MIB2 Harmann MMI how to unlock (CP off, Navi, Carplay)

Step 1. Required Components
- UART -> USB Adapter (Amazon Amazon)
- PuTTY or similar terminal app
- IDA Pro ($$$$$), Ghidra (free), or similar ARM V7-A compatible disassembler
- SD Card
- Linux computer to unpack + repack filesystem
- dumpifs and mkxfs from QNX SDP / OpenQNX. Build these from source on your linux machine to ensure proper compatibility. (available at https://github.com/ibreakifix/PorschePCMStuff pre-built for Ubuntu 19.04 x64)
- mkxfs attributes file from https://github.com/ibreakifix/PorschePCMStuff

Step 2. Connect to PCM4 via UART
- Connect GND to GND (PCM4 chassis works), RX on adapter to J5_TX on PCM4, TX to J5_RX on PCM4; pins B3 and B9.

https://cimg1.ibsrv.net/gimg/rennlist.co...3b16c3.jpg
- To connect, you can remove the connector block from the quad-lock, then route your TX/RX/GND pigtails through the opening.
- Open PuTTY, launch a serial connection to your COM port (see devmgmt.msc) - 115200, 8, N, 1
- Login with root / oaIQOqkW

Step 3. Download Root-IFS
- Issue the "stfu" command to stop verbose logging to the terminal.
- Insert SD card into PCM4, left slot
- Issue the following command to download your filesystem: "dd if=/dev/fs0 of=/net/mmx/fs/sda0/PCM4_NOR.bin".
- Issue the following command to copy your existing FEC file: "cp /mnt/efs-persist/FecContainer.fec /net/mmx/fs/sda0/orig_FecContainer.fec"
- Remove SD card and insert into your PC.
- You can also pull this image from an update SD card at ./RCC/ifs-root/*/default/ifs-root.ifs
Note: The desired image is the second ifs contained within this update file, use ctrl+f and find the second instance of file magic "EB 7E FF", your IFS image begins at this location and ends at the end of the file. If you do this, you can skip steps 4.1 to 4.3

Step 4. Unpack Root-IFS (if using downloaded image from PCM4)
- Open downloaded RCC NOR image (PCM4_NOR.bin) in your favorite hex editor
- Jump to offset 0xBA0000, ensure IFS magic of "EB 7E FF" is present. If not, issue "flashlock" on PCM4 shell to obtain correct offset, target IFS is ~15.6mb. See screenshot.
https://cimg0.ibsrv.net/gimg/rennlist.co...90dfa4.png

https://cimg8.ibsrv.net/gimg/rennlist.co...c006d9.png
- Cut and paste this block of data into a new file, name it ifsroot_stage2_orig.ifs
- Move to a linux computer with dumpifs binary (available from QNX SDP)
- Copy ifsroot_stage2_orig.ifs to some folder, open your terminal and CD to that folder.
- Copy dumpifs_helper.sh to this same folder. Chmod it to 755
- Issue "./dumpifs_helper.sh ifsroot_stage2_orig.ifs" to extract the IFS, your files will be in ./ifs_extracted. Ensure files are present as shown in the terminal output
- Place a copy of /usr/apps/MIBRoot so it can be patched with IDA, Ghidra or similar

Step 5. Patch out the FEC checks.

Step 6. Rebuild IFS image
- Place your patched MIBRoot into your extracted IFS location, overwriting the old MIBRoot. It should be located at ./ifs_extracted/apps/bin/
- Open terminal. Issue command: EXPORT QNX_TARGET="/"
- cd to whatever the parent directory is to the ifs_extracted folder we made earlier
- Download mkifs_attributes.txt from github repo. Place it in your current working directory
- Build the new IFS with mkxfs, issue command "mkxfs -t ifs -nn -o ./ -r / ./mkifs_attributes.txt ./ifs_extracted ./patched_ifs.ifs"
- Place patched_ifs.ifs back onto your SD card

Step 7. Create your new FEC file
- Open the FEC container (orig_FecContainer.fec) from earlier in your favorite hex editor
- Copy VIN from file. This should match your car's VIN, unless component protection is enabled, then it would be the VIN from the donor car
- Copy down VCRN (hex values of bytes 16-20 in file). Write it down as shown in the blue highlighted text in the screenshot. The VCRN may be obtained through measurement channels on PIWIS if you only have a 4 byte empty FEC file.

- Make a comma separated list of your existing FECs, from offset 0x43 until the checksum begins. Use hex values, add commas at every 4 bytes (8 digits), for example, from screenshot it would be 00030000,00030001,(...),06310099

- Add one last FEC to the end of that list, which will enable Android Auto: 00060900
- You can also add other FECs to your PCM4 at this time, see below. Additional coding / adaptations may be required.
- Download MIB2_FEC_Generator.sh from Github, chmod it to 755
- Issue command to generate FEC Container "MIB2_FEC_Generator.sh -f {YOUR_FEC_LIST_CSV} -n {YOUR_VCRN} -v {YOUR_VIN} -d {Output_Directory}"
- Output file is FecContainer.fec, copy this new file to your SD card

Step 8. Load new files to head unit
- Insert SD card into PCM4, left slot
- Login with root / oaIQOqkW
- Issue the "stfu" command to stop verbose logging to the terminal.
- Remount efs-persist as r/w with command "mount -uw /mnt/efs-persist/"
- Copy your new FECs with command "mv /mnt/efs-persist/FEC/FecContainer.fec /mnt/efs-persist/FEC/FecContainer.fec.orig; cp /net/mmx/fs/sda0/FecContainer.fec /mnt/efs-persist/FEC/FecContainer.fec"
- Issue commands to flash your stage2 ifs-root... THIS CAN BRICK YOUR HEAD UNIT, SO BE CAREFUL! Important note: "flash.it" is actually one word, but RL censors it, so remove the period otherwise the command won't work.
- flashunlock
- /usr/bin/flash.it -v -x -d -a0x00BA0000 -f/net/mmx/fs/sda0/patched_ifs.ifs
- flashlock
- Reboot unit by holding down power button for 30s.
- Cross fingers and hope your patch worked

Step 9. Adaptations
With PIWIS II / PIWIS III, or VCDS
- If using PIWIS II, place it into engineering mode via Settings -> Diagnostics Configuration ->

911, 918s, etc... -> Mode -> Select "E". Save + Exit
- In PIWIS, Open Diagnostics -> 911 -> 991, scan car (F12) to obtain installed modules, select head unit (Named MIB2...). In VCDS open module 5F
- Select "Manuelle Codierung ohne MCR-Regeln" -> Vehicle_configuration
- Set Bitfield (3) Google_GAL -> "on"
- Save coding, wait for system to reboot

Alternate method coding through PCM4 shell:
export LD_LIBRARY_PATH=/mnt/app/root/lib-target:/eso/lib:/mnt/app/usr/lib:/mnt/app/armle/lib:/mnt/app/armle/lib/dll:/mnt/app/armle/usr/lib
export IPL_CONFIG_DIR=/etc/eso/production
on -f mmx /eso/bin/apps/pc b:0:3221356628:7.7 1

Step 10. Done!
- Plug in your phone. You should now have Android Auto

It is important to note that this hack will be overwritten if you ever decide to perform a software update on your PCM4. You'll then have to re-complete these steps with your new version of software. Given that there are no PCM4 updates available, this will probably be a non-issue.

What if I flash a bad ifs image to my head unit?
- If this happens, MIBRoot will fail to start and you will not be able to interface with PCM4. it will appear to boot from the LCD panel, but touch and audio will not work. However, it will still boot into QNX for recovery since we are only flashing the stage2 image.
- To recover, log into QNX with root / oaIQOqkW
- Copy your original IFS root file (ifsroot_stage2_orig.ifs) to your SD card and install to left slot of PCM4.
- Issue commands:
- flashunlock
- flash.it -v -x -d -a0x00BA0000 -f/net/mmx/fs/sda0/ifsroot_stage2_orig.ifs
- flashlock
- Note: If stage2 ifs flashing fails, flash.it, flashlock and flashunlock may no longer be present on your system. Copy them to your SD card from your extracted ifs directory and run them from the SD card, for example /net/mmx/fs/sda0/flashunlock.

What if my firmware flash works but I still don't have Android Auto?
- Your VIN, VCRN, or FECs may need to be corrected, review step 7. Cars without CarPlay may need to add FECs 00030000, or 00060700 and 00060800
- If your FECs are being removed from FecContainer.fec and being placed into IllegalFecContainer.fec, then your FECs are failing the signature check. Your patch is wrong and you need to review step 5 again.
- If you did not have CarPlay or Android Auto previously, you may also need to code USB media player functionality within PIWIS II.

What if I want to return to stock?
- Connect to PCM4 via UART
- Log into QNX with root / oaIQOqkW
- Copy your original IFS root file (ifsroot_stage2_orig.ifs) to your SD card and install to left slot of PCM4.
- Issue commands:
- flashunlock
- flash.it -v -x -d -a0x00BA0000 -f/net/mmx/fs/sda0/ifsroot_stage2_orig.ifs
- flashlock

- mount -uw /mnt/efs-persist
- rm /mnt/efs-persist/FEC/FecContainer.fec
- mv /mnt/efs-persist/FEC/FecContainer.fec.orig /mnt/efs-persist/FEC/FecContainer.fec
- Done. Reboot by holding power button for 30s