Joint Interpretation Library

Security Evaluation and Certification of Digital Tachographs

JIL interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex 1B

Version 1.12
June 2003

This page is intentionally left blank

Table of contents

1 Introduction

1.1 General

1 The Digital Tachograph is a control device for recording drivers' activities, such as driving and rest periods.

2 The digital tachograph is required by law in the European Union as a result of the following legislation:

- Regulation (EC) no. 1360/2002 of 5 August 2002, amending Regulation (EEC) no. 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) no. 3820/85 and (EEC) 3821/85.

3 The EU-ministers have formulated four main topics to be addressed by the introduction of the Digital Tachograph. The Digital Tachograph:

- allows effective and efficient enforcement of drivers' activities,
- gives transport companies more possibilities to use the equipment as management tool,
- provides the drivers with clear and accurate information about their driving and rest periods,
- reduces fraud possibilities.

4 The reduction of fraud, in combination with improved possibilities for enforcement, is the main reasons for the security of the digital tachograph system. Annex 1B of EC regulation 1360/2002 [An1B] formulates security requirements for components of the digital tachograph system:

- The motion sensor,
- The vehicle unit, and,
- The tachograph cards.

5 Every manufacturer of these components will have to prove that the security requirements defined in the regulation are respected. To do so, a formal security evaluation is required.

1.2 Background

6 The security requirements for the tachograph components are defined in Annex 1B, appendix 10. They prescribe an ITSEC E3 evaluation and for the Tachograph Card they additionally refer to two Common Criteria protection profiles.

7 This mixture of criteria might potentially lead to different interpretations between the EU member states. It is also expected that several card manufacturers and evaluation facilities would favour the use of the Common Criteria evaluation method [CC] instead of the specified ITSEC evaluation method [ITSEC]. Furthermore, besides the Protection Profiles defined in Annex 1B there are newer protection profiles, which are more in line with current smart card developments, such as multi-application smartcards.

8 With respect to the issues mentioned above, common interpretations of the security requirements of Annex 1B [An1B] are necessary, in order to provide manufacturers guidance in their security approach and to ensure that Member States can verify whether the security requirements defined in the regulation are consistently interpreted.

1.3 Objective

9 The purpose of this document is to define common interpretations of the security requirements as formulated in Annex 1B. The organisations members of the JIL Working Group (BSI, CESG, DCSSI and NLNCSA) will use these common interpretations for Digital Tachograph evaluations and certifications.

10 This document could also serve as a basis for a harmonised interpretation for all member states participating in the EU Digital Tachograph Card Issuing Working Group, Taskforce 3: Security.

2 Interpretations

2.1 Certification of products

11 To be compliant with the requirements, the products shall be “security certified”. The annex 1B defines the “security certification” as: « process to certify, by an ITSEC certification body, that the recording equipment (or component) or the tachograph card under investigation fulfils the security requirements defined in Appendix 10 Generic security targets ».

12 Issue: which organisations could be considered as "ITSEC certification body"?

13 Agreed interpretation: the "ITSEC certification bodies" are certification bodies recognised in the SOGIS [SOGIS].

14 The security certificate only certifies that a product is able to address the security objectives described in the security target. For the digital tachograph, an organisation must certify that the security target is also compliant with the appendix 10.

15 Issue: which organisation must certify the compliance of the security target with appendix 10?

16 Agreed interpretation: the compliance of the security target to the appendix 10 shall be checked by the ITSEF[1] and confirmed by the certification body in the certification report.

2.2 CC or ITSEC

17 The appendix 10 contains ITSEC generic security targets for the motion sensor, the vehicle unit and the tachograph card. The target level of assurance for the evaluated product is ITSEC level E3, strength of mechanisms: high.

18 Issue: is a CC evaluation and a CC certificate acceptable?

19 Agreed interpretation: a CC certificate with sufficient security functional and assurance requirements is acceptable as an alternative to the ITSEC (details on assurance requirements are provided in Annex A).

2.3 Use of smartcard protection profiles

20 For the tachograph cards, appendix 10, chapter 4 requires for the security enforcing functions compliance with [ICPP9806] and [ESPP9911]. Furthermore chapter 3 of appendix 10 specifies, in addition to the smart card general threats and objectives as listed in [ICPP9806] and [ESPP9911], a number of tachograph card specific threats and objectives.

[1] Information Technology Security Evaluation Facility; a term commonly used for an evaluation facility performing ITSEC or CC evaluations.

21 Issue: how to evaluate with ITSEC or CC that the Tachograph Card addresses both [ICPP9806] and [ESPP9911] threats, objectives, and functional requirements and specific tachograph card additional requirements?

22 Agreed interpretation: for ITSEC evaluations, the security target shall include a copy of appendix 10.

23 Agreed interpretation: for CC evaluations, the security target shall include the relevant parts of both [ICPP9806] and [ESPP9911] with additional requirements dedicated to the tachograph application (details are provided in Annex B). Note: details on security assurance requirements are provided in Annex A.

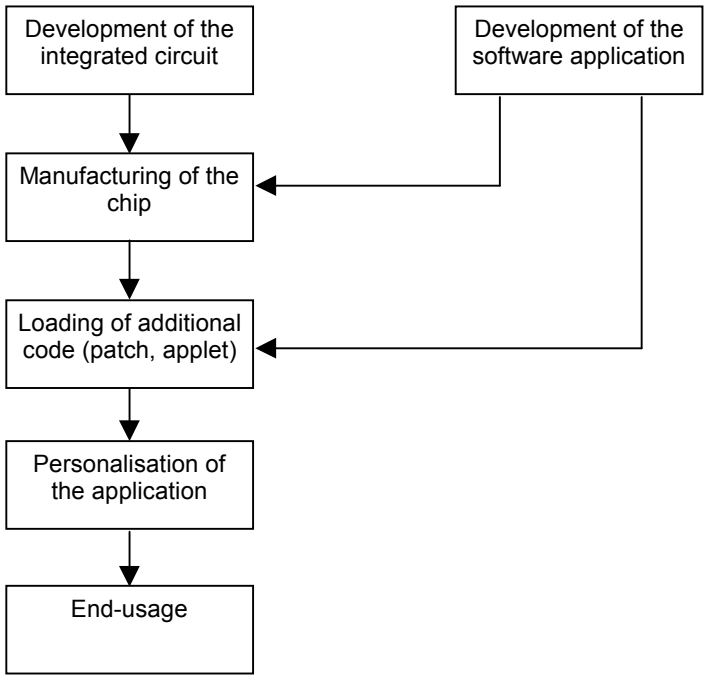
24 The IC PP and the ES PP were the only protection profiles available at the time of the creation of appendix 10.

25 Issue: can a security target claiming compliance with other protection profiles (e.g. [BSIPP02]) be recognised as compliant with appendix 10?

26 Agreed interpretation: compliance claim with other comparable protection profiles could be accepted instead of the compliance with the [ICPP9806] and the [ESPP9911] (details are provided in Annex C). Nevertheless, the ITSEF shall check that the security target is still compliant with appendix 10.

2.4 Scope of the card evaluation

27 As defined in the [ICPP9806] and the [ESPP9911], the typical life-cycle of a smartcard is:



28 Issue: is the evaluation of the personalisation and issuing process part of the card evaluation?

29 Agreed interpretation: the evaluation of the personalisation and issuing process is not part of the card evaluation because the personalisation is considered as an administrative task of the card. Therefore, the security requirements for the personalisation and issuing process as required by ITSEC are not applicable for the formal card evaluation. Likewise for a CC evaluation, the assurance components requiring an audit (mainly ALC_DVS and ACM) are not applicable for the personalisation environment.

30 The ITSEF analyses the guidance provided by the TOE developer in order to verify that the commands and, if any, the organisational requirements for the personalisation environment are well described.

31 As personalisation of the card is likely to be a contracted service, it may be wise for the contracting agency to check the effective application of the requirements but this falls outside the scope of the CC/ITSEC evaluation of the card. A CC evaluation compliant with appropriate PPs for the personalization phase (e.g. [PP0008] and [PP0009]) or the use of other security standards (e.g. [ISO17799]) is recommended.

2.5 Key generation

32 Issue: is the key generation method evaluated in the card evaluation?

33 Agreed interpretation: if the card generates keys as specified in appendix 10 section 4.9, the method used shall be evaluated. If the generation is outside the card, it may be wise to mandate evaluation of this but this falls outside the scope of the CC/ITSEC evaluation of the card.

2.6 Communication between the Tachograph Card and the Vehicle Unit

34 Issue: This problem is concerned with the additional authentication of a human user of a workshop card (see Appendix 10, UIA_302). Depending on the implementation of the workshop card it may be possible to force a Vehicle Unit to authenticate a workshop card without having the PIN of this workshop card. This could be done by intercepting the communication between Tachograph Card and Vehicle Unit and faking and transmitting a successfull PIN verification answer of the Tachograph Card to the Vehicle Unit in the right moment.

35 Agreed Interpretation: To ensure that the Tachograph Card takes care of unsuccessful authentication events, the sentence “The following assignments describe the card reaction in the case of failure of the additional authentication mechanism required in UIA_302.” (Annex 10, chapter 4.2.3) should be read as follows:

36 **Additionally t**he following assignments describe the card reaction in the case of failure of the additional authentication mechanism required in UIA_302.

37 This should ensure that the Tachograph Card (here only the workshop card) only allows a mutual authentication with the Vehicle Unit after a successful PIN Verification of a human user.

38 Issue: In document [GST_TC], FIA_UID.1.1 (TSF mediated actions) states that the card shall allow no operations before the identification of the user, and, FDP_ACF.1.2 (GENERAL_READ) states "User data may be read from the TOE by any user, …".

39 However, [CSM] defines a process to identify and authenticate a VEHICLE_UNIT, but no process is defined to identify other users.

40 Agreed interpretation: In [GST_TC] the following types of users are identified: VEHICLE_UNIT and NON_VEHICLE_UNIT. The user NON_VEHICLE_UNIT is identified by the Tachograph Card by just putting it into a card reading device (which could be a Vehicle Unit). After a successful mutual authentication between Tachograph Card and Vehicle Unit, the Tachograph Card assumes the user VEHICLE_UNIT to be identified.

41 FDP_ACF says that no matter who is identified by the Tachograph Card, user data may be read from the Tachograph Card. This means NON_VEHICLE_UNIT and VEHICLE_UNIT are allowed to read the user data. In fact, at least NON_VEHICLE_UNIT is identified by the Tachograph Card (by putting the Tachograph Card into a card reader / Vehicle Unit) and therefore no TSF mediated actions are possible before identification.

42 Note that beside the identification/authentication of a Vehicle Unit there is also an additional identification/authentication process for a human user (by PIN) using a workshop card. See UIA_302 in [GST_TC].

43 Issue: [GST_TC] § 4.2 and [GST_TC] § 4.3.2 (FDP_ACF.1.2 GENERAL_READ) says that only control cards may have an authentication process before exporting cardholder identification data, but [TCS] TCS_415 says that authentication is mandatory for exporting cardholder identification data.

44 Furthermore, there are no TSF *mediated actions* defined in FIA_UAU.1.1 for the company card.

45 Agreed Interpretation: The allowed actions for a company card seems to be missing in the specification of FIA_UAU.1 in the generic security target of Appendix 10. From the context it is clear that a company card should allow the actions as specified by appendix 2 (which are the same as for a control card). Therefore, the specification of the TOE Security Functional Requirements in [GST_TC] should be read as follows:

46 [GST_TC], Chapter 4.2.2, FIA_UAU.1.1:

47 - Control **and Company** card**s**: Export user data without security attributes except cardholder identification data.

48 and

49 [GST_TC], Chapter 4.3.2, FDP_ACF.1.2:

50	- GENERAL_READ: User data may be read from the TOE by any user, except cardholder identification data which may be read from control cards **or company cards** by VEHICLE_UNIT only.

3 Reference

[An1B] Annex 1B of Council Regulation (EC) No 1360/2002 on recording equipment in road transport.

[CSM] Annex 1B of Council Regulation (EC) No 1360/2002 on recording equipment in road transport. – Appendix 11 – Common Security Mechanisms

[GST_TC] Annex 1B of Council Regulation (EC) No 1360/2002 on recording equipment in road transport. – Appendix 10 – Generic Security Target – Tachograph Card Specification

[TCS] Annex 1B of Council Regulation (EC) No 1360/2002 on recording equipment in road transport. Appendix 2 – Tachograph Card Specification

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (Comprising Parts 1-3).

[CEM] Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 1.0, August 1999.

[ITSEC] Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, June 1991.

[ITSEM] Information Technology Security Evaluation Manual (ITSEM), Version 1.0, September 1993.

[ITSEC-JIL] ITSEC Joint Interpretation Library (JIL), Version 2.0, November 1998.

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, European Commission, Director-General XIII, Telecommunication, Information Market and Exploitation of Research, Security of telecommunication and information systems, SOG-IS (Senior Officials Group Information Systems Security), 21 November 1997, ref: 017/97 Final and revised in April 1999 as version 2.0.

[ICPP9806] Smartcard Integrated Circuit Protection Profile, version 2.0, September 1998. Registered at French certification body (DCSSI) under the number PP/9806.

[ESPP9911] Smart Card Integrated Circuit With Embedded Software Protection Profile, version 2.0, June 1999. Registered at French certification body (DCSSI) under the number PP/9911.

[BSIPP02] Smartcard IC Platform Protection Profile Version 1.0, July 2001. Registered at German certification body (BSI) under the number BSI-PP-0002-2001.

[PP0008] Smartcard Personalisation Sites without Mailer Handling Protection Profile, version 1.0, July 2000. Registered at French Certification body (DCSSI) under the number PPnc/0008.

[PP0009] Smartcard Personalisation Sites with Mailer Handling Protection Profile, version 1.0, July 2000. Registered at French Certification body (DCSSI) under the number PPnc/0009.

[ISO17799] International Standard ISO/IEC 17799:2000, Information Security Management, Code of Practice for Information Security Management

Annex A. CC Assurance requirements for ITSEC E3 SoM High (E3hAP)

A.1 Introduction

51 The Common Criteria have been developed on the basis of different national criteria and the European ITSEC. One objective of the development was, to achieve compatibility to the existing criteria as much as possible. Because not all ITSEC requirements, interpretations and guidelines could be implemented in equivalent CC assurance packages (EALs), these packages can be augmented to provide a more exact mapping.

52 One main difference between ITSEC and CC is the method of specifying the assurance requirements for the Vulnerability Analysis and for the Strength of Mechanisms/Function Analysis in terms of attack potential.

53 ITSEC defines attack potential for both, the Vulnerability Analysis and the Strength of Mechanism Analysis, by a Strength of Mechanism claim (e.g. SoM high).

54 CC defines the attack potential for:

- The Vulnerability Analysis by selection of a specific AVA_VLA component;
- The attack potential on probalistic and permutational mechanisms by a Strength of Function claim using the AVA_SOF component with a low, medium or high claim (e.g. SoF high).

A.2 Objectives

55 A specific mapping between ITSEC and Common Criteria requirements is necessary to match the Evaluation Assurance requirements stated in Annex 1B, appendix 10 (ITSEC E3-high) to the Common Criteria assurance requirements. The intention of this annex is to define an evaluation assurance package incorporating the specified ITSEC requirements for the Digital Tachograph.

A.3 Assurance components

56 The following table shows the selected CC components for the equivalent ITSEC E3-high level. This package is called E3hAP and is put alongside the CC EAL4 to allow for comparison. Augmentations above the EAL4 level are highlighted in bold and red.

Assurance Classes	Family		CC EAL4	E3hAP	Notes
Configuration Management	ACM	AUT	1	-	(see note 1)
		CAP	4	4	
		SCP	2	2	
Delivery and Operation	ADO	DEL	2	2	
		IGS	1	**2**	(see note 2 and 3)
Development	ADV	FSP	2	2	(see note 4)
		HLD	2	2	
		IMP	1	**2**	(see note 5)

Assurance Classes	Family		CC EAL4	E3hAP	Notes
		INT	-	-	
		LLD	1	1	
		RCR	1	1	
		SPM	1	-	(see note 6)
Guidance Documents	AGD	ADM	1	1	
		USR	1	1	
Life Cycle Support	ALC	DVS	1	1	
		FLR	-	-	
		LCD	1	-	(see note 7)
		TAT	1	1	
Tests	ATE	COV	2	2	
		DPT	1	**2**	(see note 8)
		FUN	1	1	
		IND	2	2	
Vulnerability Assessment	AVA	CCA	-	-	
		MSU	2	2	(see note 9)
		SOF	1	1H	(see note 10)
		VLA	2	**4**	(see note 11)

57 All components have to be used as defined in CC, CEM and the relevant final interpretations of the CCIMB. The following additional notes have to be taken into account. Where no further information is given in the following, selection of the relevant component from the EAL4 package was obvious.

58 Note 1:
ACM_AUT was not selected because ITSEC does not require tool support for configuration control at E3 level.

59 Note 2:
ITSEC E3.32 with respect to ITSEC-JIL Section 16.2 requires:

a) The term “generation” is always interpreted as “installation”.

b) "While installing the TOE, any configuration options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how the TOE was initially configured and when the TOE was installed."

Therefore ADO_IGS.2 was selected, but with the interpretation / refinement according to ITSEC-JIL as stated above. This has to be outlined in the Security Target.

60 Note 3:
For ADO_IGS an additional requirement as stated in ITSEC E3.35.3 can be important: “If the TOE contains hardware which contains security enforcing hardware components, the administrator, end-user, or self initiated diagnostic tests shall exist that can be performed on the TOE in its operational environment.” Therefore, the ST author of the Common Criteria evaluation has to check whether it is applicable to use the Functional Requirement FPT_TST within the ST.

61 Note 4:
ITSEC requires the level of rigour "describe" for the description of external interfaces and for the specification of security functions in the ITSEC Security Target. Therefore it is required to select ADV_FSP.2, which requires a more rigorous definition of the external interfaces compared to ADV_FSP.1 (i.e. ADV_FSP.1.3C: "...providing details of effects, exceptions and error messages, as appropriate."; ADV_FSP.2.3C: "...providing complete details of all effects, exceptions and error messages."). Additionally, ADV_FSP.2 is more supportive for ATE_COV.2 and ATE_DPT.2 as required.

62 Note 5:
ADV_IMP.2 was selected because ITSEC requires the full "source code or hardware drawings for all security enforcing and security relevant components". This corresponds to the ADV_IMP.2 requirement.

63 Note 6:
ADV_SPM was not selected because ITSEC E3 does not require an informal TOE security policy model.

64 Note 7:
ALC_LCD was not selected because ITSEC E3 does not require a developer defined life-cycle model.

65 Note 8:
ATE_DPT.2 was selected because ITSEC E3.12 and E3.13 require tests to cover all security enforcing and security relevant functions identified in the detailed design and all security mechanisms identifiable in the source code or hardware drawings. Comparing the three CC levels of ATE_DPT, ATE_DPT.2 is the most appropriate level which correspond to ITSEC E3.12/E3.13.

66 Note 9:
AVA_MSU.2 was selected, as it is most obvious. Nevertheless, ITSEC 3.33 additionally requires evaluator tests where necessary. This testing, can be part of the penetration testing under AVA_VLA. Therefore, it shall be decided on a case by case basis if the evaluator has to perform misuse-testing as additional part of penetration testing to confirm or disprove the misuse analysis. Specifically, if high attack potential is assumed, it is recommended to perform such independent misuse-testing.

67 Note 10:
For correspondence to ITSEC E3 high, SOF high has to be selected in the Security Target to analyse the strength of functions against high attack potential.

68 Note 11:
For correspondence to ITSEC E3 high and ITSEC-JIL Section 6.4.2, AVA_VLA.4 was selected to analyse vulnerabilities against high attack potential.

A.4 Dependencies

69 All dependencies outlined in CC Version 2.1 part 3 are fulfilled by the E3hAP.

A.5 Final note

70 If a sponsor wants to use an EAL as a basis for covering ITSEC E3 high, he can use EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2, AVA_VLA.4 and refined corresponding to the notes above.

Annex B. Specific CC-compliant Tachograph requirements

71 The Security Target of the tachograph card must conform to the required or accepted Protection Profiles as given in annex C and the assurance requirements as given in Annex A. Additionally, the tachograph cards must comply with the specific tachograph requirements as specified in Annex 1B, appendix 10.

72 This means that the ST must contain, over and above the content of the Protection Profiles a number of security requirements:

1. It should contain the three threats listed in Tachograph Card Generic Security Target, § 3.3.1 (Annex 1B, appendix 10)
2. It should contain the security objectives listed in Tachograph Card Generic Security Target, § 3.4 and 3.5
3. It should copy the security objectives for the environment in Tachograph Card Generic Security Target, § 3.6
4. It should contain the FIA requirements and complete them as in Tachograph Card Generic Security Target, § 4.2
5. It should contain the FDP_ACC and FDP_ACF requirements and complete them as in Tachograph Card Generic Security Target, § 4.3
6. It should contain more FDP_ACC and FDP_ACF requirements that fully implement Tachograph Card Generic Security Target, § 4.4
7. It should contain a full set of audit requirements, including FAU_SAA completed as in Tachograph Card Generic Security Target, § 4.5
8. It should contain FDP_SDI.2 and FDP_DAU.1 and complete them as in Tachograph Card Generic Security Target, § 4.6
9. It should contain FPT_TST.1 and complete it as in Tachograph Card Generic Security Target, § 4.7.1
10. It should contain FPT_SEP.1 (which in fact implements 4.7.2)
11. It should contain FPT_FLS.1 and complete it consistently with Tachograph Card Generic Security Target, § 4.7.3 and 4.7.4
12. It should contain FTP_ITC.1 refined suitably to meet Tachograph Card Generic Security Target, § 4.8.1
13. It should contain FCO_NRO.1 and FDP_ETC.2 refined suitably to meet Tachograph Card Generic Security Target, § 4.8.2
14. It should contain multiple instances of FCS_COP.1 and FCS_CKM.1, FCS_CKM.2, FCS_CKM.3 and FCS_CKM.4 completed, and where necessary refined in such a way that the combination fully meets Tachograph Card Generic Security Target, § 4.9 and Appendix 11

Annex C. Accepted Protection Profiles

73 Currently the following smart card Protection Profiles are available:

- For the Integrated Circuit alone:
  - PP/9806 [ICPP9806] developed by the community of chip vendors in 1998.
  - The BSI-PP-0002 [BSIPP02] developed by the Secure Semiconductors Vendors Group in 2001.
- For the platform including the IC and its embedded software:
  - The PP/9911 Protection Profile [ESPP9911] developed by the Eurosmart group in 1999. The PP/9911 requires that the IC on which the software relies is evaluated in compliance with the PP/9806.
  - The PP/0010 Protection Profile [ESPP0010] is an evolution of the PP/9911 for the evaluation of multi-application platforms.
  - The SCSUG PP [SCPP01] developed by the Smart Card Security Users Group in 2001 for the evaluation of multi-application platforms for financial and banking applications.

74 Besides the ones mentioned above, new Smart Card Protection Profiles will be developed in the coming years.

75 The use of all these Protection Profiles is not excluded, but for each Protection Profile there needs to be an assessment to determine whether the Protection Profile describes a comparable and acceptable set of functionality for a smart card IC in relationship to the security requirements of Annex 1B [An1B], and whether it is suitable to be used as a basis for a tachograph card. However, all the Protection profiles require work on:

- Completing them with the specific tachograph requirements (see Annex B)
- Bringing the assurance level in line with ITSEC level E3, strength of mechanisms: high (see Annex A)

76 Currently only the Secure Semiconductors Vendors Group Protection Profile [BSIPP02] has been assessed[2] in relationship with [ICPP9806]. Besides the specified [ICPP9806] and [ESPP9911], this PP is also considered to be acceptable for use as a basis for a tachograph card.

[2] A comparison report of [BSIPP02] and [ICPP9806] is available at request from BSI or DCSSI.