EU-MIDT

Plenary

EU-MIDT/PLE/012-2006

Digital Tachograph System

Guidelines on Type approval

Monitoring of the Implementation
of Digital Tachograph
MIDT

REF : EU-MIDT/PLE/012-2006

EU-MIDT SECRETARIAT DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	IDT Project		31/05/2003
CHECKED BY	Marie-Christine BONNAMOUR	Cybele – MIDT Secretariat	24/04/2006
APPROVED BY	Thierry GRANTURCO	Granturco & Partners – MIDT	24/04/2006
ISSUED BY	Secretariat	MIDT	17/05/2006

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION

FINAL REPORT ON TYPE APPROVAL

Foreword

The type approval procedure, at the time it was defined as one of the issue to be dealt with by SNRA in the framework on the IDT-project, was based on the assumption that card and tachograph manufacturers were able to respect the 12 months deadline stated in Article 2.3 of the Regulation (EC) n° 2135/98 and that support could have to be rapidly provided to the Member States which might have had to organise functional tests.

But it appeared immediately after the start of the project that manufacturers were in reality not in a position to comply with this deadline.

SNRA took indeed the initiative, in close cooperation with the European Commission, to organise an ad hoc meeting on this subject on 29 November 2002, two months after the kick-off meeting of the project, during which the manufacturers confirmed their impossibility to comply with the type approval procedure as defined in Chapter VIII of Commission Regulation (EC) n° 1360/2002.

It appeared also rapidly, despite the explanations given by the European Commission on this issue, that Member States do not interpret on the same way the provisions governing the type approval procedure.

Therefore, the work carried out on type approval was not the one SNRA expected to do and it has not been done in the circumstances and in the atmosphere SNRA would expected to work.

The work concentrated consequently on the necessity to organise tests, first considered as being necessarily part of the type approval procedure, which have been named Member States Process Tests (MSPT).

A feasibility study has been conducted on this issue by May-Lis FARNES which made clear that although these tests are necessary to ensure a proper issuing of tachograph cards, they can not be considered as mandatory and part of the type approval procedure, as laid down in the Council Regulation (EC) n° 2135/98 and in the Commission Regulation (EC) n° 1360/2002.

The Steering Committee decided on the 23rd of January 2003, since this issue is directly linked to the issuing of the tachograph cards, to ask the Card Issuing Working Group (CIWG) to tackle it.

The feasibility study has been issued by the IDT-project to the CIWG project on the 24th of January 2003.

The report contains the integral version of this feasibility study with some basic explanations of the type approval procedure.

1. Introduction

This document provides a feasibility study regarding the need for a **Member State Process Test** to secure the quality (functionality and interoperability) of the issuing of Tachograph cards.

The digital Tachograph and the Tachograph cards need to be typed approved. To achieve type approval they need to do the following steps :

- security evaluation
- functional test
- interoperability test

The functional and interoperability test is done with test certificates and keys only. This documents looks into the need of a test by each Member State with real certificates running the Member State card issuing process of Tachograph cards, a so-called **Member State Process Test**.

It also looks into the different possibilities of implementation and estimation of cost for the implementation.

Scope

The scope of the document is restricted to the testing of Tachograph cards by the Member States.

Essential questions posed in the document are:

- Is there a need for **Member State Process Test**?
- What is the relationship with other types of testing done by type approval?
- What would be the objectives of the **Member State Process Test**?
- How to assure accuracy and impartiality of the **Member State Process Test**?
- How to specify the **Member State Process Test**?
- How to implement the **Member State Process Test**?
- Estimate on the time for specifications and implementation of the **Member State Process Test**.
- Look into cost estimates of different possible solutions.

References

Annex I(B)	*Requirements for construction, testing, installation, and inspection* to Council Regulation (EC) No 2135/98 and appendices.
"Draft 1"	Digital Tachograph Proposed Interoperability Tests, T.E.M.P.E.S.T. Laboratory

SWEDAC-EID-SAT	Test specification of EID Cards and certificates; test procedures for the assessment of compliance with the Swedish EID Standard, SS 61 43 30-32
Interoperability	Interoperability Tachograph cards, Vägverket (SNRA)
ITSEC	ITSEC Information Technology Security Evaluation Criteria, 1991.
ICPP9806	Smartcard Integrated Circuit Protection Profile - version 2.0 - issue September 1998. Registered at French certification body under the number PP/9806.
ESPP991	Smart Card Integrated Circuit With Embedded Software Protection Profile - version 2.0 - issue June 99. Registered at French certification body under the number PP/9911.

Abbreviations

Appendix N	Unless otherwise stated, Appendix N refers to the corresponding appendix of the Annex I(B).
MSPT	Member State Process Test
SNRA	Swedish National Road Authority (Vägverket)
EID	Electronic ID (smart) card.

Feasibility Study

Motivation for Member State Process Test (MSPT)

Type Approval

For the type approval, there are three steps of testing defined in the Annex I(B), Appendix 9, together with respective certifications:

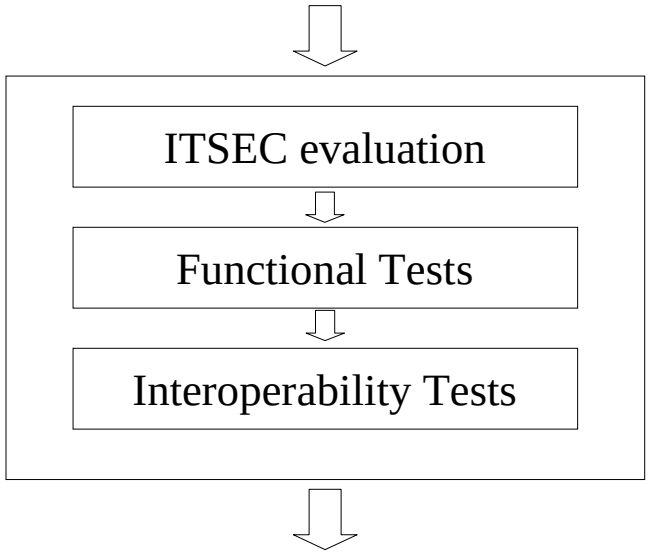


Figure 1. Type Approval

- A security certification is performed by an ITSEC authority.
- A functional certification is performed by a Member State authority.
- An interoperability certification is performed by the competent body (TEMPEST laboratory).

Some Important Experiences

Compared with electronic ID cards, such as FinEID of SwedishEID, the Tachograph cards seem to have better odds at some issues, and worse odds at other issues. The experience with the EID (ISO7816 smart cards with X.509 certificates) shows that there occur discrepancies among would-be standard-conformant products:

- Regarding smart cards, the discrepancies manifested often in minor, albeit significant, differences in interpretation of standards; ISO7816 series of standards does leave some space for interpretations and choices for the implementations.
- Regarding certificates, “dualism” and error in implementations of ASN.1 coding ware typical sources of interoperability issues.
- In addition to this, major vendors would often choose “own” structures, at “odd” places.

The following sections (0 and 0) compare the stated experiences with the situation for the Tachograph cards.

What can be expected to be better?

a) Annex I (B) is detailed in the specifications with the aim of being *unambiguous*, both for the card commands and for the data structures.
b) The specification for the "certificates" for the Tachograph cards is significantly *simpler* than the X.509v3 certificates.
c) Another thing that is inherently better is the *provision for the testing process*. The process is described later in this document, but the main thing to remember is that the Member States (and corresponding authorities) can (and must) test the manufactured units and certify the products that pass the tests. This gives the Member States the means of *enforcing so to say "proper implementations"*.

What can get wrong?

a) Implementing specifications from the Annex I (B) occurs *for the first time*. The experience calls for caution here:

    - There will be literally hundreds of thousands of cards issued by the Member State authorities.
    - Given the fundamental principles of the Union, it is safe to assume that there will be products from different providers.

    Conclusion:

    - It would be big embarrassment to end up in the situation where, say, one Member State issues cards that are not usable in some other Member State. Dealing with such a huge deployments, there is never too much of cautiousness in preparations.

b) As stated in 0, section a), the Annex attempts to be unambiguous. At the present, it is hard to claim that this is 100% true.

c) The provision for testing process may be *incomplete*. Later in the document, this is discussed in more detail (see 0,2 and 0,3). The consequence of this could be non-interoperability among the Member States.

Relationship between MSPT and other types of testing from Type Approval

The protection profiles of the Tachograph cards are defined by references ICPP9806 and ESPP991, augmented with the requirements defined in the Appendix 10 (*Tachograph card generic security target*).

Relationship to *ITSEC*

The relationship to ITSEC is defined in the Appendix 10, "Tachograph card generic security target":

- Section 6. Claimed Minimum Strength of Mechanisms

  "The minimum strength of mechanisms for the Tachograph Card is **High** as defined in [ITSEC]."

- Section 7. Level of Assurance

  "The target level of assurance for the Tachograph Card is ITSEC level **E3**, as defined in [ITSEC]."

Thus, the Member State Process relies on the ITSEC evaluations to approve that the card manufacturer indeed implements the cards with the specified target levels. In other words, one is assured that the *static characteristics* of the cards and the corresponding manufacturing process are following the above quoted requirements.

Relationship to *Tachograph cards functional tests*

Functional tests (see Appendix 9) define testing of the cards as a part of the type approval process. Those tests should be performed by the Member State Authority.

1) Administrative examination,
2) Visual inspection,
3) Physical tests,

   Description:
   Omitted.

   Relationship with the MSPT:
   Omitted – the tests are necessary by the Annex.

4) Protocol tests

   Description:
   The protocol tests verifies that the card functions according to protocols T=0 and T=1, as specified in the Annex I (B) and relevant standards (ISO 7816-1/4).

   Relationship with the MSPT:
   Basic condition for the communication with the cards is established/proved.

5) Card structure

   Description:
   This test verifies that the card has all elementary and directory files present, and access conditions are properly set, as defined in Appendix 9.

   Relationship with the MSPT:
   Static structure and characteristics of the card is established/proved.

6) Functional tests

Description:
The test verifies that commands are executed by the card and verifies the presence of a response in case of error.

Relationship with the MSPT:
The ability to perform commands is established/proved.

Observe that the Appendix does not provide specifics about the functional tests. Quote:

> *"Test at least once each allowed usage of each command (ex: test the UPDATE BINARY command with CLA = '00', CLA = '0C' and with different P1,P2 and Lc parameters). Check that the operations have actually been performed in the card (ex: by reading the file the command has been performed on)."*

This allows for **difference** among type approvals performed by different Member State authorities. Further work should be done in order to see if this could have consequences to the interoperability and if so, which.

7) Environmental Tests
Description:
Omitted.

Relationship with the MSPT:
Omitted – the test is necessary by the Annex.

Relationship to *Interoperability tests*

Interoperability tests (see Appendix 9) define testing of the cards carried out by a single laboratory under the authority and responsibility of the European Commission. Those tests are also part of the type approval process.

Description:
The tests are divided in "mutual authentication" and "activity scenarios" and are performed with a vehicle unit and a card.

Relationship with the MSPT:

1. Interoperability is asserted here trough activity scenarios, meaning that the *data structures* are only *indirectly* tested.
2. Chapter VIII (of the Annex), requirement 283, refers to interoperability tests from Appendix 9, paragraph 5. The specification for the interoperability is vague in Test 2:

> "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…"

This allows for different interpretations and different ways of executing activity scenarios. Instead, there should be a requirement to *define* the scenarios and the scenarios should be *always* executed, *for each* card type to be tested.

Obviously, the laboratory may in fact choose to implement and perform the interoperability tests in such a fashion, thus reducing the risk that some card "slip trough".

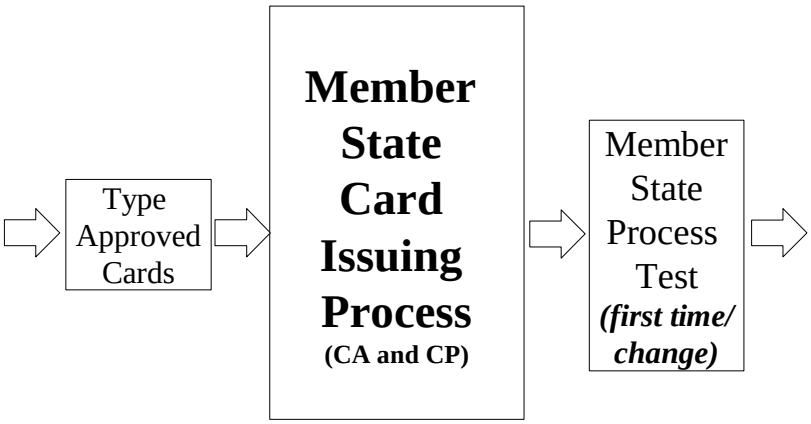
3. Chapter VIII, the requirements 285 together with 291-295 ("Exceptional procedure: first interoperability certificates") provides for possibility to have essentially an *erroneous* implementation pass the interoperability test. Requirement 285 implies that *the first* manufacturer to apply for the interoperability certificate may have the decisive role in determination of not only what the interoperability is but also of the correctness of the implementation of the specifications (of the Annex and the referred standards).

   One other way to seek for the interoperability is to have *reference implementations*. However, it is important to observe that the Annex cannot be blamed for the lack of referential implementation – it would be practically impossible to have such reference implementations, simply because since there were no existing implementations at the time of writing the Annex. Also, the whole system involves products from possibly several manufacturers.

Positioning of the Member State Process Test

The Member State Process Test is seen as a complementary to the process of type approval.

The relationship and the role of MSPT are depicted in the following way:



The basic point is that MSPT is conducted in case that some new product is to be used by a Member State authority, or some change in a product or in the process is done.

Benefits from a Member State Process Test

- Being a common test, the MSPT serves effectively as a replacement for the referential implementation of a type-approved card.
- Provision for error feedback-loop. If the MSPT finds some problems, those can be traced to either the Member State Process or to the Type Approval. This is very desirable feature, since one could improve the Member State Process, or strengthen the Functional/Interoperability Tests.
- The Member State Authorities could even use the MSPT in cases where public tenders/proposals are considered.
- The Member State Authorities get additional check on the produced and issued Tachograph cards, thus reducing the risk of inconsistencies among the member states, or, worse, replacement of erroneous cards being issued.

How to implement Member State Process Test

Objectives for the Member State Process Test

The objectives for MSPT should be to provide a *common, verifiable and repeatable* test suite that covers areas relevant to conformance testing of Tachograph cards. The areas of relevance are:

1) Protocol conformance
2) File structure conformance
3) Data structures conformance
4) Use-cases / scenarios

The areas 1) and 2) are covered in 0 (points 4)and 5)). It seems that there is no need to augment the functional tests in those areas; just to reaffirm.

Data structures on the card can be tested for conformance according to the relevant standards and specifications (ASN.1, ISO7816 series and Annex I(B) with appendices). The test suite should provide detailed visual output for the cases where conformance testing indicates some error.

Use cases and/or scenarios should assert that the cards function in the cases that are to be expected in the real life situations. The scenarios should follow the real life-cycle of the card.

The composition of the scenarios should be such to define normal/expected operations as well as unexpected and erroneous cases, specifically for the situations where “common users” are involved.

How to assure accuracy and impartiality of the Member State Process Test?

To prove accuracy *per se* is hard, if not practically impossible. The usual steps taken in the industry to assure the interoperability are:

1) Provide “reference implementations”

This would be the interoperability test suite itself.

2) Use commonly accessible “proven” software tools
This refers to libraries and other modules available to purchase or for free. Such modules should have been already used in adjacent areas of relevance.

3) Provide source code (where applicable)
In case of a dispute, the source code gives opportunity to have more detailed detection/description of the issue.

In order to provide impartiality, the tests should be performed on all types of cards, for each of the manufacturers. This is relevant to:

a) Member State Authority, assuring that *each* card type passed the tests
b) Manufacturers/providers, assuring the equal treatment.

The output of the test should be provided to the manufacturers, in order to resolve any possible interoperability issues.

Towards specification for the Member State Process Test

The scope of the MSPT could be defined as:
“Member State Process, production-cycle, testing of the protocols, files and data structures for conformance with the requirements of the Annex I (B)”.

The specification should:

1) Define test suites - *what* is being tested, according to the objectives stated in 0. The test suits will be numbered and referencing relevant requirements from Annex I (B), wherever applicable. The scenarios would be named and numbered. All inputs and required outputs (expected behaviour that can be verified by programmatic means) have to be defined.

2) Define the requirements for the software modules (discussed later, see 0), thus allowing the Member State Authorities (or anyone else interested and/or involved) to install, executed and replicate the outcome of the tests.

3) For the sake of completeness, the MSPT could even include the functional tests in some form. The rationale behind this is to provide reason/evidence for the manufacturer in case one claims that some test fails.

Implementation choices for the Member State Process Test

Language and operating system

Implementation choices should reflect guidelines presented in this document. There are two obvious choices regarding the programming language: C/C++ and Java. The experience, in Sweden, from SWEDAC-EID-SAT shows that the implementations in Java are as good as in C/C++.

Regarding the operating system, the recommendation is that the test suite should require execution on the Windows platform, with as much as possible platform-independent code. It

is assumed that all actors (NRA-s and manufacturers) have possibility to run on Windows. Also, the choice of card readers and device drivers is greater. Current implementation of PS/SC on other platforms is promising alas there are some “glitches”. Platform-specific implementation parts should be well isolated, thus allowing for use on other operating systems.

Libraries and other modules

Libraries and other software modules used for the interoperability tests should be selected to assure the best possible confidence in the correctness of the implementation of the underlying mechanisms. As stated earlier in the document, important features here would be availability of the source code and use in relevant (adjacent) areas.

Another aspect here is to avoid unnecessary implementations in the areas where satisfactory software modules are already available, thus saving time and resources.

Use-cases/scenarios

Implementation-wise, the use-cases could be considered to provide in forms of scripts, named after scenarios.

Estimates for specifications and implementation of the MSPT

Estimation of the work-effort to define the specification for the MSPT is dependent on how much of the functional test protocol developed by the Netherlands can be used. The combination of the work is not looked into in detail yet.

The test specification of the MSPT has to be defined as a first step. If it is possible and feasible to implement at common test tool (based on the specification) this should be done as a step 2.

Test specification (step 1)

It is estimated that the work-effort needed to define specifications for MSPT would be in the range 2-7 man/weeks (ca. 9.000-31.000 EURO). This depends on the scope and required level of details and the reuse of the functional test specification mentioned above.

Implementation of at test tool (step 2)

The estimate for the implementation of a test tool based on the specification of the MSPT can be done only very roughly. One reason for that is that we have not made the specification yet. It could take anything between 2 to 4 man/months of effort (ca. 35.000-70.000 EURO). A better estimate can be done once the test specifications are prepared and required software components identified.

Conclusion

The MSPT should be seen as auxiliary to the Type Approval process and thus not “compete” with it.

The MSPT will be useful in order to assure the Member States that the implementation of the products and processes is done in correct, interoperable and error-correcting manner. Both when starting the card issuing process (new processes) but also when maintaining the production line with for example new releases of software which can affect the Member State Process.

The benefits (see 0) seem to give solid ground for the further work on specification and implementation of the MSPT. The way forward has to be chosen.