C-ITS / WG6
FIA Answers on ACEA responses and further explanation of the “Shared Server Concept”

2015-11-20

Gerd Preuß

Summary

This document provides further explanation on the concept of a shared server. The document describes liability, security and usability of transferred data in separate chapters. Furthermore it answers on the ACEA concerns on the concept that were raised during the C-ITS / WG6 meeting on 2015-10-26.

Until the technical provision of a secure in-vehicle platform, FIA accepts - as an interim solution - the remote access to in-vehicle-data via a Vehicle Manufacture (VM) external server leveraging the “Extended Vehicle (ExVe) interface, if it fulfills the FIA basic requirements.

The FIA requirements for a remote access to in-vehicle data via ExVe interface are:

1. Consumer principles, like free choice, data privacy and the right to be forgotten
2. Secure, but unmonitored by VM, access for independent operators
3. Independent development of new services

A shared server is one solution to fulfil all of these requirements. The FIA is open for other technical solutions, like the “DataHub” or the open telematic platform proposal but any solution shall fulfill the FIA requirements by its technical implementation.

Currently the ExVe interface only, is not acceptable due to the fact, that monitoring is technically possible and the independent development of new services is not in the scope of the ISO standardisation. Furthermore the ISO standardisation is legally not binding.

FIA answers on ACEA concerns

In the last C-ITS Meeting on 28 October 2015; ACEA expressed two reasons for their rejection of the shared server concept.

1. ACEA: One Shared Server for all vehicle manufacturers is not acceptable.

   FIA answer: The concept of the shared server is not based on one single server. It is based on neutral storage and operation of VIN, location, private data and company data. The vehicle data like fault codes, software updates or any other sensor or ECU data remain under the control of the vehicle manufacturer.
   There can be as many “shared servers” as backend servers of the vehicle manufacturers. There is no limit to one server.

2. ACEA: In a Shared Server, the vehicle manufacturer cannot overtake liability for the transferred data.

   FIA answer: There is no need for the vehicle manufacturer to provide liability for VIN, location, private data and company data. The neutral services provider is responsible for the accuracy and the safety of these data. Personal data and company data must remain confidential. The publication of sensitive data for reasons of liability is only acceptable in justified individual cases at the request of the vehicle owner.

Personal data are the fuel for current business models. The shared server concept protects the customer and companies from being confronted with adapted advertising, which is generated by the usage of aggregated data. Data privacy legislation does not yet cover aggregated data. The shared server concept restricts the usage of aggregated data, if the customer has explicitly expressed his consent.

Shared Server Concept

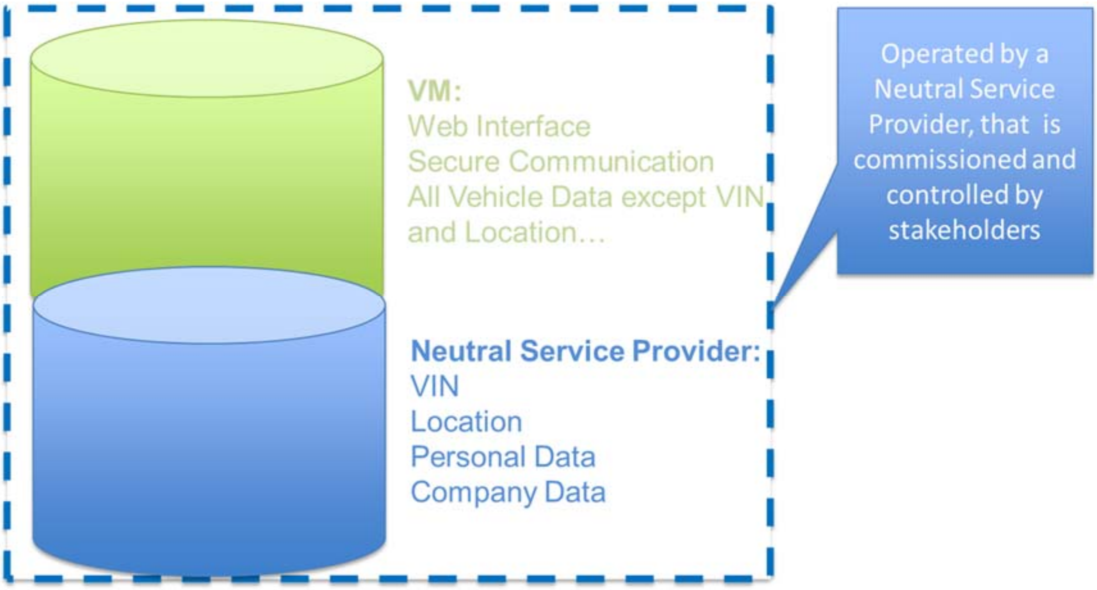
VM:
Web Interface
Secure Communication
All Vehicle Data except VIN and Location…
Neutral Service Provider:
VIN
Location
Personal Data
Company Data
Operated by a Neutral Service Provider, that is commissioned and controlled by stakeholders

Image 1: Shared Server Concept

The shared server separates the competitive data (blue) from vehicle data (green). A neutral company operates the shared server; a group of stakeholders (blue dotted line) commissions it. Vehicle Manufacturers control the data transfer to their vehicles and ensure the safe operation of the vehicle.

It is neither necessary that all VMs use the same server, nor is it necessary that both databases (blue and green) are physically placed at the same location.

The Shared Server can be adapted to the SERMI Scheme

All European automotive stakeholders agreed in 2010 on the SERMI scheme. The scheme describes how independent operators request access to security related repair and maintenance information (SERMI) in a neutral and pseudomysed way.

The shared server model can be adapted to the SERMI process. For the authentication and the certification of vehicle owners, drivers and independent operators, the conformity assessment body (CAB) is a neutral service provider and stores the pseudomysed economical and privacy critical data (blue data).

Liability

Liability in case of a Shared Server is similar to the one established in the SERMI process. The actual data of the IO and the holder of the vehicle will be stored at the CAB. The data is not known by the VM, he only knows the IDs, which confirm the existence of an authorization and the conformity of the certificates.

In case of liability, the petitioner (VM, IO, and customer) can directly request the decoding of the relevant data at the CAB. All the involved parties will then receive both the competitive data and the vehicle data.

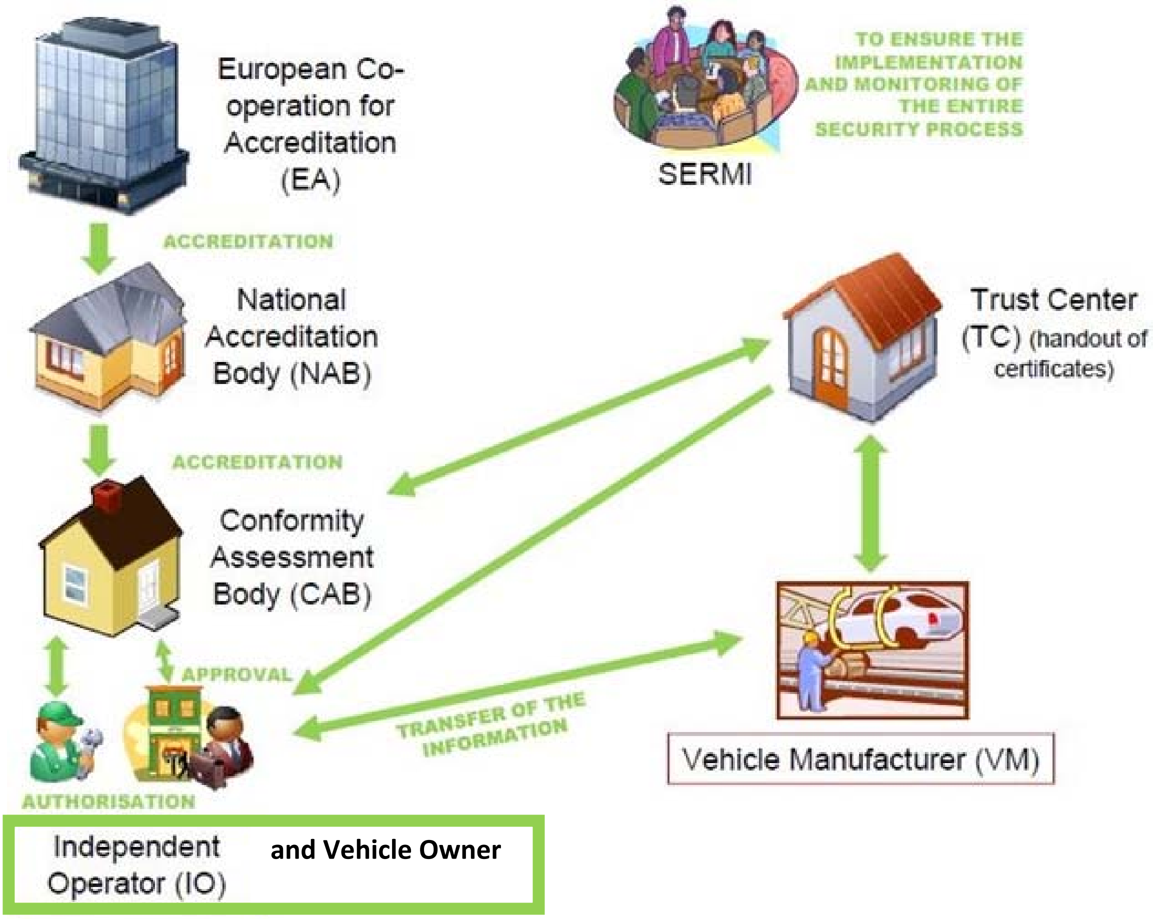
European Co-operation for Accreditation (EA)
SERMI
TO ENSURE THE IMPLEMENTATION AND MONITORING OF THE ENTIRE SECURITY PROCESS
ACCREDITATION
National Accreditation Body (NAB)
Trust Center (TC) (handout of certificates)
ACCREDITATION
Conformity Assessment Body (CAB)
APPROVAL
TRANSFER OF THE INFORMATION
Vehicle Manufacturer (VM)
AUTHORISATION
Independent Operator (IO)
and Vehicle Owner

Image 2: SERMI Scheme for the accreditation of independent workshops and mechanics, as agreed by all stakeholders can be easily adapted to the shared server concept

Security

FIA proposes to use the same security level as vehicle manufacturers are using for the extended vehicle concept, especially for the data transfer from/to the vehicle and the secure operation of the vehicle itself.

Independent Operator Employees and vehicle owners can be authenticated anonymously so that only a dedicated authority, like a CAB (or set of authorities) can recover the employee's identity. This can be achieved using a similar security framework that is also used to authenticate vehicle-to-vehicle communication. One can either use an online pseudonym authority who issues short-lived pseudonym certificates after having checked the employee's long-lived certificate; if needed, the pseudonym authority can check its records to see which employee is behind a certain pseudonym. Alternatively, one can use group signatures or privacy-preserving attribute-based credentials (Privacy-ABCs) to avoid the need for an online pseudonym authority and also avoid the bandwidth and storage costs of obtaining fresh pseudonym certificates for each signature. Instead, employees are given a single signing key that allows them to anonymously sign an arbitrary number of messages. A dedicated opening authority or inspector has a special decryption key that allows it to recover the exact identity of the signer if needed.