MBir

Mercedes IR KEY reader

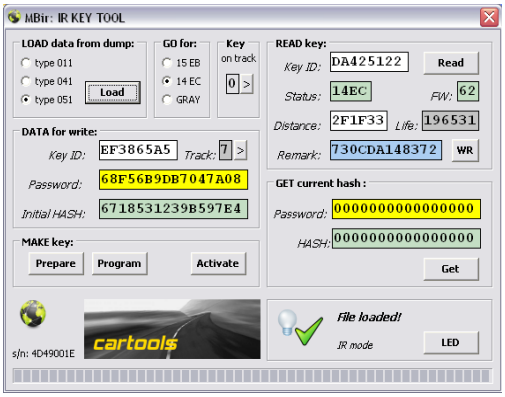
IR service key programmer

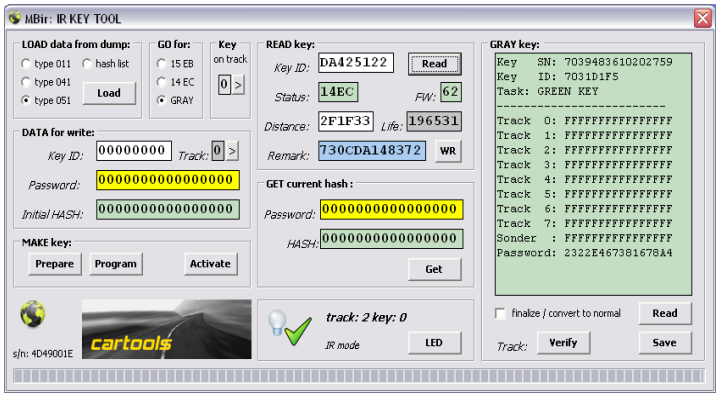
Software for MBir:

- MBir: main key reader software;
- MBsk: service key programmer (green, yellow, blue service keys);
- MBbe: aftermarket BE key EEPROM tool;
- MBpwcheck: key password checker;
- MBhash: hash list generator;
- MBhashtodump: builds fake EIS dump from HASH list for calculations on 3rd party resources;
- MBelv: for ESL access - read data blocks, hash list, ESL data blocks via IR.

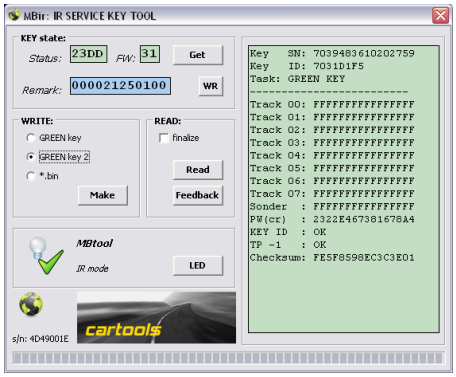
MBir software:

- key read / write / test tool;
- it is possible to make 2nd and 3rd key on track, not only first (tracks are numbered from 0 up to 7, on each track there can be 3 keys (0,1,2). If key 0 on selected key track runs out of life it can be replaced with key 1 and so on.;
- BE key support: write and "reset" to 21DF via IR is possible;
- GRAY key reading and writing;
- it is possible to work with NEC chip from key soldered on board as with regular key. Although it is possible to prepare (erase, renew) NEC chip (not BGA) using **MBir** we recommend to use **MBnec** tool instead.
- **LOAD data from dump** is used for compatibility purpose only, tool loads only SSID and KEY PASSWORD from dump. It is enough to fill three **DATA for write** fields with correct data make a valid key.
- KEY status **14EC** is for SERIES KEY, **15EB** is used for replacement keys. No matter what to choose, functionality is the same.
- If GRAY key is selected as option it is necessary to load HASH LIST too (extra window opens at the right side of software). **To know**:
  - GRAY key is used for EIS personalization (SERIES EIS, not activated or neutralized);
  - it converts itself to normal working key (14EC) when EIS personalization is finished, so two datasets are necessary: HASH list for EIS personalization and KEY DATA for finalized KEY;
  - theoretically it is possible to build KEY which is not accepted by EIS after personalization, button Verify allows to check if the KEY initial hash is valid for selected track or not;
  - for SERIES EIS personalization additional command via CAN is necessary (use DAS engineering, Vediamo etc.);
- **Remark**: it is possible to write any calibration data into KEY;
- button **LED**: to test communication with KEY (IR mode), when pressed LED in KEY shell must go ON;
- **GET current HASH**: if KEY password is known it is possible to **Get** actual **HASH** from key;
- always allow KEY to finish tasks (this appears on info screen), otherwise key may get stuck and become unusable.
- **MBir** is not preparing or writing KEYLESS keys. Although all read operations via IR are possible to check firmware version or tests for functionality.





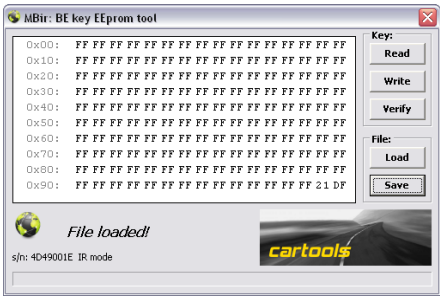
MBsk software (optional):



- service key (SK), GREEN, ORANGE, BLUE reading and writing;
- **Read** key: key content is displayed (HASH list, commands etc.);
- **Feedback**: EIS accepts data from SK and store feedback into SK, you can read it;
- to **Make** key must load HASH list prepared an previously saved using Mbgreenkey software (Mbkey toolset);

Expert use only! If somebody knows correct data and some commands what to write into SK it may take less than 2 seconds to completely destroy car (by disabling all key tracks for example).

MBbe software (optional):



- aftermarker key reader via IR (BE key);
- read, write, verify;

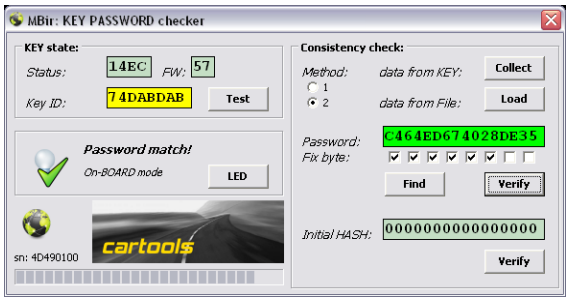
NOTE: If BE key reads with errors or is not responding at all even if it seems working with EIS it is a good idea to throw it away and use any original (used) FW28/35/40/51/55 key instead.

MBpwcheck software:

allows to verify and recover missing KEY PASSWORD bytes. Valid and activated KEY necessary (status 14BE or 15EC), both IR and NEC ON-BOARD modes supported. Usage:

- insert real working key, Test state. If key is valid button Collect becomes available;
- now you can **Collect** data from key. It is possible to load previously collected data too.
- it is a good idea to **Collect** data before KEY is dismantled for any actions like PASSWORD reading, dataset is compatible with **MBnec**, you can use it to recover and / or test KEY for consistency.
- For recovery:
  - enter password (or known part of it);
  - press Verify to check if it match;
  - or - mark bytes what are probably known (checkbox below password), press Find;
  - software will try to find missing bytes using brute force starting from 0x00;
  - If 0xFF reached with no success password field becomes red, if success – green;
  - it is possible to terminate process by pressing ESC key and continue again from current value.

Theoretically it is possible to recover all 8 bytes of password using this method, but it may take a lot of time, tens of years on a very advanced computer. In practice it is reasonable to recover up to 4 unknown bytes, not more. So it is not a tool that can solve unknown password problem at all, only tool for verify and restore purposes if some part of data is already known.



Mbhash, **Mbhashtodump software**: search for **MBkey** manual;

MBelv software: search for **MBelv** manual

IMPORTANT NOTES:

- for all optional functions additional activation is necessary (**paid options**);

DISCLAIMER:

all you do you do at your own risk.

(c) RobinDAB '2013 -