EWS4 emulator

for BMW 8HP EGS

E-series,

CAN HS 500kB

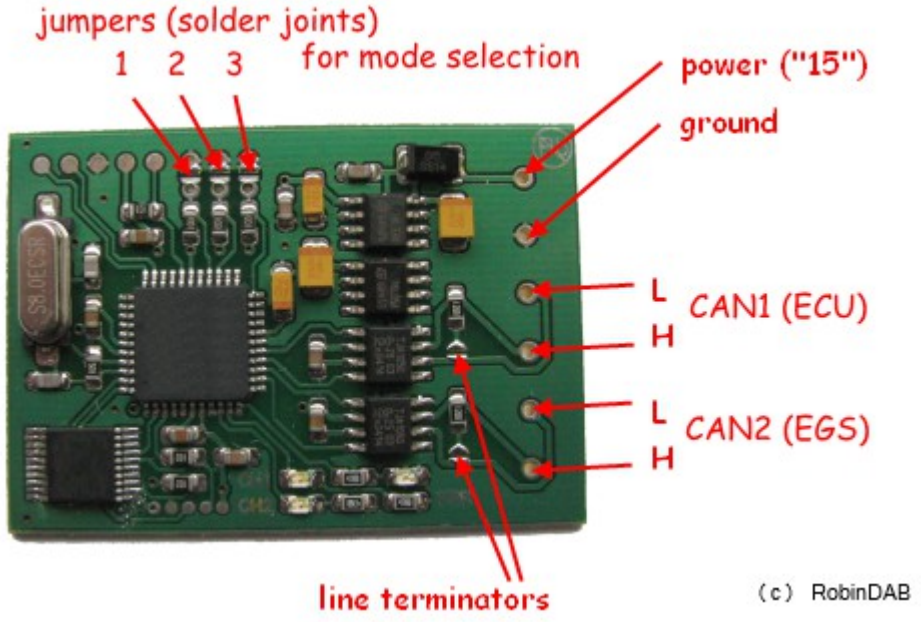
Description:

device allows to integrate replacement EGS with locked SK inside into another car. Two different operation modes possible:

- authorization only – if you already know SK_SERVER you can store it into emulator,
- key agreement and authorization – if you know SK_CLIENT, you can store it into emulator. After key agreement procedure between emulator (ECU) and EGS SK_SERVER is calculated and verified. If SK_SERVER match with one already stored and hard-locked in EGS, it switches to authorized state. If process already finished and EGS is authorized, this mode can be disabled.

Both SK provided here are from ECU point of view: ECU is server for EGS (SK_SERVER), but client for CAS (SK_CLIENT). **SK stored into CAS (for CAS – ECU alignment) is SK_CLIENT**.

How to connect and how to configure:



Jumper meanings:

JUMPER J1 shorted:

Emulator is in configuration mode. J2 and J3 settings are ignored.
It is possible to store and read out SK_SERVER and SK_CLIENT now. Suitable CAN monitor / logger must be attached to CAN1.

To store SK_SERVER:
must send two CAN frames - ID 771 (first 8 bytes) and ID 772 (remaining 8 bytes of SK).

Example: SK to store **`5C2D11C0E0CFB010176AF583C443911B`**
Must send two messages:

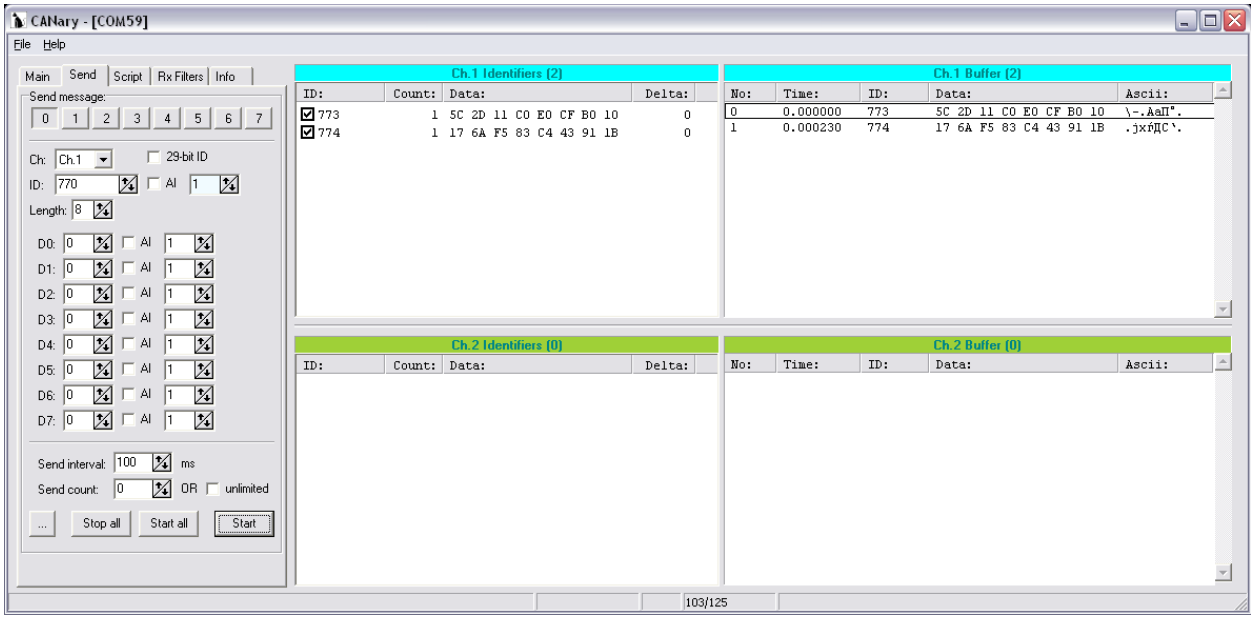
```
771   8     5C 2D 11 C0 E0 CF B0 10
772   8     17 6A F5 83 C4 43 91 1B
```

To read SK_SERVER:

```
770   8     00 00 00 00 00 00 00 00
```

Device responds with two frames: id 773 and 774 with first and last part of SK as data::

```
773   8     5C 2D 11 C0 E0 CF B0 10
774   8     17 6A F5 83 C4 43 91 1B
```



For SK_CLIENT procedure is very similar, only ID's are different. id 781 and id 782 are both used to store SK_CLIENT, id 780 is for read request, id 783 and id 784 – response.

JUMPER J2 shorted:

work mode, authorizations allowed. There must be correct SK_SERVER stored into emulator.

JUMPER J3 shorted:

work mode, authorizations and key agreement allowed. There must be correct SK_CLIENT stored into emulator. J2 settings are ignored. SK_SERVER is updated if key agreement finished. You can read it out from emulator if you wish.

Some notes about hardware:

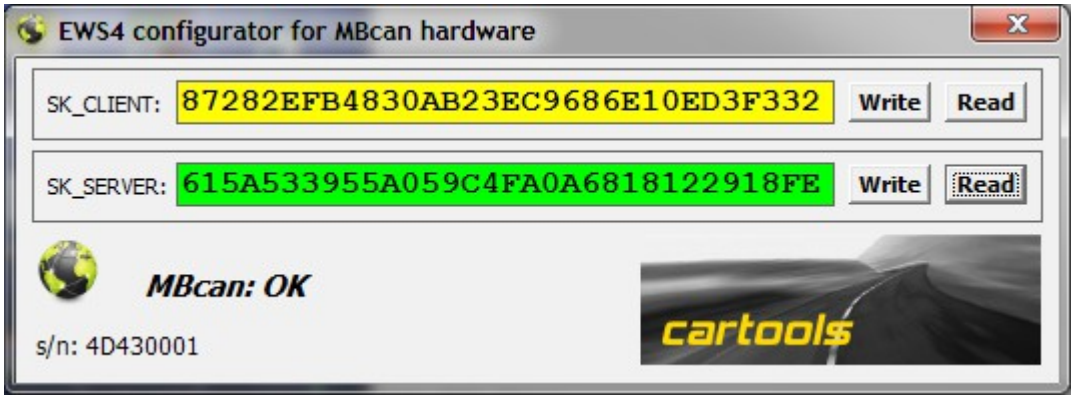
Connection:
Cut CAN wire between EGS and ECU, connect ECU side to emulator CAN1, EGS side to CAN2. In most cases it is recommended to short both jumpers for bus terminators (120 ohm load). Terminal block for screw type connections is not included in standard delivery.

Mode selection:
It is possible to change emulator mode “on the fly” without removing power from it.
If all jumpers are left open, emulator is “transparent”. No any actions, no authorizations. All messages from CAN1 are transferred to CAN2 and from CAN2 to CAN1 as is.

Power supply:
according to usage specifics. Must note that usually device must be powered on for some time even after ignition is switched off to keep communications with EGS alive before car enters into SLEEP mode (use +12 from ECU main relay etc.)

Status LEDs:
CH1, CH2 - yellow, both show activity on CAN subnets,
ERR – red, lights in case of CAN communication errors (buffer overrun, lost messages etc.). It goes on when key calculating takes place too (it doesn't always mean lost messaages, just warning).

Additional software for Mbcan users:
Designed to simplify SK read / write and speed up overall process. Available on request.



cartools