J R C T E C H N I C A L R E P O R T S

Digital Tachograph Equipment
Type Approval
Interoperability Test Specification
Version 2.3

Dominique Landat
James Bishop

2012

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Digital Tachograph Laboratory
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 361, 21027 Ispra (VA), Italy
E-mail: iot@jrc.ec.europa.eu
Tel.: +39 0332 78 9305
Fax: +39 0332 78 5145

http://ipsc.jrc.ec.europa.eu/
http://dtc.jrc.ec.europa.eu/

JRC75155

Luxembourg: Publications Office of the European Union, 2012

Printed in Ispra (Italy)

Table of Contents

1. INTRODUCTION

This publication is an update of the JRC Scientific and Technical Report EUR 24811 EN – 2011. It reports the interoperability test procedure developed for Digital Tachograph equipment as defined in Council Regulation No. 3821/85 amended by Commission Regulation 1360/2002 of 13 June 2002 [1] and Commission Regulation (EU) 1266/2009 of 16 December 2009 [5] (referred to hereinafter as the Regulation).

Interoperability Certification is one of three certifications required for type approval of Digital Tachograph equipment. The other two certifications concern functional testing, and security evaluation.

The type approval process, including an exceptional procedure for the first type approvals, is contained in the Regulation (see Chapter VIII, Annex I(B) [1]). For convenience, the text of Chapter VIII is reproduced in Chapter 11 of this document.

2. INTEROPERABILITY CERTIFICATION

2.1. The interoperability tests are performed following the *DTLab* test procedures *DTL_ITC_01* for the cards and *DTL_ITV_01* for the recording equipment.

2.2. Section 5 of *Annex I(B) Appendix 9 - Type Approval, List of Minimum Required Test*s [1] defines the requirements for interoperability tests. The contents of Appendix 9 Section 5 are reproduced below:

No.	Test	Description
1	Mutual authentication	Check that the mutual authentication between the vehicle unit and the tachograph card runs normally
2	Write/read tests	Execute a typical activity scenario on the vehicle unit. The scenario shall be adapted to the type of card being tested and involve writings in as many EFs as possible in the card Verify through a card downloading that all corresponding recordings have been properly made Verify through a card daily printout that all corresponding recordings can be properly read

2.3. The interoperability tests defined in this document aim to demonstrate that combinations of digital tachograph equipment conform to a specific subset of requirements drawn from the Regulation.

Note: The type approval process as defined in the Regulation concerns only digital tachograph recording equipment (i.e. a vehicle unit paired with its motion sensor) and tachograph cards. Successful implementation of the digital tachograph system depends on ancillary equipment (e.g. the calibration equipment used by workshops and the intelligent dedicated equipment used by controllers) for which no interoperability requirements are defined in the Regulation.

2.4. The type approval process requires that interoperability tests be performed on equipment which has received both security and functional certifications. This implies that the interoperability tests shall be performed on samples of tachograph equipment identical in all respects to those certified for functionality and security.

2.5. The interoperability tests shall be limited to a series of manipulations performed on digital tachograph equipment at the Digital Tachograph Laboratory – DTLab – which is, as specified by the *requirement 278* of the Regulation, enable to deliver the interoperability certificate (see requirement *284*).

Note: The interoperability laboratory, DTLab, may also use software tools provided by equipment manufacturers to facilitate the management of the equipment (e.g. software for preloading activity data on a driver card, or for interpreting the contents of a vehicle unit memory). Any such software tools are identified in the interoperability test modules, respectively DTL.ITC.01 for the cards and DTL.ITV.01 for the recording equipment.

2.6. As specified by the requirement *282*, the digital tachograph equipment submitted for interoperability testing shall remain at the interoperability laboratory and constitute the reference set against which new products will be tested.

2.7. Requirement *272* states that any changes to the specification of an item of tachograph equipment may require recertification, i.e. complete or partial repetition of the type approval tests. The needs for

recertification shall be established on a case-by-case basis in co-operation with the functional testing laboratory and the security certification authority.

2.8. Requirement *290* states that the interoperability laboratory shall maintain a public web site describing the state of equipment type approval. The URL of this web site is: http://dtc.jrc.ec.europa.eu/

3. ROLES AND RESPONSABILITIES

3.1. The European Commission service responsible for appointing the interoperability testing laboratory (see Annex I(B) requirement 278) is:

European Commission
Land Transport
DG MOVE D.3
Rue de Mot, 24
B-1040 Bruxelles

3.2. The interoperability test procedure is maintained by, implemented at, and available from:

Digital Tachograph Laboratory
Digital Citizen Security Unit
European Commission
Joint Research Centre, Ispra Establishment (TP.361)
Via E. Fermi, 2749
I-21027 Ispra (VA)

3.3. The Digital Tachograph Laboratory assigns `ManufacturerCodes` (Annex I(B) Appendix 1, Section 2.67) to tachograph equipment manufacturers. This information is published on the public web site when a product, card or recording equipment is type approved at the following address: *http://dtc.jrc.ec.europa.eu/manufacturer_codes.html.*

3.4. Each Member State of the European Union designates an authority responsible for approving digital tachograph system components (i.e vehicle units, motion sensors, and tachograph cards) for use in the enforcement of European Union legislation.

3.4b. Each non EU – AETR state designates an authority responsible for approving digital tachograph system components (i.e vehicle units, motion sensors, and tachograph cards) for use in the enforcement of European Agreement concerning the work of crews of vehicles engaged in International road transport (AETR) [4].

3.5. The Member/National State type approval authority may request, as stated in the requirement *271*, update or confirmation of the functional, security, or interoperability certification whenever the specifications of a component are changed (see Annex I(B) requirement *272*).

3.6. The test requests are introduced in the chronological order of their arrival and they are 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.

See Annex I(B) requirements *279* and *280*.

3.7. The interoperability laboratory shall deliver an interoperability certificate to a manufacturer of a digital tachograph component (see Annex I(B) requirement *284*).

3.8. The manufacturer presents the interoperability certificate to the type approval authority in its State.

3.9. The type approval national authority will provide to the *DTLab* a copy of the type approval certificate (see Annex I(B) requirement *289*).

3.10. Manufacturers are responsible for implementing the corrective actions required to resolve an interoperability failure.

3.11. The type approval process defined by the Regulation (see Annex I(B) Chapter 11) refers to the manufacturer of a digital tachograph component, as if this were a single entity. In the case of tachograph cards, several entities may co-operate to supply tachograph cards to a National Authority. These include, but may not be limited to:

- the manufacturer of the chip,
- the developer of the chip's operating system,
- the developer of the tachograph application software,
- the integrator of the chip and card body,
- the card personaliser.

Each of these entities may have to implement one or more corrective actions in the resolution of an interoperability failure.

3.12. The delivery of an interoperability certificate for a digital tachograph component shall be performed under a contractual agreement between the interoperability laboratory and the entity which shall present the interoperability certificate to the national type approval authority.

3.13. A copy of the interoperability certificate is published on the JRC public web at the following addresses:

- http://dtc.jrc.ec.europa.eu/tachograph_cards_status.html for a card;
- http://dtc.jrc.ec.europa.eu/vehicle_units_status.html for a vehicle unit.

4. ASSUMPTIONS

4.1. The Regulation (Annex I(B) and its Appendices) is assumed to define only minimum requirements for digital tachograph equipment.

4.2. The security enforcing functions of the vehicle unit and tachograph card are intended to prevent the analysis or debugging of equipment software in the field (see e.g. Annex I(B) Appendix 10 Generic Security Targets *RLB_204* and *RLB_304*).

Interoperability tests shall therefore only use digital tachograph system components, i.e. vehicle unit, motion sensor, tachograph card.

4.3. Annex I(B) Appendix 11 *CSM_011* requires the creation of a European root key and at least two Member State test keys, which will be used to certify the keys of the equipment samples presented for interoperability testing.

The European root and Member/National State keys are not used in the final stages of the digital tachograph equipment mutual authentication protocol (see Annex I(B) Appendix 11 *CSM_020*, and Chapter 9 of this document), which relies on the equipment private keys. To provide equipment manufacturers with a common basis for testing their implementations of the mutual authentication protocol, equipment test keys will be available from the European Root Certification Authority – ERCA.

4.4. Equipment manufacturers may opt for internal generation of equipment keys. This process ensures confidentiality of the equipment private key. Internally generated keys shall require certification by one of the Member/National State keys.

4.5. Equipment manufacturers may opt for external generation of equipment keys. In this case, manufacturers may use equipment keys and certificates provided by ERCA.

4.6. The Regulation refers to ancillary equipment for calibration (intended for use by approved workshops) and for data downloading (enforcement). These items are not part of the interoperability type approval defined in the Regulation, but issues of their interoperability with different recording equipment are likely to arise.

4.7. Prior to performing interoperability tests for the purposes of type approval, the test laboratory shall have validated the interoperability tests, with the collaboration of the equipment manufacturers, using pre-production equipment.

Results obtained during validation of methods may be covered by a non-disclosure agreement stipulated by the equipment manufacturer.

4.8. Member/National State Authorities may request tests on personalized equipment as part of their tendering process for suppliers of the material and / or services required to implement the digital tachograph infrastructure.

5. RISKS

5.1. Errors in the conception or execution of a single interoperability test lead to the deployment of incompatible digital tachograph equipment.

Equipment manufacturers shall be consulted during interoperability test definition, and shall be invited to provide training in the use of their products for test laboratory staff prior to type approval tests.

5.2. An equipment manufacturer enters the type approval process with samples of equipment whose specifications differ from the models which will eventually enter production.

Access to the reference set of tachograph equipment maintained at the interoperability laboratory shall be granted to Member/National State Authorities and to the ITSEC authorities should need arise.

5.3. Digital tachograph equipment presented for type approval testing does not implement all functionality defined in the Regulation.

For example: Annex I(B) Appendix 2 *TCS_301 The card shall provide both protocol T=0 and protocol T=1* implies that vehicle units will offer either the T = 0 or the T = 1 protocol.

If the initial interoperability tests are performed only with vehicle units implementing T = 0, interoperability is certifiable only for T = 0. Interoperability problems arising from the untested T = 1 protocol (i.e. on a tachograph card) might remain undetected.

6. TEST SAMPLES

6.1. General

6.1.1. According to the type of product, a manufacturer seeking interoperability certification shall provide the material listed in Section 6.2 or Section 6.3 to the interoperability laboratory.

6.1.2. The material shall be accompanied by one copy of the functional test certificate issued by a Member/National State's type approval authority, and one copy of the security certificate issued by an ITSEC authority.

6.1.3. The recording equipment (i.e. vehicle unit and motion sensor) and tachograph cards shall remain at the interoperability laboratory and shall constitute the reference set of equipment against which future products shall be compared

6.1.4. Ancillary equipment for calibration and / or data downloading shall not be subjected to interoperability tests within the frame of the interoperability type approval.

6.1.5. The manufacturer shall provide training in the correct use of the equipment for interoperability laboratory staff. The training shall cover installation, calibration and operation

6.2. Recording Equipment

6.2.1. Manufacturers of recording equipment shall supply the following items to the interoperability laboratory for the purposes of the type approval test.

6.2.2. The recording equipment shall be marked according to Annex I(B) requirements *169* (the approval mark for the equipment type is not mandatory) and / or *170*.

6.2.3. Four vehicle units (VU) containing the following security data elements from the interoperability test set (see Chapter 10 for further information):

- Eur.PK;
- MSCA.C 01;
- KmVU_Test motion sensor master key.

The vehicle unit certificate (Eqt.C) shall have undefined end-of-validity (EOV) and shall be produced with an appropriate Member/National State Certification Authority secret key (MSCA.SK).

6.2.4. For motion sensors which are not in the possession of the interoperability laboratory, one motion sensor, compatible with the vehicle unit. The cables connecting the motion sensor to the vehicle unit shall be 2 metres in length, and shall be supplied complete with connectors.

The motion sensor extended serial number (Ns) and pairing key (Kp) shall be encrypted with the Km_Test motion sensor master key from the interoperability test set.

The manufacturer shall provide the test laboratory with the values of the motion sensor extended serial number (Ns) and pairing key (Kp).

6.2.5. The manufacturer may provide one calibration equipment and / or one intelligent dedicated equipment (IDE) complete with cable(s) and downloading / calibration connector(s) described in Annex I(B) Appendix 6.

These items will not be subjected to any interoperability test.

6.2.6. The recording equipment manufacturer shall provide the test laboratory with the clear content of the certificates of the equipment public keys in the vehicle unit, workshop card, and control card.

The choice of Member/National State is the responsibility of the vehicle unit manufacturer.

The value of the vehicle unit certificate holder reference (CHR, see Annex I(B) Appendix 1 *2.56*

ExtendedSerialNumber or 2.35 *CertificateRequestID*) is the responsibility of the vehicle unit manufacturer.

The `ManufacturerCode` in the workshop and control card CHRs may identify either the manufacturer of the vehicle unit or of the card.

6.2.7. The recording equipment manufacturer shall provide appropriate calibration data (e.g. recording equipment constant *k*, characteristic coefficient of the vehicle *w*). These data may be inserted into the vehicle unit during laboratory staff training.

6.3. Tachograph Cards

6.3.1. Suppliers of tachograph cards shall prepare and submit five sets of four tachograph cards (one each of driver, control, company, and workshop card) to the interoperability laboratory for the purposes of the type approval test:

6.3.2. Each group of tachograph cards shall contain the following security data elements from the interoperability test set:

- Eur.PK;
- one of MSCA.C 03, 04, or 05.

The EOV values, for three groups, to be used in card certificates are defined in Table 10.4. The card certificates shall be produced by an appropriate MSCA.SK. The filth group will have, possibly, an undefined EOV value.

The workshop cards shall contain the KmWC_Test motion sensor master key from the interoperability test set.

6.3.3. The card supplier shall provide the test laboratory with the clear content of the card public key certificates.

The choice of Member/National State type approval authority is the responsibility of the card supplier.

The value of the card certificate CHR (data type *ExtendedSerialNumber* or *CertificateRequestID*) is the responsibility of the card supplier.

6.3.4. The characters required to compose the workshop card PIN shall be restricted to the numerals 0-9, to ensure that PIN entry into the VU can be achieved using only the decimal ASCII codes 48 to 57.

6.3.5. Card personalisation data are the responsibility of the card supplier.

6.3.6. The fifth group of cards, containing the following security data elements from the interoperability test set:

- Eur.PK;
- JRC.C;
- The workshop card shall contain: KmWC_Test motion sensor master key.

The Eqt.Cs shall have undefined EOV and shall be produced with the JRC.SK.

The control card may be used to download the vehicle unit data memory as required for the purposes of the test laboratory.

The workshop card shall ensure that the test laboratory can adjust the vehicle unit internal clock over the full range permitted by the vehicle unit.

7. TEST SPECIFICATIONS

7.1. General Considerations

The security enforcing functions of the digital tachograph system is likely to prevent the use of protocol analyzers for recording data exchanged between a vehicle unit and a card. Items of equipment under test are therefore considered as “black boxes” whose internal workings are unknown.

Each test description consists of an objective, a rationale, and a description of the expected behavior. Objectives refer to requirements in Annex I(B) and Appendices.

The tests are intended to create events that will be recorded in the data memories of the vehicle unit and the tachograph card. Therefore each interoperability test sequence shall be preceded by a download of the tachograph card memories and followed by the download of the vehicle unit and card memories. The differences in the contents of the data memories before and after each test sequence shall be compared with the expected behavior.

Both the vehicle unit and the tachograph card data memories shall be downloaded via the intelligent dedicated equipment (IDE) interface on the front panel of the vehicle unit (see Annex I(B) Appendix 6).

Interoperability tests involving driver, controller, and company cards shall only be performed with complete recording equipment i.e. a vehicle unit paired to its motion sensor.

7.2. Test Conditions

7.2.1. The interoperability tests are performing in the Digital Tachograph Laboratory of the JRC Ispra.

7.2.2. Unless otherwise stated, interoperability tests will be carried out under the following climatic conditions:

- ambient temperature 15°C to 35°C
- relative humidity 30% to 75%
- atmospheric pressure 860 mbar to 1060 mbar

7.2.3. Recording equipment shall be powered on for a warm-up period of approximately 30 minutes prior to commencement of interoperability tests.

7.2.4. Vehicle units shall be installed in an open framework permitting unobstructed air flow around the sides, top, bottom, and rear of the unit housing while ensuring a correct mechanical support.

7.2.5. Prior to start the interoperability tests, the cards are tested to be sure than the cards are free of major errors which can interfere with the interoperability tests. The tests performed are the mutual authentication check and the Protocolar analysis to verify the compliance with the ISO 7816-3.

7.2.6. Manual operations on the vehicle unit front-panel controls are recorded on an appropriate registration form:

- *DTL.ITC.01* for the tests on the digital tachograph cards;
- *DTL.ITV.01* for the tests on the digital tachograph recording equipment.

The data recorded shall include vehicle unit time, card identity, card slot, activity performed and observations of the test engineer.

7.3. Calibration Test

According the definition (*f*) of the Regulation, "calibration" 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).*

Calibration Test

Use each workshop card of the *DTLab* Set of Reference to calibrate the recording equipment.

Objectives

According the requirement *154* of the Regulation, the calibration function shall allow:

- to pair the motion sensor with the VU, according the type of VU this function performed automatically;
- to digitally adapt the constant of the recording equipment (k) to the characteristic coefficient of the vehicle (w) (vehicles with two or more axle ratios shall be fitted with a switch device whereby these various ratios will automatically be brought into line with the ratio for which the equipment has been adapted to the vehicle),
- to adjust (without limitation) the current time,
- to adjust the current odometer value,
- to update motion sensor identification data stored in the data memory,
- to update or confirm other parameters known to the recording equipment: vehicle identification, w, l, tyre size and speed limiting device setting if applicable.

Rationale

The workshop card pairs the vehicle unit with the motion sensor and activates the recording equipment. This is a necessary preparatory step for all subsequent interoperability tests and provides an opportunity for checking the workshop card.

Req.	Description
243	Vehicle manufacturers or fitters shall activate the installed recording equipment at the latest before the vehicle is used in scope of Regulation (EC) No. 561/2006'..
246	After its activation, the recording equipment shall fully enforce functions and data access rights.
247	The recording and storing functions of the recording equipment shall be fully operational after its activation.

Expected behaviour

Req.	Description
98	Vehicle unit records calibration activity data: • purpose of calibration; • workshop name and address; • workshop card number, card issuing Member State and card expiry date; • vehicle identification; • parameters updated or confirmed.

Req.	Description
227	Workshop card records calibration and time adjustment data: • purpose of calibration; • vehicle identification; • parameters updated or confirmed • recording equipment identification (VU part number, VU serial number, motion sensor serial number.

Remarks

Use of each workshop card demonstrates that the RSA algorithm in the vehicle unit operates correctly over the full range of *e* (encoded in the MSCA.C on the cards, see Table 10.1) prescribed by the Regulation.

Successful pairing of the vehicle unit and the motion sensor demonstrates that the motion sensor master keys are correctly encoded in the vehicle unit and the workshop card; and that the motion sensor data are correctly encrypted within the motion sensor.

CalibrationPurpose – Appendix 1 – 2.4

```
Code explaining why a set of calibration parameters was recorded. This data type is related to requirements 097 and 098.

CalibrationPurpose ::= OCTET STRING (SIZE(1)).

Value assignment:

¡00¡H reserved value,

¡01¡H activation: recording of calibration parameters known, at the moment of the VU activation,

¡02¡H first installation: first calibration of the VU after its activation,

¡03¡H installation: first calibration of the VU in the current vehicle,

¡04¡H periodic inspection.
```

The tests performed during the certification will assign the `CalibrationPurpose` codes ‘`02`’H, ‘`03`’H and ‘`04`’H.

Action in case of failure

Card Rejected: Record card identity and any useful information on the test module. The test is stopped.

Any of the points specified in the here above requirements failed: Record card identity and any useful information on the test module. The test is stopped.

7.4. Operating Mode Test

Description

Insert each driver, control, and company card into the driver and co-driver slots and record the mode of operation selected by the vehicle unit. Perform operations appropriate to each mode selected.

Objectives

Req.	Description
007	Verify that the vehicle unit switches to the mode of operation appropriate to the inserted tachograph card.
014	Upon card insertion the recording equipment shall detect whether the card inserted is a valid tachograph card and in such a case identify the card type.
109	The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder.

Rationale

Selection of a vehicle unit operating mode depends on successful deciphering of the certificate holder authorisation (CHA) encoded in the tachograph card equipment key certificate. This proves that the mutual authentication protocol completed successfully.

Expected behavior

Req.	Description

081	For each driver card insertion and withdrawal cycle vehicle unit records:
	• card holder's surname and first name(s) as stored in the card;
	• card's number, issuing Member State and expiry date as stored in the card;
	• insertion date and time;
	• vehicle odometer value at card insertion;
	• slot in which the card is inserted;
	• withdrawal date and time;
	• vehicle odometer value at card withdrawal;
	• following information about the previous vehicle used by the driver, as stored in the card:
	  • VRN and Member State registering authority of vehicle;
	  • card withdrawal date and time.

095	The recording equipment shall also record and store in its data memory: • the date and time of the last over speeding control, • the date and time of the first over speeding following this over speeding control, • the number of over speeding events since the last over speeding control.

Req.	Description
102	Vehicle unit records control activity data: • date and time of control; • control card number and card issuing Member State; • type of control (displaying).
104	The recording equipment shall record and store in its data memory the following data relevant to the 255 most recent company locks. ▪ lock-in date and time, ▪ lock-out date and time, ▪ Company Card number and card issuing Member States, ▪ Company name and address. Data previously locked by a lock removed from memory due to the limit above, shall be treated as not locked'.
121	When no other information needs to be displayed, the recording equipment shall display, by default, the following: ▪ the local time (as a result of UTC time + offset as set by the driver), ▪ the mode of operation, ▪ the current activity of the driver and the current activity of the co-driver. ▪ Information related to the driver: ▪ if his current activity is DRIVING, his current continuous driving time and his current cumulative break time, if his current activity is not DRIVING, the current duration of this activity (since it was selected) and his current cumulative break time.'
197	Driver card records vehicles used data: • date and time of first use of vehicle; • vehicle odometer value at that time, • date and time of last use of vehicle; • vehicle odometer value at that time, • VRN and Member State registering authority of vehicle.
233	Control card records control activity data: • date and time of control; • type of control (displaying); • VRN and Member State registering authority of vehicle.
237	Company card records company activity data: • date and time of activity; • type of activity (VU locking in and/or out) • VRN and Member State registering authority of vehicle.

Remarks

Where appropriate, the results are validated by the data recorded on the card, the printout and the content of vehicle unit memory.
The correct operation of both card slots of the recording equipment is verified using the following sequence of card insertions and operations to write activity data to each type of tachograph card.

Step	Card	Slot	Operation
1	Company	Driver	Lock in / out
2	Driver	Driver	None
3	Control	Driver	Display
4	Company	Co-driver	Lock in / out
5	Driver	Co-driver	None
6	Control	Co-driver	Display

Action in case of failure

Card Rejected: Record card identity and any useful information on the test module. The test is stopped.

Any of the points specified in the here above requirements failed: Record card identity and any useful information on the test module. The test is stopped.

7.5. Card Validity Test

Description

Use a workshop card to set vehicle unit date and time to a value between the expiry date of the driver / control / company card and the expiry date of the MSCA.C. Insert each card from same batch in turn into the vehicle unit driver slot and record the response of the vehicle unit.

Objectives

Req.	Description
009	The recording equipment shall ignore non valid cards inserted, except displaying, printing or downloading data held on an expired card which shall be possible.

Rationale

The MSCA.C expires after the Card.C. The mutual authentication protocol should check the validity of both card key certificates encountered.

Req.	Description
014	Upon card insertion the recording equipment shall detect whether the card inserted is a valid tachograph card and in such a case identify the card type.

Expected behaviour

The vehicle unit and the workshop card shall record time adjustment data. After time adjustment, the vehicle unit shall not record any information about the expired cards.

Req.	Description
101	Vehicle unit records time adjustment data: • date and time, old value; • date and time, new value; • workshop name and address; • workshop card number, card issuing Member State and card expiry date.
059	The vehicle unit shall record *Insertion of non-valid card* events

Remarks

Requirement *154* states that the workshop card shall permit unlimited adjustment of the vehicle unit clock. This requirement could cause a workshop card to invalidate itself, if the vehicle unit clock were set to a date later than the expiry date of the workshop card. For this reason, the test laboratory requires unlimited validity workshop cards.

Actions in case of failure

VU limits date adjustment: Use unlimited validity laboratory workshop card to set VU date.
Expired card accepted: Perform additional tests as required to establish whether failure is due to the cards or to the vehicle unit.

7.6. Activity Simulation

Description

Use driver and control cards in a simulation of system operation to create activity data in the vehicle unit data memory and on the tachograph cards.

Objectives

To create a driving activity record, including one over speeding event.

To perform control actions.

The relevant chapters of the Annex I(B), rather than specific requirements, are referenced in the following table.

Req.	Description
III.4	Monitoring driver activities
III.8	Monitoring control activities

Rationale

Creation of activity data records in the vehicle unit memory and in the tachograph cards provide documentary evidence of correct operation of the system components.

Expected behaviour

Req.	Description
35	It shall be possible for the driver and/or the co-driver to manually select WORK, AVAILABILITY, or BREAK/REST.
36	When the vehicle is moving, DRIVING shall be selected automatically for the driver and AVAILABILITY shall be selected automatically for the co-driver.
37	When the vehicle stops, WORK shall be selected automatically for the driver.
38	The first change of activity arising within 120 seconds of the automatic change to WORK due to the vehicle stop shall be assumed to have happened at the time of vehicle stop (therefore possibly cancelling the change to WORK).
39	This function shall output activity changes to the recording functions at a resolution of one minute.
56	This function (Monitoring control activities) shall monitor DISPLAYING, PRINTING, VU and card DOWNLOADING activities carried while in control mode.
84	Vehicle unit records changes of activity, driving status, and driver card insertions or withdrawals: • driving status (*Crew*, *Single*) • slot (*Driver*, *Co-Driver*), • card status in the relevant slot (*Inserted*, *Not Inserted*); • activity (*Driving*, *Availability*, *Work*, *Break/Rest*); • date and time of change.

Req.	Description
102	Vehicle unit records control activity data: • date and time of control; • control card number and card issuing Member State; • type of control (printouts).
199	Driver card records driver activity data: • date; • daily presence counter ; • total distance travelled by the driver during this day; • driver status at 00:00; whenever the driver has changed activity, and/or has changed driving status, and/or has inserted or withdrawn his card; • driving status (*Crew*, *Single*); • slot (*Driver*, *Co-Driver*); • card status in the relevant slot (*Inserted*, *Not Inserted*); • activity (*Driving*, *Availability*, *Work*, *Break/Rest*); • time of the change.
233	Control card records control activity data: • date and time of control; • type of control (driver activity printout and overspeeding printout); • VRN and Member State registering authority of vehicle.

Remarks

Vehicle motion is simulated by a servo motor actuating the motion sensor according to a programmed speed cycle which shall generate one over-speeding event.

Each batch of cards (distinguished by the MSCA.C) shall be tested. Similar to the VU Operating Mode test (Section 7.4), the following sequence of card insertions and operations shall be performed using cards from the same batch:

Step	Card	Operation
1	Driver	Vehicle motion simulation
2	Control	Printouts: Driver activities from card daily printout Overspeeding printout

Action in case of failure

This test is performed after recognition of the different types of tachograph card by the vehicle unit has been demonstrated. Possible failure modes are not known *a priori*.

7.7. Cross Check Test

Description

Insert a driver card into a vehicle unit under test, and simulate driver activity. Repeat this operation introducing the card in each vehicle unit of the Type Approved set of VUs.

Objectives

Verify that the driving activity records are correctly recorded on the card and in the vehicle unit memories.

Expected behaviour

All diving activities must be printed on the ticket of each vehicle unit.

7.8. Card Reading Test

Description

Check the reading of data from driver and workshop cards, and verify the computation of driver working time.

Objectives

Verify that a vehicle unit correctly computes driver working time from data stored on driver cards (also by another type of vehicle unit).

Req.	Description
106	The recording equipment shall be able to read from tachograph cards, where applicable, the necessary data: • to identify the card type, the card holder, the previously used vehicle, the date and time of the last card withdrawal and the activity selected at that time; • to check that last card session was correctly closed; • to compute the driver's continuous driving time, cumulative break time and cumulated driving times for the previous and the current week; • to print requested printouts related to data recorded on a driver card; • to download a driver card to external media.
107	In case of a reading error, the recording equipment shall try again, three times maximum, the same read command, and then if still unsuccessful, declare the card faulty and non valid.
127	It shall be possible to display selectively on request: • the UTC date and time, and local time offset, • the content of any of the six printouts under the same formats as the printouts themselves, • the continuous driving time and cumulative break time of the driver, • the continuous driving time and cumulative break time of the co-driver, • the cumulated driving time of the driver for the previous and the current week, • the cumulated driving time of the co-driver for the previous and the current week. • Optional: • the current duration of co-driver activity (since it was selected), • the cumulated driving time of the driver for the current week, • the cumulated driving time of the driver for the current daily work period, • the cumulated driving time of the co-driver for the current daily work period.'

Rationale

Demonstration of interoperability is to observe that different types of vehicle unit can compute driver working time from data stored in a driver card.

Expected behaviour

Req.	Description
127	It shall be possible to display selectively on request: • the cumulated driving time of the driver for the previous and the current week; • the cumulated driving time of the co-driver for the previous and the current week.

Actions in Case of Failure

Incorrect cumulated driving time calculation: Perform additional checks as required to confirm repeatability of observation.

8. VERIFICATION OF THE DIGITAL TACHOGRAPH CARDS

The tachograph cards, before and after the tests described above are analyzed using the *Collis HDT* or the *Read Annex Card Test application.* According to the outcome of the initial test, the card will either proceed to the interoperability tests in vehicle units, or the interoperability test sequence will be suspended for consultations with the card supplier.

The results of this analysis are subdivided in three parts:

- Electronic personalisation; visualization of the data as reported on the card.
- Test cases generic to all types of cards; reading of the content, communication and security.
- Tests cases on the elementary files (EF) specific to the type of card under analysis.

8.1. Generic analysis

- **ReadCardData**

Test	Verdict
ClearImageFile	passed
ReadCardContent	passed

- **Communication**

Test	Verdict
Initialisation	passed
ApplicationSelection	passed

- **Security**

Test	Verdict
MS_Certificate	passed
Card_Certificate	passed
CertificateVerification	passed
DigitalSigning	passed

8.2. Elementary File analysis

The following table highlights the tachograph card elementary files (EF) which are continuously analyzed.

	Elementary File	All types of cards
00 02	EF_ICC	X
00 05	EF_IC	X
05 01	EF_APPLICATION_IDENTIFICATION	X
C1 00	EF_CARD_CERT	X
C1 08	EF_CA_CERT	X
05 20	EF_IDENTIFICATION	X

	Elementary File	Driver Card	Workshop Card	Control Card	Company Card
05 0E	EF_CARD_DOWNLOAD_DR	X			
05 09	EF_CARDDOWNLOAD_WS		X		

	Elementary File	Driver Card	Workshop Card	Control Card	Company Card
05 21	EF_DRIVING_LICENCE_INFO	X			
05 0A	EF_CALIBRATION		X		
05 0B	EF_SENSOR_INSTALLATION_DATA				
05 02	EF_EVENTS_DATA	X	X		
05 03	EF_FAULTS_DATA	X	X		
05 04	EF_DRIVER_ACTIVITY_DATA	X			
05 05	EF_VEHICLES_USED	X	X		
05_06	EF_PLACES	X	X		
05_07	EF_CURRENT_USAGE	X	X		
05 08	EF_CONTROL_ACTIVITY_DATA	X	X		
05 22	EF_SPECIFIC_CONDITIONS	X	X		
05 0C	EF_CONTROLLER_ACTIVITY_DATA			X	
05 0D	EF_COMPANY_ACTIVITY_DATA				X

9. MUTUAL AUTHENTICATION PROTOCOL

Annex I(B) Appendix 11 *CSM_020* defines the mutual authentication protocol (see Figure 9.1), which requires the successful completion of 12 RSA operations (see circled numbers in left margin and summary in Table 9.1) before data can be written to a tachograph card. The four decision boxes labeled A to D are also described.

- Each row in Table 9.1 describes one RSA operation in terms of:
- the component performing the RSA calculation (column *Executed By*);
- the message on which the RSA calculation is performed (column *Message*);
- the RSA key used by the component (column *Key Used*) - an optional numeric subscript indicates a previous RSA operation which recovered the key;
- the result obtained by the component performing the calculation (column *Result*).

For example:

Op.1 The vehicle unit operates on the Member State CA certificate supplied by the card (TC.CA.C) using its own copy of the European root public key (VU.EUR.PK), to recover the public key of the Member State CA which issued the card (TC.CA.PK).

Op.4 The tachograph card operates on the vehicle unit certificate (VU.C) using the Member State public key recovered in Op.3 (VU.CA.PK3), to recover the public key of the vehicle unit (VU.PK).

RSA Op.	Executed By	Message	Key Used	Result
1	VU	TC.CA.C	VU.EUR.PK	TC.CA.PK
2	VU	TC.C	$TC.CA.PK_1$	TC.PK
3	TC	VU.CA.C	TC.EUR.PK	VU.CA.PK
4	TC	VU.C	$VU.CA.PK_3$	VU.PK
5	TC	Modified VU Challenge (MVC)	TC.SK	Sig (MVC)
6	TC	Sig (MVC)	$VU.PK_4$	TC AuthToken
7	VU	TC AuthToken	VU.SK	Sig (MVC)
8	VU	Sig (MVC)	$TC.PK_2$	MVC
9	VU	Modified Card Challenge (MCC)	VU.SK	Sig (MCC)
10	VU	Sig (MCC)	$TC.PK_2$	VU AuthToken
11	TC	VU AuthToken	TC.SK	Sig (MCC)
12	TC	Sig (MCC)	$VU.PK_4$	MCC

Table 9.1: Summary of CSM_020 mutual authentication protocol RSA operations

The test in decision box A checks whether the value of the Card Certificate Holder Reference (Card.CHR - an 8-byte value of type *KeyIdentifier*) is known to the vehicle unit. A vehicle unit can perform test A (and B) by maintaining a database of recently-inserted cards (also known as a *keyring*). A vehicle unit can load the key-ring with data recovered from card certificates in RSA operations 1 and 2 (public key, PK; key identifier, KID; certificate holder authorisation, CHA; and end-of-validity, EOV); and can then use the key identifier to access the data.

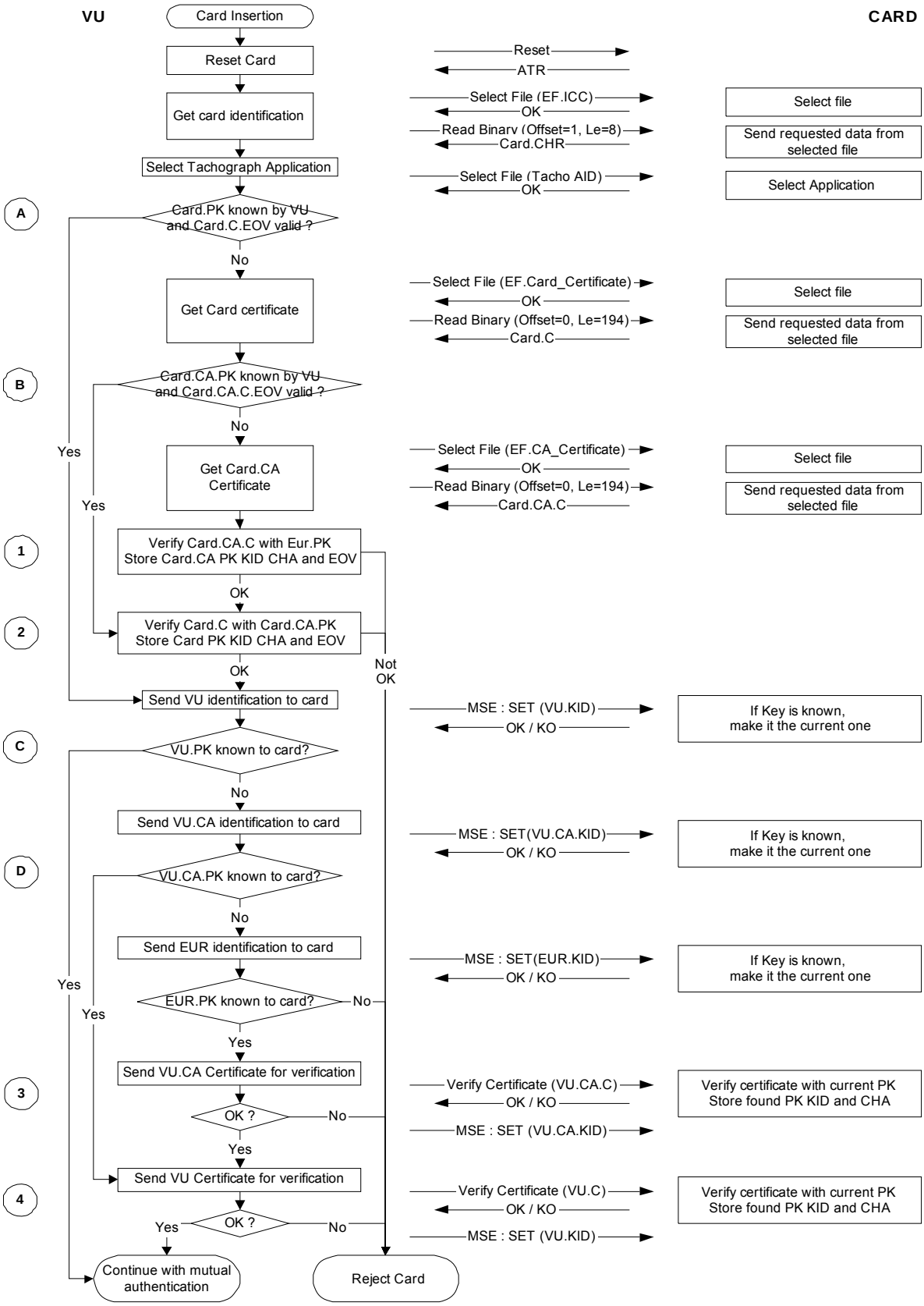

Figure 9.1: Annex I(B) Appendix 11 CSM_020 mutual authentication protocol

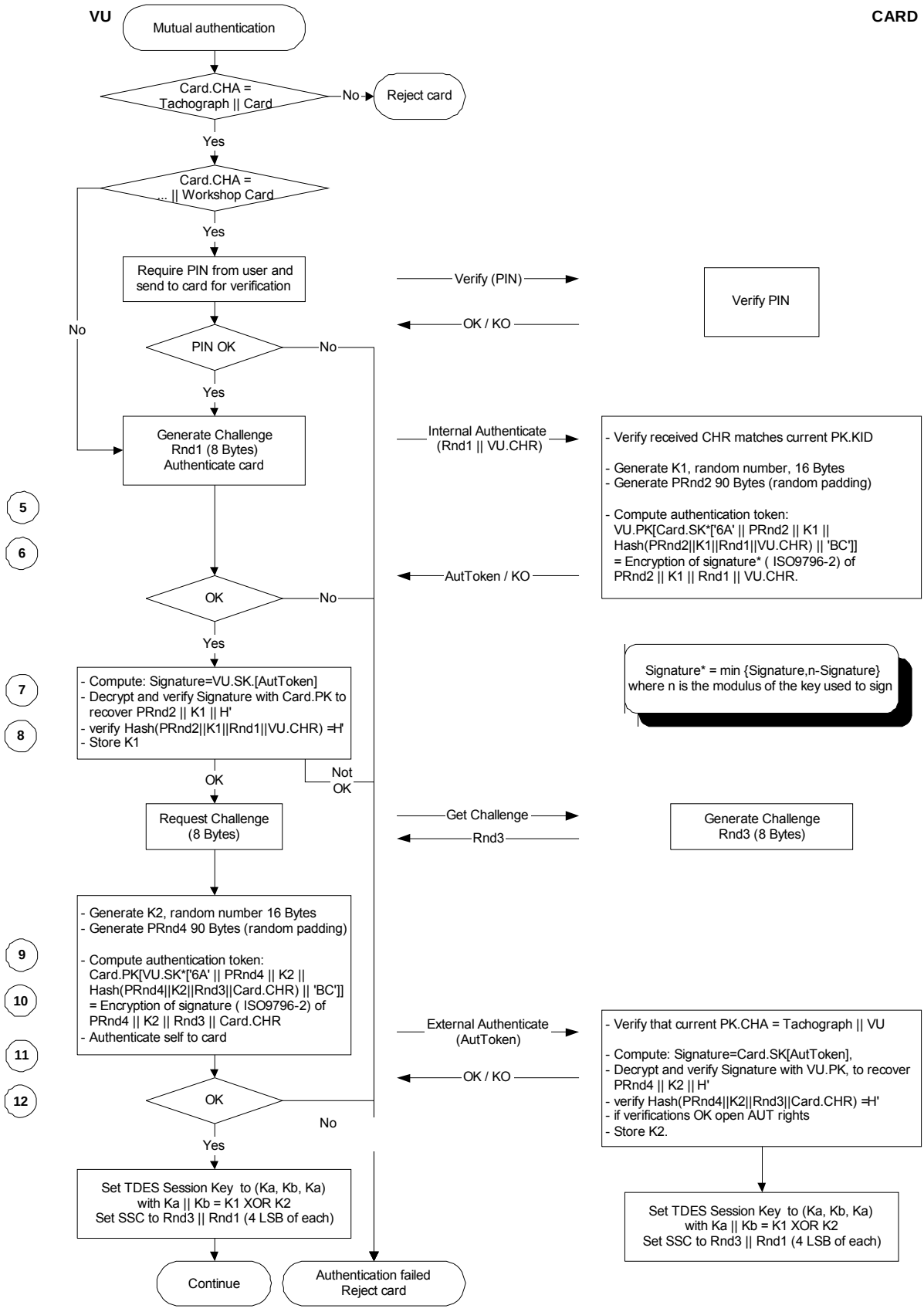

Figure 9.1: Annex I(B) Appendix 11 CSM_020 mutual authentication protocol (*cont.*)

Similarly, a card could load a key-ring with data recovered from vehicle unit certificates in RSA operations 3 and 4; with the sole exception that EOV has no meaning for a card (which has no internal clock).

For the key-ring concept to work correctly, a key identifier must uniquely identify a public key (RSA parameters n and e) and an end-of-validity date. This fact mandates the use of different MSCA keys for certifying vehicle unit keys (VU.CA.C and VU.C must both have undefined EOV) and tachograph card keys (TC.CA.C and TC.C must have limited EOV).

A well-known attack on authentication protocols involves certificate playback. For example, and with reference to Figure 9.1, an adversary attempting to write false driver activity data to a card could program a card terminal to return Card.C in place of VU.C prior to RSA Op.4. This simple exchange actually allows the CSM_020 protocol to proceed as far as the External Authenticate command prior to RSA Op.11.

The adversary obtains the card authentication token plaintext. The card blocks the protocol because when it checks the *EquipmentType* encoded in the Certificate Holder Authorisation (CHA) field of the alleged VU.C, it will find a value corresponding to a tachograph card, instead of a vehicle unit.

To block this attack earlier (e.g. after RSA Op.4), a card might check the value of the RSA modulus n contained in the alleged VU.C and block the protocol if it finds that Card.*n* equals VU.*n*. This possibility mandates the creation of unique equipment keys.

10. INTEROPERABILITY TEST KEYS AND CERTIFICATES

This section describes the collection of RSA keys, TDES keys, and digital tachograph certificates created by the European Root Certification Authority for testing purposes. The collection is available from the web site of the Digital Tachograph at Ispra (http://dtc.jrc.ec.europa.eu) or sending an email to the functional mail box erca@jrc.ec.europa.eu. The source code of the software tools used to create the collection is included to allow any interested party to create its own chains of keys and certificates.

The test set consists of chains of public key certificates linked by the Certification Authority Reference (CAR, see Annex I(B) Appendix 11 CSM_018).

The keys and certificates in the interoperability test set are registered in the database of the European Root Certification Authority. Test certificates are identified by the ASCII characters 'T' and 'K' (hexadecimal values 54h and 4Bh) in the `AdditionalInfo` fields of the Certification Authority Reference.

10.1. Values of Interoperability Test Keys

The RSA parameters of the test keys are chosen to exercise the implementations of the RSA algorithm developed by the different equipment manufacturers.

Annex I(B) Appendix 11 CSM_014 states:

RSA keys shall have (whatever the level) the following lengths: modulus n 1024 bits, public exponent e 64 bits maximum, private exponent d 1024 bits.

CSM_014 sets the following conditions on the RSA parameters:

The modulus n, and the private exponent d, shall be odd integers, falling within the range:

$$2^{1023} \square 1 \leq n \leq 2^{1024} - 1$$

The public exponent e shall be an odd integer, falling within the range:

$$3 \leq e \leq 2^{64} - 1$$

As shown by Table 9.1, public keys (*n, e*) are used in RSA operations 1, 2, 3, 4, 6, 8, 10 and 12; while private keys (*n, d*) are used in the digital signature operations 5, 7, 9, and 11.

Correct implementation of the RSA algorithm against extreme values of the public exponent e can therefore be tested by appropriate Member State CA keys. Correct operation of the digital signature algorithm can be tested by extreme values of the modulus n in equipment keys.

To ensure that implementations of the RSA algorithm are correct and complete, the interoperability test set includes keys with randomly generated and deliberately selected values of *e* and *n*.

Extreme values of the public exponent e (3 and 2^{64}-1) are used in Member State keys. Extreme values of the modulus n (close to $2^{1023} + 1$ or 2^{1024} 1) are used in equipment keys. Such keys are obtained by constraining the ranges of values from which the prime factors *p* and *q* are drawn (*n* = *pq*).

Certain values of the public exponent *e* reduce the time required to perform RSA computations. These are prime numbers in whose binary representation only two bits are set, e.g. 3 (11_2), 17 (10001_2), and

65537 (10001_{16}). To take advantage of this fact, the value 65537 is used for e in all equipment level keys.

The assignments of key values within each certificate chain are summarised in Table 10.1. Note that, having selected values for e and n, the values of the private exponent d are determined by the condition:

$$ed \equiv 1 \ mod \ \Box p-1\Box\Box q-1\Box$$

Key Serial Number	e	n	EOV	Key Usage
EUR 00	Random	Random	N/a	MSCA.C 00 05
MSCA 00	3		Undefined	VU.C 01 / 02 / 03
MSCA 01	Random			VU.C 04 / 05 / 06
MSCA 02	2^{64} - 1			VU.C 07 / 08 / 09
MSCA 03	3			TC.C 03 / 04 / 05 / 06
MSCA 04	Random		Defined	TC.C 07 / 08 / 09 / 10
MSCA 05	2^{64} - 1			TC.C 11 / 12 / 13 / 14
VU 01 / 04 / 07	65537	Low	Undefined	Authentication tokens (digital signatures)
VU 02 / 05 / 08		Random		
VU 03 / 06 / 09		High		
TC 05 / 09 / 13		Low	Defined	
TC 01 / 02 / 03 / 04 07 / 08 / 11 / 12		Random		
TC 06 / 10 / 14		High		

Table 10.1: Convention adopted for assigning RSA parameters within certificate chains

Each key in Table 10.1 is associated with a serial number encoded within the *KeyIdentifier* as described in Annex I(B) Appendix 1 sections 2.62, 2.56, 2.35, and 2.36.

Tachograph card serial numbers 01 and 02 are reserved for the purposes of the interoperability test laboratory (see Sections 6.2.5 and 10.5).

Table 10.1 show how a Member State key is used to produce a batch of equipment key certificates. Within each batch of equipment keys, there are keys with low, random, and high moduli.

10.2. Identification of Public Keys

Digital tachograph certificate contents are defined in Annex I(B) Appendix 11 CSM_017 and summarised in Table 10.2. The certificate format is defined in Annex I(B) Appendix 11 CSM_018:

The certificate issued is a digital signature with partial recovery of the certificate content in accordance with ISO/IEC 9796-2 [*3*], with the "Certification Authority Reference" appended.

The rationale for appending the CAR is given in Annex I(B) Appendix 11 CSM_018 Note 2:

CAR, being hidden by the signature, is also appended to the signature, such that the Public Key of the Certification Authority may be selected for the verification of the certificate.

The format of a *KeyIdentifier* (CAR or CHR) appropriate for Member State keys permits the identification of the Member States (data type *NationNumeric* and *NationAlpha*, see definitions in Annex I(B) Appendix 1 section 2.72 and 2.71).

The format of the CHR appropriate for equipment keys identifies the equipment manufacturer (data type *ManufacturerCode*, see definition in Annex I(B) Appendix 1 section 2.67).

The assignment of manufacturer codes is the responsibility of the interoperability laboratory.

Name	Full Name	Length [Bytes]	Remarks	Definition [Appendix 1]
CPI	Certificate Profile Identifier	1	Certificate structure descriptor value 01 for current version	2.33
CAR	Certification Authority Reference	8	Identifier of CA key used to produce the certificate.	2.62 2.36
CHA	Certificate Holder Authorisation	6	Fixed part: FFh TACHO	2.34
	Equipment Type	1	Variable part: equipment type	2.35 2.52
EOV	End of validity	4	32-bit integer: seconds elapsed since midnight 1970-01-01	2.110
CHR	Certificate Holder Reference	8	Identifier of RSA key encoded in the certificate	2.62 2.35 2.36 2.56
n	Modulus	128		2.86 2.89
e	Public exponent	8		2.86 2.91
		164		

Table 10.2: Digital tachograph certificate content

10.3. Equipment Type Assignment

Annex I(B) Appendix 1 2.52 defines the data type *EquipmentType*, encoded in the last byte of the certificate holder authorisation field (see CHA, Table 10.3).

KeyID	CHA last byte	Equipment Type
MSCA 00 - 05	0	Reserved for MS.CA.C

KeyID	CHA last byte	Equipment Type
VU 01 - 09	6	Vehicle unit
TC 01	2	Workshop card (JRC)
TC 02	3	Control card (JRC)
TC 03, 07, 11	1	Driver card
TC 04, 08, 12	2	Workshop card
TC 05, 09, 13	3	Control card
TC 06, 10, 14	4	Company card

Table 10.3: Identification of equipment types

10.4. Equipment Type Assignment

As required by Annex I(B) Appendix 11 CSM_017, digital tachograph public key certificates contain an end-of-validity date (see EOV, Table 10.2).

During a mutual authentication exchange (Annex I(B) Appendix CSM_020 and Figure 9.1) the vehicle unit checks the validity of the tachograph card by comparing UTC date and time from its internal clock (Annex I(B) requirement 027) with the EOV dates encoded in the MSCA public key certificate (MSCA.C) and the tachograph card public key certificate (Eqt.C).

The EOV dates encoded in card certificates must be appropriate for the foreseen lifetimes of the cards: 5 years for a driver card, and 1 year for a workshop card. This requires that the EOV of the MSCA certificate be later than the EOV of the card certificate.

Certificate Type	Validity [Years]
MSCA (Tachograph cards)	7
Driver / control / company cards	5
Workshop card	1
MSCA (Vehicle units)	n/a
Vehicle unit	n/a

Table 10.4: Validities of interoperability test certificates

Tachograph cards have no independent source of time, and cannot check the validity of a public key certificate received from an alleged vehicle unit (or any other card terminal). The EOV date encoded in vehicle unit certificates is therefore set to an undefined value (FFFF FFFFh; 32 bits all set to 1) according to Annex I(B) Appendix 11 CSM_017.

The dates and corresponding EOV values used in the interoperability test key set are summarised in Table 10.4.

Although the Regulation prescribes no end-of-validity for control or company cards, it is normal practice in smart card systems to define validity for all cards issued. Validities of control and company cards are therefore set to 5 years.

10.5. Keys and Certificates Required for Equipment Management

The interoperability test laboratory requires unlimited validity tachograph cards to manage the vehicle units submitted for interoperability type approval (e.g. to guarantee unlimited variation of the vehicle unit internal clock).

One workshop card and one control card personalised with unlimited validity certificates will be required. To ensure unlimited validity of these cards, an RSA key was created for the JRC, and certified with unlimited validity by the root test key.

To introduce the JRC as an MSCA:

- the unused code FCh is added to the data type definition *NationNumeric* in Annex I(B) Appendix 1 2.72;
- the ASCII string JRC (4Ah, 52h, 43h) is added to the data type definition *NationAlpha* in Annex I(B) Appendix 1 2.71.

The public keys of the tachograph cards (serial numbers 01 and 02) are certified with the JRC key, to produce a special certificate chain (see Figure 10.1).

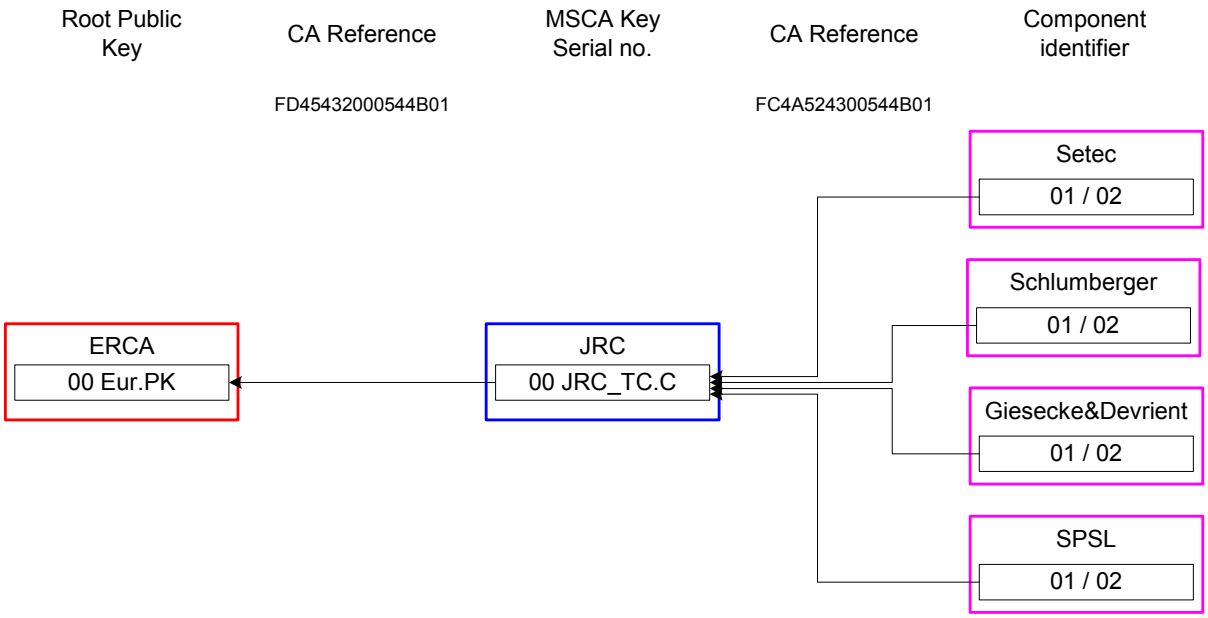

Figure 10.1: Certificate chains for equipment management cards

The tachograph cards for management of the vehicle units shall not undergo interoperability type approval tests.

11. LEGISLATION

The text of Regulation 1360/2002 Annex I(B) chapter VIII amended with 1266/2009 – *Type Approval of Recording Equipment and Tachograph Cards* is reproduced here for reference purposes.

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 paper, for use by the recording equipment, shall be considered as a component of the recording equipment.

269 Recording equipment shall be submitted for approval complete with any integrated additional devices.

270 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.

271 Member States type approval authorities will not grant a type approval certificate in accordance with Article 5 of this Regulation, as long as they do not hold:

- a security certificate,
- a functional certificate
- and an interoperability certificate,

for the recording equipment or the tachograph card, subject of the request for type approval.

272 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.

273 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.

2. Security Certificate

274 The security certificate is delivered in accordance with the provisions of Appendix 10 to this Annex.

274a In the exceptional circumstance that the security certification authorities refuse to certify new equipment on the grounds of obsolescence of the security mechanisms, type approval shall continue to be granted only in this specific and exceptional circumstance, and when no alternative solution, compliant with the Regulation, exists.

274b In this circumstance the Member State concerned shall, without delay, inform the European Commission, which shall, within twelve calendar months of the grant of type approval, launch a procedure to ensure that the level of security is restored to its original levels.

3. Functional certificate

275 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.

275a Manufacturers shall provide the relevant samples of type approved 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.

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

277 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.

277a The functional certificate of any recording equipment component shall also indicate the type approval numbers of all other type approved compatible recording equipment components.

4. Interoperability certificate

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

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

280 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.

281 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 274a.

282 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.

283 The interoperability tests shall be carried out, in accordance with the provisions of paragraph 5 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.

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

285 If the interoperability tests are not successful with one or more of the recording equipment or tachograph card(s), as requested by Requirement 283, the interoperability certificate shall not be delivered, until the requesting manufacturer has realised the necessary modifications and has succeeded with 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.

286 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.

287 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.

5. Type approval certificate

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

289 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.

290 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.

6. Exceptional procedure: first interoperability certificates

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

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

293 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 realise the necessary modifications.

294 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.

295 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 294, shall be postponed until the initial interoperability problems have been solved. Those requests are then processed in the chronological order of their registration.

12. REFERENCES

1 - Commission Regulation (EC) No 1360/2002 of 13th June 2002; Official Journal of the European Communities L207, 05.08.2002.

2 - ISO 9001 (1994) *Quality Systems – Quality Assurance in Design, Development, Production, Installation and Servicing Functions*

3 - ISO / IEC 9796-2 (1997-09-01) *Information Technology – Security Techniques – Digital signature schemes giving message recovery*

4 –ECE/TRANS/SC.1/2006/2/Add.1 (2008-02-29) – United Nations – Economic and Social Council – *European Agreement concerning the work of crews of vehicles engaged in international road transport (AETR)*

5 - Commission Regulation (EU) No 1266/2009 of 16th December 2009; Official Journal of the European Union L339, 22.12.2009.

European Commission
Joint Research Centre – Institute for Institute for the Protection and Security of the Citizen

Title: **Digital Tachograph Equipment, Type Approval Interoperability Test Specification - Version2.3**

Authors: Dominique Landat, James Bishop

Luxembourg: Publications Office of the European Union

2012 – 41 pp. – 21.0 x 29.7 cm

Abstract

This publication is an update of the JRC Scientific and Technical Report EUR 24811 EN – 2011. It reports the interoperability test procedure developed for Digital Tachograph equipment as defined in Council Regulation No. 3821/85 amended by Commission Regulation 1360/2002 of 13 June 2002 and Commission Regulation (EU) 1266/2009 of 16 December 2009. Interoperability Certification is one of three certifications required for type approval of Digital Tachograph equipment. The other two certifications concern functional testing, and security evaluation.

JRC75155

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.