MBcan

Mercedes FBS2 / FBS3 logger and tool

for CAN network 125 / 250 / 500 kb

Highlights:

- makes possible to see what happens on CAN wires: authorizations, status, FBS service messages;
- allows to neutralize (renew) FBS components;
- makes possible to personalize older "SERIES" EIS where additional command to K-line is necessary to launch personalization;
- in case of FBS2 and EIS it is possible to calculate key password from CAN and key data.

How to connect:

Although there is an OBD plug, in most cases device must be attached to PT-CAN (powertrain CAN) or control unit directly. Sometimes it is necessary to attach additional 120 ohm CAN terminator.

Device pinout is according to OBD standarts -

- **CAN HI**: pin 6
- **CAN LO**: pin 14
- **GND**: pins 4 and 5
- **K-line**: pins 1 and 7
- **+BAT** (+12v): pin 16 (not necessary while using CAN, mandatory for K-line)

FBS3 functionality:

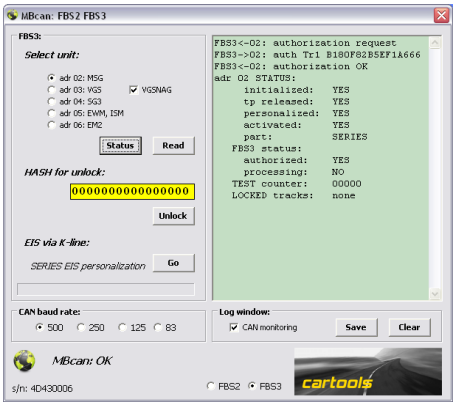
Every FBS3 unit has its own address. ECU has address 02, transmission - 03 etc. EIS itself has 00, ESL - 01. EIS is a master of all FBS3 related communications and is accessible via IR, ESL is a submodule of EIS and is accessible via K-line.

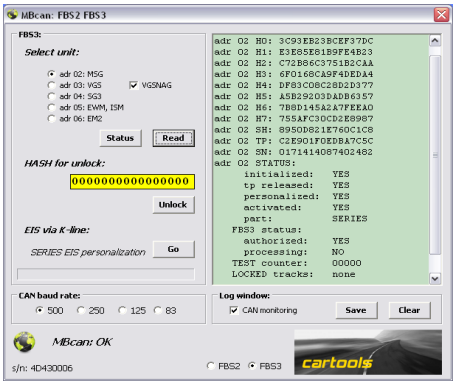
MBcan emulates EIS from a FBS3 unit point of view. Be careful while sending requests to CAN while EIS is alive: EIS see response, but never issued any request by before. That may cause undefined behaviour. CAN line monitoring (logging) is absolutely safe if you are not sending requests.

On picture communication between ECU and EIS is shown (very simple car, only ECU needs authorization). What we see - **1**: ECU send request for authorization, **2**: EIS send response (current track and actual hash), **3**: ECU responds (hash accepted or rejected).

In addition we manually requested **Status** of address 02 and got answer from ECU showing it is authorized now and ready to start. Alternative and more safe way is to request data via EIS using diagnostic session (must see EIS request and ECU response in logger window (if monitoring is enabled)

If more FBS3 modules attached must see activity and communication with all of them (transmission, ISM / DSM etc…). They must initiate authorization requests and EIS must respond to them.





Button **Read** requests hash list from control unit as shown on picture. This function is very useful when working with control units "on the bench" without car. For example to read out SONDER HASH for unit renew jobs or FINAL HASH for FBS3 emulator.

NOTE: hash list and status from 7G control units (automatic transmission) is readable using two different methods. If check box is marked it is read out via diagnostic session like DAS/Xentry does. If unchecked, it is read as ordinary FBS module located on address 03. In this case IGNITION ON signal is mandatory.

Unlock: enter HASH for unlock calculated from actual SONDER HASH (use 3rd party services). Press Unlock. There must be feedback from control unit after some seconds (check what's in logger window). Check status.

NOTE: if wrong HASH is entered FBS3 unit may get stuck for some minutes. It simply tries to calculate impossible things, nothing to worry about. Same thing may happen if you erase coding / VIN by accident before neutralization what is definitely wrong and may cause neutralization procedure to fail.

SERIES EIS personalization: this small K-line job is implemented because personalization command for w210 and similar ones not exist in DAS software at all (HTT only for old EIS). For later units DAS works fine.

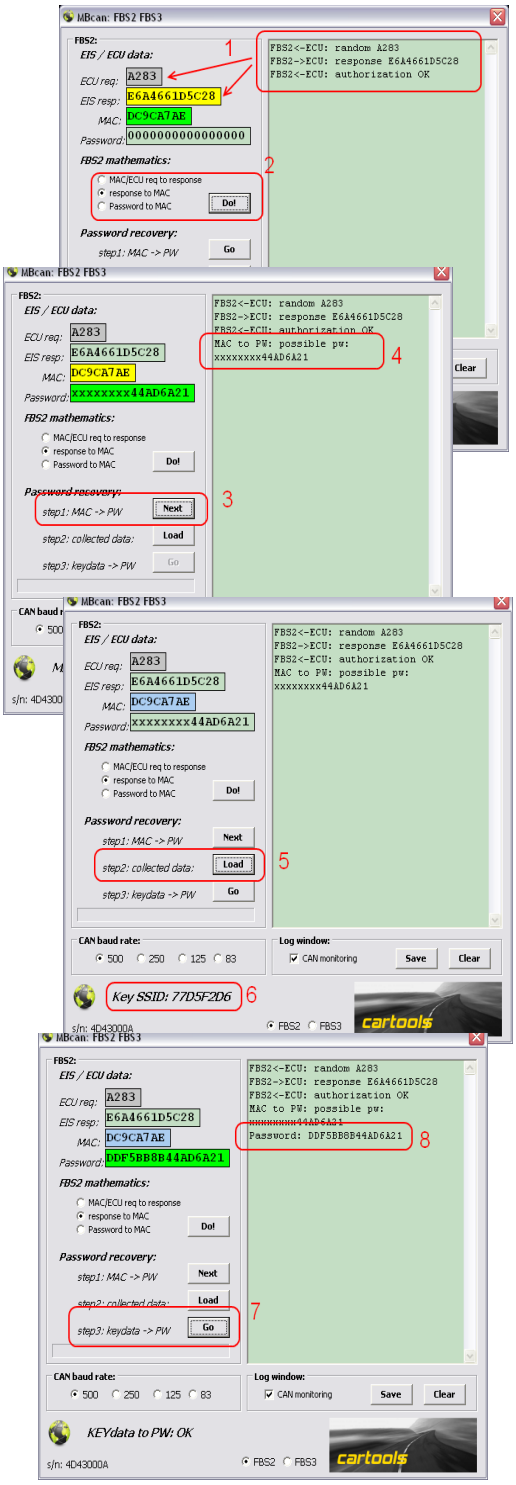
DISCLAIMER: tool is designed for jobs which are not covered by DAS / Xentry / other diagnostic tools. If it is possible to do missing jobs using DAS – it is not out mission.

FBS2 functionality:

Connect MBcan to CAN lines as in case of FBS3, try to start a car. Must see three authorization related messages in log window: random from ECU, response from EIS and authorization result from ECU (accepted or not).

You can play with these values (FBS2 mathematics) to understand what happens and how they are calculated. Common task is to get MAC, it is a function from KEY password. When making calculations result is displayed on green background, incoming data is displayed on yellow background.

If we have valid MAC we can use it to program FBS2 emulator. Or may try to recover KEY PASSWORD from MAC. How to proceed is described below:



step 1: MAC to PASSWORD, press **Go**! Calculation is launched. It is possible to interrupt it at any time by pressing ESC button on keyboard. Full cycle takes about 1 hour at average PC / Laptop. Result is displayed in log window. If success, last 4 bytes of password are recovered (xxxxxxxx44AD6A21 in our case) . More than one result is possible, it is recommended to continue until no more combinations possible (software will say when calculation is finished).

step 2: must load KEY data collection (must use **MBir** and password checker utility to get data from key). If data is OK and loaded, SSID is displayed.

NOTE: it is possible to complete task using MBir password checker utility too, both do same job.

step 3: keydata to password: press "Go" and wait for result.. Overall process may take up to some hours on average PC.

About this method:

- in most cases it is possible to get KEY password much faster using invasive methods and/or using device programmer;
- this method works only if EIS dump isn't corrupted;
- any method is good enough. This is only another way how to do this job..
- advantages: only 5 minutes are necessary to log communications and collect all necessary data. Car is not necessary while calculations take place;
- only older cars covered, usually with HC705 mcu's inside EIS.

MBcan additional functionality:

- usable as a tool for CARTOOLS CAN emulator configuration, all utilities are free of charge for all Mbcan users;
- extended **PSA, VAG, NISSAN** utilities are **paid options** (additional activation necessary) and are not a subject of MBcan basic set.