



CAScontrol2 + EGS 6HP / DSG

EWS / CAS emulator and logger,

EWS2, EWS3, EWS-EGS, CAS / ECU dump tool

Highlights:

- You can read EWS2 ISN directly from EWS – ECU communication line.
- You can read EWS3 rolling codes from line and calculate EWS3 ISN from two following rolling codes.
- It is possible to use tool as EWS2 or EWS3 emulator.
- It is possible to unblock EGS 6HP via CAS_BUS line if RAM is readable from EGS or ISN is known.
- Dongle is useful for various calculations – CAS dump explorer, KEY decrypt, ISN extract from dump, ISN restore from rolling codes etc.

Connection:

- EWS line, +12v, GND – pins are marked on opposite side of dongle
- Must note that pullup inside dongle is weak, must use external pullup (500...1K ohms) if using device as emulator. Or pull-down to ground when monitoring CAS / EWS without ECU attached. Observe what LED does – must flash periodically if line is alive and there are messages on it. If you are logging fully working system (ECU + CAS/EWS) no any additional action necessary.
- Choose **action** you wish...

EWS2 mode: everything is as simple as possible:

Send – ISN is sent to line,

Read – ISN is logged from line.

In case of EWS2 ISN is always 12 bit long. That's why first digit is always replaced by 0.

EWS3 logger mode:

Calc - get ISN from RC1 and RC2 values. ISN box is highlighted in green if ISN is calculated.

Read – continuously read rolling code from line.

If 10 valid rolling codes are read out from line, RC1 box is updated. Now switch off ignition, turn it on again. If new (updated) rolling code received, software waits for another 10 valid codes to be sure they all match each together, then updates RC2 box and calculates ISN.

In case of EWS3 ISN is 16 bits (2 bytes) long, rolling codes are 32-bit values.

EWS3 emulator mode:

Align - send ISN for alignment with ECU. Alignment procedure is described in official BMW documents. In some words:

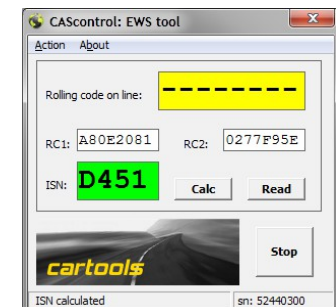
- step1: must set EWS / CAS or emulator for alignment, fixed ISN code is sent to ECU now,
- step2: must send command for ECU to accept this value. Use INPA, DIS, Tool32 or any other suitable diagnostic tool.

NOTE: INPA script tries to communicate with CAS/EWS first. Must ignore error and continue!

Send – continuously sends rolling code to line.

Next RC – next rolling code is calculated. If button is pressed when send takes place, new rolling code is transferred immediately to line. Otherwise displayed only.

Proceed as CAS – check this box if ECU wish to see CAS instead of EWS. Don't worry about this option, for most of known ECU's it doesn't matter at all.



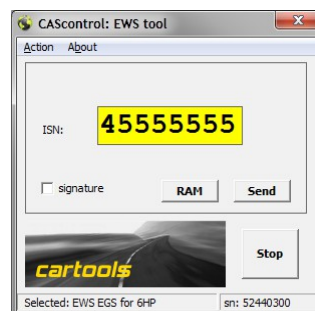
EWS-EGS for 6HP / DSG:

Send - send ISN (or ISN signature if check box marked) to EGS.

Or:

RAM – load RAM from file and send what is necessary for EGS. If RAM file is valid, ISN box becomes green. Otherwise warning message displayed.

Then you may use any diagnostic tool to check EGS status and unlock it (reset ISN) if necessary.



Some things to know:

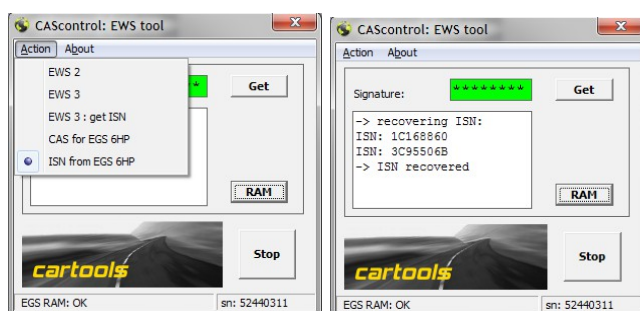
- CAS transmits messages to EGS via CAN network and via **CAS_BUS**. If three invalid messages are received EGS goes into "tampered" mode - **STAT_AUTHENTICATED_WERT = 2**. No more messages accepted, no matter if valid or not until EGS is restarted. If necessary you must disconnect CAS or cut CAN wires to authorize EGS using CAScontrol2.
- On startup must see **STAT_AUTHENTICATED_WERT = 0**.
- EGS is authorized (no matter via CAS_BUS or via CAN) if **STAT_AUTHENTICATED_WERT = 1**.
- EGS-ISN is 4 bytes long, usually last 2 bytes are common with ECU.

ISN calculation for EWS-EGS (optional):

RAM – load RAM from file, then

GET – calculates all possible (valid) ISN values for actual EGS data.

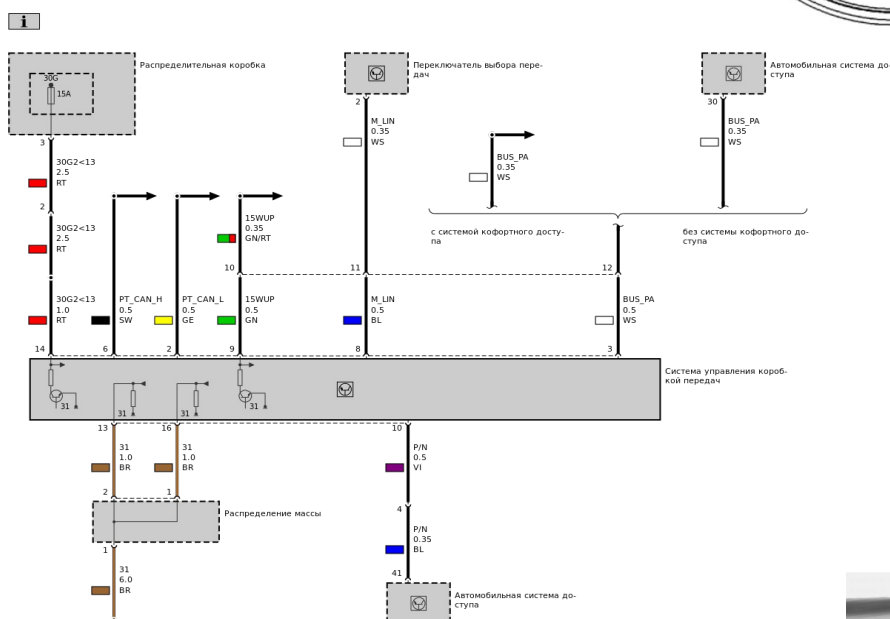
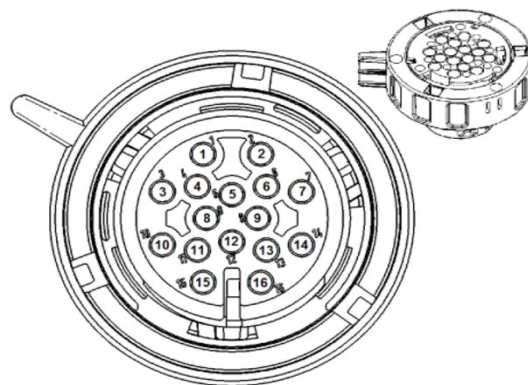
Additional tables for calculation (16 Gb) must be installed locally on PC, located at C:\CRT\



Connection to EGS 6HP (GS19D) – it is a good idea to make some wiring harness:

pins 9, 14: +12v;
pins 13, 16: GND;
pin 6: PTCAN Hi;
pin 2: PTCAN Lo;
pin3: PA_BUS (CAS_BUS)

CAScontrol line must be connected directly to PA_BUS. Diagnostic tool you can attach directly to PTCAN. Terminate CAN with 120 ohm resistor.



(c) RobinDAB '2011 - 2026

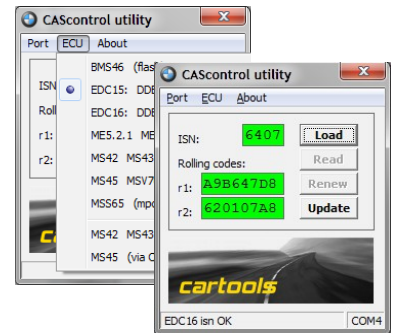


DUMP TOOLS:

1. ECU: ISN from dump or via OBD socket

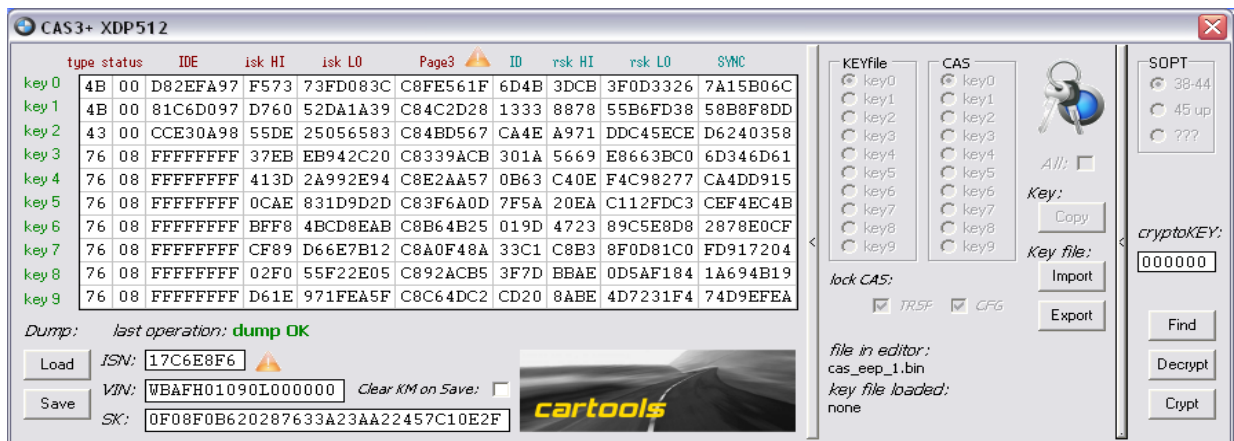
supported ECU's:

- BMS46 - flash dump,
- EDC15: DDE3, DDE4 - eeprom,
- EDC16: DDE5 and up - eeprom,
- ME5.2.1, ME7.2, ME9, ME9+ (ME9.2) - flash,
- MS42, MS43, MS45, MS45.1 - flash or via OBD
- MSS54 - flash,
- MSS65 - MPC dump



in case of EDC it is possible to view / edit stored rolling code map: you can check it for consistency if you wish. All checksums are recalculated at file save.

2. CAS1 CAS2 CAS3 CAS3+ dump tool:



Designed to explain CAS, copy keys from one dump to another etc.

Software shows any checksum errors (red highlights) and correct them at save. It is possible to export and import key/keys from one CAS dump to another through key file, clear mileage, read and change ISN. Allows to crypt / decrypt CAS data (both types of crypto supported).

It is possible to copy complete key data into separate file (KEY FILE), import any key into another dump to any place. Exported KEY FILE is accepted by HTpro Hitag2 key programmer too.

If CAS is crypted and you are trying to decode it via EWS3 ISN (need real and full 4 bytes as for EGS) :

SOPT 38 - 44: there are 16 possible answers. If CAS works in EWS3 mode any is good. If EWS4 mode is active only one is valid, must test then all for validity until correct one found. It is a good idea to use EWS4 emulator for such purpose.

SOPT 45 and up: 64 possible answers instead of 16, same story.

If CAS is decrypted using SK (EWS4) or real Page3 there is only one correct answer – you can read Page3 from existing key using key reader by entering correct key password: key isk LO and isk HI.

NOTE: you can update key data only if CAS is in decrypted state. Otherwise unrecoverable file damage may occur.

3. ISN restore from rolling codes (CAS in EWS3 mode)

Use utility if:

- ISN is lost by accident;
- dump is crypted and you need to know real ECU ISN.

Choose CAS type, load dump, press **Go**. If success you will see calculated ISN. Press **Go** once again, must see same ISN value at different calculation **step**.

