PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2007/20

MultiApp ID Tachograph 36K card: GEOS platform and TachographV1.1 application masked on SLE66CX360PE

Paris, 16th November 2007,

Courtesy Translation

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.
Certification does not, however, constitute a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.dcssi@sgdn.pm.gouv.fr

Certification report reference

DCSSI-2007/20

Product name

MultiApp ID Tachograph 36K card: GEOS platform and TachographV1.1 application masked on SLE66CX360PE

Product reference and version

Ref. T1002264 A7 / version 1.1

Protection profile conformity

BSI-PP-0002-2001 [PP0002]

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4 augmented

ADO_IGS.2, ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_MSU.3, AVA_VLA.4

Developers

GEMALTO
6 rue de la verrerie, 92197 Meudon, FRANCE

Infineon Technologies AG
Postfach 80 09 49, D-81609 München, GERMANY

Sponsor

GEMALTO
6 rue de la verrerie 92197 Meudon, FRANCE

Evaluation facility

Serma Technologies
30 avenue Gustave Eiffel, 33608 Pessac, France
Phone: +33 (0)5 57 26 08 75, email : e.francois@serma.com

Recognition arrangements

CCRA

SOG-IS

The product is recognised at EAL4 level.

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

Content

1. The product

1.1. Presentation of the product

The evaluated product is « MultiApp ID Tachograph 36K card: GEOS platform and TachographV1.1 application masked on SLE66CX360PE**,** Ref. T1002264 A7 / version 1.1 **»** developed by GEMALTO and INFINEON.

This product is a smart cart designed to by used in electronic tachographs (recorded equipment in road transport) or on personal computer (to achieve the control operations of the vehicle activities).
The main functions of this card are:

- to store card identification and card holder identification data which are used by the vehicle unit to identify the cardholder, in order to provide accordingly functions and data access rights, and ensure cardholder accountability for his activities,
- to store cardholder activities data, events and faults data and control activities data, related to the cardholder.

The functional requirements for a tachograph card are specified in [EEC/A1B].
During the end-usage phase of a tachograph card life cycle (phase 7), only vehicle units may write user data to the card.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.
The security target is based on [PP/9911].
This security target is compliant to [PP0002] protection profile.

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.
The certified version of the product can be identified by bytes T1 to T7 of its his ATR (Answer To Reset) :

ATR: 3B 97 95 C0 2A 31 FE 35 **D0 00 48 01 05 A3 11**

T1 to T7 bytes of this ATR have the following meaning:

- T1= Component code (D0)
- T2= Hardmask number on this component (00)
- T3= Hardmask version number (48)
- T4= Softmask number on this hardmask (01)
- T5= Softmask version number (05)
- T6= Applet number on this hardmask (A3)
- T7= Applet version number (11)

1.2.2. Security services

The product provides mainly the following security services:

- Basic security services:
  - self test when starting a work session;
  - error Messages and exception management;
  - data erasure;
  - data integrity;
  - data and operation hiding from outside observations;
  - protection linked to the card manager;
- Cryptographic related services:
  - RSA and 3DES key generation;
  - signature creation and verification;
  - 3DES encryption and decryption;
  - message hashing;
  - MAC generation and verification;
  - trusted Path;
  - PIN management;
- Security management services:
  - access Authorization management;
  - domain Separation;
- Physical monitoring.

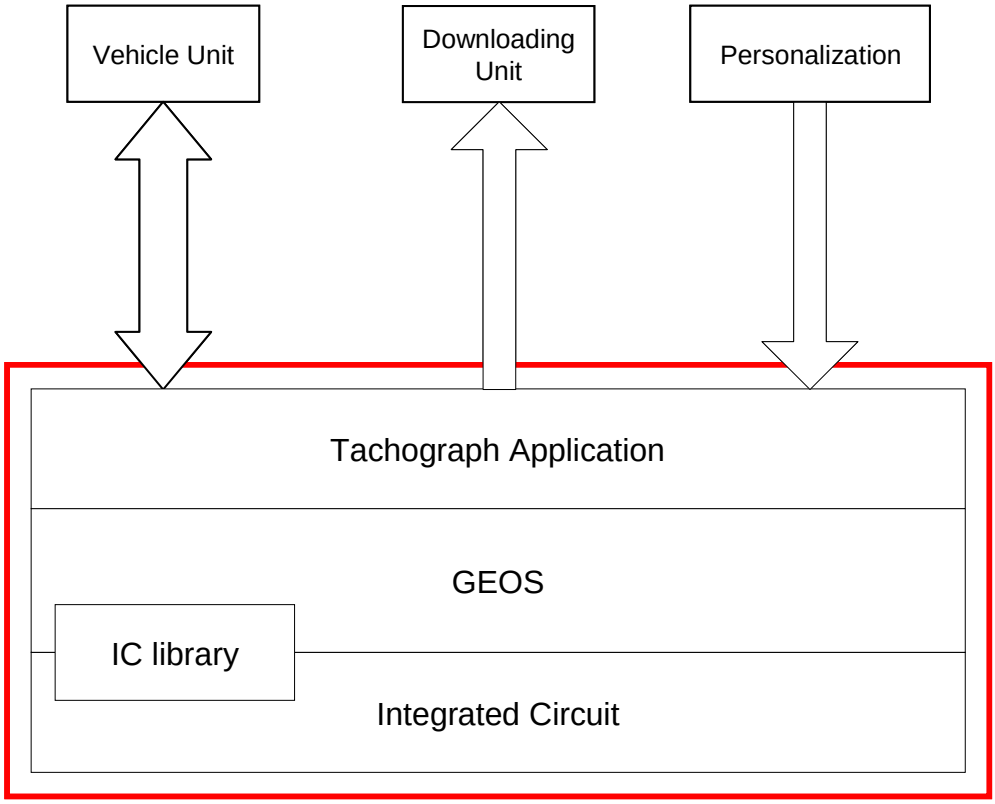
These services are fully described in chapter 6 of the security target [ST].

1.2.3. Architecture

The product consists of :

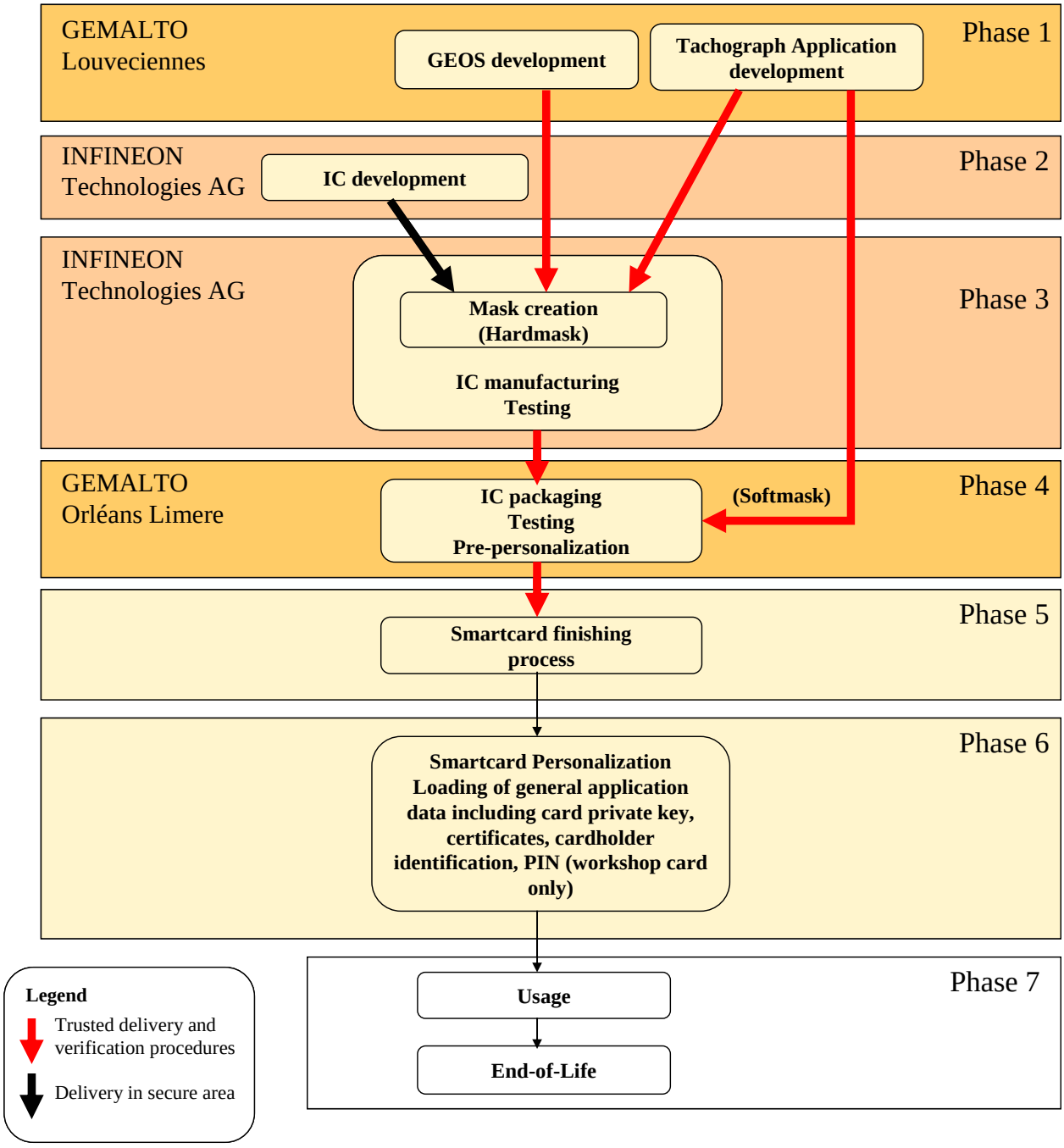
- the microcontroller SLE66CX360PE/ m1536a13 (version A13) and his cryptographic libraries RSA2048 (version 1.4) et RMS (version 2.5), developed and produced by INFINEON;
- the GEOS Operating System, developed by GEMALTO, masked on the ROM's microcontroller (reference : S1021079 A7, version : 23);
- the Tachograph application TachographV1.1, version 1.1, developed by GEMALTO, masked on the ROM's microcontroller (reference : S1022443 A9, version : 3);
- and bug fix code (softmask) developed by GEMALTO, loaded in EEPROM (reference : S1025378 A4, version : 12).

The figure below gives a description of the TOE and its boundaries (the limits of the TOE in red).



1.2.4. Life cycle

The product's life cycle is organised as follow:



In the evaluation context, phases 1 to 4 correspond to the evaluated product development, the delivery is between phases 4 and 5, installation, generation and startup are within phases 4, and finally, phases 5 to 7 correspond to the evaluated product usage.

The product has been developed on the following site:

GEMALTO Louveciennes

36-38, route de la Princesse
78431 Louveciennes
France

The IC design and manufacturing are made by Infineon Technologies AG on the following site:

INFINEON Technologies AG

CCM MTH, Postfach 80 09 49
D-81609 München
Allemagne

The IC packaging is made by Gemalto on the following site:

GEMALTO Limere

Avenue de la Pomme de Pin,
45590 Saint Cyr En Val
France

The user of the product is the cardholder.
The administrator of the product is the personalizer (phase 6). It is recommended to the personalizer to operate in a secure environment and to use security procedures maintaining confidentiality and integrity if the evaluated product as well as its manufacturing and test data (see 3.2, O.TEST_OPERATE).

1.2.5. Evaluated configuration

The product evaluated is the microcontroller with the embedded software identified on § 1.1
The certificate applies to the “locked” configurations of the product (the GlobalPlatform LOAD, INSTALL and DELETE commands are permanently deactivated).
The certificate applies to the following configurations (which is set on personalization phase):

- driver Card,
- company Card,
- workshop Card,
- control Card.

The product tested by the evaluation facility is typical to final product.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC], with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods, validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CCIC] and [CCAP] guides have been applied.

2.2. Evaluation work

The evaluation has been performed according to the composition scheme as defined in the guide [COMP] in order to assess that no weakness is introduced from the integration of the software in the microcontroller already certified.
Therefore, the results of the evaluation of the microcontroller "SLE66CX360PE/m1536a13 with RSA 2048 V1.4 and specifc IC dedicated software" at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [PP0002] protection profile[1]. This microcontroller has been certified the 14th September 2005 under the reference BSI-DSZ-CC-0322-2005.
The microcontroller robustness level gas been confirmed in September and October 2006 in a surveillance process.

The evaluation relies on the evaluation results of the « Java Card Open Platform (reference T100921) » product certified the 10th May 2006 under the reference 2006/08 (see [2006/08]).

The evaluation technical report [ETR], delivered to DCSSI the 9th November 2007, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has not been analysed by DCSSI.

[1] Even if the microcontroller's certificate doesn't explicitly cover ADO_IGS.2 requirement, it is considered here that, because this component doesn't include any application (as a generic IC), it satisfies per default this assurance requirement. So the composition rules are satisfied in that case.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality by a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product "MultiApp ID Tachograph 36K card: GEOS platform and TachographV1.1 application masked on SLE66CX360PE, Ref. T1002264 A7 / version 1.1" submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

The user of the certified product shall respect the operational environmental security objectives summarized specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- procedures on phases 5 to 7 shall ensure protection of masked chip material/information under delivery including the following objectives (O.DLV_PROTECT):
  - non-disclosure of any security relevant information;
  - identification of the elements under delivery;
  - meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgement);
  - physical protection to prevent external damage;
  - secure storage and handling procedures (including rejected masked chips);
  - traceability of masked chips during delivery including origin and shipment details, reception, reception acknowledgement, and location material/information;
- procedures on phases 5 to 7 shall ensure that corrective actions are taken in case of improper operation in the delivery process (O.DLV_AUDIT);
- procedures on phases 5 to 7 shall ensure that people involved in the delivery process have got the required skill, training and knowledge to meet the procedure requirements (O.DLV_RESP);
- the Application Data must be delivered between phase 5 to 7 through a trusted delivery and verification procedure that shall maintain the integrity and confidentiality of the Application Data (O.DLV_DATA);
- appropriate functionality testing of the masked chip shall be used in phases 5 and 6. During all manufacturing and testing operations, security procedures shall be used through phases 5 and 6 to maintain confidentiality and integrity of the masked chip (O.TEST_OPERATE);
- secure communication protocols and procedures shall be used between smartcard and terminal on phase 7 (O.USE_DIAG);

- the issuer must ensure that Secret & Private keys, when outside the masked chip, are handled securely. The disclosure of these keys may give hackers access to the masked chip. The private keys include the European private key, the Countries' Private keys and the vehicle unit private keys The secret keys include VOP TDES keys (OE.Secret_Private_Keys);
- the issuer must ensure that all certificates used in the Tachograph system are handled properly inside a reliable PKI. This includes the revocation of a certificate when the corresponding key is not secure (OE.Qualified certificates).

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.
2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, the Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Name of the component
ACM Configuration management	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**2**	Problem tracking CM coverage
ADO Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**2**	Generation log
ADV Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal TOE security policy model
AGD Guidance	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Life-cycle support	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**2**	Testing: low-level design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing – sample
AVA Vulnerability assessment	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**3**	Analysis and testing for insecure states
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**4**	Highly resistant

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - PHAESTOS-2 Security Target, reference ST_D1038709, version 1.2, August 2007 For the needs of publication, the following security target has been provided and validated in the evaluation: - MultiApp ID Tachograph 36K: Security Target, reference ST_D1038709_public, version 1.2, August 2007
[ETR]	Evaluation technical report : - PHAESTOS-2 project - Evaluation Technical Report, reference Phaestos-2_RTE_v1.2.fm, version 1.2, 9th November 2007
[CONF]	PHAESTOS2: Configuration List, reference LIS_06-000407, version 1.4, September 2007
[GUIDES]	Administration guidance: - PHAESTOS2: Administrator Guide, reference GUI_06-000409, version 1.0, July 2007 User guidance: - PHAESTOS2: User Guide, reference GUI_06-000410, version 1.0, July 2007
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI under the reference BSI-PP-0002-2001.*
[PP/9911]	Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999. *Certifié par la DCSSI sous la référence PP/9911.*
[2006/08]	Rapport de certification 2006/08 - Java Card Open Platform (référence T100921), 10 mai 2006, SGDN/DCSSI
[EEC/A1B]	Council Regulation No 3821/85 on recording equipment in road transport – Annex 1B Requirements for construction, Installation and Inspection

Annex 3. Certification references

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, SGDN/DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of CEM version 2.3 is identical to the international ISO/IEC 18045:2005.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.