EGEA Working Group 2 (WG2) – Diagnostics

- Updated Minutes-

WG2 Meeting on OBD Connector
Tuesday 5th of September 2017, 10h00 – 15h30

EGEA Offices

Participants

ABL official representative	Arild Hansen [AH]
AICA official representative - diagnostic/ Robert Bosch	Marco Le Brun [MLB]
AICA official representative - diagnostic/ Texa	Elvis Colla [EC]
ASA/ Hella Gutmann Solutions	Ralf Kolberg [RK]
ASA official representative / Robert Bosch	Harald Neumann [HN]
FVU official representative / Autocom	Christer Larsson [CL]
GEA official representative	Dave Garratt [DG]
GEA / Autologic	Andrew Betteley [AB]
GEA / Continental	Pete Houlden [PH]
GEA / Premier Diagnostics	Ralph Wilce [RW]
GEA official representative / SP Diagnostics	Winston Lee [WL]
GIEG official representative / Actia Automotive	David Elizalde [DE]
GIEG official representative / CAPELEC	Georges Petelet [GP]
RAI official representative / Snap-on Tools	Robert Hoevenaar [RH]
EGEA	Neil Pattemore [NP]
EGEA	Eléonore van Haute [EVH]
Guest (morning only) / Concepts & Services Consulting	Gangolf Feiter [GF]

1. Opening and welcome by Elvis Colla
   - Roll call was done (see above list of participants).
   - EC welcomed all members and particularly our guest Gangolf Feiter, Chairman of ISO TC22/SC31/WG2 'Vehicle diagnostic protocols'. EC then gave a short background on the importance of the OBD connector and highlighted the need to keep the direct access to in-vehicle data via the OBD port open as this is vital for the aftermarket since the introduction of the first ECU.

2. Revision of vehicle type-approval legislation: background information on OBD Connector amendment
   - EVH gave an updated report on the state of affairs of the discussion around RMI and the OBD connector in the framework of the revision of vehicle type-approval legislation (see attached presentation). NP added that initially the OBD port has been legislated only for emissions and

not for the entire vehicle OBD information, moreover vehicle manufacturers have officially announced that they will close the OBD port and keep it open only for emissions, this is why this amendment is crucial for the survival of the aftermarket.

- She then explained that we are now in a final stage of the revision of the Type Approval Regulation – the Trilogue. It is expected to reach an agreement as soon as possible by the end of this year mainly to address the emission scandal.
- The trilogue phase of negotiation between the 3 EU legislators (EU Commission, EU Parliament and EU Council) is starting on the 6th of September and we need to make sure that EGEA/AFCAR position is taken into consideration as much as possible.
- EGEA/AFCAR tabled 35 amendments with the support of the Parliament in order to improve the new Type Approval draft regulation in the interest of the aftermarket. These amendments need now to pass through the negotiation discussions (trilogue phase).
- Actions: Support at this stage is very much expected from EGEA and AFCAR members to contact their ministries at national level and call them to support the AFCAR amendments. FIGIEFA/AFCAR is currently coordinating/organising all meetings with the ministries at national level. Members will be therefore be contacted and requested to support these activities. GP added that in France coordination must be done also with the ministry in charge of roadworthiness testing who is very much interested in these discussions as this will have a serious impact on emission testing via OBD if there is a risk to lose the OBD port.

3. AFCAR/ EGEA Position: Keeping the OBD connector open, whilst ensuring appropriate security
    - EVH presented the AFCAR/EGEA position on the OBD connector and went through the AFCAR amendment proposal (see attached presentation).
    - To address potential safety and security issues when using the OBD connector, she explained that AFCAR members decided that independent operators could accept for new types of vehicle, a company accreditation and certification scheme for the safe and secure use of tools connected to the OBD connector. This accreditation scheme could be based on the SERMI scheme as an industry standard for secure data access if and when really needed as pointed out by NP. By introducing these security measures, Member States should be more willing to keep the OBD connector open.

4. General explanation of the current work for certificated access to the vehicle and its data in ISO (Gangolf Feiter)
    - GF gave an extensive presentation on the certificated access to the vehicle and its data in ISO (see attached presentations).
    - He then explained that at US level, 'SAE J3138 - Guidance for securing the Data Link Connector (DLC)' is currently being drafted to give guidance on how to ensure the security of the OBD port.
    - To address security there are 3 topics to be considered:
        - Authentication: mainly for the equipment;
        - Authorisation: that may differ by ECU, purposes or data set. The granularity can be as vast as is wanted;
        - Encryption: increasingly used.
    - Discussion whether a central trust centre was needed and could be introduced in the ISOs work of WG2. Unfortunately, GF answered that this is out of scope of WG2. This must be addressed by EU legislation.
    - Due to ~~security reasons~~ the requirements for certificated access and encryption, GF explained that in the future, reverse engineering may no longer be possible, but will depend on the type and level of security implemented by the VM. Only in case that the ECU asks for authentication in a specific way and/or the communication is encrypted then reverse engineering will not be possible anymore. He also indicated that a way to overcome ~~it~~ how to access the vehicle data for revere engineering is to get a sort of "special key" from the VM by the accredited independent tool manufacturer, but this may require legislative support.

- GF then presented a possible alternative for the aftermarket for encrypted In-Vehicle Networks → the Secured Vehicle Interface (SVI) with a single point of access whether wired or wireless (see attached presentation). That gateway is responsible to serve all applications running. Today the approach to the OBD connector is "overkilled" as cyber-attacks are possible because the in-vehicle network is not secured enough by VMs.
- Discussion on the fact that certification might not be needed according to GF, better security should instead be established in the vehicle (SVI).
- Discussion on the fact that a joint solution should be found between the OBD connector, the certification, the security, the SVI and the OTP (Open Telematics Platform). WG2 would need to analyse how the SVI solution can be connected to the OTP in the future. AB noted that SVI is not triggering the new technology, and this should be taken into account during the analysis.
- Discussion on certification in the framework of ePTI standardisation activities and the need to have such certificates at PTI test stations/workshops levels (in some EU countries where repairers can do PTI). If SVI is used for ePTI, there could be only one single check of safety systems/software check via gateway.
- Certification: After discussion, members agreed that legislation is needed behind any form of certification. The solution would be to have one scheme for certification in the EU which would be mandated by EU legislation. The easiest way would be to have certificates generated by VMs and then distributed through a central point. Certificates should be per vehicle.

- Next steps & Actions:
  - The SVI proposal will be officially presented in the US at the AAPEX show this year, the Autocare consortium in the US is already supporting the SVI proposal. EGEA should therefore establish its official position and inform EU institutions in Brussels accordingly.
  - WG2 to analyse how the SVI proposal would fit with the OTP and OBD connector and what is the impact for EGEA.
  - EGEA to be more aggressive and to highlight that security issues are not due to the OBD port, but have been generated by lack of security in the IVN (In-Vehicle Network).

5. Brief report on US discussions (Gangolf Feiter)
   - See point above.

6. How to ensure security of the OBD port: by Certification?
   - For who?
   - For what services?
   - What data access and scope?
   - For When?
   - Validity duration?
   - Process of accessing and using certificates (process structure, cost, legislation, etc..)?

   - GF went through these various issues and explained in his presentation (see attached) what is the position of ISO/TC 22/SC 31/WG 2.

7. Third party positions
   - Due to lack of time, this point was not addressed.

8. TRL Study on access to in-vehicle data and resources: first exchanges and analysis of the final report published on 22nd of August 2017
   - EVH and NP explained that an analysis is currently being done by the secretariat and a first draft will be circulated very soon to WG2 members for comments. EC and MLB already gave their assessment and provided the secretariat with their comments. At the same time AFCAR is also

drafting a press release/paper which will then be circulated to all AFCAR members for approval before official release.

- Action: all WG2 members are invited to send their feedback/appraisal of the TRL Study to the secretariat in order to feed the EGEA analysis and future position paper.

9. Final decision on the EGEA position of OBD connector and future strategy, if appropriate
    - Due to lack of time and further discussion needed on the security concepts, final decision during this meeting could not be reached.
    - Decisions & actions: It was therefore decided to create a dedicated Sub WG2 on secure in-vehicle data access. The Security SWG2 shall submit a short position paper to WG2 within 3 weeks.
    - This subWG2 would be composed of the following experts: MLB, Tony Malaterre (tbc), RH, NP, WL, Emiliano Pasin (delegating Katia Ferrero).
    - The Security EGEA Paper should take into consideration existing and under development standards (AH and others). NP will circulate the new 'AFCAR security proposal' as soon as it is available, and this concept should also be analysed by subWG2.

10. Thank you and closure
    - Due to the complexity of the issue, the members did unfortunately not reach any clear and official position as some elements such as the security still need to be analysed and worked on further. It was agreed with all members that a next WG2 meeting should be scheduled very soon as further time is needed to elaborate EGEA position.
    - EC thanked all members for this meeting.
    - Action: to organise the next WG2 meeting in October 2017.

Elvis Colla
Eléonore van Haute