Clio IV / Captur (2015+) card learning when all keys lost

As you know, PINCODE read procedure by diagnostic is restricted for 2015+ Clio IV / Captur vehicles. It's easy to override PINCODE read restriction when one valid card is available, but key learning gets more complicated when all cards were lost: HFM module must to be removed from the car, wires to be soldered directly to NEC MCU to upload Data Flash content.

This article will describe step-by-step key learning procedure when all cards were lost without intervention to the HFM module. All you need is a blank card (of correct type) 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 (V2.93 or higher).

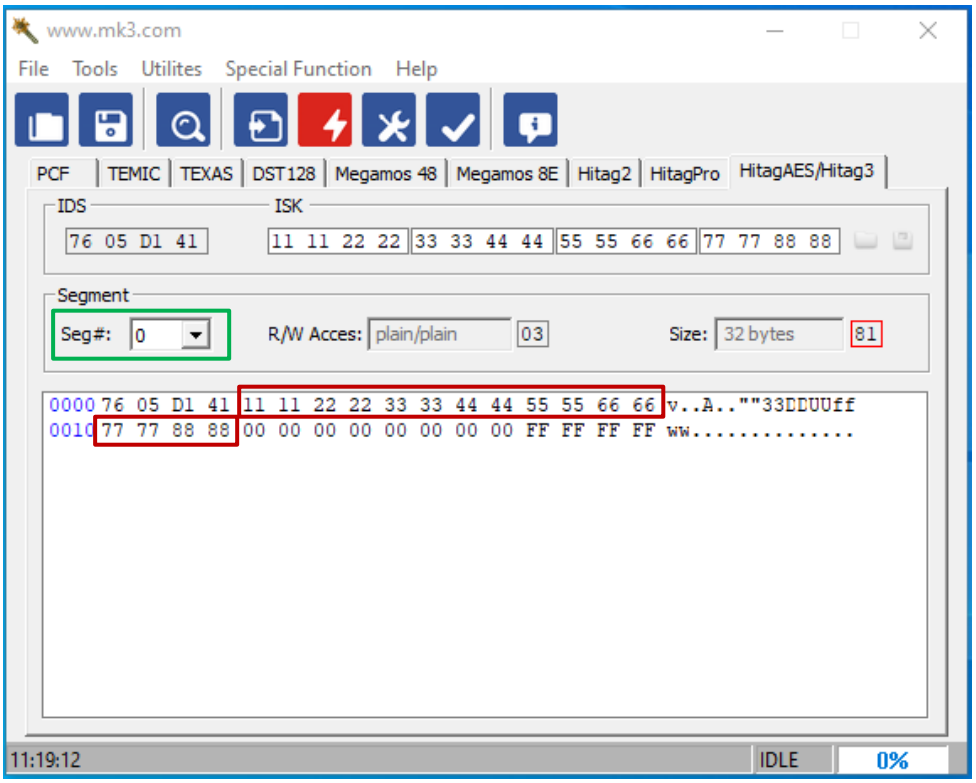
Fig. 1 Transponder programmer **Master Key III**

1. Connect Renault ECU Tool to car and reset HFM module to VIRGIN. PINCODE read protection is removed during RESET-TO-VIRGIN procedure.

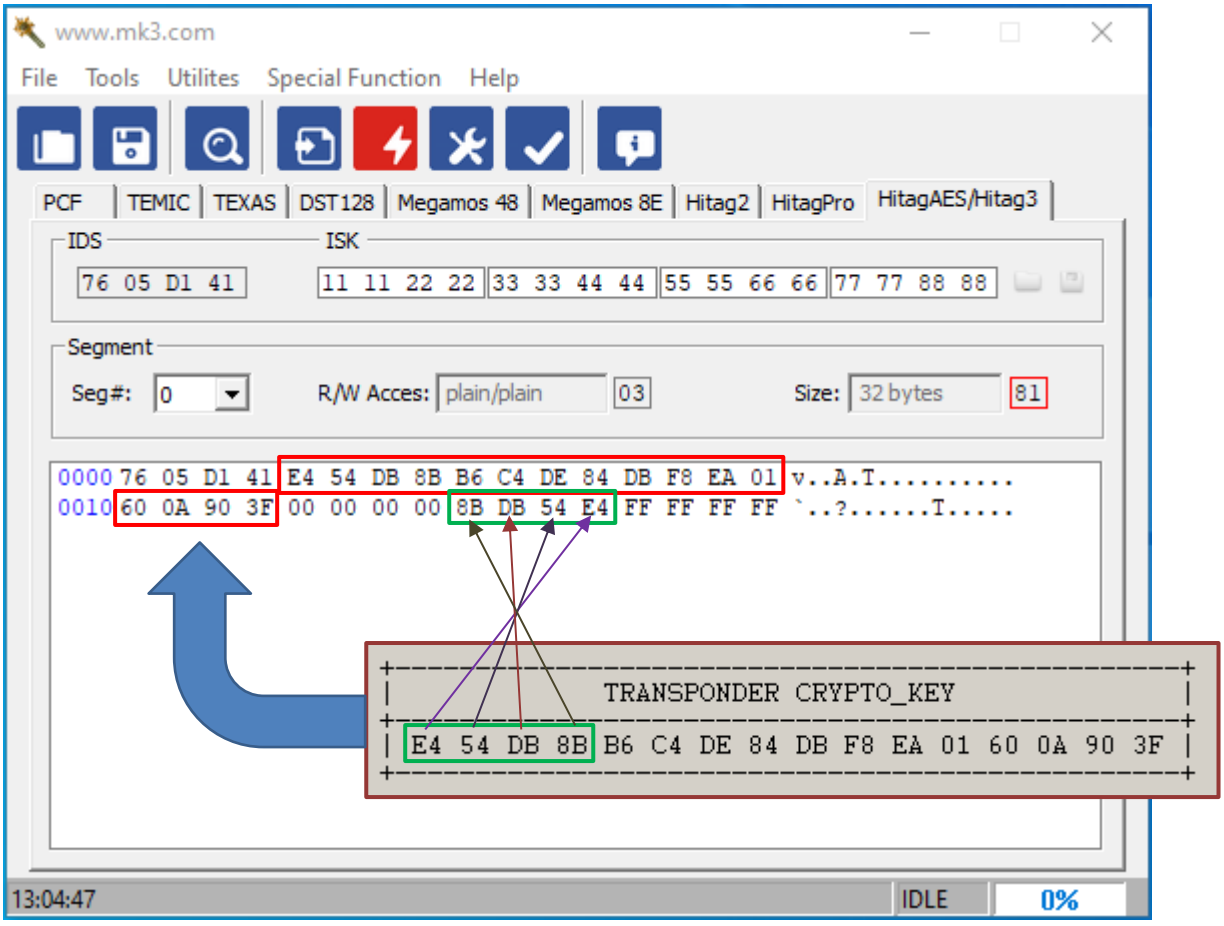
2. Read **PINCODE** and **TRANSPONDER CRYPTO_KEY**. Just press <**Read Identification**> button for this.

```
[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]         |              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
```

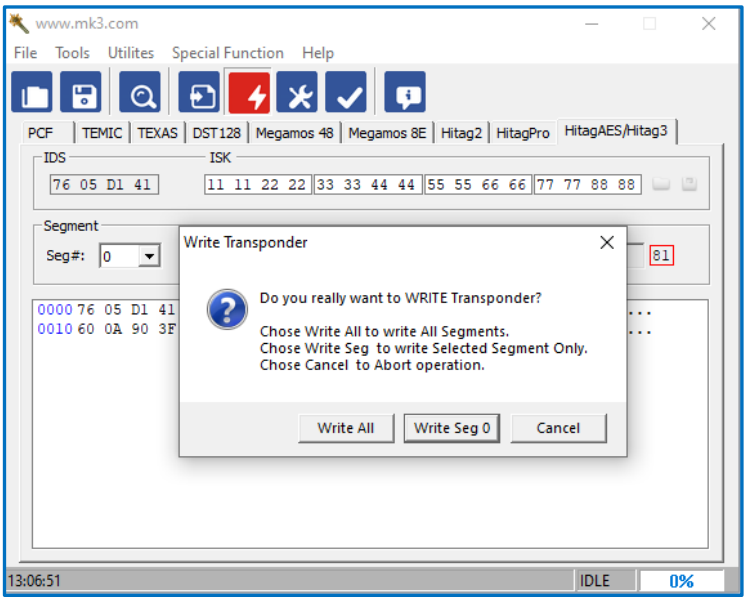
3. Read blank card using transponder programmer. You can see factory default crypto key in **Segment 0**.



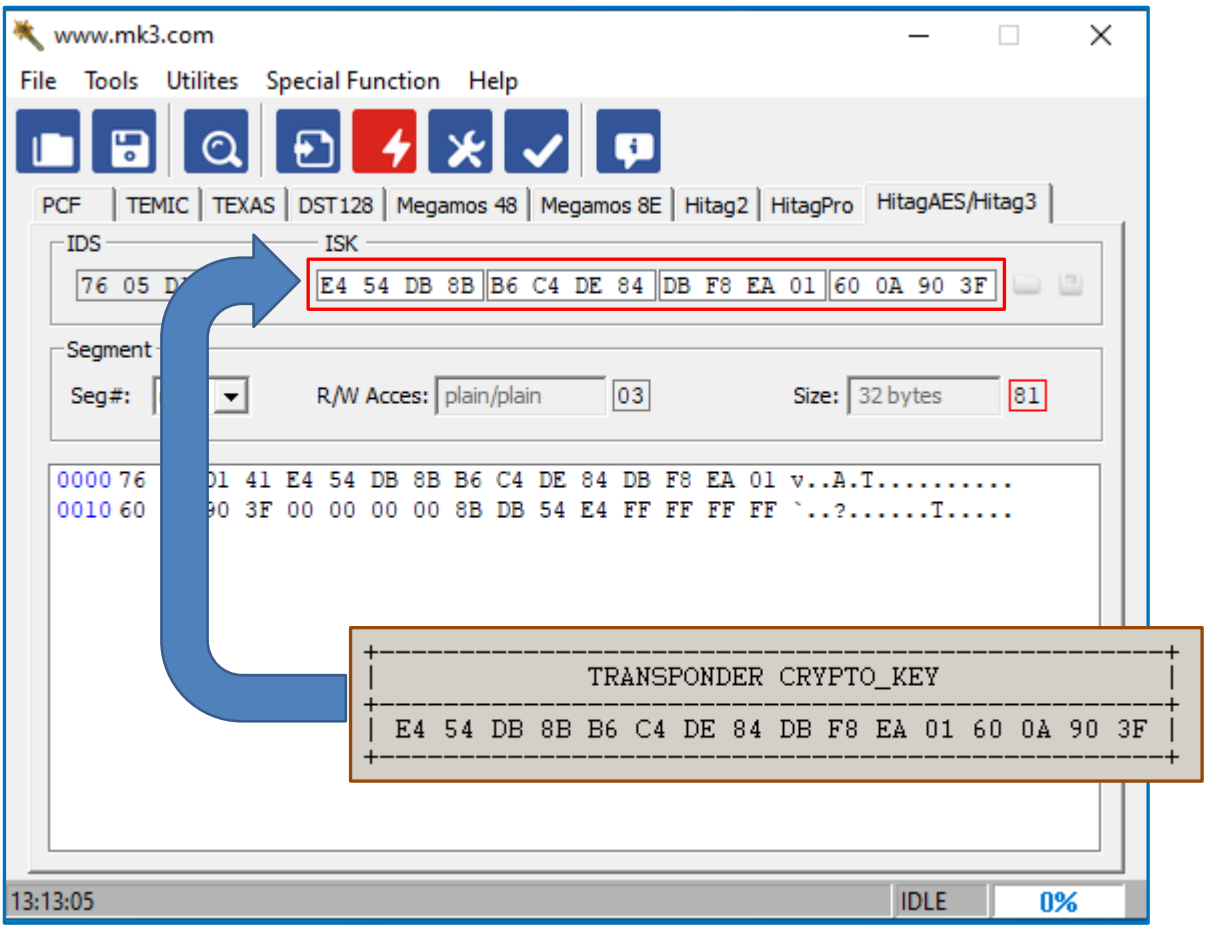
4. Replace factory default key **11112222333344445555666677778888** with the one, you did read during step 2. Also replace 4 bytes in green frame with highest four bytes of **TRANSPONDER CRYPTO_KEY** in reversed order.



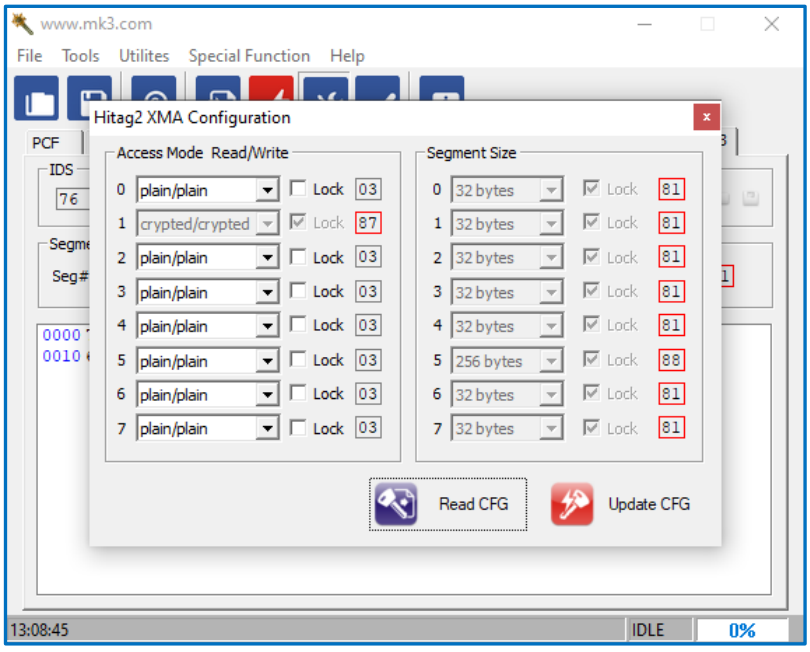
5. Program modified data to transponder.



6. Transfer **TRANSPONDER CRYPTO_KEY** to **ISK** field of transponder programmer.



7. Read transponder configuration.

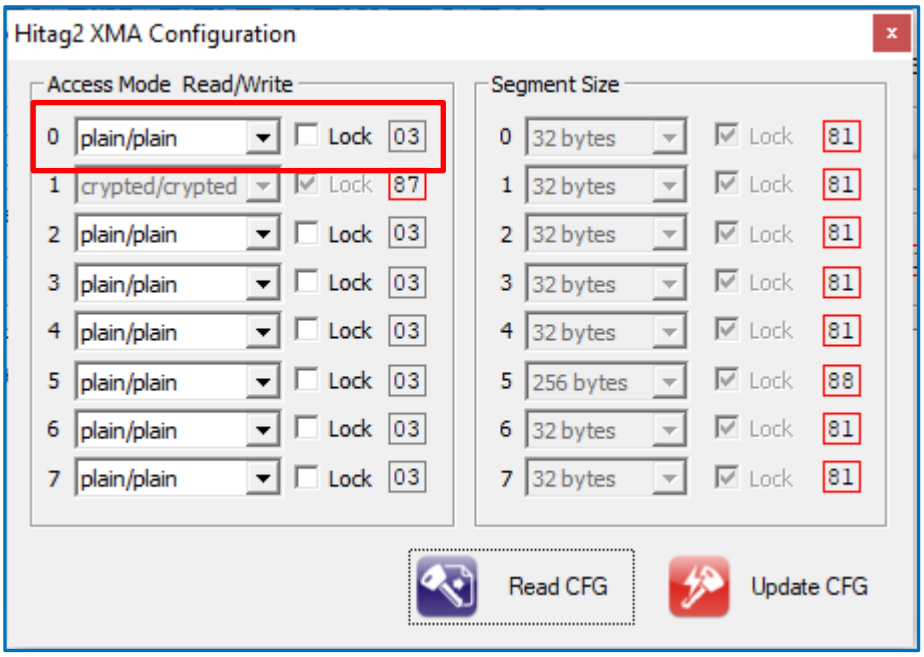


8. Change R/W Access for **Segment 0** from factory default "**plain/plain**" (value **03**) to "**crypted/crypted**" (value **07**) and press <**Update CFG**>.

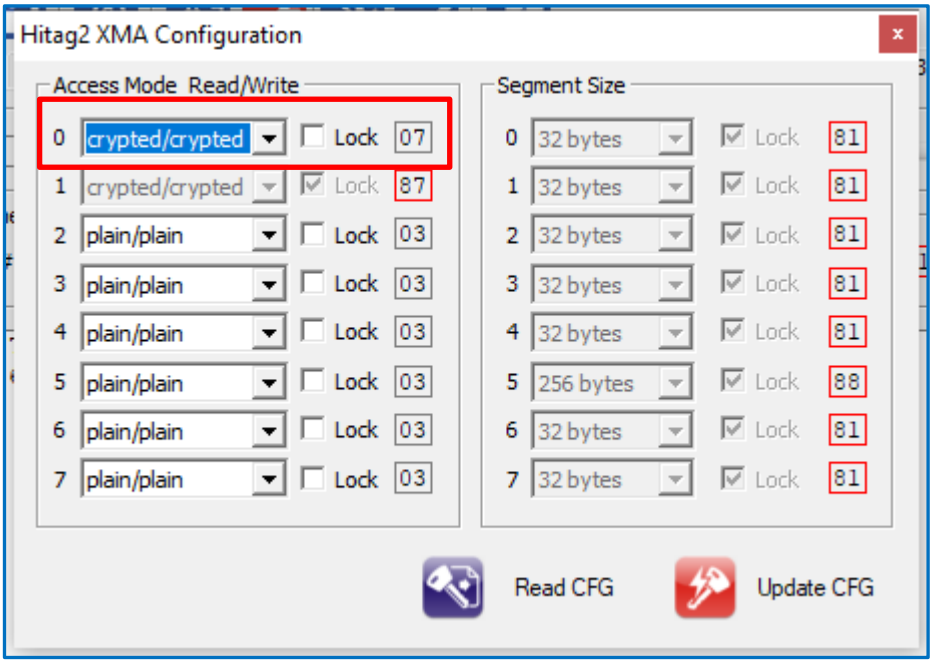
This step is very important- without doing this card still will be recognized as BLANK.

Do not set LOCK bit!!!

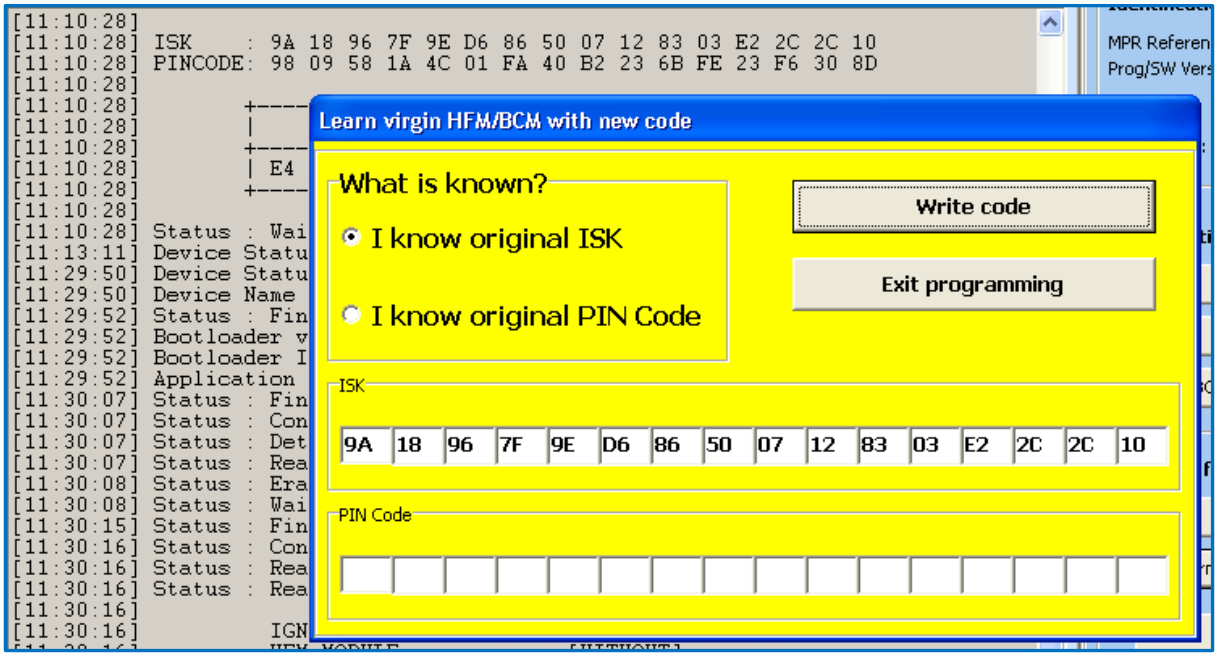
BEFORE



AFTER



9. 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 final result:

```
[12:28:14] Status : Reading BCM programming state...DONE
[12:29:01] Status : Gaining security access...OK
[12:29:01] Status : Launching BCM learning mode...DONE
[12:29:07] Status : Learning ISK to BCM...DONE
[12:29:07]
[12:29:07] Status : +----------------------------------------+
[12:29:07] Status : |   BCM LEARNING successfully completed  |
[12:29:07] Status : |           Cycle ignition key           |
[12:29:07] Status : |       to store programmed values       |
[12:29:07] Status : +----------------------------------------+
[12:29:07]
[12:29:07] Status : Waiting For Commands
```