MBnec

Mercedes NEC KEY onboard tool

NEC FW28, 35, 40, 51, 57

Software for MBnec:

- MBnec: main software;
- MBeistoesl: pasword conversion tool, KEY PASSWORD to ESL PASSWORD;

MBnec software:

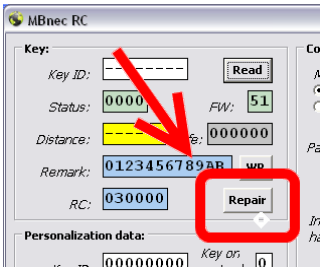
Supported firmware versions: 28,35,40,51,57, possible to prepare and write KEY, possible to read password and initial hash from working key (firmware versions 51 and 57).

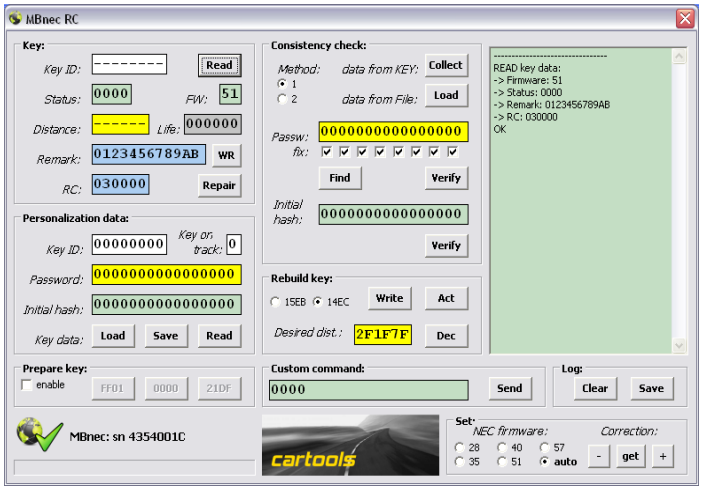
Terms and conventions used:

KEY – we mean NEC from working key soldered on adapter board or placed into ZIF socket;
PREPARE – it is NOT erase, actually we change KEY status to enable necessary actions.

Software features:

- **Key**: data readout, key identification, RC (remote repair), **RC repair** is possible if KEY status is 0000, repair must be done before key rebuilding;
- **Personalization data**: data necessary for KEY rebuild; **Read** is possible if KEY status is 0000;
- **Consistency check**: collect data from key for verify before performing any actions, consistency check, recovery. How to recover data and why it is necessary is described later;
- **Rebuild key**: write key data, activate, decrease distance until desired value reached;
- **Prepare key** window: go for desired KEY status -
  - **FF01** to prepare key for plain write to make a working key or GRAY key (resulting a 14EC status), usually destroys part of data. If trying to go for 0000 after FF01 usually password recovery is necessary (some password bytes are cleared to 0x00);
  - **0000** to read out PASSWORD from working key or repair, use it for FW40, FW51, FW57. **NOTE**: password readout is not possible from FW40 NEC. Sometimes it is a little tricky to get status 0000. May play with corrections (+, -) or decrease distance by one, then repeat procedure until success.
  - **21DF** to prepare key for crypto write (resulting a 15EB status), original data is completely destroyed and not recoverable.
  - before pressing any button you must first enable action (set checkbox). This is done for security reasons, if key is prepared it is not usable without rebuilding. Always collect data for consistency check first!





PASSWORD READING - step by step:

STEP 1: identify key
- read key - to verify firmware and to see current distance. You can copy current key DISTANCE to DESIRED DISTANCE field now, for future use. Key must be in ACTIVATED state (fully working key).
- if car has 2 or more keys, use one with largest LIFE remaining: it is much faster to rebuild it, less counter decrease steps necessary.

STEP 2: collect data for consistency check
- collect key data for consistency check, save data into file (offered when readout is complete). It is not possible to collect data from NOT ACTIVATED key (consistency check is impossible).

STEP 3: prepare key for necessary status
- prepare key - go to status 0000.

STEP 4: read personalization data
- Reading is possible only if status is 0000. If success you will see data on screen. Save data. Sometimes some bytes are lost due to unknown reason. Not a problem to recover them using data collected previously.

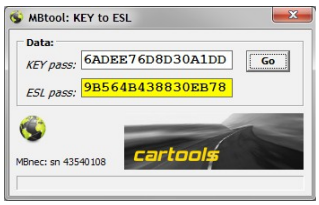
STEP 5: verify and validate key data (consistency check)
- password is copied automatically to CONSISTENCY CHECK window. Questionable bytes where 0 or F exist are replaced by 00 and appropriate check box (FIX) is unchecked. Press FIND to recover these bytes. Otherwise press VERIFY to be sure that everything is OK and you have valid data.
- two recovery methods possible, choose one:
  - method 1: slower, but works 100% (default);
  - method 2: faster, may sometimes fail, depends on how key is activated;
- if it is necessary to recover up to 3 bytes no matter which method to use, it takes some seconds with any method.
- if password is corrected and verified, password field background becomes green. Key ID, Key on track and password fields in PERSONALIZATION DATA window are updated if necessary.
- now you can verify and validate initial hash. To do that valid password is mandatory.
- **IMPORTANT**: do not forget to save data!

STEP 6: rebuild key
- if everything seems to be OK you can rebuild key now.
- write, activate, decrease counters to their previous values. It is possible to avoid counter decrease if you recalculate new initial hash from final hash using key calculation software (MBkey, SKC, online etc...).

SOME USABLE HINTS AND GUIDELINES:

- tool is sensitive to power supplied by USB;
- always prefer PCB instead of ZIF socket, avoid excess of flux;
- tool has not built-in short circuit protection, be very careful! 1st pin orientation is marked on sticker;
- before trying tool on real key with important data inside play with sample chip to be sure everything works fine.

MBeistoesl software:
- password conversion: KEY PASSWORD to ESL PASSWORD;
- conversion time is 10 minutes (safety time).



DISCLAIMER:

all you do you do at your own risk.

(c) RobinDAB '2013 -