On-Board Authorisation Concept "OBAC"

FIA

April 2025

FiA

242 CLUBS

147 COUNTRIES

80M+ MEMBERS

NORTH & CENTRAL AMERICA
29 Clubs
20 Countries

EUROPE
103 Clubs
50 Countries

MENA
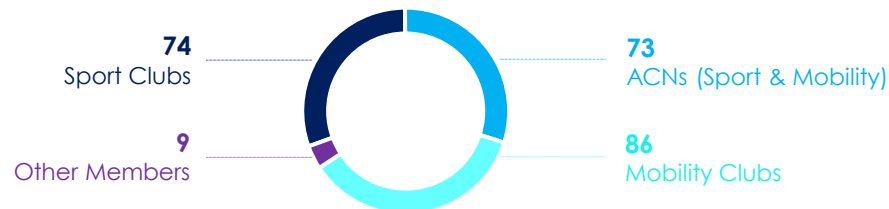32 Clubs
21 Countries

SOUTH AMERICA
14 Clubs
11 Countries

AFRICA
27 Clubs
21 Countries

ASIA PACIFIC
37 Clubs
24 Countries

ONE OF THE WORLD'S LARGEST NOT-FOR-PROFIT CONSUMER ORGANISATIONS

FIA IS IN A UNIQUE POSITION TO FACILITATE COMMUNICATION AND EXCHANGE OF IDEAS AMONG THE 80M+ ROAD USERS IT REPRESENTS

74 Sport Clubs

73 ACNs (Sport & Mobility)

9 Other Members

86 Mobility Clubs
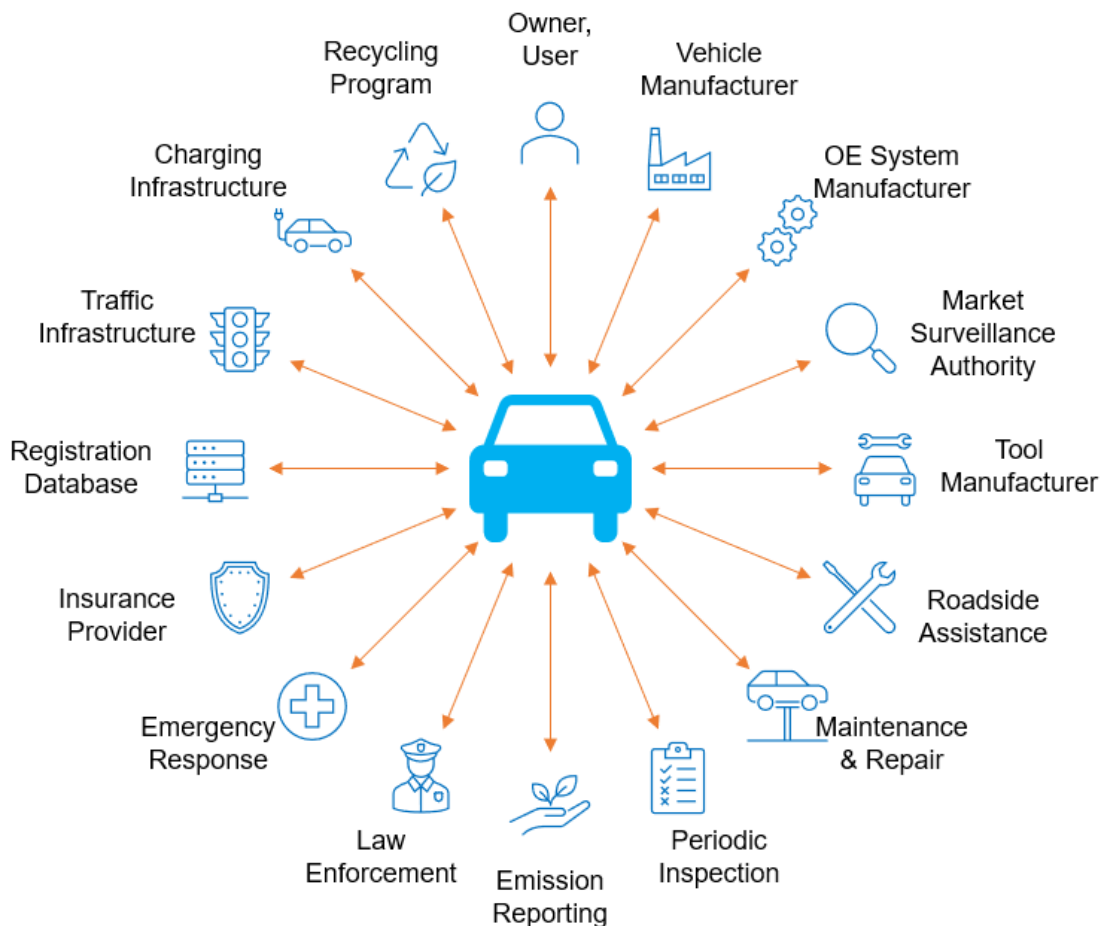
Get the balance right

The Fédération Internationale de l'Automobile (FIA) counts over 240 Member Organisations (AAA in Australia, CAA in Canada, ADAC in Germany, TCS in Switzerland, The AA in the UK…) representing over 80 million road users from 164 countries.

The FIA policy priorities are:

❑ Connected vehicles

❑ Increasing road safety

❑ Protecting the environment

❑ Safeguarding mobility

The FIA acts as a consumer advocate, highlighting the need for a delicate balance between security over the vehicle lifetime and secure data access.

On-board authorisation concept needed

- ☐ Manufacturers, independent service providers, suppliers, authorities, market surveillance and car owners have numerous requests toward vehicle resources.

- ☐ A single, generic and harmonised solution for vehicle on-board authorisation / authentication is needed to handle such requests.

- ☐ A solution must comply with all cybersecurity provisions, needs to prevent any unauthorized access and allow for oversight by the respective authorities.

- ☐ A harmonised vehicle on-board authorisation / authentication concept balances security, user rights, and stakeholder needs over the vehicle´s lifetime.

Passport for authentication / authorisation

❑ Recent regional and national regulation demand a concept to authenticate and authorise real and virtual agents with respect to vehicle resources.

❑ Such and access concept needs to prevent unauthorized access and comply with all regional / national cybersecurity / privacy laws.

❑ The proposed authorisation / authentication concept would be globally harmonised on-board of the vehicle and can accommodate particular regional / national off-board requirements.

❑ A passport system would link off- and on-board authorisation / authentication, which need to work together in the interest of security, fairness, and practicality over lifetime.

PASSPORT

Two important aspects to address secure access

To move forward and address the needs for off- and on-board authorisation / authentication, 2 options may be possible. The following should be considered carefully with security, consumer choice, practicality, and innovation in mind:

1. **Put the consumer in the center of connectivity,** grant them to consent and help to protecting their privacy.

2. **Collaborate as CPs and NGOs and analyze** the entire connected mobility ecosystem (see p. 3) incl. existing regulation and standards to subsequently propose a solution.

A stocktaking exercise is in order

A first step should be a stocktaking exercise to clarify the authentication and authorisation requirements in different regions and nations.

The FIA offers to collect evidence and facts around the globe, through a study with the following objectives:

- ❑ **Literature overview:** review off-/on-board vehicle authorization systems applied globally
- ❑ **Stakeholder input:** structured interviews with delegates from CPs and stakeholders
- ❑ **Framework benchmarking:** overview of relevant technical standards and regulations
- ❑ **Implementation guidance:** recommendations for further work at the WP.29 and GR´s

Such study should yield actionable **results to be discussed at the 197th session of WP.29 in November 2025**

What to expect

Outline of activities throughout 2025

March Kickoff for stocktaking study

June Interim report to WP.29

November Final results to WP.29, decision on further steps

Thank you

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