Smart Tachograph

Type-approval guidelines

V0.5

Michel Chiaramello
Jacques Kunegel
Luigi Sportiello
David Bakker
June 4th, 2018
Table of contents

1 Introduction ........................................................................................................... 5

2 Type-approval schemes .......................................................................................... 6
  2.1 Tachograph Cards type-approval scheme ....................................................... 7

2.2 Type-approval schemes for recording equipment ............................................... 8
  2.2.1 Recording equipment type-approval, composed by a (single body) Vehicle Unit and a Motion Sensor ............................................................................................................ 9

  2.2.2 Recording equipment type-approval, composed by a Vehicle Unit (Main Body), an External GNSS Facility and a Motion Sensor ......................................................... 10

  2.2.3 Recording equipment type-approval, composed by a Vehicle Unit main body, an External Remote Communication Facility and a Motion Sensor ................................. 11

  2.2.4 Recording equipment type-approval, composed by a Vehicle Unit main body, an External GNSS Facility, an External Remote Communication Facility and a Motion Sensor 12

  2.2.5 (single body) Vehicle Unit and Motion Sensor component type-approvals. Single VU/MS manufacturer, first type-approval of each component ............................ 13

  2.2.6 (single body) Vehicle Unit and Motion Sensor component type-approvals. Different VU/MS manufacturers, first type-approval of each component .......................... 14

  2.2.7 Vehicle Unit (main body), External GNSS Facility and Motion Sensor component type-approvals. Single VU/MS/EGF manufacturer, first type-approval of each component ........................................................................................................ 16

  2.2.8 Vehicle Unit (main body), External GNSS Facility and Motion Sensor component type-approvals. Different VU/MS/EGF manufacturers, first type-approval of each component .................................................. 17

  2.2.9 Vehicle Unit (main body), External Remote Communication Facility and Motion Sensor component type-approvals. Single VU/MS/ERCF manufacturer, first type-approval of each component ........................................................................ 19

  2.2.10 Vehicle Unit (main body), External Remote Communication Facility and Motion Sensor component type-approvals. Different VU/MS/ERCF manufacturers, first type-approval of each component ................................................ 20

  2.2.11 Vehicle Unit (main body), External GNSS Facility, External Remote Communication Facility and Motion Sensor component type-approvals. Single VU/MS/EGF/ERCF manufacturer, first type-approval of each component ................................................................. 22

  2.2.12 Vehicle Unit (main body), External GNSS Facility, External Remote Communication Facility and Motion Sensor component type-approvals. Different VU/MS/EGF/ERCF manufacturers, first type-approval of each component ............... 23

  2.2.13 Example of component type-approval with other(s) previously type-approved components: (single body) Vehicle Unit with previously type-approved Motion Sensor. Single VU/MS manufacturer. ........................................................................................................ 25

  2.2.14 Example of component type-approval with other(s) previously type-approved components: (single body) Vehicle Unit with previously type-approved Motion Sensor. Different VU/MS manufacturers. ........................................................................................................ 26

  2.2.15 Example of component type-approval with other(s) previously type-approved components: Motion Sensor with with previously type-approved (single body) Vehicle Unit. Single VU/MS manufacturer. ........................................................................................................ 28
2.2.16 Example of component type-approval with other(s) previously type-approved components: Motion Sensor with previously type-approved (single body) Vehicle Unit. Different VU/MS manufacturers. .......................................................... 29

2.2.17 Example of component type-approval with other(s) previously type-approved components: External GNSS Facility Facility with previously type-approved Vehicle Unit(Main Body) and Motion Sensor. Single VU/EGF/MS manufacturer. .................................................. 31

2.2.18 Example of component type-approval with other(s) previously type-approved components: External GNSS Facility Facility with previously type-approved Vehicle Unit and Motion Sensor. Different VU/MS manufacturers. .................................................. 32

2.2.19 Example of component type-approval with other(s) previously type-approved components: External Remote Communication Facility with previously type-approved Vehicle Unit(Main Body) and Motion Sensor. Single VU/MS manufacturer. .................................................. 34

2.2.20 Example of component type-approval with other(s) previously type-approved components: External Remote Communication Facility with previously type-approved Vehicle Unit(Main Body) and Motion Sensor. Different VU/MS manufacturers. .................................................. 35

2.3 Schemes for revisions/extensions of type-approvals .................................................. 37

2.3.1 Type-approval revision schemes for tachograph cards ........................................... 38

2.3.2 Type-approval extension schemes for tachograph cards ........................................... 39

2.3.3 Type-approval revision schemes for recording equipment ........................................... 40

2.3.4 Type-approval extension schemes for recording equipment ........................................... 41

2.3.5 Type-approval revision schemes for components of recording equipment .......................... 42

2.3.6 Type-approval extension schemes for components of recording equipment. .......................... 44

3 Guidance for tachograph sealing ................................................................................. 46

3.1 Overview of the legal requirements ............................................................................. 46

3.2 What needs to be sealed? ............................................................................................. 47

3.3 What doesn’t need to be sealed? .................................................................................... 48

4 Annexes ......................................................................................................................... 50

4.1 Annex 1 Rationale for type approvable components ..................................................... 50

4.2 Annex 2 Commented legislative requirements for the type approval process .............. 57

4.3 Annex 3 Commented legislative requirements related to markings ................................. 69

4.4 Annex 4: List of suggested Second-Generation Tachograph cryptographic functional tests ................................................................................................................................. 70

4.4.1 Vehicle Units ............................................................................................................. 70

4.4.2 Tachograph Cards .................................................................................................... 71

4.4.3 External GNSS Facilities .......................................................................................... 73

4.4.4 Motion Sensors ........................................................................................................ 74

4.5 Annex 5 Commented legislative requirements concerning seals .................................. 75

4.6 Annex 5: Frequently Asked Questions .......................................................................... 88

List of abbreviations and definitions ............................................................................... 90
**Abstract**

This report contains guidelines for Smart Tachograph type-approval, for use by stakeholders, such as type-approval authorities, tachograph cards or recording equipment manufacturers, vehicle manufacturers, ...

A number of type-approval schemes are provided for tachograph cards, recording equipment or their components, graphically representing stakeholders’ exchanges at all steps.

Recording equipment or component type-approval schemes are considered.

Various recording equipment setups are also taken into account.

Schemes for first type-approval are detailed, as well as schemes for type-approval extensions or revisions.

Guidelines are also provided regarding parts and/or connections that need to be sealed.

In Annexes of this report:

- A rationale explaining which are the type-approvable components is provided, as well as commented legislative requirements for the type approval process, markings, and seals.
- A list of suggested Second-Generation Tachograph cryptographic functional tests is provided.

At the end of the document, Frequently Asked Questions are provided.
1 Introduction

Several Regulations provide requirements regarding type-approval of Smart Tachographs:

- COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 of 18 March 2016 brings clarifications to the definitions and provisions of REGULATION (EU) No 165/2014,

This report contains guidelines for Smart Tachograph type-approval and sealing, for use by stakeholders, such as type-approval authorities, tachograph cards or recording equipment manufacturers, vehicle manufacturers, ...

Its purpose is to facilitate understanding of the requirements regarding type-approval and sealing found in these Regulations.
2 Type-approval schemes

This Chapter provides type-approval schemes:

- for tachograph cards
- for recording equipment or its components

In all schemes, manufacturer means manufacturer or its agent.

Notes:

- Interoperability tests may only begin after the JRC has received from the requesting manufacturer(s) a complete recording equipment or a complete set of tachograph cards.
- All tachograph cards functional tests specified in Annex 1C Appendix 9 section 2.1 Card Body Printed Design (requirements (227) to (236)) may alternately be attached to the Card Personalisation, and performed with the other tests specified in section 8.1 Personalisation – Optical Personalisation.
- The tests proving that vehicle units, tachograph cards, motion sensors and external GNSS facilities support all the cryptographic mechanisms specified in Annex 1C Appendix 11 are part of their functional tests. Indeed such tests are not fully covered by interoperability tests. For instance, the tests proving that vehicle units, tachograph cards, motion sensors and external GNSS facilities support link certificates usage is not part of the interoperability tests. Annex 4 (in section 44.4) contains a list of suggested cryptographic tests to be carried out during functional testing.
2.1 Tachograph Cards type-approval scheme

This Chapter provides the tachograph cards type-approval schemes.

<table>
<thead>
<tr>
<th>Tachograph Card Manufacturer</th>
<th>Recognised Certification Body</th>
<th>Type-Approval Authority</th>
<th>JRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests Tachograph Card security certificate</td>
<td>Delivers Tachograph Card security certificate when certification is granted</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requests Tachograph Card functional certificate</td>
<td>Provides samples of candidate Tachograph Card and test material</td>
<td>Provides documentation for performing Tachograph Card functional tests</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provides Tachograph Card functional certificate, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results</td>
<td>Requests for interoperability tests</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides set of material and documents necessary for performing interoperability tests</td>
<td>Provides Tachograph Card security certificates</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provides Tachograph Card functional certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivers interoperability certificate after interoperability tests have been successfully passed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requests for Tachograph Card type-approval</td>
<td>Provides Tachograph Card security certificates</td>
<td>Provides Tachograph Card interoperability certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Makes available as many samples as necessary for the type-approval procedure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides specifications and information to be attached to the type-approval certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides information folder (package) for the Tachograph Card</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issues Tachograph Card type-approval certificate if compliant with administrative and technical requirements</td>
<td>Sends copies to the JRC</td>
<td>Issues type approval mark</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.2 Type-approval schemes for recording equipment

This Chapter provides examples of various type-approval schemes that are possible to follow.

The schemes are not exhaustive and don’t cover all possible cases.

Other schemes may be derived from the schemes described in this document and can be added later if needed.
2.2.1 Recording equipment type-approval, composed by a (single body) Vehicle Unit and a Motion Sensor

In this scheme, there is one single recording equipment manufacturer and one single type-approval authority.

Recording Equipment Manufacturer | Recognised Certification Body | Type-Approval Authority
--- | --- | ---
Requests VU/MS security certificates | Delivers VU/MS security certificates when certification is granted | Requests functional certificate
Delivers VU/MS security certificates when certification is granted | Provides samples of candidate VU/MS and test material | Provides documentation for performing VU/MS functional tests
Requests functional certificate | Provides documentation for performing VU/MS functional tests | Provides recording equipment functional certificate after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results
Provides recording equipment functional certificate after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results | Provides set of material and documents necessary for performing interoperability tests | Provides VU/MS security certificates
Provides VU/MS security certificates | Provides recording equipment functional certificate | Delivers interoperability certificate after interoperability tests have been successfully passed
Delivers interoperability certificate after interoperability tests have been successfully passed | Requests for interoperability tests | Issues recording equipment type-approval certificate if compliant with administrative and technical requirements
Requests for interoperability tests | Provides VU/MS security certificates | Sends copies to the JRC
Provides VU/MS security certificates | Provides recording equipment interoperability certificate | Issues type approval mark (same number for VU/MS)
Provides recording equipment interoperability certificate
Makes available as many samples as necessary for the type-approval procedure
Provides specifications and information (incl. regarding seals) to be attached to the type-approval certificate | Provides information folder (package) for the recording equipment
Issues recording equipment type-approval certificate if compliant with administrative and technical requirements
Sends copies to the JRC
Issues type approval mark (same number for VU/MS)

Notes:
- Antennas may be inside the VU housing
- Splitters, if any, are not represented
2.2.2 Recording equipment type-approval, composed by a Vehicle Unit (Main Body), an External GNSS Facility and a Motion Sensor

In this scheme, there is one single recording equipment manufacturer and one single type-approval authority.

**Recording Equipment Manufacturer**
- Requests VU(main body)/MS/EGF security certificates
- Provides samples of candidate VU(main body)/MS/EGF and test material
- Provides documentation for performing VU(main body)/MS/EGF functional tests

**Recognised Certification Body**
- Requests functional certificate
- Provides VU(main body)/MS/EGF security certificates when certification is granted
- Provides recording equipment interoperability certificate
- Makes available as many samples as necessary for the type-approval procedure
- Provides specifications and information (incl. regarding seals) to be attached to the type-approval certificate
- Provides information folder (package) for the recording equipment

**Type-Approval Authority**
- Requests for interoperability tests
- Provides set of material and documents necessary for performing interoperability tests
- Provides VU(main body)/MS/EGF security certificates
- Provides recording equipment functional certificate

**JRC**
- Requests for interoperability tests
- Provides VU(main body)/MS/EGF security certificates
- Provides recording equipment functional certificate
- Delivers interoperability certificate after interoperability tests have been successfully passed

**Issues recording equipment type-approval certificate if compliant with administrative and technical requirements**
- Sends copies to the JRC
- Issues type approval mark (same number for VU(main body)/MS/EGF)

Notes:
- Antennas may be inside the VU/EGF housing
- Splitters, if any, are not represented
2.2.3 Recording equipment type-approval, composed by a Vehicle Unit main body, an External Remote Communication Facility and a Motion Sensor

In this scheme, there is one single recording equipment manufacturer and one single type-approval authority.

- **Recording Equipment Manufacturer**
  - Requests VU(main body)/MS security certificates
  - Delivers VU(main body)/MS security certificates when certification is granted
  - Requests recording equipment functional certificate
  - Provides samples of candidate VU(main body)/MS/ERCF and test material
  - Provides documentation for performing VU(main body)/MS/ERCF functional tests
  - Provides recording equipment functional certificate, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results
  - Requests for interoperability tests
  - Provides set of material and documents necessary for performing interoperability tests
  - Provides VU(main body)/MS security certificates
  - Provides recording equipment functional certificate
  - Issues recording equipment type-approval certificate if compliant with administrative and technical requirements
  - Sends copies to the JRC

- **Recognised Certification Body**
  - Provides samples of candidate VU(main body)/MS/ERCF and test material
  - Provides documentation for performing VU(main body)/MS/ERCF functional tests
  - Provides VU(main body)/MS security certificates

- **Type-Approval Authority**
  - Provides VU(main body)/MS security certificates
  - Provides recording equipment functional certificate
  - Delivers interoperability certificate after interoperability tests have been successfully passed
  - Provides VU(main body)/MS security certificates
  - Provides recording equipment functional certificate

- **JRC**
  - Requests for interoperability tests
  - Provides set of material and documents necessary for performing interoperability tests
  - Provides VU(main body)/MS security certificates
  - Provides recording equipment functional certificate
  - Issues recording equipment type-approval certificate if compliant with administrative and technical requirements
  - Sends copies to the JRC

Notes:
- Antennas may be inside the VU/ERCF housing
- Splitters, if any, are not represented
2.2.4 Recording equipment type-approval, composed by a Vehicle Unit main body, an External GNSS Facility, an External Remote Communication Facility and a Motion Sensor

In this scheme, there is one single recording equipment manufacturer and one single type-approval authority.

Recording Equipment Manufacturer
- Requests VU(main body)/MS/EGF security certificates
- Provides candidate VU(main body)/MS/EGF/ERCF and test material
- Provides documentation for performing VU(main body)/MS/EGF/ERCF functional tests
- Provides recording equipment functional certificate, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results
- Requests for interoperability tests
- Provides set of material and documents necessary for performing interoperability tests
- Provides VU(main body)/MS/EGF security certificates
- Provides recording equipment functional certificate

Recognised Certification Body
- Delivers VU(main body)/MS/EGF security certificates when certification is granted
- Requests recording equipment functional certificate
- Provides samples of candidate VU(main body)/MS/EGF/ERCF
- Provides documentation for performing VU(main body)/MS/EGF/ERCF functional tests
- Provides recording equipment functional certificate, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results

Type-Approval Authority
- Issues recording equipment type-approval certificate if compliant with administrative and technical requirements
- Sends copies to the JRC
- Issues type approval mark (same number for VU(main body)/MS/EGF/ERCF)

JRC
- Requests for interoperability tests
- Provides set of material and documents necessary for performing interoperability tests
- Provides VU(main body)/MS/EGF security certificates
- Provides recording equipment functional certificate

Notes:
- Antennas may be inside the EGF/ERCF housing
- Splitters, if any, are not represented
2.2.5 (single body) Vehicle Unit and Motion Sensor component type-approvals. Single VU/MS manufacturer, first type-approval of each component.

In this scheme, there is one single VU/MS manufacturer and one single type-approval authority.

- **VU/MS Manufacturer**: Requests VU/MS security certificates, delivers VU/MS security certificates when certification is granted.
- **Recognised Certification Body**: Requests VU/MS functional certificates, provides samples of candidate VU/MS and test material, provides documentation for performing VU/MS functional tests.
- **Type-Approval Authority**: Provides VU and MS functional certificates, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which VU/MS functional interfaces have been certified.
- **JRC**: Requests for interoperability tests, provides set of material and documents necessary for performing interoperability tests, provides VU/MS security certificates, provides VU/MS functional certificate.
- **Recognised Certification Body**: Delivers interoperability certificate after interoperability tests have been successfully passed.
- **VU/MS Manufacturer**: Requests for VU and MS component type-approvals, provides VU/MS security certificates, provides interoperability certificate, makes available as many samples as necessary for the type-approval procedure, provides specifications and information (incl. regarding seals) to be attached to the VU/MS type-approval certificates, provides information folder (package) for VU/MS.
- **Type-Approval Authority**: Issues VU and MS component type-approval certificate, indicating the type-approval number of the other interoperable component, if compliant with administrative and technical requirements, sends copies to the JRC, issues type approval marks (for VU and MS).

Notes:
Antennas may be inside the VU housing
Splitters, if any, are not represented.
2.2.6 (single body) Vehicle Unit and Motion Sensor component type-approvals. Different VU/MS manufacturers, first type-approval of each component

In this scheme, there are two manufacturers, one for the VU, one for the MS. Let’s assume that they belong to different Member States, and that there are two different type-approval authorities.

Alternately, there may be one type-approval authority only. That’s the case if both manufacturers request functional/type-approval certificate in the same Member State.

Similarly, this scheme assumes that there are two different Security Bodies involved, one certifying the VU, one certifying the MS. Alternately, there may be only one Security Body involved. That’s the case if both manufacturers select the same Security Body for certifying their products.

This scheme needs some kind of agreement, partnership, cooperation or contract between manufacturers. VU-MS interface specification must be available and agreed by both manufacturers (if proprietary). Type-approval authorities coordinate themselves during the parallel type approval procedure.

This scheme needs some kind of communication, synchronisation or harmonization between type-approval authorities.

Notes:
- Antennas may be inside the VU housing
- Splitters, if any, are not represented
2.2.7 Vehicle Unit (main body), External GNSS Facility and Motion Sensor component type-approvals. Single VU/MS/EGF manufacturer, first type-approval of each component

In this scheme, there is one single VU/MS/EGF manufacturer and one single type-approval authority.

VU/MS/EGF Manufacturer Requests VU/MS/EGF security certificates

Recognised Certification Body Delivers VU/MS/EGF security certificates when certification is granted

Requests VU/MS/EGF functional certificates

Provides samples of candidate VU/MS/EGF and test material

Provides documentation for performing VU/MS/EGF functional tests

Provides VU/MS/EGF functional certificates, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which VU/MS/EGF functional interfaces have been certified

Requests interoperability tests

Provides set of material and documents necessary for performing interoperability tests

Provides VU/MS/EGF security certificates

Provides VU/MS/EGF functional certificate

Delivers interoperability certificate after interoperability tests have been successfully passed

Requests for VU/MS/EGF component type-approvals

Provides VU/MS/EGF security certificates

Provides interoperability certificate

Makes available as many samples as necessary for the type-approval procedure

Provides specifications and information (incl. regarding seals) to be attached to the VU/MS/EGF type-approval certificates

Provides information folder (package) for VU/MS/EGF

Issues VU/MS/EGF component type-approval certificate, indicating the type-approval number of the other interoperable components, if compliant with administrative and technical requirements

Issues type approval marks (for VU, MS and EGF)

Sends copies to the JRC

Working document 16

Notes:
Antennas may be inside the VU/EGF housing
Splitters, if any, are not represented
2.2.8 Vehicle Unit (main body), External GNSS Facility and Motion Sensor component type-approvals. Different VU/MS/EGF manufacturers, first type-approval of each component

In this scheme, there are up to three manufacturers, one for the VU, one for the MS and one for the EGF. Let’s assume that they belong to different Member States, and that there are three different type-approval authorities.

Alternately, there may be one or two type-approval authority only. That’s the case if one or more manufacturers request functional/type-approval certificate in the same Member State.

Similarly, this scheme assumes that there are up to three different Security Bodies involved, one certifying the VU, one certifying the MS and one certifying the EGF. Alternately, there may be only one or two Security Bodies involved. That’s the case if one or more manufacturers select the same Security Body for certifying their products.

This scheme needs some kind of agreement, partnership, cooperation or contract between manufacturers. VU-MS interface specification must be available and agreed by VU-MS manufacturers (if proprietary). Type-approval authorities coordinate themselves during the parallel type approval procedure.

This scheme needs some kind of communication, synchronisation or harmonization between type-approval authorities.
2.2.9 Vehicle Unit (main body), External Remote Communication Facility and Motion Sensor component type-approvals. Single VU/MS/ERCF manufacturer, first type-approval of each component.

In this scheme, there is one single VU/MS/ERCF manufacturer and one single type-approval authority.

### Diagram

- **VU/MS/EGF Manufacturer**
  - Requests VU/MS security certificates
  - Provides VU/MS security certificates when certification is granted
  - Makes available as many samples as necessary for the type-approval procedure
  - Provides specifications and information (incl. regarding seals) to be attached to the VU/MS/ERCF type-approval certificates
  - Provides information folder (package) for VU/MS/ERCF
  - Issues VU/MS/ERCF component type-approval certificate, indicating the type-approval number of the other interoperable components, if compliant with administrative and technical requirements
  - Sends copies to the JRC
  - Issues type approval marks (for VU, MS and ERF)

- **Recognised Certification Body**
  - Requests VU/MS/ERCF functional certificates
  - Provides documentation for performing VU/MS/ERCF functional tests
  - Provides VU/MS/ERCF functional certificates, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which VU/MS/ERCF functional interfaces have been certified

- **Type-Approval Authority**
  - Requests for interoperability tests
  - Provides set of material and documents necessary for performing interoperability tests
  - Provides VU/MS security certificates
  - Provides VU/MS/ERCF functional certificate
  - Delivers interoperability certificate after interoperability tests have been successfully passed

- **JRC**
  - Requests for interoperability tests
  - Provides set of material and documents necessary for performing interoperability tests
  - Provides VU/MS security certificates
  - Provides VU/MS/ERCF functional certificate
  - Delivers interoperability certificate after interoperability tests have been successfully passed

Notes:
- Antennas may be inside the VU/ERCF housing
- Splitters, if any, are not represented
2.2.10 Vehicle Unit (main body), External Remote Communication Facility and Motion Sensor component type-approvals. Different VU/MS/ERCF manufacturers, first type-approval of each component

In this scheme, there are up to three manufacturers, one for the VU, one for the MS and one for the ERCF. Let’s assume that they belong to different Member States, and that there are three different type-approval authorities.

Alternately, there may be one or two type-approval authority only. That’s the case if one or more manufacturers request functional/type-approval certificate in the same Member State.

Similarly, this scheme assumes that there are up to two different Security Bodies involved, one certifying the VU, one certifying the MS. Alternately, there may be only one Security Body involved. That’s the case if the MS manufacturer select the same Security Body as the VU manufacturer for certifying its product.

This scheme needs some kind of agreement, partnership, cooperation or contract between manufacturers. VU-MS interface specification must be available and agreed by VU-MS manufacturers (if proprietary). Type-approval authorities coordinate themselves during the parallel type approval procedure.

This scheme needs some kind of communication, synchronisation or harmonization between type-approval authorities.

Notes:
Antennas may be inside the VU/ERCF housing
Splitters, if any, are not represented
### Smart Tachograph Type-approval guidelines v0.5 - DRAFT

<table>
<thead>
<tr>
<th>VU Manufacturer</th>
<th>Recognised Certification Body 1</th>
<th>MS Type-Approval Authority 1</th>
<th>JRC</th>
<th>MS Type-Approval Authority 2/3</th>
<th>Recognised Certification Body 2</th>
<th>MS Manufacturer</th>
<th>ERCF Manufacturer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests VU security certificate &amp; VU functional certificate</td>
<td>Provides VU security certificate</td>
<td>Provides VU security certificate</td>
<td>Provides MS security certificate</td>
<td>Requests MS/ERCF functional certificates &amp; MS security certificates</td>
<td>Provides MS/ERCF functional certificates</td>
<td>Delivers MS security certificate when certification is granted</td>
<td>Request MS security certificate</td>
</tr>
<tr>
<td>Provides samples of candidate VU and test material</td>
<td>Provides documentation for performing VU functional tests</td>
<td>Provides VU functional certificate, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which VU functional interfaces have been certified</td>
<td>Provides VU functional certificate</td>
<td>Provides MS/ERCF functional certificates</td>
<td>Request MS/ERCF functional certificates</td>
<td>Provides functional and security certificates for VU &amp; ERCF</td>
<td>Provides MS/ERCF functional certificates</td>
</tr>
<tr>
<td>Provides MS/ERCF functional and security certificates</td>
<td></td>
<td></td>
<td>Provides VU security certificate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requests for interoperability tests</td>
<td>Provides set of material and documents necessary for performing interoperability tests</td>
<td>Provides VU/MS security certificates &amp; VU/MS/ERCF functional certificates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivers interoperability certificate after interoperability tests have been successfully passed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requests for VU component type-approval</td>
<td>Provides interoperability certificate</td>
<td>Provides MS/ERCF functional certificates</td>
<td></td>
<td>Issue MS/ERCF component type-approval certificate, indicating the type-approval number of the interoperable components, if compliant with administrative and technical requirements</td>
<td>Send copies to the JRC</td>
<td>Issue type approval marks for MS/ERCF</td>
<td></td>
</tr>
<tr>
<td>Provides interoperability certificate</td>
<td></td>
<td></td>
<td></td>
<td>Provide information folder (package) for MS/ERCF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issues VU component type-approval certificate, indicating the type-approval number of the interoperable components, if compliant with administrative and technical requirements</td>
<td>Sends copies to the JRC</td>
<td>Issues type approval marks for VU</td>
<td></td>
<td>Issue MS/ERCF component type-approval certificate, indicating the type-approval number of the interoperable components, if compliant with administrative and technical requirements</td>
<td>Send copies to the JRC</td>
<td>Issue type approval marks for MS/ERCF</td>
<td></td>
</tr>
<tr>
<td>Issues VU security certificate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Working document
2.2.11 Vehicle Unit (main body), External GNSS Facility, External Remote Communication Facility and Motion Sensor component type-approvals. Single VU/MS/EGF/ERCF manufacturer, first type-approval of each component

In this scheme, there is one single VU/MS/EGF/ERCF manufacturer and one single type-approval authority.

<table>
<thead>
<tr>
<th>VU/MS/EGF/ERCF Manufacturer</th>
<th>Recognised Certification Body</th>
<th>Type-Approval Authority</th>
<th>JRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests VU/MS/EGF security certificates</td>
<td>Delivers VU/MS/EGF security certificates when certification is granted</td>
<td>Requests VU/MS/EGF/ERCF functional certificates</td>
<td>Provides samples of candidate VU/MS/EGF/ERCF and test material</td>
</tr>
<tr>
<td>Provides documentation for performing VU/MS/EGF/ERCF functional tests</td>
<td>Provides VU/MS/EGF/ERCF functional certificates, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which VU/MS/EGF/ERCF functional interfaces have been certified</td>
<td>Requests for interoperability tests</td>
<td>Provides set of material and documents necessary for performing interoperability tests</td>
</tr>
<tr>
<td>Provides VU/MS/EGF security certificates</td>
<td>Provides VU/MS/EGF/ERCF functional certificate</td>
<td>Delivers interoperability certificate after interoperability tests have been successfully passed</td>
<td>Provides VU/MS/EGF security certificates</td>
</tr>
<tr>
<td>Provides VU/MS/EGF/ERCF component type-approvals</td>
<td>Provides interoperability certificate</td>
<td>Makes available as many samples as necessary for the type-approval procedure</td>
<td>Provides specifications and information (incl. regarding seals) to be attached to the VU/MS/EGF/ERCF type-approval certificates</td>
</tr>
<tr>
<td>Provides information folder (package) for VU/MS/EGF/ERCF</td>
<td>Issues VU/MS/EGF/ERCF component type-approval certificate, indicating the type-approval number of the other interoperable components, if compliant with administrative and technical requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sends copies to the JRC</td>
<td>Issues type approval marks (for VU, MS, EGF and ERCF)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes:
- Antennas may be inside the EGF/ERCF housing
- Splitters, if any, are not represented
2.2.12 Vehicle Unit (main body), External GNSS Facility, External Remote Communication Facility and Motion Sensor component type-approvals. Different VU/MS/EGF/ERCF manufacturers, first type-approval of each component

In this scheme, there are up to four manufacturers, one for the VU, one for the MS, one for the EGF and one for the ERCF. Let’s assume that they belong to different Member States, and that there are four different type-approval authorities.

Alternately, there may be one, two or three type-approval authorities only. That’s the case if one or more manufacturers request functional/type-approval certificate in the same Member State.

Similarly, this scheme assumes that there are up to three different Security Bodies involved, each of them certifying a component (VU, MS, EGF). Alternately, there may be only one or two Security Bodies involved. That’s the case some manufacturers select the same Security Body as others for certifying their product.

This scheme needs some kind of agreement, partnership, cooperation or contract between manufacturers. VU-MS interface specification must be available and agreed by VU-MS manufacturers (if proprietary). Type-approval authorities coordinate themselves during the parallel type approval procedure.

This scheme needs some kind of communication, synchronisation or harmonization between type-approval authorities.

Notes:
Antennas may be inside the EGF/ERCF housing
Splitters, if any, are not represented
2.2.13 Example of component type-approval with other(s) previously type-approved components: (single body) Vehicle Unit with previously type-approved Motion Sensor. Single VU/MS manufacturer.

In this scheme, there is one single VU/MS manufacturer and one single type-approval authority (which has previously type-approved the MS).

### Diagram Description

- **VU/MS Manufacturer**
  - Requests VU security certificate
  - Sends copies to the JRC
  - Provides VU functional certificate, after VU functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which VU functional interfaces have been certified
  - Requests for VU component type-approval (with MS)
  - Provides VU security certificates
  - Provides interoperability certificate
  - Makes available as many samples as necessary for the type-approval procedure
  - Provides specifications and information (incl. regarding seals) to be attached to the VU type-approval certificate
  - Provides information folder (package) for VU

- **Recognised Certification Body**
  - Request VU functional certificate
  - Provides samples of candidate VU and test material
  - Provides documentation for performing VU functional tests
  - Provides VU functional certificate, after VU functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which VU functional interfaces have been certified

- **Type-Approval Authority**
  - Requests for interoperability tests
  - Provides set of material and documents necessary for performing interoperability tests
  - Provides VU/MS security certificates
  - Provides VU/MS functional certificate
  - Provides MS type-approval certificate

- **JRC**
  - Requests for interoperability tests
  - Provides set of material and documents necessary for performing interoperability tests
  - Provides VU/MS security certificates
  - Provides VU/MS functional certificate
  - Provides MS type-approval certificate

**Notes:**
- Antennas may be inside the VU housing
- Splitters, if any, are not represented

**Note:** the manufacturer has already the MS security, functional and type-approval certificates.

**Note:** the JRC may already have the MS functional, security and type-approval certificates.

**Note:** the type-approval Authority has already the MS security, functional and type-approval certificates, so the VU manufacturer doesn’t have to provide them.
2.2.14 Example of component type-approval with other(s) previously type-approved components: (single body) Vehicle Unit with previously type-approved Motion Sensor. Different VU/MS manufacturers.

In this scheme, there are two manufacturers, one for the VU, one for the MS. Let’s assume that they belong to different Member States, and that there are two different type-approval authorities.

Alternately, there may be one type-approval authority only. That’s the case if both manufacturers request functional/type-approval certificate in the same Member State.

In this scheme, there is only one Security Body involved, because there is no action regarding the MS security.

This scheme needs some kind of agreement, partnership, cooperation or contract between manufacturers. VU-MS interface specification must be available to VU manufacturer (if proprietary).

This scheme needs some kind of communication, synchronisation or harmonization between type-approval authorities.

Notes:
Antennas may be inside the VU housing
Splitters, if any, are not represented
**Smart Tachograph Type-approval guidelines v0.5 - DRAFT**

**VU Manufacturer**
- Requests VU security certificate
- Delivers VU security certificate when certification is granted
- Provides VU functional certificate
- Provides samples of candidate VU and test material
- Provides documentation for performing VU functional tests
- Provides VU functional certificate, after functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which VU functional interfaces have been certified
- Provides MS functional, security and type-approval certificate (if needed)
- Requests for interoperability tests
- Provides set of material and documents necessary for performing interoperability tests
- Delivers interoperability certificate after interoperability tests have been successfully passed
- Requests for VU component type-approval with MS
- Provides VU security certificate
- Provides interoperability certificate
- Makes available as many samples as necessary for the type-approval procedure
- Provides specifications and information (incl. regarding seals) to be attached to the VU type-approval certificate
- Provides information folder (package) for VU
- Issues VU component type-approval certificate, indicating the type-approval number of the interoperable VU, if compliant with administrative and technical requirements
  - Sends copies to the JRC
  - Issues type approval mark for VU

**Recognised Certification Body**
- Provides VU security certificate
- Provides VU functional certificate
- Provides MS functional, security and type-approval certificates (if not already provided)
- Provides set of material and documents necessary for performing VU functional tests
- Provides VU and MS security certificate
- Provides VU and MS functional certificates
- Provides MS type-approval certificate
- Provides interoperability certificate

**Type-Approval Authority 1**
- Provides VU security certificate
- Provides MS security, functional and type-approval certificates (if not already provided)
- May exchange information / provide advice during functional test certification
- Provides VU functional certificate

**JRC**
- Informs about new VU type-approval with MS
- Provides VU security certificate
- Provides VU functional certificate

**Type-Approval Authority 2**
- Provides VU type-approval certificate
- Provides revised MS type-approval certificate
- Issues revised or extended MS component type-approval certificate, indicating the type-approval number of the interoperable VU, if compliant with administrative and technical requirements
  - Sends copies to the JRC

**MS Manufacturer**
- Issues VU and MS security certificate
- Provides VU and MS functional certificates
- Provides MS type-approval certificate
- Delivers interoperability certificate after interoperability tests have been successfully passed
- Requires VU security certificate
- Recognised Certification Body
- Provides VU security certificate
- Provides VU security certificate
- Provides VU functional certificate
- Provides VU functional certificate
- Provides set of material and documents necessary for performing interoperability tests
- Provides VU and MS security certificate
- Provides VU and MS functional certificates
- Provides MS type-approval certificate
- Issues revised or extended MS component type-approval certificate, indicating the type-approval number of the interoperable VU, if compliant with administrative and technical requirements
  - Sends copies to the JRC

Note: MS type-approval authority has already the MS security and functional certificates

Note: the JRC may already have the MS functional, security and type-approval certificates.
2.2.15 Example of component type-approval with other(s) previously type-approved components: Motion Sensor with with previously type-approved (single body) Vehicle Unit. Single VU/MS manufacturer.

In this scheme, there is one single VU/MS manufacturer and one single type-approval authority (which has previously type-approved the MS).

Notes:
- Antennas may be inside the VU housing
- Splitters, if any, are not represented

Note: the manufacturer has already the VU security, functional and type-approval certificates.

Note: the JRC may already have the VU security, functional and type-approval certificates.

Note: the type-approval Authority has already the VU security, functional and type-approval certificates, so the MS manufacturer doesn’t have to provide them.
2.2.16 Example of component type-approval with other(s) previously type-approved components: Motion Sensor with previously type-approved (single body) Vehicle Unit. Different VU/MS manufacturers.

In this scheme, there are two manufacturers, one for the VU, one for the MS. Let’s assume that they belong to different Member States, and that there are two different type-approval authorities.

Alternately, there may be one type-approval authority only. That’s the case if both manufacturers request functional/type-approval certificate in the same Member State.

In this scheme, there is only one Security Body involved, because there is no action regarding the VU security.

This scheme needs some kind of agreement, partnership, cooperation or contract between manufacturers. VU-MS interface specification must be available to MS manufacturer (if proprietary).

This scheme needs some kind of communication, synchronisation or harmonization between type-approval authorities.

Notes:
Antennas may be inside the VU housing
Splitters, if any, are not represented
2.2.17 Example of component type-approval with other(s) previously type-approved components: External GNSS Facility Facility with previously type-approved Vehicle Unit(Main Body) and Motion Sensor. Single VU/EGF/MS manufacturer.

In this scheme, there is one single VU(Main Body)/EGF/MS manufacturer and one single type-approval authority (which has previously type-approved the VU(Main Body)/MS)

**VU/EGF/MS Manufacturer**
- Requests EGF security certificate
- Delivers EGF security certificate when certification is granted
  - Request EGF functional certificate
  - Provides samples of candidate EGF and test material
  - Provides documentation for performing EGF functional tests
  - Provides EGF functional certificate, after EGF functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which VU functional interfaces have been certified
  - Requests for interoperability tests (if needed)
  - Provides set of material and documents necessary for performing interoperability tests
  - Provides VU/EGF/MS security certificates
  - Provides VU/EGF/MS functional certificate, provides VU/MS type-approval certificates
  - Delivers interoperability certificate after interoperability tests have been successfully passed

**Recognised Certification Body**

**Type-Approval Authority**

**JRC**

**Working document**
- Sends copies to the JRC

Notes:
- Antennas may be inside the VU/EGF housing
- Splitters, if any, are not represented

**Notes:**
- The manufacturer has already the VU/MS security, functional and type-approval certificates.
- The JRC may already have the VU/MS security, functional and type-approval certificates.
- The type-approval Authority has already the VU/MS security, functional and type-approval certificates, so the EGF manufacturer doesn’t have to provide them.
2.2.18 Example of component type-approval with other(s) previously type-approved components: External GNSS Facility with previously type-approved Vehicle Unit and Motion Sensor. Different VU/MS manufacturers.

In this scheme, there are up to three manufacturers, one for the VU, one for the EGF, and one for the MS. Let’s assume that they belong to different Member States, and that there are three different type-approval authorities.

Alternately, there may be one or two type-approval authorities only. That’s the case if some manufacturers request functional/type-approval certificate in the same Member State.

In this scheme, there is only one Security Body involved, because there is no action regarding the VU/MS security.

This scheme needs some kind of agreement, partnership, cooperation or contract between manufacturers.

This scheme needs some kind of communication, synchronisation or harmonization between type-approval authorities.

Notes:
- Antennas may be inside the VU/EGF housing
- Splitters, if any, are not represented
2.2.19 Example of component type-approval with other(s) previously type-approved components: External Remote Communication Facility with previously type-approved Vehicle Unit(Main Body) and Motion Sensor. Single VU/MS manufacturer.

In this scheme, there is one single VU(main body)/ERCF/MS manufacturer and one single type-approval authority (which has previously type-approved the VU(Main Body) and the MS)

<table>
<thead>
<tr>
<th>VU/ERCF/MS Manufacturer</th>
<th>Type-Approval Authority</th>
<th>JRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request ERCF functional certificate</td>
<td>Provides samples of candidate ERCF and test material</td>
<td>Requests for interoperability tests (if needed)</td>
</tr>
<tr>
<td>Provides ERCF functional certificate, after ERCF functional tests have been successfully passed (min. list in Ann. 1C App. 9), with detailed list of passed tests and results, and indicating ISO or CEN standards against which ERCF functional interfaces have been certified</td>
<td>Provides set of material and documents necessary for performing interoperability tests</td>
<td>Provides VU/MS security certificates</td>
</tr>
<tr>
<td>Requests for interoperability tests (if needed)</td>
<td>Provides VU/ERCF/MS functional certificates, provides VU/MS type-approval certificates</td>
<td>Provides VU/MS type-approval certificates</td>
</tr>
<tr>
<td>Delivers interoperability certificate after interoperability tests have been successfully passed (if needed)</td>
<td></td>
<td>Delivers interoperability certificate after interoperability tests have been successfully passed (if needed)</td>
</tr>
<tr>
<td>Requests for ERCF component type-approval (with VU/MS)</td>
<td>Provides interoperability certificate (if needed)</td>
<td>Note: the type-approval Authority has already the VU/MS security, functional and type-approval certificates.</td>
</tr>
<tr>
<td>Provides interoperability certificate (if needed)</td>
<td>Makes available as many samples as necessary for the type-approval procedure</td>
<td>Note: the manufacturer has already the VU/MS security, functional and type-approval certificates.</td>
</tr>
<tr>
<td>Provides specifications and information (incl. regarding seals) to be attached to the ERCF type-approval certificate</td>
<td>Provides information folder (package) for ERCF</td>
<td>Note: the JRC may already have the VU/MS security, functional and type-approval certificates.</td>
</tr>
<tr>
<td>Issues ERCF component type-approval certificate, indicating the type-approval number of the interoperable VU/MS, if compliant with administrative and technical requirements</td>
<td>Issues revised or extended VU/MS type-approval certificate (mentioning ERCF)</td>
<td>Note: the JRC may already have the VU/MS security, functional and type-approval certificates.</td>
</tr>
<tr>
<td></td>
<td>Sends copies to the JRC</td>
<td>Note: the type-approval Authority has already the VU/MS security, functional and type-approval certificates, so the ERCF manufacturer doesn’t have to provide them.</td>
</tr>
</tbody>
</table>

Notes:
- Antennas may be inside the VU/ERCF housing
- Splitters, if any, are not represented
2.2.20 Example of component type-approval with other(s) previously type-approved components: External Remote Communication Facility with previously type-approved Vehicle Unit (Main Body) and Motion Sensor. Different VU/MS manufacturers.

In this scheme, there are up to three manufacturers, one for the VU, one for the ERCF, and one for the MS. Let’s assume that they belong to different Member States, and that there are three different type-approval authorities.

Alternately, there may be one or two type-approval authorities only. That’s the case if some manufacturers request functional/type-approval certificate in the same Member State.

In this scheme, there is no Security Body involved, because there is no action regarding the VU/MS security, and the ERCF is not covered by a security certification.

This scheme needs some kind of agreement, partnership, cooperation or contract between manufacturers.

This scheme needs some kind of communication, synchronisation or harmonization between type-approval authorities.

Notes:
- Antennas may be inside the VU/ERCF housing
- Splitters, if any, are not represented
Provide VU/MS security, functional and type-approval certificates (if not already provided)

May exchange information / provide advice during functional certification

Provides ERCF functional certificate

Note: VU/MS type-approval authorities have already the VU/MS security, functional and type-approval certificates.

Informs about start of a new ERCF type-approval with VU/MS

Note: the JRC may already have the VU/MS security, functional and type-approval certificates.
2.3 Schemes for revisions/extensions of type-approvals

This Chapter provides details of revisions/extensions schemes of tachograph cards, recording equipment, or components type-approval.

Type-approval revisions/extensions are confirmed by type-approval authorities after planned modifications in hardware, software or nature of materials are notified by manufacturers of type-approved equipment.

Type-approval authorities will confirm revisions when such modifications are considered as minor and extensions when such modifications are considered as substantial.

Type-approval authorities may require an update or a confirmation of the relevant functional, security and/or interoperability certificates. They may also require new functional tests to be conducted.

Alternately, type-approval authorities may require to issue a new type approval (e.g. in the case a new security certificate or a new interoperability certificate must be issued).

The schemes are generic and can be applied for various vehicle unit compositions. Where the most complex case is addressed, the type-approval scheme can be simplified as needed.

Note concerning tachograph cards:

In the case a card issuing body of a Member State applies a national optical or electrical personalisation to a previously type-approved card, a type-approval revision/extension shall be asked to the relevant type approval authority. The type-approval authority may require that new functional tests are conducted, and that an update of the card functional certificate is issued.

The requested new functional tests may be selected among the ones in the minimum list in Annex 1C Appendix 9, section 8.1 Personalisation – Optical personalization. Suitable tests related to the electrical personalisation of the card may also be added in case of changes on the card personalisation environment.
2.3.1 Type-approval revision schemes for tachograph cards

This Chapter provides the tachograph cards type-approval revisions schemes.

<table>
<thead>
<tr>
<th>Tachograph Card Manufacturer</th>
<th>Recognised Certification Body</th>
<th>Type-Approval Authority</th>
<th>JRC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Requests confirmation of Tachograph Card security certificate</td>
<td>Confirms Tachograph Card security certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confirms Tachograph Card security certificate</td>
<td>Informs about modifications in software or hardware or nature of material</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submits an application for the modification of the Tachograph Card type approval</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides the updated Tachograph Card information package in consolidated form, and a detailed description of the modifications made.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confirms Tachograph Card functional certificate</td>
<td>Issues revised Tachograph Card type-approval certificate, including revised information to be attached, and indicating the nature of the modifications made and the date of approval</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sends copies to the JRC</td>
<td></td>
</tr>
</tbody>
</table>
2.3.2 Type-approval extension schemes for tachograph cards

This Chapter provides the tachograph cards type-approval revisions schemes. In this scheme, manufacturer means manufacturer or its agent.

The JRC is the single laboratory which issues the interoperability certificates, under the authority and responsibility of the Commission.

---

<table>
<thead>
<tr>
<th>Tachograph Card Manufacturer</th>
<th>Recognised Certification Body</th>
<th>Type-Approval Authority</th>
<th>JRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests confirmation of Tachograph Card security certificate</td>
<td>Confirms Tachograph Card security certificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirms Tachograph Card security certificate</td>
<td>Informs about modifications in software or hardware or nature of material</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Submits an application for the modification of the Tachograph Card type approval</td>
<td>Provides the updated Tachograph Card information package, in consolidated form, and a detailed description of the modifications made.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requests new functional tests to be conducted (if needed)</td>
<td>Provides samples of candidate Tachograph Card and test material (if needed)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provides documentation for performing requested Tachograph Card functional tests (if needed)</td>
<td>Confirms, or provides updated Tachograph Card functional certificate, after requested functional tests have been successfully passed, with detailed list of passed tests and results</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issues extended Tachograph Card type-approval certificate, containing the number of the extension, the reason for the extension and the date of approval</td>
<td>Sends copies to the JRC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3.3 Type-approval revision schemes for recording equipment

This Chapter provides recording equipment type-approval revisions schemes.

In this scheme, manufacturer means manufacturer or its agent.

The JRC is the single laboratory which issues the interoperability certificates, under the authority and responsibility of the Commission.

Recordin...
2.3.4 Type-approval extension schemes for recording equipment

This Chapter provides the recording equipment type-approval revisions schemes.

In this scheme, manufacturer means manufacturer or its agent.

The JRC is the single laboratory which issues the interoperability certificates, under the authority and responsibility of the Commission.
2.3.5 Type-approval revision schemes for components of recording equipment

This Chapter provides type-approval revisions schemes for components of recording equipment.
**Smart Tachograph Type-approval guidelines v0.5 - DRAFT**

**Component Manufacturer**
- Requests confirmation of component security certificate (if applicable)
- Confirms component security certificate
- Informs about modifications in software or hardware or nature of material of the component
- Submits an application for the modification of the component type approval
- Provides the updated component information package, in consolidated form, and a detailed description of the modifications made
- Sends copies to the JRC
- Confirms component functional certificate
- Issues revised component type-approval certificate, including revised information to be attached, and indicating the nature of the modifications made and the date of approval
- Sends copies to the JRC

**Recognised Certification Body**
- Provides component revised type-approval certificate
- Provides revised type-approval certificates of the other components

**Type-Approval Authority for the component**
- Informs about start of a revision of the component type-approval with the others components
- Confirms component security certificate

**Type-Approval Authorities**
- Issue revised component type-approval certificates for the other components, indicating the type-approval number and revision of the interoperable components
- Sends copies to the JRC

**Other components Manufacturers**
- Informs about start of a revision of the component type-approval with the others components
- Confirms component security certificate
- Provides component revised type-approval certificate
2.3.6 Type-approval extension schemes for components of recording equipment.

This Chapter provides type-approval extension schemes for components of recording equipment.
**Smart Tachograph Type-approval guidelines v0.5 - DRAFT**

- **Component Manufacturer**
  - Requests confirmation of component security certificate (if applicable)
  - Confirms component security certificate
  - Informs about modifications in software or hardware or nature of material of the component
  - Submits an application for the modification of the component type approval
  - Provides the updated component information package, in consolidated form, and a detailed description of the modifications made

- **Recognised Certification Body**
  - Requests new functional tests to be conducted (if needed)
  - Provides samples of candidate component and test material (if needed)
  - Provides documentation for performing requested recording equipment functional tests (if needed)
  - Confirms, or provides updated component functional certificate, after requested functional tests have been successfully passed, with detailed list of passed tests and results
  - Issues extended component type-approval certificate, containing the number of the extension, the reason for the extension and the date of approval
  - Sends copies to the JRC

- **Type-Approval Authority for the component**
  - Informs about start of a component type-approval extension with the other components
  - Confirms component security certificate

- **Type-Approval Authorities**
  - Confirms or provides updated component functional certificate
  - Provides component revised type-approval certificate

- **Other Components Manufacturers**
  - Informs about start of a new component type-approval with the other components
  - Issue extended component type-approval certificates for the other components containing the number of the extension, the reason for the extension and the date of approval
  - Sends copies to the JRC

- **Recognised Certification Body**
  - Provides extended type-approval certificates of the other components

---

**Working document 45**
3 Guidance for tachograph sealing

3.1 Overview of the legal requirements

This section provides guidelines for parts and/or connections of smart tachographs that must be sealed, in the scope of the requirements:

- • of Regulation (EU) No 165/2014, CHAPTER 4. Installation and inspection, Article 22,
- • of the Commission Implementing Regulation (EU) 2016/799, as modified by Commission Implementing Regulation (EU) 2018/502, Chapter 5. Installation of recording equipment, 5.3 Sealing,

(see full details of commented regulation text about seals in Annex 5 Commented legislative requirements concerning seals).

According to point 4 of Article 22 of Regulation (EU) No 165/2014:

“Any connections to the tachograph which are potentially vulnerable to tampering, including the connection between the motion sensor and the gearbox, and the installation plaque where relevant, shall be sealed.”

According to requirement (398) of Commission Implementing Regulation (EU) 2016/799, as modified by Commission Implementing Regulation (EU) 2018/502, Section 5.3 Sealing:

“(398) The following parts shall be sealed:

— Any connection which, if disconnected, would cause undetectable alterations to be made or undetectable data loss (this may e.g. apply for the motion sensor fitting on the gearbox, the adaptor for M1/N1 vehicles, the external GNSS connection or the vehicle unit);
— The installation plaque, unless it is attached in such a way that it cannot be removed without the markings thereon being destroyed.”


ADA_034 The following sealing requirements shall apply:

— the adaptor housing shall be sealed (see ADA_017),
— the housing of the embedded sensor shall be sealed to the adaptor housing, unless it is not possible to remove the sensor from the adaptor housing without breaking the seal(s) of the adaptor housing (see ADA_018),
— the adaptor housing shall be sealed to the vehicle,
— the connection between the adaptor and the equipment which provides its incoming pulses shall be sealed on both ends (to the extent of what is reasonably possible).

Any seal in scope of these requirements shall be certified according to EN 16882:2016 standard.

### 3.2 What needs to be sealed?

The table below provides a list of requested sealing points, along with the relevant rationales.

<table>
<thead>
<tr>
<th>Sealing point</th>
<th>Rationale/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection between the motion sensor and the gearbox</td>
<td>Requested by Article 22 of Regulation (EU) No 165/2014. This connection is potentially vulnerable to tampering. The speed signal is one of the main target for attackers.</td>
</tr>
<tr>
<td>Fixation of the installation plaque to the vehicle</td>
<td>Requested by Article 22 of Regulation (EU) No 165/2014. Only applicable for installation plaques which are attached in such a way that they can be removed without the markings thereon being destroyed.</td>
</tr>
<tr>
<td>(When an adaptor is used) Fixation of the housing of the embedded sensor to the adaptor housing</td>
<td>Requested by Appendix 16 of Commission Implementing Regulation (EU) 2016/799, as modified by Commission Implementing Regulation (EU) 2018/502 (ADA_034). Only applicable if it is possible to remove the sensor from the adaptor housing without breaking the seal(s) of the adaptor housing.</td>
</tr>
<tr>
<td>(When an adaptor is used) Fixation of the adaptor housing to the vehicle</td>
<td>Requested by Appendix 16 of Commission Implementing Regulation (EU) 2016/799, as modified by Commission Implementing Regulation (EU) 2018/502 (ADA_034).</td>
</tr>
<tr>
<td>(When an adaptor is used) Both ends of the connection between the adaptor and the equipment which provides its incoming pulses</td>
<td>Requested by Appendix 16 of Commission Implementing Regulation (EU) 2016/799, as modified by Commission Implementing Regulation (EU) 2018/502 (ADA_034). Sealing is only requested, to the extent of what is reasonably possible).</td>
</tr>
</tbody>
</table>
### 3.3 What doesn’t need to be sealed?

The table below provides a list of points that don’t need to be sealed, along with the relevant rationales.

<table>
<thead>
<tr>
<th>Potential sealing point</th>
<th>Rationale/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection of the installation plaque to the vehicle</td>
<td>Not requested, for installation plaques which are attached in such a way that they cannot be removed without the markings thereon being destroyed.</td>
</tr>
<tr>
<td><em>(When an adaptor is used)</em> Fixation of the housing of the embedded sensor to the adaptor housing</td>
<td>Requested by Appendix 16 of Commission Implementing Regulation (EU) 2016/799, as modified by Commission Implementing Regulation (EU) 2018/502 (ADA_034). Only applicable if it is possible to remove the sensor from the adaptor housing without breaking the seal(s) of the adaptor housing.</td>
</tr>
<tr>
<td><em>(When an adaptor is used)</em> Any end of the connection between the adaptor and the equipment which provides its incoming pulses</td>
<td>Not requested, if it is reasonably not possible to seal the end of the connection (absence of fixation point, lack of space, ...)</td>
</tr>
<tr>
<td>The connection between the motion sensor and the vehicle unit</td>
<td>This is because the connection is digitally secured (through pairing of the vehicle unit and the EGF, followed by mutual authentication between the vehicle unit and the EGF, and the secured communication ensuring confidentiality of exchanged data). Tamper evidence can be traced, by auditing the following events: motion data error, vehicle motion conflict, motion sensor authentication failure, unauthorised change of motion sensor, vehicle unit authentication failure (by motion sensor).</td>
</tr>
<tr>
<td><em>(When an EGF is used)</em> The connection between the vehicle unit (main body) and the EGF</td>
<td>This is because the connection is digitally secure (through initial coupling of the vehicle unit and the EGF, mutual authentication between the vehicle unit and the EGF, and the secured communication ensuring authenticity and integrity of exchanged data). Tamper evidence can be traced, by auditing the following events: absence of position information from GNSS receiver,</td>
</tr>
<tr>
<td><strong>The connection between the vehicle unit (main body) and the external remote communication facility</strong></td>
<td>communication error with the external GNSS facility, tamper detection of GNSS, external GNSS facility authentication failure, external GNSS facility certificate expired.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>The connection between the vehicle unit and the speed limiter of the vehicle</strong></td>
<td>This is because the communication link is transparent and has no impact on the security of the transmitted data. Data are encrypted by the vehicle unit and decrypted by a control card. Disconnections can be traced, by auditing the communication error with the remote communication facility events.</td>
</tr>
</tbody>
</table>
4 Annexes

In these annexes, text copied from Regulation text appears in red.

Wherever needed, the red text reflects the consolidation of:

- COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 of 18 March 2016,

4.1 Annex 1 Rationale for type approvable components


**Article 2 Definitions**

(a) ‘tachograph’ or ‘recording equipment’ means the equipment intended for installation in road vehicles to display, record, print, store and output automatically or semi-automatically details of the movement, including the speed, of such vehicles, in accordance with Article 4(3), and details of certain periods of activity of their drivers;

Note concerning definition (a): tachograph cards are not a ‘tachograph’ or ‘recording equipment’ component, because they are not intended for installation in road vehicles.

(b) ‘vehicle unit’ means the tachograph excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may be a single unit or several units distributed in the vehicle, provided that it complies with the security requirements of this Regulation; the vehicle unit includes, among other things, a processing unit, a data memory, a time measurement function, two smart card interface devices for driver and co-driver, a printer, a display, connectors and facilities for entering the user’s inputs;

Notes concerning definition (b):
- Antennas and cables, if any, connecting the antennas to another part of the VU are considered as belonging to the vehicle unit.
- The provided list of units constituting the vehicle unit is not exhaustive, only examples are given.

(c) ‘motion sensor’ means a part of the tachograph providing a signal representative of vehicle speed and/or distance travelled;
(d) ‘tachograph card’ means a smart card, intended for use with the tachograph, which allows identification by the tachograph of the role of the cardholder and allows data transfer and storage;

(h) ‘digital tachograph’ means a tachograph using a tachograph card in accordance with this Regulation;


Article 2
Definitions

For the purposes of this Regulation, the definitions laid down in Article 2 of Regulation (EU) No 165/2014 shall apply. In addition, the following definitions shall apply:

(2) ‘external GNSS facility’ means a facility which contains the GNSS receiver when the vehicle unit is not a single unit, as well as other components needed to protect the communication of data about position to the rest of the vehicle unit;

Note concerning definition (2): An external GNSS facility is indeed a component of a vehicle unit (but in this case the vehicle unit is distributed in several parts).

(6) ‘remote early detection facility’ means the equipment of the vehicle unit which is used to perform targeted roadside checks;

Similarly to the GNSS facility, this means that the remote early detection facility (also called remote communication facility) is indeed a component of a vehicle unit, in the case it is “external”, i.e. when the vehicle unit is distributed in several parts (a vehicle unit main body and an external remote communication facility).

(8) ‘tachograph component’ or ‘component’ means any of the following elements: the vehicle unit, the motion sensor, the record sheet, the external GNSS facility and the external remote early detection facility;

Note concerning definition (8): the tachograph card doesn’t belong to this list.

(10) 'vehicle unit' means: the tachograph excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may be a single unit or several units distributed in the vehicle, provided that it complies with the security requirements of this Regulation; the vehicle unit includes, among other things, a processing unit, a data memory, a time measurement function, two smart card
interface devices for driver and co-driver, a printer, a display, connectors and facilities for entering the user’s inputs;

The vehicle unit also includes a GNSS receiver and a remote communication facility.

The vehicle unit may be composed of the following type approvable components:

- vehicle unit, as a single component (including GNSS receiver and remote communication facility),

- vehicle unit main body (including remote communication facility), and external GNSS facility,

- vehicle unit main body (including GNSS receiver), and external remote communication facility,

- vehicle unit main body, external GNSS facility, and external remote communication facility.

If the vehicle unit is composed of several units distributed in the vehicle, the vehicle unit main body is the unit containing the processing unit, the data memory, the time measurement function, etc.

In this Regulation, in order to simplify the text and ease understanding, “vehicle unit (VU)” is used for “vehicle unit or vehicle unit main body”.

Note concerning definition (10): this definition expands definition (b) of REGULATION (EU) No 165/2014, and defines the type approvable components of the vehicle unit.

Annex 1C provides again the following definitions.

(w) ‘external GNSS facility’ means a facility which contains the GNSS receiver when the vehicle unit is not a single unit as well as other components needed to protect the communication of position data to the rest of the vehicle unit;

Note concerning definition (w): this definition is slightly different from definition (2) in COMMISSION IMPLEMENTING REGULATION (EU) 2018/502 of 28 February 2018, amending COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 of 18 March 2016, but the meaning of both definitions is the same: ‘position data’ is used in definition (w) while ‘data about position’ is used in definition (2).

(dd) ‘motion sensor’ means: a part of the tachograph, providing a signal representative of vehicle speed and/or distance travelled;

(ll) “remote communication facility” or “remote early warning facility” means: the equipment of the vehicle unit which is used to perform targeted roadside checks;
So the components which may be parts of the tachograph and for which an application for type approval can be made are fully defined:
- vehicle unit
- vehicle unit (main body)
- (external) remote communication facility
- (external) GNSS facility
- motion sensor

The following diagrams represent different set-ups that may be type approved. Antennas are represented as being outside the vehicle unit, external GNSS facility or external remote communication housing, but they may alternately be inside.

Use case 1: vehicle unit with internal GNSS receiver and internal remote communication facility

(the vehicle unit is a single part)
Use case 2: vehicle unit composed of vehicle unit main body and external GNSS facility.

(the vehicle unit main body contains the remote communication facility)
Use case 3: vehicle unit composed of vehicle unit main body and external remote communication facility

(the vehicle unit main body contains the GNSS receiver)
Use case 4: vehicle unit composed of vehicle unit main body, external GNSS facility and external remote communication facility
4.2 Annex 2 Commented legislative requirements for the type approval process

REGULATION (EU) No 165/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 February 2014 defines the type approval process as follows:

(u) ‘type-approval’ means a process to certify, by a Member State, in accordance with Article 13, that the tachograph, its relevant components or the tachograph card to be introduced to market fulfil the requirements of this Regulation;

Then, requirements are detailed:

CHAPTER III
TYPE-APPROVAL
Article 12
Applications
In these articles, vehicle unit actually means “vehicle unit or one of its components (vehicle unit main body, external GNSS facility, external remote communication facility)”. This is clarified by Article 4 of COMMISSION IMPLEMENTING REGULATION (EU) 2018/502 of 28 February 2018, amending COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 of 18 March 2016.

1. Manufacturers or their agents shall submit an application for approval of a type of vehicle unit, motion sensor, model record sheet or tachograph card to the type-approval authorities designated to that effect by each Member State.

2. Member States shall communicate to the Commission by 2 March 2015 the name and contact details of the designated authorities referred to in paragraph 1, and shall provide updates thereafter as necessary. The Commission shall publish a list of designated type-approval authorities on its website and shall keep that list updated.

3. An application for type-approval shall be accompanied by the appropriate specifications, including necessary information regarding the seals, and by security, functionality and interoperability certificates. The security certificate shall be issued by a recognised certification body designated by the Commission.

It must be understood that a type-approval application for an external remote communication facility doesn’t have to be accompanied by a security certificate (hence, there is no external remote communication Protection Profile).

Functionality certificates shall be issued to the manufacturer by the type-approval authority.

The interoperability certificate shall be issued by a single laboratory under the authority and responsibility of the Commission.
The JRC is the single laboratory which issues the interoperability certificates, under the authority and responsibility of the Commission.

4. In respect of tachographs, their relevant components, and tachograph cards:

(a) the security certificate shall certify the following for the vehicle unit, tachograph cards, motion sensor, and connection to the GNSS receiver when the GNSS is not embedded in the vehicle units:

(i) compliance with security targets;

(ii) fulfilment of the following security functions: identification and authentication, authorisation, confidentiality, accountability, integrity, audit, accuracy and reliability of service;

Comments:

Components subject to security certification are: vehicle unit (or vehicle unit main body), external GNSS facility, motion sensor, tachograph card.

External remote communication facility is not subject to security certification (as already explained above).

(b) the functional certificate shall certify that the tested item fulfils the appropriate requirements in terms of functions performed, environmental characteristics, electromagnetic compatibility characteristics, compliance with physical requirements and compliance with other applicable standards;

(c) the interoperability certificate shall certify that the tested item is fully interoperable with the necessary tachographs or tachograph card models.

5. Any modification in software or hardware of the tachograph or in the nature of materials used for its manufacture shall, before being applied, be notified to the authority which granted type-approval for the equipment. That authority shall confirm to the manufacturer the extension of the type-approval, or may require an update or a confirmation of the relevant functional, security and/or interoperability certificates.

6. No application in respect of any one type of vehicle unit, motion sensor, model record sheet or tachograph card may be submitted to more than one Member State.

7. The Commission shall, by means of implementing acts, adopt detailed provisions for the uniform application of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 42(3).

March 2016 defines detailed provisions for the uniform application of this article. These guidelines also bring additional support.

Article 13

Granting of type-approval

A Member State shall grant type-approval to any type of vehicle unit, motion sensor, model record sheet or tachograph card which complies with the requirements set out in Articles 4 and 11, provided that the Member State is in a position to check that production models conform to the approved type.

Any modifications or additions to an approved model must receive additional type-approval from the Member State which granted the original type-approval.

Article 14

Type-approval mark

Member States shall issue to the applicant a type-approval mark conforming to a pre-established model, for each type of vehicle unit, motion sensor, model record sheet or tachograph card which they approve pursuant to Article 13 and Annex II. Such models shall be adopted by the Commission through implementing acts in accordance with the examination procedure referred to in Article 42(3).

Article 15

Approval or refusal

The competent authorities of the Member State to which the application for type-approval has been submitted shall, in respect of each type of vehicle unit, motion sensor, model record sheet or tachograph card which they approve, send within one month a copy of the type-approval certificate accompanied by copies of the relevant specifications, including those relating to the seals, to the authorities of the other Member States. Where the competent authorities do not approve the application for type-approval, they shall notify the authorities of the other Member States that approval has been refused and shall communicate the reasons for their decision.

Article 16

Compliance of equipment with type-approval

1. If a Member State which has granted type-approval as provided for in Article 13 finds that any vehicle units, motion sensors, record sheets or tachograph cards bearing the type-approval mark issued by it do not conform to the type which it has approved, it shall take the necessary measures to ensure that production models conform to the approved type. The measures taken may, if necessary, extend to withdrawal of type-approval.
2. A Member State which has granted type-approval shall withdraw such approval if the vehicle unit, motion sensor, record sheet or tachograph card which has been approved is not in conformity with this Regulation or if it displays any general defect during use which makes it unsuitable for the purpose for which it is intended.

3. If a Member State which has granted type-approval is notified by another Member State of one of the cases referred to in paragraphs 1 or 2, it shall, after consulting the notifying Member State, take the steps laid down in those paragraphs, subject to paragraph 5.

4. A Member State which ascertains that one of the cases referred to in paragraph 2 has arisen may forbid until further notice the placing on the market and putting into service of the vehicle unit, motion sensor, record sheet or tachograph card concerned. The same applies in the cases referred to in paragraph 1 with respect to vehicle units, motion sensors, record sheets or tachograph cards which have been exempted from EU initial verification, if the manufacturer, after due warning, does not bring the equipment into line with the approved model or with the requirements of this Regulation.

In any event, the competent authorities of the Member States shall within one month notify one another and the Commission of any withdrawal of type-approval or of any other measures taken pursuant to paragraphs 1, 2 or 3, and shall specify the reasons for such action.

5. If a Member State which has granted a type-approval disputes the existence of any of the cases specified in paragraphs 1 or 2 notified to it, the Member States concerned shall endeavour to settle the dispute and the Commission shall be kept informed.

If talks between the Member States have not resulted in agreement within four months of the date of the notification referred to in paragraph 3, the Commission, after consulting experts from all Member States and having considered all the relevant factors, such as economic and technical factors, shall within six months of the expiry of that four-month period adopt a decision which shall be notified to the Member States concerned and communicated at the same time to the other Member States. The Commission shall in each case lay down the time-limit for implementation of its decision.

…

Article 18

Justification of refusal decisions

All decisions pursuant to this Regulation refusing or withdrawing approval of a type of vehicle unit, motion sensor, model record sheet or tachograph card shall specify in detail the reasons on which they are based. A decision shall be
communicated to the party concerned, who shall at the same time be informed of the remedies available under the law of the relevant Member State and of the time-limits for the exercise of such remedies.


... Article 4

Procedure for type-approval of a tachograph and tachograph components

1. A manufacturer or its agent shall submit an application for type-approval of a tachograph or any of its components, or group of components, to the type-approval authorities designated by each Member State. It shall consist of an information folder containing the information for each of the components concerned including, where applicable, the type-approval certificates of other components necessary to complete the tachograph, as well as any other relevant documents.

2. A Member State shall grant type-approval to any tachograph, component or group of components that conforms to the administrative and technical requirements referred to in Article 1(2) or (3), as applicable. In that case, the type-approval authority shall issue to the applicant a type-approval certificate that shall conform to the model laid down in Annex II to this Regulation.

3. The type-approval authority may request the manufacturer or its agent to supply any additional information.

4. The manufacturer or its agent shall make available to the type-approval authorities, as well as to the entities responsible for issuing the certificates referred to in Article 12(3) of Regulation (EU) No 165/2014, as many tachographs or tachograph components as are necessary to enable the type-approval procedure to be conducted satisfactorily.

5. Where the manufacturer or its agent seeks a type-approval of certain components or groups of components of a tachograph, he shall provide the type-approval authorities with the other components, already type-approved, as well as other parts necessary for the construction of the complete tachograph, in order for those authorities to conduct the necessary tests.

Article 5

Modifications to type-approvals
1. The manufacturer or its agent shall inform without delay the type-approval authorities that granted the original type-approval, about any modification in software or hardware of the tachograph or in the nature of the materials used for its manufacture which are recorded in the information package and shall submit an application for the modification of the type-approval.

2. The type-approval authorities may revise or extend an existing type-approval, or issue a new type-approval according to the nature and characteristics of the modifications. A ‘revision’ shall be made where the type-approval authority considers that the modifications in software or hardware of the tachograph or in the nature of materials used for its manufacture are minor. In such cases, the type-approval authority shall issue the revised documents of the information package, indicating the nature of the modifications made and the date of their approval. An updated version of the information package in a consolidated form, accompanied by a detailed description of the modifications made, shall be sufficient to meet this requirement. An ‘extension’ shall be made where the type-approval authority considers that the modifications in software or hardware of the tachograph or in the nature of materials used for its manufacture are substantial. In such cases, it may request that new tests be conducted and inform the manufacturer or its agent accordingly. If those tests prove satisfactory, the type-approval authority shall issue a revised type-approval certificate containing a number referring to the extension granted. The type-approval certificate shall mention the reason of the extension and its date of issue.

3. The index to the information package shall indicate the date of the most recent extension or revision of the type-approval, or the date of the most recent consolidation of the updated version of the type-approval.

4. A new type-approval shall be necessary when the requested modifications to the type-approved tachograph or its components would lead to the issuance of a new security or interoperability certificate.

8. TYPE-APPROVAL OF RECORDING EQUIPMENT AND TACHOGRAPH CARDS

8.1 General points

For the purpose of this chapter, the words “recording equipment” mean “recording equipment or its components”. No type approval is required for the cable(s) linking the motion sensor to the VU, the external GNSS facility to the VU or the external remote communication facility to the VU. The paper, for use by the recording equipment, shall be considered as a component of the recording equipment.

Comment:

This means that any cable-connection between the VU and an external remote communication facility (e.g. vehicle CAN bus) is NOT part of the type-approval of the VU.

Any manufacturer may ask for type approval of recording equipment component(s) with any other recording equipment component(s), provided each component complies with the requirements of this annex. Alternately, manufacturers may also ask for type approval of recording equipment.

As described in definition (10) in Article 2 of this Regulation, vehicle units have variants in components assembly. Whatever the vehicle unit components assembly, the external antenna and (if applicable) the antenna splitter connected to the GNSS receiver or to the remote communication facility are not part of the vehicle unit type approval.

Nevertheless, manufacturers having obtained type approval for recording equipment shall maintain a publicly available list of compatible antennas and splitters with each type approved vehicle unit, external GNSS facility and external remote communication facility.

(425) Recording equipment shall be submitted for approval complete with any integrated additional devices.

(426) Type approval of recording equipment and of tachograph cards shall include security related tests, functional tests and interoperability tests. Positive results to each of these tests are stated by an appropriate certificate.

(427) Member States type approval authorities will not grant a type approval certificate as long as they do not hold:
— a security certificate (if requested by this Annex),
— a functional certificate,
— and an interoperability certificate (if requested by this Annex) for the recording equipment or the tachograph card, subject of the request for type approval.

Comments:
No security certificate is requested for type-approving an external remote communication module.

(428) Any modification in software or hardware of the equipment or in the nature of materials used for its manufacture shall, before being used, be notified to the authority which granted type-approval for the equipment. This authority shall confirm to the manufacturer the extension of the type approval, or may require an update or a confirmation of the relevant functional, security and/or interoperability certificates.

(429) Procedures to upgrade in-situ recording equipment software shall be approved by the authority which granted type approval for the recording equipment. Software upgrade must not alter nor delete any driver activity data stored in the recording equipment. Software may be upgraded only under the responsibility of the equipment manufacturer. Type approval of software modifications aimed to upgrade a previously type approved recording equipment may not be refused if such modifications only apply to functions not specified in this Annex. Software upgrade of a recording equipment may exclude the introduction of new character sets, if not technically feasible.

8.2 Security certificate

(431) The security certificate is delivered in accordance with the provisions of Appendix 10 of this Annex. Recording equipment components to be certified are vehicle unit, motion sensor, external GNSS facility and tachograph cards.

(432) In the exceptional circumstance that the security certification authorities refuse to certify new equipment on the ground of obsolescence of the security mechanisms, type approval shall continue to be granted only in these specific and exceptional circumstances, and when no alternative solution, compliant with the Regulation, exists.

(433) In this circumstance the Member State concerned shall, without delay, inform the European Commission, which shall, within twelve calendar months of the grant of the type approval, launch a procedure to ensure that the level of security is restored to its original levels.

8.3 Functional certificate

(434) Each candidate for type approval shall provide the Member State's type approval authority with all the material and documentation that the authority deems necessary.
Manufacturers shall provide the relevant samples of type approval candidate products and associated documentation required by laboratories appointed to perform functional tests, and within one month of the request being made. Any costs resulting from this request shall be borne by the requesting entity. Laboratories shall treat all commercially sensitive information in confidence.

A functional certificate shall be delivered to the manufacturer only after all functional tests specified in Appendix 9, at least, have been successfully passed.

The type approval authority delivers the functional certificate. This certificate shall indicate, in addition to the name of its beneficiary and the identification of the model, a detailed list of the tests performed and the results obtained.

The functional certificate of any recording equipment component shall also indicate the type approval numbers of the other type approved compatible recording equipment components tested for its certification.

The functional certificate of any recording equipment component shall also indicate the ISO or CEN standard against which the functional interface has been certified.

8.4 Interoperability certificate

Interoperability tests are carried out by a single laboratory under the authority and responsibility of the European Commission.

The laboratory shall register interoperability test requests introduced by manufacturers in the chronological order of their arrival.

Requests will be officially registered only when the laboratory is in possession of:
— the entire set of material and documents necessary for such interoperability tests,
— the corresponding security certificate,
— the corresponding functional certificate.

The date of the registration of the request shall be notified to the manufacturer.

No interoperability tests shall be carried out by the laboratory, for recording equipment or tachograph cards that have not been granted a security certificate and a functional certificate, except in the exceptional circumstances described in Requirement 432.

Comments:

The JRC may accept to officially register interoperability test requests if the requesting manufacturer provides a letter from the recording equipment /
tachograph card evaluator or certifier, stating that the evaluation result has been positive, so that the emission of the security certificate is only a question of administrative tasks. However the JRC will only issue the interoperability certificate for recording equipment / tachograph card after the relevant security certificate(s) has been received.

(444) Any manufacturer requesting interoperability tests shall commit to leave to the laboratory in charge of these tests the entire set of material and documents which he provided to carry out the tests.

(445) The interoperability tests shall be carried out, in accordance with the provisions of Appendix 9 of this Annex, with respectively all the types of recording equipment or tachograph cards: — for which type approval is still valid or, — for which type approval is pending and that have a valid interoperability certificate.

(446) The interoperability tests shall cover all generations of recording equipment or tachograph cards still in use.

(447) The interoperability certificate shall be delivered by the laboratory to the manufacturer only after all required interoperability tests have been successfully passed.

Comments:

An interoperability certificate for a recording equipment covers the complete recording equipment (i.e. the whole set of components constituting the recording equipment). There is no individual interoperability certificate for a component (e.g. an external remote communication facility).

(448) If the interoperability tests are not successful with one or more of the recording equipment or tachograph card(s), the interoperability certificate shall not be delivered, until the requesting manufacturer has realised the necessary modifications and has succeeded the interoperability tests. The laboratory shall identify the cause of the problem with the help of the manufacturers concerned by this interoperability fault and shall attempt to help the requesting manufacturer in finding a technical solution. In the case where the manufacturer has modified its product, it is the manufacturer's responsibility to ascertain from the relevant authorities that the security certificate and the functional certificates are still valid.

(449) The interoperability certificate is valid for six months. It is revoked at the end of this period if the manufacturer has not received a corresponding type approval certificate. It is forwarded by the manufacturer to the type approval authority of the Member State who has delivered the functional certificate.

(450) Any element that could be at the origin of an interoperability fault shall not be used for profit or to lead to a dominant position.
8.5 Type-approval certificate

(451) The type approval authority of the Member State may deliver the type approval certificate as soon as it holds the three required certificates.

(452) The type approval certificate of any recording equipment component shall also indicate the type approval numbers of the other type approved interoperable recording equipment.

(453) The type approval certificate shall be copied by the type approval authority to the laboratory in charge of the interoperability tests at the time of deliverance to the manufacturer. The laboratory competent for interoperability tests shall run a public web site on which will be updated the list of recording equipment or tachograph cards models:
— for which a request for interoperability tests have been registered,
— having received an interoperability certificate (even provisional),
— having received a type approval certificate.

(454) The laboratory competent for interoperability tests shall run a public web site on which will be updated the list of recording equipment or tachograph cards models:
— for which a request for interoperability tests have been registered,
— having received an interoperability certificate (even provisional),
— having received a type approval certificate.

8.6 Exceptional procedure: first interoperability certificates for 2nd generation recording equipment and tachograph cards

(455) Until four months after a first couple of 2nd generation recording equipment and 2nd generation tachograph cards (driver, workshop, control and company cards) have been certified to be interoperable, any interoperability certificate delivered (including the first ones), regarding requests registered during this period, shall be considered provisional.

(456) If at the end of this period, all products concerned are mutually interoperable, all corresponding interoperability certificates shall become definitive.

(457) If during this period, interoperability faults are found, the laboratory in charge of interoperability tests shall identify the causes of the problems with the help of all manufacturers involved and shall invite them to realize the necessary modifications.

(458) If at the end of this period, interoperability problems still remain, the laboratory in charge of interoperability tests, with the collaboration of the
manufacturers concerned and with the type approval authorities who delivered the corresponding functional certificates shall find out the causes of the interoperability faults and establish which modifications should be made by each of the manufacturers concerned. The search for technical solutions shall last for a maximum of two months, after which, if no common solution is found, the Commission, after having consulted the laboratory in charge of interoperability tests, shall decide which equipment(s) and cards get a definitive interoperability certificate and state the reasons why.

(459) Any request for interoperability tests, registered by the laboratory between the end of the four month period after the first provisional interoperability certificate has been delivered and the date of the decision by the Commission referred to in requirement 455, shall be postponed until the initial interoperability problems have been solved. Those requests are then processed in the chronological order of their registration.
4.3 Annex 3 Commented legislative requirements related to markings

Annex 1C of Regulation 165/2014, as defined by COMMISSION IMPLEMENTING REGULATION (EU) 2018/502 of 28 February 2018, amending COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 of 18 March 2016, specifies markings that must be shown on the descriptive plaque to be affixed on each separate component of the recording equipment.

(225) A descriptive plaque shall be affixed to each separate component of the recording equipment and shall show the following details:
— name and address of the manufacturer,
— manufacturer's part number and year of manufacture,
— serial number,
— type-approval mark.

(226) When physical space is not sufficient to show all above mentioned details, the descriptive plaque shall show at least: the manufacturer's name or logo, and part number.

When a recording equipment type-approval has been granted, the descriptive plaque affixed on each separate component of the recording equipment bears the same type-approval mark (type-approval number of the recording equipment).

When a component type-approval has been granted to each separate component of a recording equipment, the descriptive plaque affixed on each component of the recording equipment bears a different type-approval mark (type-approval number of the component).

Type-approval number shall include number, plus extension/revision numbers (if any).
4.4 Annex 4: List of suggested Second-Generation Tachograph cryptographic functional tests

As stated in section 2, during the Interoperability Testing not all cryptographic features and possibilities specified in Appendix 11 of Annex IC will be fully tested. Therefore, for every type of Tachograph component, this Appendix suggests which tests for the Second-Generation Tachograph cryptographic mechanisms have to be carried out during Functional Testing. Please note that the list of tests is generic and informative only and it is not intended to be exhaustive.

4.4.1 Vehicle Units

Each of the allowed domain parameters for elliptic curve cryptography specified in Appendix 11 Part B should be individually tested in a VU personalized with VU certificates using these domain parameters. The domain parameters for the MSCA and ERCA certificates on each VU, as well as the length of its symmetric keys, shall be chosen consistently with the VU certificates. Link certificates for the VU shall be personalized in accordance with point 2 below.

Then, at least the following test cases should be taken into consideration:

1. For each VU personalisation, all of the card commands specified in Appendix 2 used to initiate cryptographic calculations, to transmit the result of such calculations or to perform operations related to cryptographic certificates, shall be tested with all key lengths applicable for the VU given its personalisation.
   - Example 1: For a VU personalized with BrainpoolP256r1 VU keys, the signature calculation necessary prior to sending the EXTERNAL AUTHENTICATE command can be tested only with the BrainpoolP256r1 parameters. However, by testing this command with all possible VU personalisations, the signature calculation will be tested for all possible domain parameters.
   - Example 2: For a VU personalized with BrainpoolP256r1 VU keys, the private key generation process necessary prior to sending the GENERAL AUTHENTICATE command should be tested with all six possible domain parameters.

   Testing of these commands can be done either by inserting test cards with suitable cryptographic personalisation (and if necessary manually performing the action that leads to the execution of the command), or by using a test tool capable of simulating tachograph cards.

2. The full Mutual Authentication process towards cards should be tested for all possible VU personalisations, considering the case where VU and card are issued under the same ERCA certificate, but also including the use of a Link certificate by the VU or by the card. For both situations, at least Link certificates shall be used that link...
Smart Tachograph Type-approval guidelines v0.5 - DRAFT

- an older root certificate to a newer one using the same domain parameters
- an older root certificate to a newer one using a key length one generation stronger
- if possible, an older root certificate to a newer one using a key length two generations stronger.

3. It has to be tested that a VU stores an imported (authentic) Link certificate, such that it is capable to use this certificate in subsequent mutual authentication procedures. See req. CSM_159 in Appendix 11 and its amendment.

4. It has to be tested that the VU ignores expired card and EGF certificates, even if these certificates have been stored by the VU previously and are retrieved from the VU’s memory during the Mutual Authentication process.

5. For each VU personalisation, support for Secure Messaging has to be tested, including authentication-only and encrypt-then-authenticate modes, correct Secure Messaging structure and Secure Messaging session abortion.

6. If the VU uses an External GNSS Facility, the points 1 - 4 above shall be tested on the EGF interface as well, with the necessary changes as specified in Appendix 11.

7. For all possible VU personalisations, the data download process has to be tested.

8. The full pairing process to a motion sensor shall be tested for all possible VU personalisations, including the following situations:
   - The involved workshop card contains 1, 2 or 3 different generations of $K_{M-WC}$
   - The involved motion sensor contains 1, 2 or 3 different encryptions of its serial number and pairing key.

9. The process of securing the remote communication over DSRC shall be tested for all possible VU personalisations, such that the encryption and MAC calculation necessary prior to sending the RTM data over the DSRC link are tested with all three possible lengths of the VU-specific DSRC keys.

### 4.4.2 Tachograph Cards

For each of the four card types and for each of the allowed domain parameters for elliptic curve cryptography specified in Appendix 11 Part B, at least one test card shall be personalized having that card type and with card certificates using these domain parameters. The domain parameters for the MSCA and ERCA certificates on each card, as well as the length of the symmetric keys, shall be chosen consistently with the card certificate(s). Link certificates shall be
personalized on these cards in accordance with point 2 below. Control and workshop cards shall be personalized with all following combinations: one, two or three different DSRC Master Key(s).

Then, at least the following test cases should be taken into consideration:

1. For each card personalization, all of the card commands specified in Appendix 2 used to initiate cryptographic calculations, to transmit the result of such calculations or to perform operations related to cryptographic certificates shall be tested with all key lengths applicable for that card given its personalization and type.
   
   o Example 1: For a card personalized with (a) BrainpoolP256r1 card key(s), the signature verification necessary after receiving an EXTERNAL AUTHENTICATE command may be tested for at least the BrainpoolP256r1 and NIST-P256 domain parameters (depending on the Link certificates used). However, by testing this command with at least three test cards, the signature verification may be tested for all possible domain parameters.
   
   o Example 2: For a card personalized with (a) BrainpoolP256r1 card key(s), the key agreement process necessary after receiving a GENERAL AUTHENTICATE command can be tested only with the BrainpoolP256r1 parameters. However, by testing this command for all card personalizations, the key agreement process will be tested for all possible domain parameters.
   
   o Example 3: The MAC verification and decryption necessary after receiving a PROCESS DSRC MESSAGE command shall be tested with control and workshop cards for all following combinations: the card contains 1, 2 or 3 DSRC Master Keys of all lengths specified in Appendix 11. The PROCESS DSRC MESSAGE has to be tested with messages encrypted with all possible key lengths.

Testing of these commands can be done either by inserting the test cards in VUs with suitable cryptographic personalisation (and if necessary manually performing the action that leads to the execution of the command), or by using a test tool capable of simulating a VU.

2. The full Mutual Authentication process towards VUs should be tested for all possible card personalisations, considering the case where VU and card are issued under the same ERCA certificate, but also including the use of a Link certificate by the VU or by the card. For both situations, at least Link certificates shall be used that link

   o an older root certificate to a newer one using the same domain parameters

   o an older root certificate to a newer one using a key length one generation stronger
3. It has to be tested that a card stores an imported (authentic) Link certificate, such that it is capable to use this certificate in subsequent mutual authentication procedures. The test is necessary only if according to req. CSM_168 in Appendix 11 the certificate storage capability is implemented.

4. It has to be tested that the card ignores an expired VU certificate, even if this VU certificate has been stored by the card previously and is retrieved from the card’s memory during the Mutual Authentication process.

5. For each card personalisation, support for Secure Messaging has to be tested, including authentication-only and encrypt-then-authenticate modes, correct Secure Messaging structure and Secure Messaging session abortion.

6. For all possible card personalisations, the data download process has to be tested.

7. For all possible control card personalisations the signature verification protocol of req. CSM_236 in Appendix 11 has to be tested, taking also into considerations those cases where a Link certificate is needed.

8. The mechanism to update the card internal time based on the effective date of received ‘valid source of time’ certificates (see req. CSM_167) shall be tested.

4.4.3 External GNSS Facilities

For each of the allowed domain parameters for elliptic curve cryptography specified in Appendix 11 Part B, at least one test EGF shall be personalized with EGF certificates using these domain parameters. The domain parameters for the MSCA and ERCA certificates on these EGFs shall be chosen consistently. Link certificates shall be personalized on these EGFs in accordance with the second main bullet below.

Then, at least the following tests should be taken into consideration:

1. For each EGF personalisation, all commands specified in Appendix 2 on the VU-EGF interface used to initiate cryptographic calculations, to transmit the result of such calculations or to perform operations related to cryptographic certificates must be tested with all key lengths applicable for that EGF given its personalization.

   o Example 1: For an EGF personalized with a BrainpoolP256r1 EGF key, the signature verification necessary after receiving an EXTERNAL AUTHENTICATE command may be tested for at least the BrainpoolP256r1 and NIST-P256 domain parameters (depending on the Link certificates used). However, by testing this command with
at least three test EGFs, the signature verification may be tested for all possible domain parameters.

Example 2: For an EGF personalized with a BrainpoolP256r1 EGF key, the key agreement process necessary after receiving a GENERAL AUTHENTICATE command can be tested only with the BrainpoolP256r1 parameters. However, by testing this command with all EGF personalizations, the key agreement process will be tested for all possible domain parameters.

2. The full Mutual Authentication process towards a VU (performed during initial coupling) shall be tested for each possible EGF personalisation, considering the case where VU and EGF are issued under the same ERCA certificate, but also including the use of a Link certificate by the VU and by the EGF. For both situations, at least Link certificates shall be used that link
   - an older root certificate to a newer one using the same domain parameters
   - an older root certificate to a newer one using a key length one generation stronger
   - if possible, an older root certificate to a newer one using a key length two generations stronger.

3. It has to be tested that an EGF stores an imported (authentic) Link certificate, such that it is capable to use this certificate in subsequent mutual authentication procedures. The test is necessary only if the certificate storage capability is implemented.

4. It has to be tested that the EGF ignores an expired VU certificate during coupling (cf. CSM_208), but does not check for this during normal operation (cf. CSM_211).

5. For each EGF personalisation, support for Secure Messaging has to be tested, including authentication-only and encrypt-then-authenticate mode, correct Secure Messaging structure and Secure Messaging session abortion.

4.4.4 Motion Sensors

Motion sensors shall be personalized with all following combinations: one, two or three encryptions of its serial number and pairing key, having different lengths. The full pairing process to a VU shall be tested for each of these motion sensors.
4.5 Annex 5 Commented legislative requirements concerning seals

REGULATION (EU) No 165/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 February 2014 mentions in its Article 12 information about seals, which has to be included in any application for type-approval of recording equipment or one of its component.

CHAPTER III
TYPE-APPROVAL
Article 12
Applications

1. Manufacturers or their agents shall submit an application for approval of a type of vehicle unit, motion sensor, model record sheet or tachograph card to the type-approval authorities designated to that effect by each Member State.

2. Member States shall communicate to the Commission by 2 March 2015 the name and contact details of the designated authorities referred to in paragraph 1, and shall provide updates thereafter as necessary. The Commission shall publish a list of designated type-approval authorities on its website and shall keep that list updated.

3. An application for type-approval shall be accompanied by the appropriate specifications, including necessary information regarding the seals, and by security, functionality and interoperability certificates. The security certificate shall be issued by a recognised certification body designated by the Commission.

Comment: what seals must be considered is defined in Article 22 of REGULATION (EU) No 165/2014 (see below).

Such information must be communicated by Member States having issued type-approval certificates to other Member States, so that their Control Authorities can use it for vehicle control.

Article 15
Approval or refusal

The competent authorities of the Member State to which the application for type-approval has been submitted shall, in respect of each type of vehicle unit, motion sensor, model record sheet or tachograph card which they approve, send within one month a copy of the type-approval certificate accompanied by copies of the relevant specifications, including those relating to the seals, to the authorities of the other Member States. Where the competent authorities do not approve the application for type-approval, they shall notify the authorities of the other
Member States that approval has been refused and shall communicate the reasons for their decision.

Article 22 sets up installation and inspection related requirements regarding seals.

Approved fitters, workshops or vehicle manufacturers must seal the tachograph as specified in its type-approval certificate.

CHAPTER IV
INSTALLATION AND INSPECTION
Article 22

Installation and repair

1. Tachographs may be installed or repaired only by fitters, workshops or vehicle manufacturers approved by the competent authorities of the Member States for that purpose in accordance with Article 24.

2. Approved fitters, workshops or vehicle manufacturers shall, in accordance with the specifications included in the type-approval certificate referred to in Article 15, seal the tachograph after having verified that it is functioning properly, and, in particular, in such a way as to ensure that no manipulation device can tamper with or alter the data recorded.

They must also place their mark on the seals and enter electronic security data for seal authentication checks in digital tachographs. Member States must send to the Commission the register of the marks and information related to security data used by fitters, workshops or vehicle manufacturers under their authority. The Commission must keep this information available to Member States.

3. The approved fitter, workshop or vehicle manufacturer shall place a special mark on the seals which it affixes and, in addition, for digital tachographs, shall enter the electronic security data for carrying out authentication checks. The competent authorities of each Member State shall send to the Commission the register of the marks and electronic security data used and the necessary information related to the electronic security data used. The Commission shall give Member States access to that information upon request.

Comment: electronic security data consist in workshop card numbers.

After successful installation, approved fitters, workshops or vehicle manufacturers must also affix a clearly visible and easily accessible installation plaque, and seal the connections that are vulnerable to tampering, at least:

- the connection between the motion sensor and the gearbox,
- the installation plaque.
4. For the purpose of certifying that the installation of the tachograph took place in accordance with the requirements of this Regulation, an installation plaque shall be affixed in such a way as to be clearly visible and easily accessible.

5. Tachograph components shall be sealed as specified in the type-approval certificate. Any connections to the tachograph which are potentially vulnerable to tampering, including the connection between the motion sensor and the gearbox, and the installation plaque where relevant, shall be sealed.

This Article also defines the circumstances under which seals may be removed, broken and/or replaced, and requests to trace the necessary justification, using a standard form defined by the Commission. Seal replacement must occur after a check and calibration by an approved workshop.

A seal shall be removed or broken only:

— by fitters or workshops approved by the competent authorities under Article 24 for repair, maintenance or recalibration purposes of the tachograph, or by control officers properly trained and, where required authorised, for control purposes;

— for the purpose of vehicle repair or modification which affects the seal. In such cases, a written statement stating the date and time at which the seal was broken and giving the reasons for the seal removal shall be kept on board the vehicle. The Commission shall develop a standard form for the written statement through implementing acts.

In all cases, the seals shall be replaced by an approved fitter or workshop without undue delay and at the latest within seven days of their removal.

Before replacing seals, a check and calibration of the tachograph shall be performed by an approved workshop.


First of all, Chapter 1 defines smart tachographs calibration data.

1. DEFINITIONS

(f) ‘calibration’ of a smart tachograph means: updating or confirming vehicle parameters to be held in the data memory. Vehicle parameters include vehicle identification (VIN, VRN and registering Member State) and vehicle characteristics (w, k, l, tyre size, speed-limiting device setting (if applicable), current UTC time, current odometer value);

during the calibration of a recording equipment, the types and identifiers of all type-approval relevant seals in place shall also be stored in the data memory;
any update or confirmation of UTC time only, shall be considered as a time adjustment and not as a calibration, provided it does not contradict Requirement 409;

calibrating recording equipment requires the use of a workshop card;

Chapter 3, CONSTRUCTION AND FUNCTIONAL REQUIREMENTS FOR RECORDING EQUIPMENT, requirement (120) details further the list of calibration data.

3. CONSTRUCTION AND FUNCTIONAL REQUIREMENTS FOR RECORDING EQUIPMENT
3.12.10 Calibration data

(120) The following data shall be recorded for each of these calibrations:
— purpose of calibration (activation, first installation, installation, periodic inspection),
— workshop name and address,
— workshop card number, card issuing Member State and card expiry date,
— vehicle identification,
— parameters updated or confirmed: w, k, l, tyre size, speed limiting device setting, odometer (old and new values), date and time (old and new values),
— the types and identifiers of all the seals in place.

Comment: type and identifiers of type-approval relevant seals (as a minimum, seals for the connection between the motion sensor and the gearbox, seals for the installation plaque) are parameters belonging to the set of calibration parameters of smart tachographs.

Requirement (202) specifies the calibration function, which includes the capability to update the types and identifiers of all the seals in place.

3.21 Calibration

(202) The calibration function shall allow:
— to automatically pair the motion sensor with the VU,
— to automatically couple the external GNSS facility with the VU if applicable,
— to digitally adapt the constant of the recording equipment (k) to the characteristic coefficient of the vehicle (w),
— to adjust the current time within the validity period of the inserted workshop card,
— to adjust the current odometer value,
— to update motion sensor identification data stored in the data memory,
— to update, if applicable, external GNSS facility identification data stored in the data memory,
— to update the types and identifiers of all the seals in place,
— to update or confirm other parameters known to the recording equipment: vehicle identification, w, l, tyre size and speed limiting device setting if applicable.

Section 3.24 Performance characteristics specifies environmental conditions regarding seals.

(215) The seals used in the smart tachograph shall withstand the same conditions than those applicable to the tachograph components to which they are affixed.

Comment: Seals for protecting the motion sensor connection to the gearbox must withstand the same conditions as the motion sensor itself. Seals for protecting the installation plaque must withstand the same conditions as the vehicle area it is affixed to. This is also specified in detail in EN 16882:2016.

Section 4.5.4.2.6 Calibration and time adjustment data specifies data to be stored in the workshop card after each smart tachograph calibration.

Chapter 4. CONSTRUCTION AND FUNCTIONAL REQUIREMENTS FOR TACHOGRAPH CARDS

4.5.4.2.6 Calibration and time adjustment data

(336) The workshop card shall be able to hold records of calibrations and/or time adjustments performed while the card is inserted in a recording equipment.

(337) Each calibration record shall be able to hold the following data:
— purpose of calibration (activation, first installation, installation, periodic inspection),
— vehicle identification,
— parameters updated or confirmed (w, k, l, tyre size, speed limiting device setting, odometer (new and old values), date and time (new and old values),
— recording equipment identification (VU part number, VU serial number, motion sensor serial number, remote communication facility serial number and external GNSS facility serial number, if applicable),
— seal type and identifier of all seals in place,
— ability of the VU to use first generation tachograph cards (enabled or not).

Comment: the type and identifier of all seals in place belongs to the calibration data record to be stored in workshop cards after each installation and inspection.

Chapter 5.2 specifies information that must be marked on the installation plaque, after each installation and inspection.

5. INSTALLATION OF RECORDING EQUIPMENT

5.2 Installation plaque
(395) After the recording equipment has been checked on installation, an installation plaque, engraved or printed in a permanent way, which is clearly visible and easily accessible shall be affixed onto the recording equipment. In cases where this is not possible, the plaque shall be affixed to the vehicle’s ‘B’ pillar so that it is clearly visible. For vehicles that do not have a ‘B’ pillar, the installation plaque should be affixed to the doorframe on the driver's side of the vehicle and be clearly visible in all cases. After every inspection by an approved fitter or workshop, a new plaque shall be affixed in place of the previous one.

(396) The plaque shall bear at least the following details:

— name, address or trade name of the approved fitter or workshop,
— characteristic coefficient of the vehicle, in the form “w = ... imp/km”,
— constant of the recording equipment, in the form “k = ... imp/km”,
— effective circumference of the wheel tyres in the form “l = ... mm”,
— tyre size,
— the date on which the characteristic coefficient of the vehicle and the effective circumference of the wheel tyres were measured,
— the vehicle identification number,
— the presence (or not) of an external GNSS facility,
— the serial number of the external GNSS facility, if applicable,
— the serial number of the remote communication device, if any,
— the serial number of all the seals in place,
— the part of the vehicle where the adaptor, if any, is installed,
— the part of the vehicle where the motion sensor is installed, if not connected to the gear-box or an adaptor is not being used,
— a description of the colour of the cable between the adaptor and that part of the vehicle providing its incoming impulses,
— the serial number of the embedded motion sensor of the adaptor.

Comment: the serial number of all the seals in place must be written on the installation plaque. Serial number means the unique identifier number defined in requirement (201) below.

Chapter 5.3 Sealing gathers requirements regarding the seals themselves.

5.3 Sealing

(398) The following parts shall be sealed:

— Any connection which, if disconnected, would cause undetectable alterations to be made or undetectable data loss (this may e.g. apply for the motion sensor fitting on the gearbox, the adaptor for M1/N1 vehicles, the external GNSS connection or the vehicle unit);
— The installation plaque, unless it is attached in such a way that it cannot be removed without the markings thereon being destroyed.

Comments: the minimum connections that must be sealed are:
- the motion sensor fitting on the gearbox
- the installation plaque
- seals related to the adaptor for M1/N1 vehicles (if used)

Even if given here just in a list of examples, the external GNSS connection to the vehicle unit doesn’t need to be sealed, because this connection is digitally secured.

(398a) The seals mentioned above shall be certified according to the standard EN 16882:2016.

(399) The seals mentioned above may be removed:
— In case of emergency,
— To install, to adjust or to repair a speed limitation device or any other device contributing to road safety, provided that the recording equipment continues to function reliably and correctly and is resealed by an approved fitter or workshop (in accordance with Chapter 6) immediately after fitting the speed limitation device or any other device contributing to road safety or within seven days in other cases.

(400) On each occasion that these seals are broken a written statement giving the reasons for such action shall be prepared and made available to the competent authority.

(401) Seals shall hold an identification number, allocated by its manufacturer. This number shall be unique and distinct from any other seal number allocated by any other seals manufacturer.

This unique identification number is defined as: MMNNNNNNNNN by non-removable marking, with MM as unique manufacturer identification (database registration to be managed by EC) and NNNNNNNN seal alpha-numeric number, unique in the manufacturer domain.

Comment: the unique seal alpha-numeric number is called serial number in section 5.2 Installation plaque.

(402) The seals shall have a free space where approved fitters, workshops or vehicle manufacturers can add a special mark according the Article 22(3) of Regulation (EU) No 165/2014. This mark shall not cover the seal identification number.

(403) Seals manufacturers shall be registered in a dedicated database when they get a seal model certified according to EN 16882:2016 and shall make their identification seals numbers public through a procedure to be established by the European Commission.

(404) Approved workshops and vehicle manufacturers shall, in the frame of Regulation (EU) No 165/2014, only use seals certified according to EN
16882:2016 from those of the seals manufacturers listed in the database mentioned above.

(405) Seal manufacturers and their distributors shall maintain full traceability records of the seals sold to be used in the frame of Regulation (EU) No 165/2014 and shall be prepared to produce them to competent national authorities whenever need be.

(406) Seals unique identification numbers shall be visible on the installation plaque.

Chapter 6 sets up requirements about periodic inspections, during which controls regarding seals are made.

6. CHECKS, INSPECTIONS AND REPAIRS

Requirements on the circumstances in which seals may be removed, as referred to in Article 22(5) of Regulation (EU) No 165/2014, are defined in Chapter 5.3 of this annex.

6.3 Installation inspection

‘(408) When being fitted to a vehicle, the whole installation (including the recording equipment) shall comply with the provisions relating to maximum tolerances laid down in Chapter 3.2.1, 3.2.2, 3.2.3 and 3.3. The whole installation shall be sealed in accordance with Chapter 5.3 and it shall include a calibration.

6.4 Periodic inspections

(409) Periodic inspections of the equipment fitted to the vehicles shall take place after any repair of the equipment, or after any alteration of the characteristic coefficient of the vehicle or of the effective circumference of the tyres, or after equipment UTC time is wrong by more than 20 minutes, or when the VRN has changed, and at least once within two years (24 months) of the last inspection.

(410) These inspections shall include the following checks:

— that the recording equipment is working properly, including the data storage in tachograph cards function and the communication with remote communication readers,
— that compliance with the provisions of chapter 3.2.1 and 3.2.2 on the maximum tolerances on installation is ensured,
— that compliance with the provisions of chapter 3.2.3 and 3.3 is ensured,
— that the recording equipment carries the type approval mark,
— that the installation plaque, as defined by Requirement 396, and the descriptive plaque, as defined by Requirement 225, are affixed,
— the tyre size and the actual circumference of the tyres,
— that there are no manipulation devices attached to the equipment,
— that seals are correctly placed, in good state, that their identification numbers are valid (referenced seal manufacturer in the EC database) and that their
identification numbers correspond to the installation plaque markings (see requirement 401).

Comments: correct placement of seals, good state of the seals, validity of the seals identification, and correspondence between the installation plaque and the seals identification numbers must be checked during every periodic inspection.

(411) If one of the events listed in Chapter 3.9 (Detection of Events and/or Faults) is found to have occurred since the last inspection and is considered by tachograph manufacturers and/or national authorities as potentially putting the security of the equipment at risk, the workshop shall:
   a. make a comparison between the motion sensor identification data of the motion sensor plugged into the gearbox with that of the paired motion sensor registered in the vehicle unit;
   b. check if the information recorded on the installation plaque matches with the information contained within the vehicle unit record;
   c. check if the motion sensor serial number and approval number, if printed on the body of the motion sensor, matches the information stored in the recording equipment data memory;
   d. compare identification data marked on the descriptive plaque of the external GNSS facility, if any, to the ones stored in the vehicle unit data memory;

(412) Workshops shall keep traces in their inspection reports of any findings concerning broken seals or manipulations devices. These reports shall be kept by workshops for at least 2 years and made available to the Competent Authority whenever requested to do so.

(413) These inspections shall include a calibration and a preventive replacement of the seals whose fitting is under the responsibility of workshops.

Comment: preventive replacement of seals shall occur.

Appendix 1 provides data format details about seals.

Appendix 1

2.71. ExtendedSealIdentifier

Generation 2:

The extended seal identifier uniquely identifies a seal (Annex IC requirement 401).

ExtendedSealIdentifier ::= SEQUENCE {
   manufacturerCode OCTET STRING (SIZE(2)),
   sealIdentifier OCTET STRING (SIZE(8))
}
**manufacturerCode** is a code of the manufacturer of the seal.

**sealIdentifier** is an identifier for the seal which is unique for the manufacturer.

### 2.128. SealDataCard

**Generation 2:**

This data type stores information about the seals that are attached to the different components of a vehicle and is intended for storage on a workshop card. This data type is related to Annex 1C requirement 337.

SealDataCard ::= SEQUENCE {
  noOfSealRecords INTEGER (1..5),
  sealRecords SET SIZE (noOfSealRecords) OF SealRecord
}

**noOfSealRecords** is the number of records in sealRecords.

**sealRecords** is a set of seal records.

Comment: sealDataCard is an element of 2.174. WorkshopCardCalibrationRecord. Up to 5 different seal records can be stored for one vehicle installation.

### 2.129. SealDataVu

**Generation 2:**

This data type stores information about the seals that are attached to the different components of a vehicle and is intended for storage in a Vehicle Unit.

SealDataVu ::= SEQUENCE SIZE (5) OF {
  noOfSealRecords INTEGER (1..5),
  sealRecords SET SIZE (noOfSealRecords) OF SealRecord
}

**sealRecords** is a set of seal records. If there are less than 5 seals available the value of the EquipmentType in all unused sealRecords shall be set to 16, i.e. unused.

Comment: sealDataVU is an element of 2.174. VuCalibrationRecord. Up to 5 different seal records can be stored for one vehicle installation.

### 2.130. SealRecord

**Generation 2:**

SealRecord ::= SEQUENCE {
  equipmentType EquipmentType,
  extendedSealIdentifier ExtendedSealIdentifier
}
**equipmentType** identifies the type of equipment the seal is attached to.

**extendedSealIdentifier** is the identifier of the seal attached to the equipment.

Comment: sealRecord relates a particular seal to the component it is attached to.

The Vehicle Unit functional tests include some checks about seals.

2. VEHICLE UNIT FUNCTIONAL TESTS

2.4 Sealing 398, 401 to 405

Comment: the check is only about compliance with requirements 398, 401 and 405 (see above).

Motion sensor functional tests also include some checks about seals.

3. MOTION SENSOR FUNCTIONAL TESTS

2.4. Sealing 398, 401 to 405

Comment: the check is only about compliance with requirements 398, 401 and 405 (see above)

Appendix 16 also contains requirements about seals which are attached to the adaptor.

Appendix 16 ADAPTOR FOR M1 AND N1 CATEGORY VEHICLES

4.4. Security requirements

ADA_018 It shall not be possible to remove the embedded motion sensor from the adaptor without breaking the seal(s) of the adaptor housing, or breaking the seal between the sensor and the adaptor housing (see ADA_034).

Comment: there are different kinds of seals seal(s) related to the adapter (see ADA_034 below).

5. INSTALLATION OF THE RECORDING EQUIPMENT WHEN AN ADAPTOR IS USED

5.1. Installation

ADA_029 Adaptors to be installed in vehicles shall only be installed by vehicle manufacturers, or by approved workshops, authorised to install, activate and calibrate digital and smart tachographs.

ADA_030 Such approved workshop installing the adaptor shall adjust the input interface and select the division ratio of the input signal (if applicable).

ADA_031 Such approved workshop installing the adaptor shall seal the adaptor housing.

Comment: this is one kind of seals affixed by workshops on adaptors. Other seals are specified in section 5.2.
ADA_032 The adaptor shall be fitted as close as possible to that part of the vehicle which provides its incoming pulses.

ADA_033 The cables for providing the adaptor power supply shall be red (positive supply) and black (ground).

Section 5.2 Sealing sets up requirements for seals related with adaptors.

5.2. Sealing

ADA_034 The following sealing requirements shall apply:
— the adaptor housing shall be sealed (see ADA_017),
— the housing of the embedded sensor shall be sealed to the adaptor housing, unless it is not possible to remove the sensor from the adaptor housing without breaking the seal(s) of the adaptor housing (see ADA_018),
— the adaptor housing shall be sealed to the vehicle,
— the connection between the adaptor and the equipment which provides its incoming pulses shall be sealed on both ends (to the extent of what is reasonably possible).

Comments: there are different possible types of seals related to adaptors:
— seal for the adaptor housing,
— seal of the sensor housing to the adaptor housing,
— seal of the adaptor housing to the vehicle,
— seal of the adaptor to the equipment which provides its incoming pulses (on both ends).

Chapter 6 sets up requirements about periodic inspections, during which controls regarding seals related to adaptors are made.

6. CHECKS, INSPECTIONS AND REPAIRS
6.1. Periodic inspections

ADA_035 When an adaptor is used, each periodic inspection (periodic inspections means in compliance with Requirement [409] through to Requirement [413] of Annex 1C) of the recording equipment shall include the following checks:
— that the adaptor carries the appropriate type approval markings,
— that the seals on the adaptor and its connections are intact,
— that the adaptor is installed as indicated on the installation plaque,
— that the adaptor is installed as specified by the adapter and/or vehicle manufacturer,
— that mounting an adaptor is authorised for the inspected vehicle.

ADA_036 These inspections shall include a calibration and a replacement of all seals, whatever their state.

Section 7.2 sets up requirements about the adaptor functional tests, regarding seals.

7.2. Functional certificate
ADA_040 A functional certificate of an adaptor or of recording equipment including an
adaptor shall be delivered to the adaptor manufacturer only after all the following
minimum functional tests have been successfully passed.

2. Visual inspection
2.4. Sealing ADA_017, ADA_018, ADA_034
4.6 Annex 5: Frequently Asked Questions

Can a motion sensor which is type-approved for use with a vehicle unit from one manufacturer be automatically be type-approved with the vehicle unit of another manufacturer?

→ No. Interoperability between motion sensor and VU is not required. Interoperability is required only between cards and recording equipment. For example, to get a type-approval of the motion sensor with another vehicle unit, modifications may be needed in this vehicle unit (e.g. provide additional data not specified in Annex 1C to the motion sensor).

Let’s assume a motion sensor has been type-approved with a vehicle unit from one manufacturer. Do other tachograph manufacturers have to support this motion sensor in order to get a type-approval for their vehicle units with it?

→ No, the other manufacturers can use other motion sensors.

However, it is required that a manufacturer of whatever component (promotor) asking for type-approval comes with (at least) one full recording equipment (i.e. with all the parts representing the setup with which a type-approval is requested, see below General remarks).

If a motion sensor requires this “additional data” (not specified in Annex 1C) from the vehicle unit, can a vehicle unit manufacturer get a type-approval for its vehicle unit if it works only with such a motion sensor?

→ Yes, in that case the type-approval certificate of the VU will indicate that only this motion sensor is compatible with this VU.

When a manufacturer hands over a component within the tachograph system (a tachograph, a motion sensor or a DSRC module) to JRC, is there any time limit for other manufacturers to hand over their components to determine if their components are compatible with said component?

→ The very first interoperability certificate granted for the first “smart DT setup” will be provisional. From the date of this very first certificate and for four months, all certificates granted will be provisional. At the end of this 4 months period, if no interoperability issue has been detected, the certificates will become definitive. If during that period, an interoperability issue is detected, the parties will be called to find a solution.

Once the 4 months period is over, one must go back to normal procedure (i.e. if an interoperability issue is detected, the manufacturer shall correct it before getting the type-approval, whatever the time it requires).
General remarks: Like in Annex1B, Annex1C considers the type-approval of recording equipment components. Each component can get its own type-approval, and the type-approval will indicate with which other components it can operate (type-approval reference setup). It is the responsibility of a component manufacturer to decide about this ‘type-approval reference setup’, which is the only valid and legal setup. It shall then supply these other components to the laboratories if required for the certifications tests.

What is new in Annex1C is the possibility to get a type-approval for a complete recording equipment. However this recording equipment will become logically unique and invariable. If there is a revision of one of the component of this recording equipment, the full recording equipment needs to be type-approved again.

All these aspects are detailed in the main body of these guidelines.

**Are the samples for functional tests supposed to be sent to the type-approval authority, as shown on the various schemes in this document?**

→ The samples to be used for functional tests can be sent directly to the laboratory which has been accredited by the type approval authority for functional tests. The functional tests themselves are performed under control of the type-approval authority. The functional test laboratory has not been shown in the picture, for simplification purpose.
List of abbreviations and definitions


DT  Digital Tachograph
EGF  External GNSS Facility
ERCF  External Remote Communication Facility
MS  Motion Sensor
TA  Type-Approval
TC  Tachograph Card
VU  Vehicle Unit