



From smart tachograph version 1 to version 2 – Amendment to Annex IC

**Group of Experts on AETR
13 October 2020**

Legal background

- Mobility Package I requires additional functionalities to be implemented in the smart tachograph
- Need to amend Annex IC by August 2021
- A version 2 of the smart tachograph to be implemented by August 2023 in newly registered vehicles
- Vehicles engaged in international road transport to be retrofitted by end 2025

Deliberations in the EU Council about AETR

- EU Member States have been debriefed by European Commission about the state of the play of the negotiations in AETR. A formal EU position will be submitted to AETR soon.
- 4-year transitional period in the AETR would mean:
 - **By the end of 2025, the full international EU fleet will be fitted with the smart tachograph v2**
 - **While smart tachograph v1 would only start in newly registered non-EU AETR vehicles as from 2026**
- This was not considered acceptable for EU Member States : not compatible with the objectives to improve road safety and to create a level playing field between EU and non-EU AETR countries

Deliberations in the EU Council about AETR

- **Position of the EU Member States :**
 - The smart tachograph version 2 should be implemented in AETR (without the “intermediate” step of smart tachograph version 1)
 - AETR to be granted a reasonable transitional period, which will not jeopardize the objectives of the smart tachograph. Compared to the requirements imposed on EU hauliers, non-EU AETR hauliers could be granted two additional years (to equip new vehicles with the smart tachograph 2 and to retrofit the fleet of vehicles used in international transport)

New functionalities

From Mobility Package I

- Border crossing detection
- Recording of the vehicle position when load/unload takes place
- Enforcement of driving times and rest periods from 28 to 56 days
 - increase of records to be stored
- Recording of the type of load (goods/passengers)
- Transmission via DSRC of maximum driving time being exceeded

Others

- OSNMA (Open Service Navigation Message Authentication)
- Software update
- Internal motion sensor
- Automatic selection of beginning/end driving place
- Bi-directional ITS interface communication

1. Border crossing detection

- A map must be stored in the tachograph
 - NUTS 0 (EU MMSS, EEA, Candidate countries and UK)
 - Link to the map available at JRC website for download by tachograph manufacturers
 - JRC will create a hash that will be used by tachograph manufacturers to verify the authenticity of the map
 - Tachograph manufacturers will be responsible for storing the map with a secured procedure.
 - Map updates shall be carried out in authorised workshops, according to the secure procedure set up by each manufacturer.

Border crossing - recording

- Data recorded: position, time, country of origin and country of destination. Country not included in the map will be “rest of the world”
- Border-crossing will be stored in both VU and card
- Storage capacity: VU (20/day - 365 days), card (20/day - 56 days)

2. Recording of the position at load/unload

- The operation shall be manually entered through the tachograph menu
- Three possibilities load/unload or simultaneous load-unload
- To be entered, at the latest, when the operation has finished
- GNSS position and time shall be stored together with the operation type
- Storage capacity: VU (25/day - 365 days), card (25/day - 56 days)

3. Type of load (goods/passengers)

- A by-default load type (goods/passengers) will be stored in the tachograph upon activation and first calibration.
- The by-default setting in the tachograph may be changed by a workshop
- The by-default load type will be stored in the card upon card insertion

4. Increase of records from 28 to 56 days

- Impact in terms of card storage capacity
- The simple approach would be to double the current size of all files, but optimisation is necessary
- For instance, the current maximum number of activity changes can be kept

		Min	Max
n ₁	NoOfEventsPerType	6	12
n ₂	NoOfFaultsPerType	12	24
n ₃	NoOfCardVehicleRecords	84	200
n ₄	NoOfCardPlaceRecords	84	112
n ₆	CardActivityLengthRange	5 544 bytes (28 days * 93 activity changes)	13 776 Bytes (28 days * 240 activity changes)
n ₇	NoOfCardVehicleUnitRecords	84	200
n ₈	NoOfGNSSCDRecords	252	336
n ₉	NoOfSpecificConditionRecords	56	112

Increase of records from 28 to 56 days

	Records	Records/day
Current records		
Place beginning/end daily driving period	112	2
3-hours accumulated driving time	336	6
Driver activity	6,552	117
New records		
Border crossing records	1,120	20
Load/unload records	1,400	25
Load type changes	336	6

DSRC indication - exceeding driving time

RTM20 - Continuous driving time
RTM21 - Daily driving time
RTM22 - Weekly driving time
RTM23 - Accumulated driving time during the current and last week

6. Automatic selection of begin/end driving place

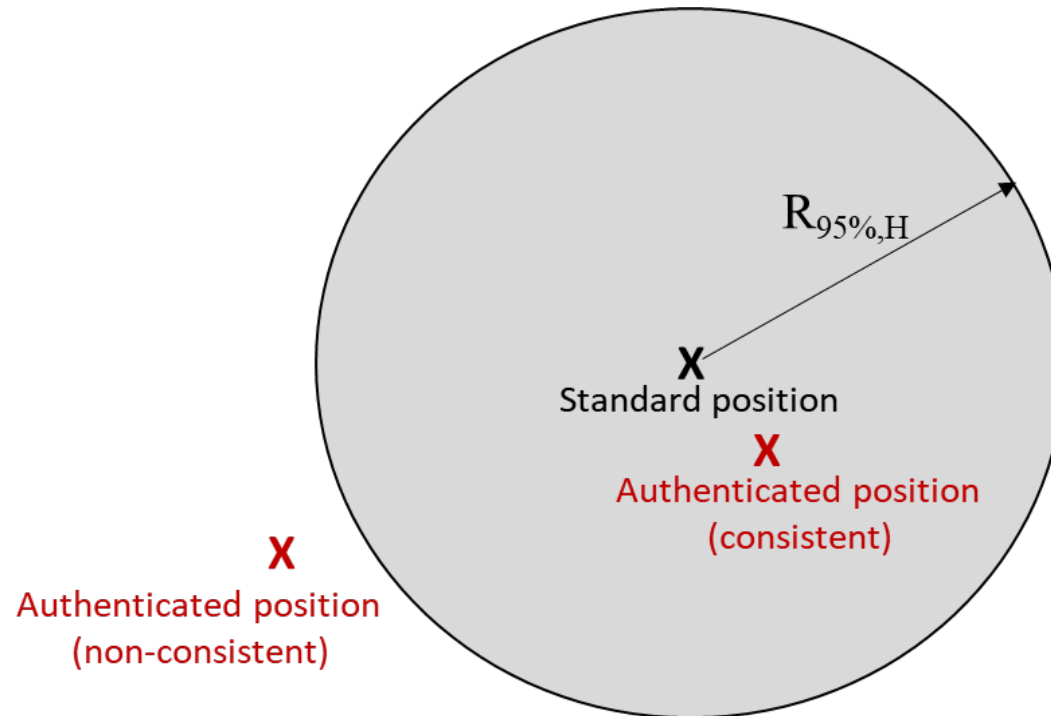
- Pending issue not implemented due to the absence of a digital map in the VU
- The VU will automatically propose a begin/end place, which can be confirmed or modified by the driver.

7. Galileo authentication service (OSNMA)

- OSNMA provides trust in the signal
- Galileo transmits encoded messages that are decoded by the receiver
- OSNMA is time-dependent
- OSNMA needs an external source of time which is reliable: tachograph clock (security-certified)
- Maximum automatic time adjustment is 1 sec/day (currently is unlimited)
- The accuracy of the clock has been increased from 2 to 1 sec/day
- Accuracy of the clock will apply in the full temperature range of operation of the clock (- 20°C to 70°C)
- “time conflict” event recorded when GNSS time and tachograph time differ by more than 1 sec/day.

Determination of the position

- How can we combine Galileo with other constellations, whilst still keeping the trust in the signal?
- Chipset compatible with Galileo, GPS and Glonass.
- Galileo is the only constellation providing authentication



Additional measures to prevent simultaneous tampering of GNSS signal and motion sensor

- GNSS receiver will be able to detect and inform the VU about possible RFI attacks
 - The VU will store the attack as “GNSS anomaly”
 - The attack will be recorded as either “jamming” or “other attacks (spoofing)”
- Addition of two new conditions triggering “motion conflict” event:
 - Conflict based on speed: motion sensor speed vs GNSS speed
 - Conflict based on distance: distance between two consecutive GNSS points and motion sensor distance
 - Conflict based on movement detection: between motion sensor vs internal sensor

9. Internal sensor

- Independent from GNSS and motion sensor
- Lodged inside the VU
- “motion conflict” event will be triggered if motion sensor does not detect movement and the internal sensor detects movement.
- Type of sensor, condition of movement and period to trigger an event are manufacturer dependent
- Period of reaction no longer than 3 hours

10. Software update

- Software update will cover:
 - Modification of all functionalities referred to in point 2.2 of Annex IC
 - The addition of new functionalities directly related to the enforcement of EU legislation on road transport
 - Modification of the modes of operation referred to in point 2.3 of Annex IC
 - Modification of the file structure (eg size increase)
 - Deployment of software patches to address software defects or reported attacks on the functions of the recording equipment
- Software update requires the implementation of additional hardware: 40% in usual hardware resources and 65% for map updates or enlargements (additional capacity that would cover for 3 MPI's and current AETR countries)
- Provided that no new hardware is needed