BINUNLOCK LLC

Professional vehicle diagnostic software

EME Replacement Solutions

Responsible workflow and EEPROM decision guide

A high-level companion to emeOBD for authorized BMW G30 EME replacement work: evidence capture, EEPROM acceptance and signature interpretation, ISN-reset decision gates, commissioning boundaries, validation, and escalation.

ENGLISH · WINDOWS · 12 AUGUST 2026

Qualified technicians only.
This publication intentionally does not contain high-voltage disassembly, depowering, measurement, hot-air, soldering, bypass, programming, or security-circumvention instructions. Use current OEM service information and locally required HV procedures.

PUBLICATION

Contents and document control

This is a clean BinUnlock companion guide for the current emeOBD application. It explains decision and evidence boundaries without reproducing or substituting physical repair instructions.

PRODUCT
emeOBD

PUBLISHER
BinUnlock LLC

DOCUMENT
EME Replacement Solutions

OFFICIAL SITE
https://binunlock.com/

APPLICATION FILE NAME
`Document of EME.pdf`

EDITION
English · 12 August 2026

READ THE OPERATING GUIDE TOO

How to use.pdf is the control-by-control manual. This document focuses on responsible replacement decisions, file interpretation, and workshop gates.

NO IMPLIED REPAIR APPROVAL

The existence of an emeOBD button, an accepted file size, an extracted VIN, or a 16-byte ISN does not authorize or validate a replacement.

CHAPTER 01

Safety and authority boundary

EME replacement may place personnel near a high-voltage powertrain and may affect immobilization, drive readiness, charging, and network security state. Software output cannot certify any of those conditions.

QUALIFIED PERSONNEL AND CURRENT OEM INFORMATION

Vehicle preparation, depowering, absence-of-voltage verification, removal, transport, storage, installation, reconnection, measurement, programming, and return-to-service must be performed only by appropriately trained and authorized personnel under current vehicle-specific OEM instructions and applicable law.

Non-negotiable stop conditions

- [ ] Vehicle ownership or work authorization unclear
- [ ] Qualified HV personnel unavailable
- [ ] Vehicle electrical state is unknown
- [ ] Replacement-part provenance/compatibility unknown
- [ ] Source EEPROM provenance or read quality uncertain
- [ ] Physical VIN does not match job record
- [ ] Current OEM repair information unavailable
- [ ] Support power cannot be stabilized
- [ ] Original diagnostic evidence not preserved
- [ ] Recovery/commissioning path unavailable

Responsibilities by domain

Domain	Responsible authority	emeOBD role
HV safety and physical work	Qualified technician + current OEM/local procedure	None; the application does not establish or display HV-safe state.
Replacement compatibility	OEM parts/programming information and authorized workshop decision	Displays identity/software-root evidence only.
EEPROM provenance	Workshop acquisition/read process and chain of custody	Checks length and simple byte patterns only.
ISN reset decision	Authorized repair plan and operator	Extracts supported data and sends the active reset request when selected.
Commissioning and handover	OEM process, approved diagnostic/programming tools, qualified technician	Supports identity and DTC evidence; does not certify completion.

LAWFUL USE

Use the tool only on vehicles and data you are authorized to service. Do not use the reset operation to defeat security controls, conceal provenance, or bypass a required authorization process.

CHAPTER 02

What emeOBD can and cannot establish

Verified active capabilities

- Discover a responding BMW gateway by directed IPv4 broadcast.
- Read BMW MAC/CAR VIN text, EME VIN, and recognized software-root records.
- Accept only three exact EEPROM file lengths.
- Search WBA/WMW/5UX VIN candidates in strict prefix priority.
- Recognize four specific signature branches and extract 16 bytes for two of them.
- Send one G30 EME ISN-reset transaction.
- Build structured normal and shadow DTC reports from catalogue matches and current vehicle context.
- Send normal/shadow erase and EME reset requests.
- Save every visible DTC report line and export the current manuals.

Outside the application

- Part-number and hardware/software compatibility determination.
- EEPROM checksum, authenticity, completeness, or source validation.
- HV isolation, removal/installation, opening, rework, measurement, or repair.
- Programming, flashing, coding, vehicle-order changes, or full commissioning.
- Security authorization, seed/key calculation, or bypass.
- Complete UDS response and DTC status decoding.
- Functional safety, Ready state, gear selection, charging, or roadworthiness certification.
- Legal ownership or data-use authorization.

Evidence strength

emeOBD observation	What it supports	What it does not prove
Gateway row with VIN	A UDP peer returned text containing the expected VIN marker.	Cryptographic responder identity or physical vehicle match.
Connected identity fields	The selected network route returned parseable identity/root data.	Replacement compatibility or completed commissioning.
Accepted EEPROM length	The file has one of three expected byte counts.	Correct family, intact read, checksum, or provenance.
32-character EME ISN	A Kind 3/4 signature yielded 16 bytes at its defined offset.	That the value belongs to the selected car or should be written.
Reset definite-success branch	The final response bytes met the application's C0 01 test.	Complete vehicle-level replacement success.
DTC report count 0 / `(NO DTC)`	No catalogue key was listed; silence or an absorbed post-connect I/O failure may produce the same structured report and completion modal.	A valid response or fault-free ECU.

USE EVIDENCE IN COMBINATION

A responsible decision combines physical VIN, work order, OEM part data, approved diagnostics, gateway/EME identity, software roots, source-file provenance/hash, before/after DTC, and functional validation.

CHAPTER 03

Job intake and replacement decision

Do not begin with the reset button. Begin with a documented failure, approved test plan, identity set, and a replacement strategy validated through OEM sources.

1. Record customer complaint, vehicle identity, mileage, current drive/charge symptoms, and prior repair/programming history.
2. Obtain owner/work-order authorization for diagnosis, data handling, control-unit replacement, and any security-relevant operation.
3. Use the approved diagnostic system to capture the complete vehicle test, EME identification, normal/shadow/event memories, measured plans, and relevant power/network faults.
4. Determine through the authorized repair plan that EME replacement—not wiring, power, cooling, network, software, another ECU, or an external component—is required.
5. Verify replacement part provenance and hardware/software applicability using current OEM part/programming information. emeOBD software roots are supporting evidence, not the compatibility authority.
6. Define whether an ISN reset is actually required, what source data is approved, and what programming/coding/commissioning steps follow.
7. Confirm that qualified personnel, safety equipment, stable power, programming capability, and a recovery path are available for the entire job.

Replacement readiness table

Question	Pass evidence	Fail response
Is the EME the diagnosed root cause?	Approved diagnostic test plan and recorded results.	Continue diagnosis; do not replace on DTC text alone.
Is the replacement correct?	OEM part/supersession and programming applicability confirmed.	Quarantine the part.
Is source data trustworthy?	Known unit/read method, exact byte count, hash, immutable original, repeatability where required.	Acquire a correct read through an approved process.
Can the job be commissioned?	Required authorized programming/coding tools and procedure available.	Do not remove/install prematurely.
Can failure be recovered safely?	Power, communication, original files, reports, escalation contact, and approved recovery steps ready.	Stop before mutation.

DTC IS NOT A PARTS ORDER

emeOBD catalogue lines are substring matches in complete response hex. They must be confirmed with full diagnostic status, fault conditions, measured tests, and the vehicle-specific repair plan.

CHAPTER 04

EEPROM file acceptance

Open eeprom works entirely offline. Its click clears the visible EEPROM VIN and EME ISN fields before the picker opens. Cancel performs no file work, but those fields remain blank. For a selection, it checks exact length before reading all bytes and performing simple searches. File acceptance is a parser gate—not a quality certificate.

512 KiB	768 KiB	848 KiB
`0x80000` · 524,288 bytes	`0xC0000` · 786,432 bytes	`0xD4000` · 868,352 bytes

File-handling procedure

1. Acquire the source binary through the approved read procedure for the identified unit. This guide does not describe hardware access or reading.
2. Store the untouched original in a protected, read-only job folder. Record source unit, operator, tool/method, time, and exact byte count.
3. Calculate a cryptographic hash using the workshop's approved evidence tool and record it. Create a separate working copy.
4. Select **Open eeprom**; the fields clear before the picker. Choose only the working copy. If you cancel, no file is read and the fields remain blank.
5. Compare the accepted length with the acquisition record. Record the displayed VIN candidate, ISN result/message, and bottom status. Do not modify the file to influence the parser.

Rejected-file rules

Observation	Interpretation	Required action
Different byte count	The active parser refuses the file before VIN/signature analysis.	Verify source family and acquisition. Re-read through the approved method if required.
Accepted length, no VIN	No WBA/WMW/5UX candidate was found by the simple priority search.	Do not insert a VIN. Verify dump provenance/completeness.
Accepted length, no ISN signature	None of the supported branches matched in the scanned range.	Do not infer zero ISN or use stale button state. Escalate applicability/read quality.
File changes between checks	Working data is unstable or another process modified it.	Stop, preserve both hashes, and reacquire a controlled copy.

NEVER FORCE ACCEPTANCE

Padding, truncating, duplicating, concatenating, or editing bytes to reach an accepted size destroys evidential value and may produce false signature/VIN matches.

CHAPTER 05

VIN and ISN signature interpretation

VIN candidate search

The full binary is searched in fixed prefix priority: `WBA` first, then `WMW`, then `5UX`. The first hit for the first prefix present wins. At most 17 characters are copied from that location; a near-end hit is shorter.

The search does not require a formal EEPROM record, printable 17-character VIN, check digit, or match to the connected vehicle.

Four ISN branches

Kind 1

`28 17 00 00 00 00 00 00`

Displays the F-series/MDG1 no-EME-ISN message and disables reset.

Kind 2

`17 28 00 00 FF FF`

Same visible message and disabled state.

Kind 3

`83 6A 00 00`

Requires bytes +4/+5 not both zero. Extracts 16 bytes at signature +45 and enables reset.

Kind 4

`6A 02 00 00 FF FF`

Extracts 16 bytes at signature +61 and enables reset.

Search order and boundary

- At each candidate offset, Kind 1 is tested before Kind 2, then Kind 3, then Kind 4.
- The scan advances from the beginning only through `Length - 200`.
- Supported-looking signatures in the final 199 bytes are ignored.
- The first supported branch encountered is used; later candidates do not replace it.
- Kind 3 and Kind 4 render exactly 16 bytes as 32 uppercase hexadecimal characters without separators.

WHAT TO RECORD

File name, original/working hashes, exact byte count, VIN candidate, branch kind, signature offset from an approved independent analysis if needed, 32-character result, and reset enabled/disabled state.

FALSE-POSITIVE POSSIBILITY

These are byte-pattern searches, not a schema-aware EEPROM decoder. A coincidental signature and in-range bytes can satisfy the parser. Validate source family and data through authorized technical evidence before writing anything.

CHAPTER 06

Reset eligibility and state hazards

The UI preserves several exact legacy state rules. A qualified operator must understand them because the enabled button alone is not an eligibility decision.

Latest file result	Visible ISN field	Reset button state	Meaning
Kind 1 or 2	F-series/MDG1 message	Explicitly disabled	The parser selected a no-EME-ISN branch.
Kind 3 or 4	32 uppercase hex characters	Explicitly enabled	The parser extracted 16 bytes at the branch's fixed offset.
No supported signature	No valid 32-character result	Previous state preserved	The enabled/disabled appearance may belong to an earlier file.
Fresh application, before file	Blank/dash display	Starts enabled	This matches active form behavior; it is not permission to run.

CRITICAL UI RULE

A fresh or stale enabled button can coexist with an empty/invalid ISN. The reset decoder also accepts empty input, ignores an odd final nibble, and removes only ASCII spaces. Therefore the operator—not the enabled state—must enforce a verified 32-character Kind 3/4 result.

Pre-reset data gate

- [ ] Current file open completed without error
- [ ] Accepted exact file length
- [ ] Kind 3 or Kind 4 applicability established
- [ ] No manual edits or separators
- [ ] Current file hash matches job record
- [ ] Expected VIN candidate independently reconciled
- [ ] Visible ISN contains exactly 32 hex characters
- [ ] Correct car and ZGW freshly identified

Decoder edge cases

Input	Decoder behavior	Safe policy
`AA BB …`	ASCII spaces are removed, then pairs decoded.	Use the parser's own no-separator result.
Odd number of characters	Last nibble silently ignored.	Reject locally; never dispatch.
Empty string	No appended ISN bytes.	Reject locally; never dispatch.
Non-hex pair	Parse exception enters operation error branch.	Return to the source file; do not guess.

CHAPTER 07

Pre-replacement evidence workflow

Capture a reproducible Before state while the original installation and communication route are still available. This evidence becomes essential if programming, replacement, or reset changes network identity or fault memory.

1. Verify the BinUnlock LLC-signed application, active customer, and license expiry. Record the release identification used by the workshop.
2. Prepare stable vehicle support power and the approved diagnostic Ethernet route. Close competing sessions.
3. Select **Scan Network**, scan, and match the returned VIN to the physical car.
4. Highlight the verified row and select **Select ZGW IP**. Its handler copies the peer IP, closes/hides the scan window, then automatically invokes the main **Connect to CAR** action. Observable I/O begins in that chained Connect route.
5. Wait for the automatic Connect workflow to finish, then record ZGW IP, BMW MAC, BMW CAR VIN, EME VIN, connection status, and the complete BTLD/SWFL/HWEL output.
6. Select **Read Error**. Save the visible list as the immutable normal Before report.
7. Select **Read shadow**. Save the visible list as the immutable shadow Before report.
8. Export/save a complete approved diagnostic-system report outside emeOBD, including full fault status and ECU identification.
9. Preserve every authorized source binary with acquisition notes, exact byte count, and hash before physical work begins.

Before-state record

Artifact	Minimum content	Purpose
Vehicle identity	Physical VIN, work order, registration/asset context as permitted.	Prevents cross-vehicle selection.
emeOBD identity	ZGW IP, BMW MAC/CAR VIN, EME VIN, roots, timestamp.	Documents network/control-unit state.
Normal DTC Before	Visible list + operation status + timestamp.	Preserves standard memory evidence.
Shadow DTC Before	Separate visible list + status + timestamp.	Preserves shadow memory evidence.
OEM diagnostic report	Complete vehicle test, statuses, ECU IDs, test-plan findings.	Provides authoritative interpretation beyond substring matches.
Source data	Original file, working copy, source unit/method, length, hash.	Supports provenance and recovery.
Replacement data	Part number, serial/label, provenance, applicability decision.	Supports compatibility and chain of custody.

SAVE BEFORE ERASING

Erase operations can remove diagnostic evidence. A replacement job must not begin with clearing faults merely to simplify the screen.

CHAPTER 08

Physical-work boundary

This guide deliberately stops at the handoff to qualified physical service work. The safe sequence, special tools, electrical state, measurements, waiting periods, fasteners, seals, cooling procedures, and part handling are vehicle- and market-specific.

A

Software evidence complete

Before identities, roots, DTC reports, OEM diagnosis, data provenance, replacement applicability, and recovery plan are recorded.

B

Qualified physical procedure

Authorized personnel follow current OEM HV/vehicle instructions. emeOBD is not used as an electrical safety indicator.

C

Return to controlled software state

Only after the physical procedure declares the vehicle ready for diagnostics/programming does the approved commissioning workflow resume.

Topics intentionally not provided

- High-voltage depowering or isolation steps
- Absence-of-voltage test points or meter use
- Connector, cover, busbar, or fastener sequences
- Cooling-system opening/filling/bleeding
- Module opening, sealing, or internal access
- Hot-air, soldering, desoldering, or bench wiring
- EEPROM hardware reading/writing methods
- Security bypass or authorization circumvention
- Programming/coding sequences or data packages
- Vehicle Ready/drive/charge test conditions

Handoff checklist

- [ ] Named qualified technician accepts the task
- [ ] Vehicle-specific HV classification understood
- [ ] Replacement unit and seals/consumables verified
- [ ] Source files and diagnostic reports secured
- [ ] Correct current OEM procedure identified
- [ ] Required PPE/tools/controlled area available
- [ ] Original/replacement identifiers photographed/recorded
- [ ] Software operator knows when diagnostics may resume

DO NOT IMPROVISE FROM GENERIC INSTRUCTIONS

Even a technically plausible generic disassembly or hot-work sequence may be unsafe or wrong for the exact vehicle/part revision. Stop and obtain the correct authorized procedure.

APPLICATION STATE DURING PHYSICAL WORK

Close emeOBD only while idle. Do not leave an active diagnostic or reset operation running while power, network, or hardware connections are changed.

CHAPTER 09

ISN reset and commissioning boundary

Use emeOBD's ISN reset only when the approved replacement plan explicitly calls for it and every current-state check passes. Programming, coding, authorization, and final commissioning remain external responsibilities.

Pre-dispatch decision

Gate	Required evidence
Authorization	Documented lawful repair authorization and approved step calling for the reset.
Vehicle identity	Physical VIN, work order, fresh ZGW selection, BMW CAR VIN, and EME VIN reconciled.
Source data	Known file provenance/hash, accepted length, expected VIN candidate, verified Kind 3/4 branch, exactly 32 hex characters.
Vehicle state	Physical work completed and current OEM procedure declares the vehicle ready for the diagnostic action.
Communication/power	Fresh stable connect, no competing session, correct supported power state.
Recovery	Plan for definite success, ambiguous response, timeout, and communication loss.

NO CONFIRMATION OR SHARED HOST CHECK

Clicking **Run and reset EME ISN** is the commit point. The application immediately constructs a fresh TCP client using the ZGW field text verbatim; empty, whitespace-only, or malformed text reaches the socket/error branch.

Active response boundary

- The application creates a new TCP/6801 connection and sends one C001 write request containing the decoded ISN.
- There is no active SecurityAccess/seed-key sequence in this operation.
- Final remaining response bytes `C0 01` select the definite-success branch.
- Every other nonexceptional response selects the “Possible that the EME ISN is reset” branch.
- A connection/parse/I/O exception does not establish final ECU state.

Commissioning handoff

1. Record exact emeOBD result and time; do not paraphrase an ambiguous result as success.
2. Allow the network/control unit to settle under the approved procedure.
3. Rediscover/reconnect and record current identity and software roots.
4. Use authorized OEM tools and data for any required programming, coding, security authorization, teach-in, or validation.
5. Do not erase faults until the Before evidence is secure and the diagnostic plan calls for it.
6. Complete the validation gates on the next pages before handover.

CHAPTER 10

Post-work validation

Validate at four levels: identity, communication, diagnostics, and vehicle function. An application dialog is never the sole handover criterion.

1	2	3	4
Identity correct car, gateway, EME VIN, roots, programmed/coded part	**Communication** stable reconnect after all resets and required sleep/wake cycles	**Diagnostics** complete OEM vehicle test plus normal and shadow evidence	**Function** OEM-defined safety, drive, charging, thermal, and handover checks

1. After the approved physical/programming work, restore the vehicle to the defined diagnostic state and allow all relevant ECUs to boot.
2. Run a fresh emeOBD network scan and match the displayed VIN to the vehicle. Select the verified row; the route copies the IP, closes/hides Scan, and automatically invokes **Connect to CAR**.
3. After that chained Connect action finishes, record BMW MAC, BMW CAR VIN, EME VIN, connection status, and software roots. Compare with Before data and the intended replacement/programming result.
4. Read normal EME DTC. Save a new, uniquely named After report before erasing.
5. Read shadow EME DTC. Save a separate After report.
6. Run a complete approved diagnostic-system vehicle test. Interpret statuses and execute required test plans.
7. Erase only when the repair plan requires it; then reconnect/re-read rather than relying on the erase completion message.
8. Perform current OEM commissioning and functional tests, including every safety-related check applicable to the exact vehicle.
9. Resolve or formally document every remaining fault. Do not hand over a vehicle with unknown readiness, charging, drive, thermal, network, security, or HV state.

Handover gate

Item	Pass condition
Identity	All physical, OEM-tool, and emeOBD identifiers are reconciled and expected.
Software state	Required programming/coding/authorization completed and documented by the approved tool.
Diagnostics	Normal/shadow and full vehicle results reviewed; remaining faults have an approved disposition.
Function/safety	Every OEM-defined return-to-service test passed under the required qualified conditions.
Records	Before/After evidence, files/hashes, parts, actions, outcomes, and approvals stored in the work order.

CHAPTER 11

Troubleshooting and escalation

Finding	Responsible response	Unsafe shortcut to avoid
Source length is unsupported	Verify unit/family and approved acquisition. Re-read correctly if required.	Padding or truncating to an accepted length.
VIN candidate absent or wrong	Quarantine the data, verify source/provenance, and compare with independent decoding.	Editing the binary or ignoring mismatch.
Kind 1/2 message	Reset is explicitly disabled. Reassess family/applicability under the repair plan.	Trying to bypass the disabled state.
No supported signature	Preserve file/status and validate applicability/read quality independently; the prior Reset ISN enabled/disabled state is preserved.	Using the button based on whichever prior state remains.
Multiple plausible signatures	Remember the first supported branch wins. Use independent structure-aware analysis before deciding.	Choosing a later value by preference.
Gateway/EME identity mismatch	Stop, restore controlled network conditions, rescan, and reconcile the physical car.	Proceeding because connection status says Connected.
ISN result is not exactly 32 hex characters	Reject before dispatch and return to the current-file parse/provenance check.	Typing, trimming, or completing it by guess.
Ambiguous ISN-reset response	Preserve exact message, determine current ECU state, and escalate through the approved recovery plan.	Blindly clicking reset again.
Timeout/communication loss during reset	Maintain safe power, record time/error, reconnect only when permitted, and diagnose current state.	Power-cycling or disconnecting in panic.
Erase/reset “success” but state unchanged	Response content was not positively validated. Re-read and use approved diagnostics.	Repeating state-changing commands.
DTC report count 0 / `(NO DTC)`	Treat as ambiguous; verify endpoint/response with complete diagnostics.	Declaring a valid response or fault-free EME.
Vehicle fails OEM functional gate	Stop handover, preserve all evidence, and continue approved diagnosis/recovery.	Erasing faults to obtain a clean report.

ESCALATE WITH STATE, NOT JUST A SCREENSHOT

Provide the full before/after chronology, vehicle/part identities, network/power conditions, file size/hash/provenance, branch/result, exact action and message, software roots, complete diagnostic reports, and every attempted recovery step.

PRESERVE CURRENT STATE

After an unexpected mutation outcome, stop unnecessary resets, erases, programming attempts, sleep/wake cycles, and file changes. Each uncontrolled change can remove evidence or alter the recovery path.

CHAPTER 12

Records, privacy, and support

A complete replacement record connects authorization, diagnostic reasoning, parts/data provenance, safety handoffs, software actions, and final functional validation.

Record group	Recommended contents
Authority and safety	Work authorization, repair-plan reference, qualified personnel, HV/physical-procedure completion record, safe handoff times.
Vehicle and parts	Physical VIN, work order, original/replacement part numbers and identifiers, provenance, applicability decision.
Application	emeOBD release/signature check, registered customer/expiry, workstation/Windows context.
Network identity	ZGW IP, BMW MAC/CAR VIN, EME VIN, roots, before/after timestamps.
Source data	Original and working file names, exact lengths, hashes, source unit/method/operator/time, parser branch/result.
Actions	Every read, erase, reset, ISN-reset, programming/coding step, exact time, operator, and complete outcome.
Diagnostics	Before/After normal and shadow exports plus complete approved diagnostic-system reports.
Handover	Commissioning reports, remaining-fault disposition, OEM functional/safety tests, approver, customer notes.

Data protection

- VIN, HWID, license, diagnostic, EEPROM, part, and customer records may be sensitive. Apply the work-order system's access, encryption, retention, and deletion policy.
- Keep immutable originals separate from working copies. Never overwrite the only Before report.
- Share only what the authorized support case needs; redact unrelated customer information.
- Do not post license files, EEPROM binaries, full VIN/HWID screenshots, or customer reports publicly.

Suggested job structure

```
Vehicle_<VIN>/
  00_Authorization_and_Safety/
  01_Identity_and_OEM_Diagnosis/
  02_EEPROM_Original_ReadOnly/
  03_EEPROM_Working_Copy/
  04_DTC_Before/
  05_Operations_and_Programming/
  06_DTC_After/
  07_Commissioning_and_Handover/
```

OFFICIAL SUPPORT

Use https://binunlock.com/. The green favicon in emeOBD opens the same fixed address.