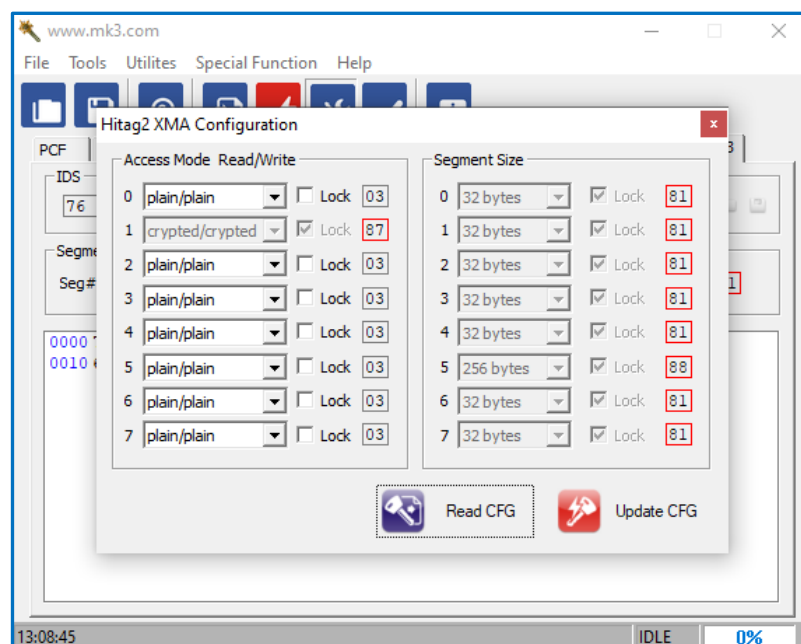
- Program modified data to transponder.



6. Transfer **TRANSPONDER CRYPTO\_KEY** to ISK field of transponder programmer.



7. Read transponder configuration.



8. Change R/W Access for **Segment 0** from factory default “plain/plain” (value 03) to “crypted/crypted” (value 07) and press <Update CFG>.

This step is very important- without doing this card still will be recognized as BLANK.

**Do not set LOCK bit!!!**

**BEFORE**

Hitag2 XMA Configuration

Access Mode	Read/Write	Lock
0	plain/plain	03
1	crypted/crypted	87
2	plain/plain	03
3	plain/plain	03
4	plain/plain	03
5	plain/plain	03
6	plain/plain	03
7	plain/plain	03

Segment Size	Lock
0 32 bytes	81
1 32 bytes	81
2 32 bytes	81
3 32 bytes	81
4 32 bytes	81
5 256 bytes	88
6 32 bytes	81
7 32 bytes	81

Read CFG Update CFG

**AFTER**

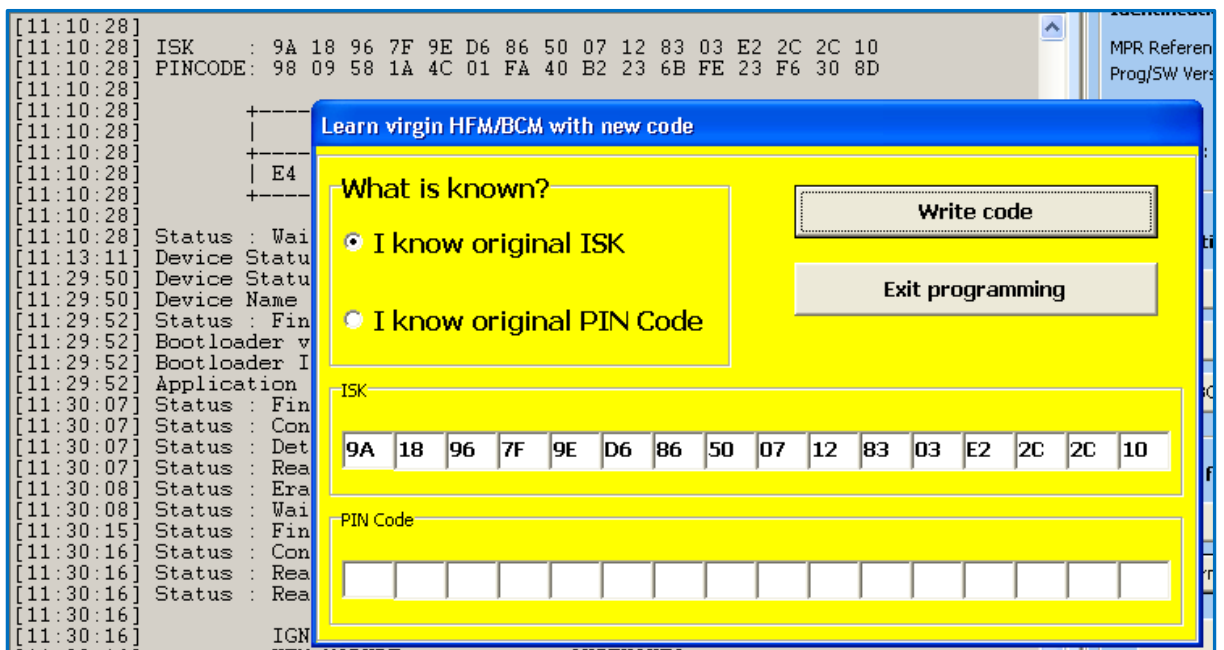
Hitag2 XMA Configuration

Access Mode	Read/Write	Lock
0	crypted/crypted	07
1	crypted/crypted	87
2	plain/plain	03
3	plain/plain	03
4	plain/plain	03
5	plain/plain	03
6	plain/plain	03
7	plain/plain	03

Segment Size	Lock
0 32 bytes	81
1 32 bytes	81
2 32 bytes	81
3 32 bytes	81
4 32 bytes	81
5 256 bytes	88
6 32 bytes	81
7 32 bytes	81

Read CFG Update CFG

- Learn HFM module.** Enter **ISK** or **PINCODE** extracted at the step 2 and use already pre-programmed card during HFM learning.



Job done. This is a final result:

