On-Board Authorisation Concept

Further clarification and outlook at next steps

Informal working group on Cyber Security and Over-The-Air
Software Updates (CS/OTA) – TFCS-30-04

Submitted by the Secretary
of IWG CS/OTA

<u>Working Paper</u> **TFCS-29-07 Minutes**
29th TFCS, 12th & 13th March 2024

VI. Accessibility & privacy by design

[…]

The representatives from CECRA and FIGIEFA stated interest in a suggested drafting group and the representative from CITA expressed support for the FIA proposal. […]

The representative from the European Commission stated support to keep the topic on the agenda but explained that the detailed proposal, intention and how to align with national/regional law would not be totally clear. […]

The co-chair […] stated that further clarification of the proposal by FIA would be required to solve raised unclarities and open questions. FIA confirmed to update their proposal including technical requirements for clarification.

UN Regulation No. 155

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

1.3.   This Regulation is without prejudice to other UN Regulations, regional or national legislations governing the access by authorized parties to the vehicle, its data, functions and resources, and conditions of such access. It is also without prejudice to the application of national and regional legislation on privacy and the protection of natural persons with regard to the processing of their personal data.

7.2.2.5. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.

Authentication shall be understood as the process of verifying the identity of a user, system, or application trying to access a resource like a generic tool.
  - In simpler terms, it answers the question: "Who are you and is it really you?"

Authorisation shall be understood as the process of determining what actions or operations (IO) a verified user, system, or application is allowed to perform on a resource.
  - In simpler terms, it answers the question: "What are you allowed to do?"

For purposes of authentication and authorisation, a digital certificate shall securely state:
  - "I am who I claim to be, and I am authorised to access level a, b, c, d etc."

Such authentication information shall be contained in a digital certificate. A neutral trust centre shall confirm this, and the vehicle shall require this as prerequisite for authorisation.
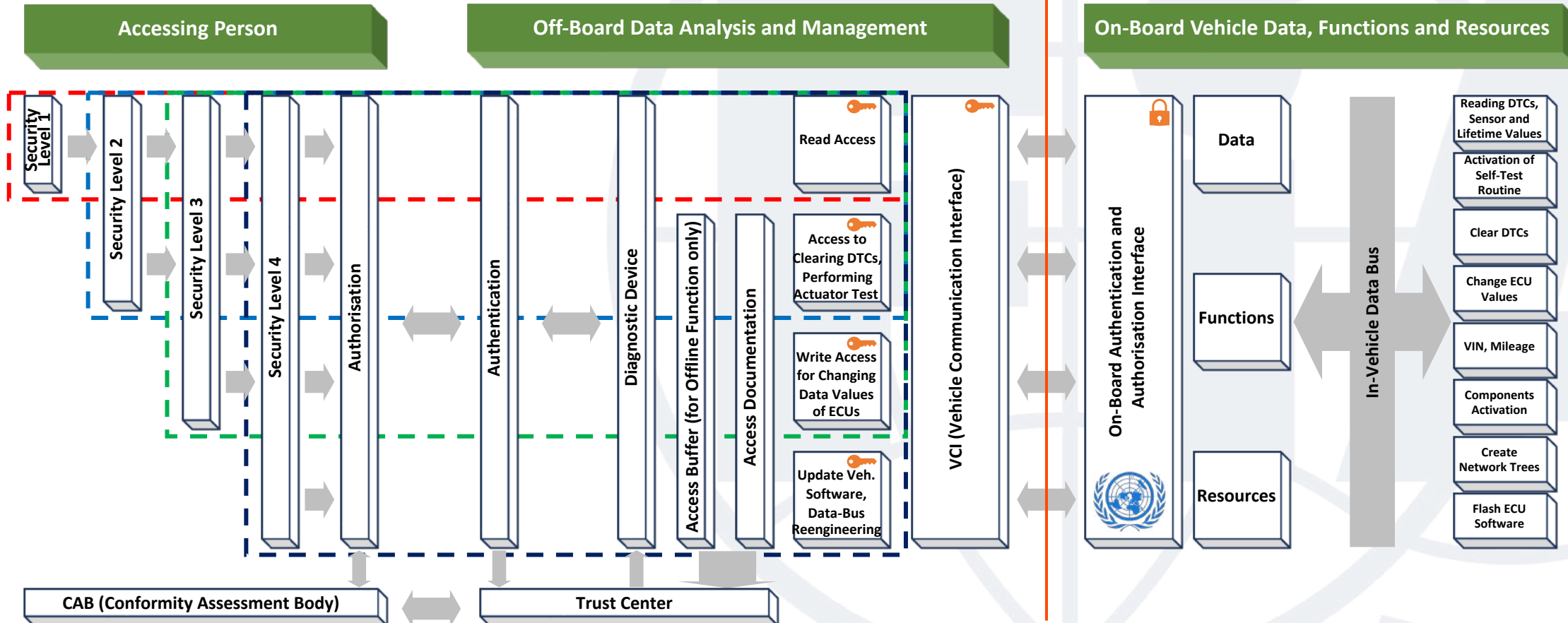
Multi-factor authentication may be used to confirm that a user really is who they claim to be.

➤ Implementation of UN R155 and UN R156 regulatory requirements by different Contracting Parties in national / regional legislations require a matching **on-board authentication and authorisation concept.**

➤ The FIA and Mobility Club's proposal seeks to regulate a **secure on-board part of an authentication and authorisation concept.** It does <u>not</u> seek to grant access to in-vehicle data and functions.

➤ The **off-board authentication and authorisation concept** shall be left to regulation and control on national / regional levels.

An authorisation concept shall split responsibilities and differentiate between off- / on-board data & functions

Architecture example for off-board and on-board authentication and authorisation - *conceptual* -

🔑 Devices serving as "key"
> responsibility of individual Contracting Parties

🔒 Devices serving as "lock"
> responsibility of UNECE

Accessing Person

Off-Board Data Analysis and Management

On-Board Vehicle Data, Functions and Resources

Security Level 1 · Security Level 2 · Security Level 3 · Security Level 4 · Authorisation · Authentication · Diagnostic Device · Access Buffer (for Offline Function only) · Access Documentation

🔑 Read Access

🔑 Access to Clearing DTCs, Performing Actuator Test

🔑 Write Access for Changing Data Values of ECUs

🔑 Update Veh. Software, Data-Bus Reengineering

VCI (Vehicle Communication Interface)

🔒 On-Board Authentication and Authorisation Interface

Data · Functions · Resources

In-Vehicle Data Bus

Reading DTCs, Sensor and Lifetime Values · Activation of Self-Test Routine · Clear DTCs · Change ECU Values · VIN, Mileage · Components Activation · Create Network Trees · Flash ECU Software

CAB (Conformity Assessment Body)

Trust Center

Source: ÖAMTC, adapted

UN Regulation No. 155

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

*The proposed changes to the current text of the regulation are indicated in **bold** for new text and should be further refined in a working group to which FIA invites all interested parties.*

5.1.1.   The Approval Authority or the Technical Service shall verify by means of document checks that the vehicle manufacturer has taken the necessary measures relevant for the vehicle type to:
[…]
(f)   ....[1]

7.2.2.2.   The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:
[…]
(i)   ....[1]

1) Amendments to address the on-board authentication and authorisation concept shall be added here

1. **FIA is inviting interested parties to join the drafting work on amendments to UN R155 based on:**
   - WP.29 Programme of Work states in Table 5, p. 24 as one of its Tasks / Deliverables: "Develop deliverables regarding recommendations for SW updates after registration and address items passed by GRVA"

2. **The outcome of such a working group will be reported back to the IWG on CS/OTA for further consideration.**

3. **The concept of Privacy by Design (TFCS-28-03) will be discussed at a later meeting of the IWG on CS/OTA.**

PUT CITIZENS IN THE POLE POSITION

Maintain the balance between vehicle security and accessibility over the vehicle's lifetime

Respect privacy citizens and put them in control