At stake: Discriminatory access to in-vehicle data with FIAT 500L, FIAT 500X and Doblo models

EGEA members have recently tried to establish diagnostic communication using their multi-brand diagnostic tools via the standardised OBD port with various new FIAT models and discovered that access to in-vehicle data is limited or requires a certificate from FIAT to access the in-vehicle data. It appears that access is now controlled via an internal security gateway.

Following our initial investigations, this is the current status:

- A Security Gateway module has been placed between the OBD connector and the in-vehicle networks which requires a certificate to allow access to in-vehicle data and functions

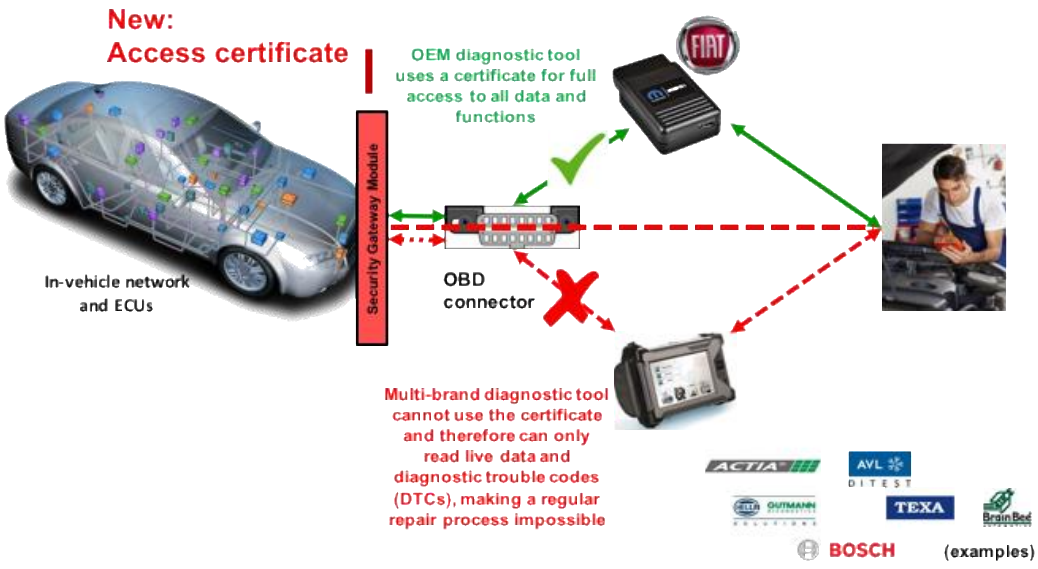

Figure 1: Restricted functionality of independent diagnostic tools imposed by the certificate

- Without a certificate, live data and fault codes can be read, but no other functions are accessible.
- In order to erase fault codes, command actuators or perform adjustments (i.e. normal diagnostic, repair and maintenance functions), or access to the infotainment system, the FIAT certificate must be used.
- This FIAT certificate is requested via the cloud based FIAT application and provides time limited access – which may be either/or session based, or valid for a limited time e.g. 24 hours.
- This certificate can only be obtained on-line and in real time by using the proprietary FIAT diagnostic system. Access is specific for each mechanic, who must create, and is subsequently identified by, their own account (individual username and password). This also presupposes that any technician has an internet connection to be able to get that certificate (e.g. workshop or roadside repair)

- The certificate is only valid for the specific vehicle connected to the FIAT diagnostic tool at the time of request.
- Independent operators need to register with FIAT and are now forced to buy the official FIAT diagnostic tool to access the certificate request process. Independent workshops will no longer be able to conduct a diagnostic and repair process using an independent multibrand diagnostic tool.

1. Non-compliance with Euro 5/6 legislation to the detriment of Independent Operators

The intention of the Euro 5/6 legislation is also to ensure the ability for independent tool manufacturers to develop and provide multi-brand diagnostic tools (see specific RMI provisions for multi-brand independent tool producers – EC No. 692/2008, Appendix 5). Additionally, the legislation implements mandatory requirements for the use of reprogramming standards for independent multi-brand diagnostic tools, which would not be needed if only proprietary OE tools were required.

With this new process, independent diagnostic tool manufacturers' products cannot be used to provide full diagnostic, repair or maintenance services on these FIAT vehicles. Although EGEA members have requested to FIAT to allow their tools to either generate or use a certificate, this is not currently possible and no solution has been proposed.
Even if the original FIAT scan tool is available to anyone, accreditation would still be required for each individual repairer, which also directly creates a monitoring issue.

EGEA is concerned if certificates are implemented by other vehicle manufacturers (e.g. Mercededs, Volvo and VW), this approach would go against the Euro 5/6 legislation which aims to ensure a fair level playing field and would bring unsustainable costs to the independent operators and restrict the services they could perform.

The arbitrary imposition of proprietary certificates by FIAT therefore appears to introduce a process limited to FIAT proprietary diagnostic tool which therefore does not allow conformity with the requirements of the existing Euro 5/6 legislation (Regulation715/2007/EC & Regulation 698/2008/EC) as this process blocks the ability to develop and use generic diagnostic tools for multi-make repairers.

2. How to address this?

An agreed and legislatively referenced process (e.g. the SERMI scheme, cf. Euro 5 Regulation 692/2008/EC) already exists for certificate validation and exchange for pass-through programming (specifically for anti-theft and emission related functions). This process ensures that both the access and any subsequent software updates remain the domain of the vehicle manufacturer for these specific anti-theft and emissions related requirements.

In order to avoid that each OEM implements their own proprietary certification process, it is proposed that this scheme which is already anchored into legislation and will be used by both vehicle manufacturers and independent operators, is extended to provide an independent single point of access for the certification process across the EU.

This scheme would then allow independent operators to use their multi-brand tools without supplementary burdens and barriers. The arbitrary imposition of proprietary certificates by FIAT therefore appears to contradict this principle.

3. Certification process

Diagnostic tool manufacturers - certification requirements:

- The diagnostic tool manufacturer will require an assessment procedure from the conformity assessment body that results in their approval and authorisation which are then registered with the trust centre, and which should remain valid for a significant period (e.g. 1 year or more).
- Each independent diagnostic tool manufacturer should be able to obtain access credentials for each OEM via an independent single point of distribution and validation (e.g. trust centre).

As part of the assessment procedure, the diagnostic tool manufacturer may need to show to the CAB that the certificate is safely managed, and that subsequently all operations of each diagnostic tool are properly logged via an independent agency (e.g. the SERMI trust centre coordinating the validity of the workshop, technician and diagnostic tool credentials).

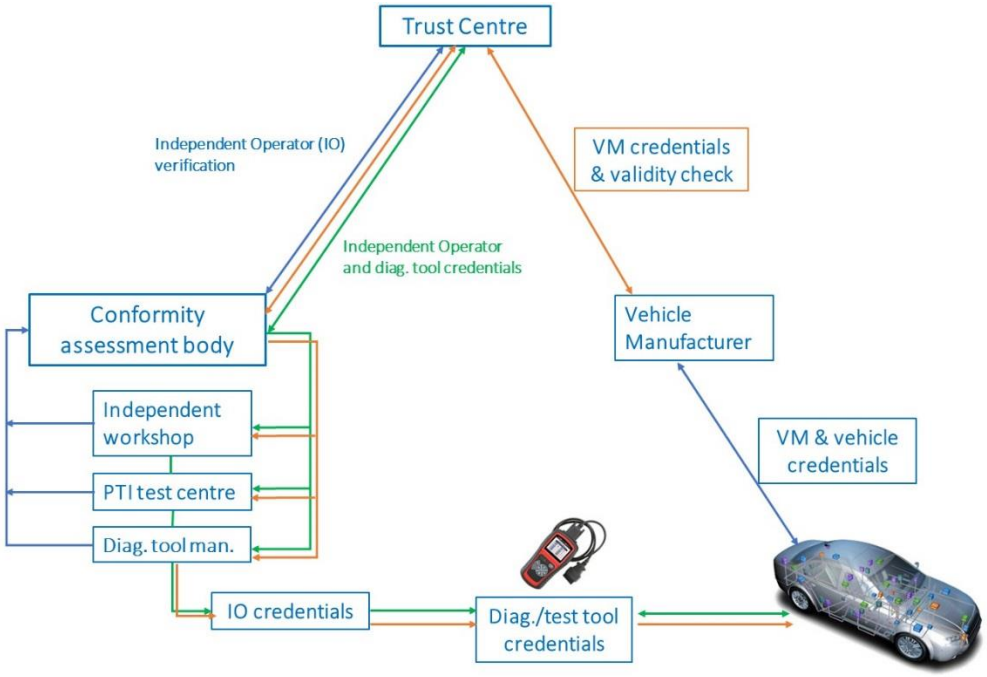

Figure 2. How the SERMI scheme could provide a single point of access and validation of certificates and credentials

The SERMI scheme already provides the structure for the independent single point of access and validation, but would need to be augmented to provide further assessment processes for connected devices.

Today, the SERMI scheme provides a structure to assess an independent workshop and its associated technician(s). Once an assessment has been successfully conducted, the workshop is allocated an identity certificate and the technician a personal identity number (PIN) which provide 'approval' for the workshop and 'authorisation' for the technician . Both the certificate and PIN and registered in the Trust Centre and when the workshop technician wants to access 'security related RMI', these credentials are checked by the VM at the Trust Centre and if valid, access is provided to the technician. This could be directly extended to include PTI test centres and inspectors.

The SERMI scheme could also evolve to provide a new assessment of a diagnostic tool/device manufacturer, in parallel to the way that a workshop is assessed. Additionally, a unique identity number (UIN) could be allocated to the device that will communicate with the vehicle, in a similar way to the technician's PIN. Both of the certificate and the UIN would then be registered at the Trust Centre.

It would also be possible for vehicle manufacturers to store certificates at the Trust Centre (similar principle to the proposal in C-ITS) which would be allocated to the workshop when they request a certificate to access a vehicle. This would be conducted as part of the tool being connected to a vehicle and the request being sent to the Trust Centre. The Trust Centre would check the validity of the workshop, technician PIN, device manufacturer and device UIN and then log the request association, before releasing the certificate to be used by the specific workshop/tool/vehicle combination.
It would still be important to ensure that there was legislative control of the vehicle manufacturers' certificates to avoid any burdens, distorted competition, anti-competitive controls or dissuasive costs being associated with the use of the certificate.

4. Legislation is required to support the certification process

Legislation is needed to define a standardised process for accessing and using the credentials required for diagnostics, repair, maintenance, roadworthiness testing and the remote reading of data when the vehicle is being driven.

The principle of using an independent single point of access to certificates is established both within the SERMI scheme, but also in the 'Certificate policy for the deployment of European Cooperative Intelligent Transport Systems (C-ITS)'.

This is why EGEA feels that a independent single point of access is the correct solution which is already accepted by the legislator, vehicle manufacturers and the aftermarket and therefore should be specified as part of a legislative requirement for the handling of certificates.

The basic principles of the process for the access and use of credentials needs to include if a certificate is required, and when it is required – i.e. what conditions apply (vehicle stationary, vehicle moving, anti-theft related, roadworthiness testing etc.). Additionally, and specifically for diagnostic tool manufacturers, a certificate that supports the legitimate process of reverse engineering must be available without additional conditions which would be dissuasive to its use.

The costs and conditions of certificates must also be monitored by the EC to avoid 'control and contractual conditions' that would create anti-competitive activities.

***

The process of accessing and using certificates to establish a user's credentials through certification, authentication and authorization includes:

Certification:

A digital certificate will be used to access the vehicle and/or the appropriate data under specific conditions. according to the standard ISO 20828. The digital certificate shall be stored in a secure hardware token with access and copy protection. The identifier is created by the CAB and in the case of a physical person, their identity is only known to the CAB.

The proposed certificate will use a public key infrastructure (PKI) for the relationship between a key holder and a relying party that allows a relying party to use a certificate relating to the key holder for at least one application using a public key-dependent security service.

Note: PKI includes a certification authority, a certificate data structure, means for the relying party to obtain current information on the revocation status of the certificate, a certification policy, and methods to validate the certification practice.

It is therefore considered necessary that the process of providing access to, or the use of, this certificate should not be used in any way that imposes burdens, distorted competition, anti-competitive controls, dissuasive costs and should be available via a single point for all vehicle manufacturers.

Authentication

The process of actually confirming the identity of the user or the device connecting to the vehicle. This is based on a certificate emanating from a trusted source and will include the information used to verify the claimed identity of an entity, such as an individual, defined role, corporation or institution.

It is therefore proposed that the appropriate certificates are accessible via a single point for all vehicle manufacturers, thereby minimising the burdens for all parties.

Authorisation:

Authorisation is the process of providing the user with permission to have access to data/functions. This may include access to specific data/information, specific functions or duration of access.

The proposed process is based on the inspection performed by the Conformity Assessment Body (CAB) that assesses an individual employee or product of an approved Independent Operator company who is entitled to be given access to the vehicle and its data. The individual employee or product will be allocated a secure hardware token containing a personal digital certificate and a PIN issued by a designated Trust Center.

Credentials

Credentials should refer to the verification of user identity or tools for authentication. This may be part of a certificate or other authentication process that is used to confirm a user's identity.

The process used to provide this verification must not be used in any way that imposes burdens, distorts competition, introduces anti-competitive controls and dissuasive costs or other barriers to undistorted competition.