PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Certification report 2003/12

ICitizen Tachograph :
Tachograph card version 0.9.0
(reference : M256LFCHRON_SI_A5_05_01)

Courtesy Translation

Warning

This report is designed to provide principals with a document enabling them to certify the level of security offered by a product under the conditions of use or operation laid down in this report for the version evaluated. 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 user and administration guides evaluated, as well as with the product security target, which presents threats, environmental scenarios and presupposed 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 in and of itself a product recommendation from the certifying organization, and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Foreword

Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated 18 April, 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 fulfill 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 ITSEC and Common Criteria certification procedures have been published and are available in French on the following Internet site:

www.ssi.gouv.fr

The international site concerning Common Criteria certification can be accessed at the following Internet address:

www.commoncriteria.org

Certificate Recognition Arrangement

The SOG-IS European **Recognition Arrangement** of 1999 enables all the States which have signed the agreement[1] to recognize the certificates issued by their certifying authority. The European mutual arrangement applies up to ITSEC E6 and CC EAL7. Certificates recognized within the framework of this agreement are issued with the following label:

The central information system security department also signs **recognition agreements** with approved foreign organizations whose head offices are located outside the Member States of the European Community. These agreements may allow for certificates issued by France to be recognized by the signatory countries. They may also stipulate that certificates issued by any one party are to be recognized by all parties. The recognition of certificates may also be limited to a predetermined assurance level.

[1] As of April 1999, the following countries had signed the SOG-IS agreement: the United Kingdom, Germany, France, Spain, Italy, Switzerland, the Netherlands, Finland, Norway, Sweden and Portugal.

The Common Criteria Recognition Arrangement enables the countries that have signed the agreement[1] to recognize certificates issued within the framework of the Common Criteria program The mutual recognition applies up to level EAL4 and to ALC_FLR family. Certificates recognized within the framework of this agreement are issued with the following label:

The following table presents the web sites of the national certification organizations of the countries which have signed the Common Criteria Recognition Arrangement:

Country	Certifying organization	Web site
France	DCSSI	www.ssi.gouv.fr
United Kingdom	CESG	www.cesg.gov.uk
Germany	BSI	www.bsi.bund.de
Canada	CSE	www.cse-cst.gc.ca
Australia-New Zealand	AISEP	www.dsd.gov.au/infosec
United States	NIAP	www.niap.nist.gov

[1] As of January 2003, the following certificate-issuing countries had signed the agreement: France, Germany, the United Kingdom, the United States, Canada and Australia-New Zealand; the countries which do not issue certificates but which have signed the agreement are: Spain, Finland, Greece, Israel, Italy, Norway, the Netherlands, Sweden, Austria and Japan.

Contents

1. Evaluated product

1.1. Context

The European Commission regulation (EEC) 3821/85 on recording equipment in road transport provides the basis for the current analog tachograph, which records the driving time, breaks, rest periods as well as periods of other work undertaken by the driver.
The commission has moved to strengthen enforcement in this area. Council Regulation 2135/98, which amends Regulation (EEC) 3821/85, introduces a new generation of fully digital tachographs. The digital tachograph is a more secure and accurate recording and storage device than the present equipment. The new device will record all the vehicle's activities, for example distance, speed and driving times and rest periods of the driver. The system will include a printer, for use in roadside inspections and the driver will be given a card incorporating a microchip, which he must insert into the tachograph when he takes control of the vehicle.
Commission Regulation (EC) 1360/2002 [EC 1360/2002] and its annex 1B [EC/A1B], published on 5 august 2002 defines technical specifications for the digital tachograph.
Four types of cards will be available: driver cards, workshop cards, company cards and control cards.

1.2. Product identification

The evaluated product is the masked chip **ICitizen Tachograph version 0.9.0** developed by Schlumberger Systèmes and Infineon Technologies AG, made up of the following elements :

Element	Version	Developer
Application Tachograph	SC_V0.9.0	Schlumberger Systèmes
GEOS – Generic Operating System	PLATFORM_T_SC_04_02;9	Schlumberger Systèmes
Library ACE	1.0	Infineon Technologies AG
Library RMS	1.3	Infineon Technologies AG
Chip SLE66CX322P	GC/B14	Infineon Technologies AG

The evaluated masked chip reference is **M256LFCHRON_SI_A5_05_01**.
The reference given by Infineon to Schlumberger Systèmes for the mask made up of the operating system GEOS and the Tachograph application is SB 102.
The masked chip is the basis for the different type of card. The choice of type of card is done in personalisation phase (Figure 2).

1.3. Developers

Schlumberger Systèmes

36-38 rue de la Princesse
BP45
78431 Louveciennes Cedex
France

Infineon Technologies AG

Postfach 80 17 60
81617 München
Germany

1.4. Evaluated product description

1.4.1. Architecture

The evaluated product can be modelised like this :

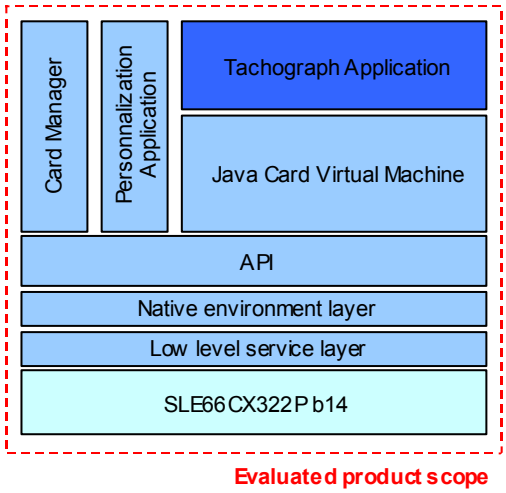

Figure 1 – Evaluated product Architecture

A more detailed description of the application architecture is provided in documentation [HLD].

1.4.2. Life-cycle

The evaluated product lifecycle is part of a 7-step-smartcard-lifecycle:

- Development of the operating system GEOS and the Tachograph application, within Louveciennes development site (§2.5.4) (step 1);
- SLE66CX322P chip development by Infineon (step 2);
- Mask creation by infineon, then manufacturing of the masked chip (step 3);
- Packaging of the masked IC and pre-personnalisation of each micro-module within Orléans manufacturing site (§2.5.4) (step 4);
- Smartcard finishing process (step 5). Each micro-module are securely delivered by Schlumberger Systèmes between step 4 and 5;
- Smartcards personnalisation (step 6);
- Smartcard usage by its holder (step 7). Smartcard end-of-life (corresponding to its destruction) is also included in this step;

From the point of view of the evaluation, steps 1 to 4 correspond to the evaluated product development, the delivery is between steps 4 and 5, installation, generation and startup are within step 4, and finally, steps 5 to 7 correspond to the evaluated product usage.

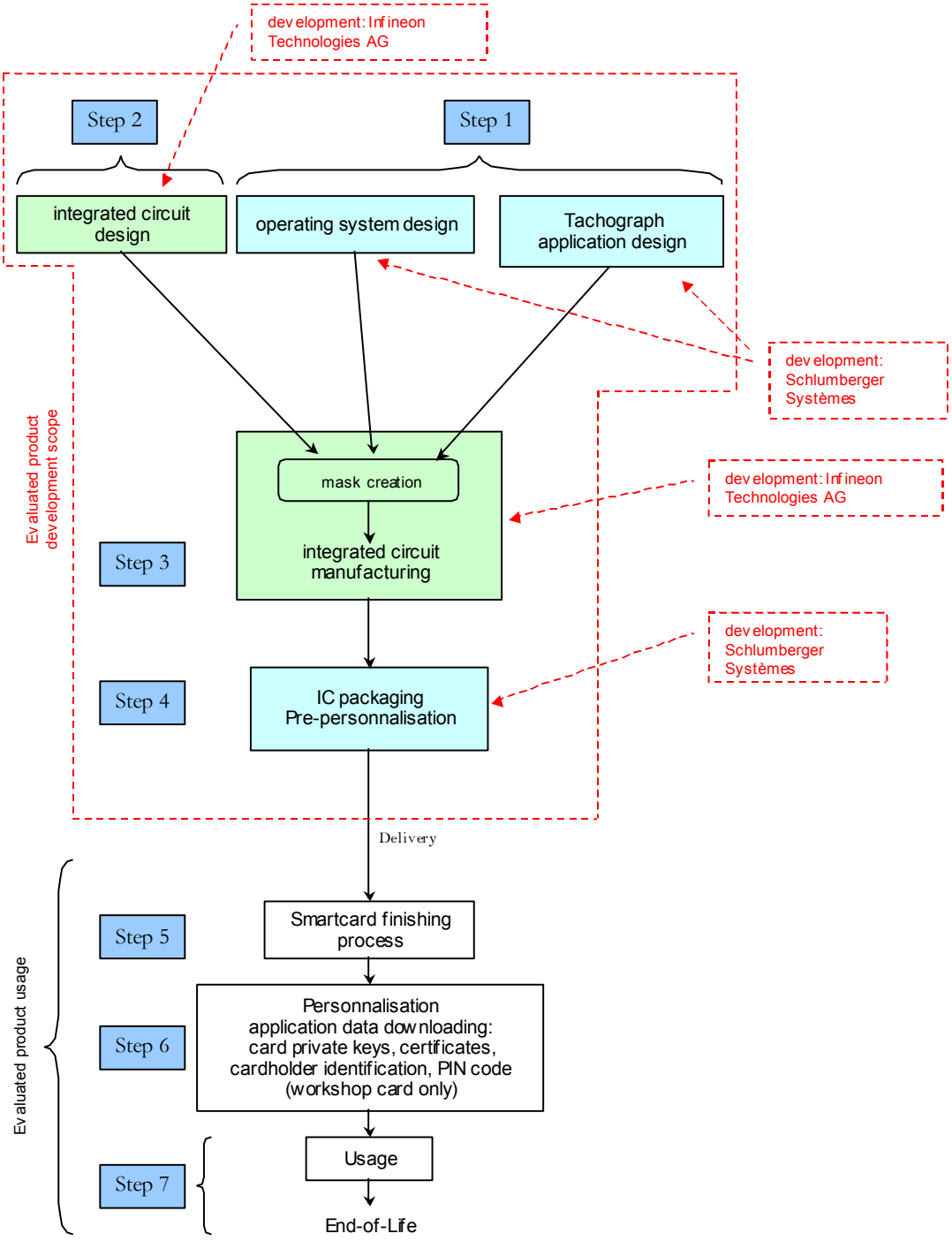

Figure 2 – Evaluated product lifecycle within the smartcard life-cycle

1.4.3. Evaluated product scope

The evaluated product is the masked chip, made up of the SLE66CX322P/b14 chip developed by Infineon Technologies AG including RMS library release 1.3 and ACE library release 1.0, the operating system GEOS reference PLATFORM_T_SC_04_02;9 and the Tachograph application reference SC_V0.9.0 developed by Schlumberger Systèmes. The evaluated product is the product in end of pre-personnalisation step (step 4, Figure 2).

1.5. Usage and administration

1.5.1. Usage

The user of the product is the cardholder. The guide for cardholders is guide [USR].

1.5.2. Administration

The administrator of the product is the personalizer (step 6). The guide for the personalizer is the guide [ADM].
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 (security objective for the environment O.TEST_OPERATE, § 3.11.4).

2. The evaluation

2.1. Evaluation facility

SERMA Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Phone : +33 (0)5 57 26 08 64

E-mail : m.dus@serma.com

The evaluation took place from **November 2002** to **July 2003**.

2.2. Evaluation sponsor

Schlumberger Systèmes

36-38 rue de la Princesse
BP45
78431 Louveciennes Cedex
France

2.3. Evaluation referential

The evaluation has been conducted in accordance with Common Criteria [CC], with the evaluation methodology defined within the CEM manual [CEM], and with the whole finalised interpretations listed within evaluation reports.

2.4. Security target evaluation

The security target [ST] defines the evaluated product and its operational environment.
All security functional requirements and security assurance requirements from the security target are taken from part 2 and part 3 of Common Criteria [CC].
The security target meets ASE class requirements.

2.5. Product evaluation

The evaluation consists in checking that the product and its documentation is compliant to security functional and assurance requirements defined in the security target [ST] of the product.
The product evaluation relies on the certificate of the chip «Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, a27 and b14» issued y BSI in august 2003 under the reference BSI-DSZ-CC-0223-2003 [322P-B14]. This certificate attests that SLE66CX322P chip reaches EAL5 assurance level augmented with ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 and that it is compliant with PP/BSI-0002 protection profil «Smartcard Integrated Circuit Protection Profile v2.0» [SSVG]. The validity of this certificate is recognized by the French scheme in accordance with the SOG-IS mutual recognition

arrangement [SOG-IS]. The chip being certified by the German scheme, work being done within ICitizen Tachograph evaluation was about the mask evaluation and its integration on the chip, in accordance with interpretations about composition of an integrated circuit and an embedded software [JIL-Comp].

2.5.1. Product development

ADV assurance class – development – defines requirements for the stepwise refinement of the product's security functions from its summary specification in the security target [ST] down to the actual implementation. Each of the resulting product's security function representations provide information to help the evaluator determine whether the functional requirements of the product have been met.
Documents associated to ADV class analysis shows that security functional requirements are correctly and completely refined into the different levels of the product representation (functional specifications (FSP), subsystems (HLD), modules (LLD) and implementation (IMP)), down to the implementation of its security functions.
Documents provided for ADV – development – class evaluation meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.2. Documentation

From the point of view of the evaluation, the administrator is the personalizer and users are cardholders. Four types of card are available: driver cards, workshop cards, company cards and control cards.
User guides [USR] and administrator guides [ADM] meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.3. Delivery and installation

Two deliveries are considered. Firstly, the source code delivery to Infineon: Schlumberger Systèmes sends to Infineon (step 1 to 3) source codes of the operating system and the tachograph application, in order to mask these applications on SLE66CX322P chips. Secondly, Schlumberger Systèmes sends to the smartcard product manufacturer the pre-personalized micro-modules (step 4 to 5). This delivery corresponds to the transition between evaluated product development and evaluated product usage. Schlumberger Systèmes offers two possible deliveries: either secure transportation to the smartcard product manufacturer or put micro-modules to the smartcard product manufacturer disposal, in order to the latter to securely transport micro-modules.
The delivery procedure [DEL] meets corresponding requirements: it permits to have a proof of the delivery-origin and to detect any modification of the product that could apply on the product.
The product installation corresponds to pre-personalisation step (step 4). Installation, generation and start-up procedures [IGS] permit to obtain a secure configuration of the application. Furthermore, recorded information in a log file on the pre-personalisation site permit to find out and to determine when and how each micro-module has been pre-personalized.
Documents provided for ADO – Delivery and operation – class evaluation meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.4. Development environment

The configuration system is used in accordance with the configuration management plan [ACM].
The configuration list [LGC] identifies elements mapped by the configuration management system. Configuration elements identified in this list are maintained by the configuration management system. Application generation procedures are effective to assure that the right configuration elements are used to generate the application.
The operating system and the tachograph application are developed at the following site of Schlumberger Systèmes:

36-38 rue de la Princesse
78431 Louveciennes
France

The IC is packaged and pre-personalized at the following site of Schlumberger Systèmes:

284, avenue de la Pomme de Pin
45060 Saint-Cyr-En-Val
France

Security measures described in procedures provide the sufficient level of protection to maintain the confidentiality and the integrity of the evaluated product and its documentation.
The evaluator checked that procedures are followed in a manner consistent with that described in the development and configuration management documentation (Appendix 1 and Appendix 2). A site visit has been performed at these two sites. The site visit report is under the reference [Audit].
Documents provided for ACM – configuration management – and ALC – Lifecycle support – class evaluation meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.5. Functional testing

The evaluator checked that all security functions and functional specification interfaces of the product are mapped to at least a functional test described in the test documentation. He checked also that all security functions, as described within the high-level design documentation [HLD] and within the low-level design documentation [LLD], are covered by the developer tests.
Tests have been performed on the version identified in paragraph 1.2, in following configurations:

- Pre-personalized masked chip;
- Smartcard containing the micro-module personalized (step 7) for each configuration types: driver, workshop, company and control cards.

2.5.6. Vulnerability assessment

Vulnerabilities identified by the developer have been checked through an analysis and through penetration testing. The evaluator concludes that vulnerabilities identified by the developer are correctly covered.
The evaluator performed an independent vulnerability analysis that results do not point out any additional vulnerability.
The product, within its operational environment, is resistant to an attacker possessing a **high** level attack potential.

3. Conclusions of the evaluation

3.1. Evaluation technical report

The Evaluation Technical Report [RTE] describes results from the evaluation of ICitizen Tachograph version 0.9.0.

3.2. Evaluation level

ICitizen Tachograph version 0.9.0 has been evaluated in compliance to Common Criteria [CC] and its methodology [CEM] at level **EAL4**[1] **augmented** with following assurance components, compliant to Common Criteria part 3:

Components	Descriptions
ADO_IGS.2	Generation log
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
ATE_DPT.2	Testing: low-level design
AVA_MSU.3	Analysis and testing for insecure states
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

For all these product evaluation level components, following verdicts have been issued:

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Pass
ASE_ENV.1	Security environment	Pass
ASE_INT.1	ST introduction	Pass
ASE_OBJ.1	Security objectives	Pass
ASE_PPC.1	PP claims	Pass
ASE_REQ.1	IT security requirements	Pass
ASE_SRE.1	Explicitly stated IT security requirements	Pass
ASE_TSS.1	Security Target, TOE summary specification	Pass
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	Pass
ACM_CAP.4	Generation support and acceptance procedures	Pass
ACM_SCP.2	Problem tracking CM coverage	Pass
Class ADO	**Delivery and operation**	

[1] In Appendix 5, a table gives a brief description of existing Evaluation Assurance Levels (EAL) defined in Common Criteria [CC].

ADO_DEL.2	Detection of modification	Pass
ADO_IGS.2	Installation, generation, and start-up procedures	Pass
Class ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	Pass
ADV_HLD.2	Security enforcing high-level design	Pass
ADV_IMP.2	Implementation of the TSF	Pass
ADV_LLD.1	Descriptive low-level design	Pass
ADV_RCR.1	Informal correspondence demonstration	Pass
ADV_SPM.1	Informal TOE security policy model	Pass
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Pass
AGD_USR.1	User guidance	Pass
Class ALC	**Life cycle support**	
ALC_DVS.2	Sufficiency of security measures	Pass
ALC_LCD.1	Developer defined life-cycle model	Pass
ALC_TAT.1	Well-defined development tools	Pass
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Pass
ATE_DPT.2	Testing: high-level design	Pass
ATE_FUN.1	Functional testing	Pass
ATE_IND.2	Independent testing - sample	Pass
Class AVA	**Vulnerability assessment**	
AVA_MSU.3	Validation of analysis	Pass
AVA_SOF.1	Strength of TOE security function evaluation	Pass
AVA_VLA.4	Highly resistant	Pass

Tableau 2 – Components and their corresponding verdicts

3.3. Functional requirements

The product meets the following[1] **security functional requirements** [ST]:

- Potential violation analysis (FAU_SAA.1)
- Selective proof of origin (FCO_NRO.1)
- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key distribution (FCS_CKM.2)
- Cryptographic key access (FCS_CKM.3)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)

[1] In 0, we can find a complete table explaining the evaluated product security functional requirements (in French).

- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Basic data authentication (FDP_DAU.1)
- Export of user data without security attributes (FDP_ETC.1)
- Export of user data with security attributes (FDP_ETC.2)
- Import of user data without security attributes (FDP_ITC.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Authentication failure handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- Unforgeable authentication (FIA_UAU.3)
- Single-use authentication mechanisms (FIA_UAU.4)
- Timing of identification (FIA_UID.1)
- User-subject binding (FIA_USB.1)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Management of TOE security functions data (FMT_MTD.1)
- Specification of management functions (FMT_SMF.1)
- Security roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Resistance to physical attack (FPT_PHP.3)
- TOE security functions domain separation (FPT_SEP.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)
- TOE security functions testing (FPT_TST.1)
- Inter-TSF trusted channel (FTP_ITC.1)

3.4. Strength of functions

Only authentication function (PIN code) for workshop card have been subject to an estimation of their strength.
Strength of security functions meets the high level (**SOF-high**).

3.5. Cryptographic mechanisms analysis

On sponsor's request, the DCSSI cryptographic laboratory has evaluated cryptographic mechanisms of ICitizen Tachograph version 0.9.0 masked chip. Results of this analysis are summarized within Appendix 3.

3.6. Regulation EC 1360/2002 Compliance

In accordance with interpretation guide of annex 1B of the regulation EC 1360/2002 [JIL-Tacho], the evaluator checked the security target's [ST] compliance with appendix 10 of annex 1B of regulation EC 1360/2002 [EC 1360/2002].
The evaluation assurance level rechead by the product is **EAL4 augmented** with ADO_IGS.2, ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_MSU.3 et AVA_VLA.4 (Tableau 1). This evaluation level **corresponds** to level **E3hAP** defined within the guide [JIL-Tacho], augmented with ACM_AUT.1, ADV_SPM.1, ALC_DVS.2, ALC_LCD.1, AVA_MSU.3.
The evaluator checked that security target [ST] of the product meets the interpretations into Annex A and B of [JIL-Tacho] guide, concerning the evaluation assurance level and the security functional requirements. Therefore, in accordance to this guide, the security evaluation level of ICitizen Tachograph version 0.9.0 can be considered as reaching **ITSEC E3 high** level, evaluation level required by annex 1B of regulation EC 1360/2002 [EC/A1B].

3.7. Protection profile claim

The certificate of the chip SLE66CX322P/b14 [322P-B14] attests that its security target is compliant with BSI-PP-0002 [SSVG] protection profile.

3.8. European recognition (SOG-IS)

This certificate has been issued in accordance to SOG-IS recognition agreement. Requirements of this agreement require the delivery of a security target.

3.9. International recognition (CC RA)

This certificate has been issued in accordance to CC RA recognition arrangement. Requirements of this arrangement require the delivery of a security target.
Following augmentations are not mutually recognized in accordance with the provisions of the CC RA [CC RA]: ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4 (Tableau 1).

3.10. Usage restrictions

Operational environment have to respect security objectives for the environment (§ 3.11), as well as recommendations within user guidance [USR] and administrator guidance [ADM].
Results from the evaluation are valid only for the configuration specified in this certification report.

3.11. Security objectives for the environment

Security objectives for the environment are the followings [ST]:

3.11.1. Security objectives on step 1

- The smartcard embedded software shall be designed in a secure manner, by using exclusively software development tools (compilers, assemblers, linkers, simulators etc...) and software-hardware integration testing tools (emulators) that will grant the integrity of program and data (O.DEV_TOOLS);

- The Embedded Software developer shall use established procedures to control storage and usage of the classified development tools and documentation, suitable to maintain the integrity and the confidentiality of the assets of the masked chip. It must be ensured that tools are only delivered and accessible to the parties authorized personnel. It must be ensured that confidential information on defined assets are only delivered to the parties authorized personnel on the need to know basis (O.DEV_DIS_ES);
- The smartcard embedded software must be delivered from the smartcard embedded software developer (step 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable (O.SOFT_DLV);
- Initialisation data shall be accessible only by authorized personnel (physical, personnel, organizational, technical procedures) (O.INIT_ACS);
- Samples used to run tests shall be accessible only by authorized personnel (O.SAMPLE_ACS).

3.11.2. Security objectives on product delivery (step 4 to 7)

- Procedures 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 shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non conformance to this process (O.DLV_AUDIT);
- Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and to act to be fully in accordance with the above expectations (O.DLV_RESP).

3.11.3. Security objectives on delivery from step 1 to 4, 5 and 6

- The Application Data must be delivered from the Smart Card embedded software developer (step 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data (O.DLV_DATA).

3.11.4. Security objectives on step 4 to 6

- Appropriate functionality testing of the masked chip shall be used in phases 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5, 6 to maintain confidentiality and integrity of the masked chip and of its manufacturing and test data (O.TEST_OPERATE).

3.11.5. Security objectives on step 7

- Secure communication protocols and procedures shall be used between smartcard and terminal (O.USE_DIAG).

3.11.6. Additional security objectives

- 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 key include the European private key, the Countries' Private keys and the VU 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).

3.12. Result summary

The whole evaluation work performed by the evaluation centre is accepted by the certification body who testify that ICitizen Tachograph version 0.9.0 identified in paragraph 1.2 and described in paragraph 1.4 of this report is compliant with requirements specified into the security target [ST]. The whole evaluation work and theirs results are described within the evaluation technical report [RTE].

Furthermore, the certification body also testify that ICitizen Tachograph version 0.9.0 meets all security requirements defined within appendix 10 of annex 1B of regulation EC1360/2002 [EC/A1B] concerning generic security objectives of tachograph card. The security certificate is delivered in accordance with the provisions of this appendix and the security assurance level of the product reaches the evaluation level ITSEC E3 fort required by annex 1B [EC/A1B].

Appendix 1. Louveciennes site visit report concerning the development environment

The development site of **Schlumberger Systèmes located 36-38, rue de la princesse, BP 45, 78431 Louveciennes Cedex, France**, has been visited, during the evaluation of the product ICitizen Tachograph version 0.9.0, in order to check the compliance to evaluation criteria and provided documents for the following items:

- Configuration management: **ACM** (ACM_AUT.1, ACM_CAP.4, ACM_SCP.2);
- Delivery: **ADO** (ADO_DEL.2);
- Lifecyle support: **ALC** (ALC_DVS.2).

Development of the Operating System GEOS and Tachograph application occurs in Louveciennes office. Once the development is complete, software source code is securely delivered to Infineon Technologies AG.
The site visit performed by the evaluation center with a representative of the DCSSI, has allowed concluding that this site meets the criteria.

Appendix 2. Orléans site visit report concerning the development environment

The development site of **Schlumberger Systèmes located 284, avenue de la Pomme de Pin 45060 Saint-Cyr-En-Val, France**, has been visited, during the evaluation of the product ICitizen Tachograph version 0.9.0, in order to check the compliance to evaluation criteria and provided documents for the following items:

- Configuration management: **ACM** (ACM_AUT.1, ACM_CAP.4, ACM_SCP.2);
- Delivery: **ADO** (ADO_DEL.2);
- Lifecyle support: **ALC** (ALC_DVS.2).

The masked chip is delivery by Infineon to Schlumberger Systèmes at its site in Orléans. Within this site, the chip is packaged into a micro-module and pre-personalized. Then it is delivered to a final customer.
The site visit performed by the evaluation center with a representative of the DCSSI, has allowed concluding that this site meets the criteria.

Appendix 3. Cryptographic mechanisms analysis

Common Criteria [CC] do not require an assessment of strength of cryptographic mechanisms implemented within security functions specified into the security target of the product in evaluation. However, considering they represent an important part of the product security level, the certification body proposes the analysis of this type of mechanism, which results are below. These results do not alter the Common Criteria certificate of product's compliance to its security target.

- Mechanisms into **personalization** phase:
  - **Mutual authentication**

    This mechanism's level is considered high.
  - **Data integrity protection**

    In *secure channel MAC* mode, only data integrity is ensured. The level of the integrity mechanism is considered low. However, being into a secure environment and using security procedures during personalization phase allow countering this weakness. These recommendations are already required within protection profile 99/11 [PP/9911] and repeated within the product security target [ST], through the security objective for the environment O.TEST_OPERATE (§ 3.11.4)
  - **Data confidentiality and integrity protection**

    In *secure channel ENC* mode, data confidentiality and integrity is ensured. The level of this mechanism is considered high, provided session keys are not used more than 2^{20} times, and detection of an incorrect MAC stops the secure channel.
- Mechanisms into **usage** phase:
  - **Mutual authentication**

    This mechanism is compliant to specifications described within annex 1B [EC/A1B] of the regulation EC 1360/2002.
  - **Data integrity protection**

    This mechanism is compliant to specifications described within annex 1B.
  - **Data confidentiality and integrity protection**

    This mechanism is compliant to specifications described within annex 1B.
- **Random number reprocessing** mechanism :

  The level of this mechanism is considered low. It does not provide extra security, however, it does not either alter the random number generation quality of SLE66CX322P chip.

Appendix 4. Functional requirements for the evaluated product

Warning: descriptions of following functional components are given as a rough guide. Only a careful reading of the security target [ST] can bring a precise description of security functional requirements, which the product meets.

Class FAU	**Security audit**
Security audit analysis	
FAU_SAA.1	*Potential violation analysis* Le produit doit implémenter un seuil de détection élémentaire, défini selon une règle fixée (spécifiée dans la cible de sécurité [ST]).
Class FCO	**Communication**
Non-repudiation of origin	
FCO_NRO.1	*Selective proof of origin* Le produit doit, suite à la requête du destinataire et/ou de l'émetteur, donner la preuve de l'origine des informations (spécifiées dans la cible de sécurité [ST]).
Class FCS	**Cryptographic support**
Cryptographic key management	
FCS_CKM.1	*Cryptographic key generation* Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiés qui peuvent être basés sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.2	*Cryptographic key distribution* Le produit doit distribuer des clés cryptographiques conformément à une méthode de distribution spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.3	*Cryptographic key access* Les accès aux clés cryptographiques doivent être effectués conformément à une méthode d'accès spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.4	*Cryptographic key destruction* Le produit doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée

	(spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Data authentication	
FDP_DAU.1	*Basic data authentication* Le produit doit être capable de garantir l'authenticité des informations contenues dans des objets spécifiés dans la cible de sécurité [ST] (e.g. des documents).
Export to outside TSF control	
FDP_ETC.1	*Export of user data without security attributes* Le produit doit appliquer les règles de sécurité appropriées lors de l'exportation de données de l'utilisateur à l'extérieur. Les données de l'utilisateur exportées par cette fonction sont exportées sans les attributs de sécurité qui leur sont associés.
FDP_ETC.2	*Export of user data with security attributes* Le produit doit appliquer les règles de sécurité appropriées en utilisant une fonction qui associe précisément et sans ambiguïté les attributs de sécurité avec les données de l'utilisateur qui sont exportées.
Import from outside TSF control	
FDP_ITC.1	*Import of user data without security attributes* Les attributs de sécurité doivent représenter correctement les données de l'utilisateur et doivent être fournis séparément de l'objet.
Residual information protection	
FDP_RIP.1	*Subset residual information protection* Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets lors de l'allocation ou de la désallocation de la ressource.
Stored data integrity	
FDP_SDI.2	*Stored data integrity monitoring and action* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées et entreprendre des actions (spécifiées dans la cible de sécurité [ST]) suite à une détection d'erreur.
Class FIA	**Identification and authentication**
Authentication failures	
FIA_AFL.1	*Authentication failure handling* Le produit doit être capable d'arrêter le processus d'établissement d'une

	session après un nombre spécifié de tentatives d'authentification infructueuses d'un utilisateur. Il doit aussi, après la clôture du processus d'établissement d'une session, être capable de désactiver le compte de l'utilisateur ou le point d'entrée (e.g. station de travail) à partir duquel les tentatives ont été faites jusqu'à ce qu'une condition définie par un administrateur se réalise.
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
User authentication	
FIA_UAU.1	*Timing of authentication* Le produit autorise un utilisateur à exécuter certaines actions, spécifiées dans la cible de sécurité [ST], avant que son identité ne soit authentifiée.
FIA_UAU.3	*Unforgeable authentication* Le mécanisme d'authentification doit être capable de détecter et d'empêcher l'utilisation de données d'authentification qui ont été contrefaites ou copiées.
FIA_UAU.4	*Single-use authentication mechanisms* Le mécanisme d'authentification doit fonctionner avec des données d'authentification à usage unique.
User identification	
FIA_UID.1	*Timing of identification* Le produit autorise les utilisateurs à exécuter certaines actions, identifiées dans la cible de sécurité [ST], avant d'être identifiés.
User-subject binding	
FIA_USB.1	*User-subject binding* La relation entre les attributs de sécurité de l'utilisateur et un sujet agissant pour le compte de cet utilisateur doit être maintenue.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.2	*Secure security attributes* Le produit doit garantir que les valeurs assignées aux attributs de sécurité sont valides par rapport à l'état sûr.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Management of TSF data	
FMT_MTD.1	*Management of TSF data* Les utilisateurs autorisés peuvent gérer les données des fonctions de sécurité du produit.
Specification of Management Functions	

FMT_SMF.1	*Specification of Management Functions* Le produit doit fournir les fonctions de gestion de la sécurité spécifiées dans la cible de sécurité [ST].
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiées dans la cible de sécurité [ST]).
Class FPR	**Privacy**
Unobservability	
FPR_UNO.1	*Unobservability* Le produit n'autorise pas certains utilisateurs (spécifiées dans la cible de sécurité [ST]) à déterminer si certaines opérations (spécifiées dans la cible de sécurité [ST]) sont en cours d'exécution.
Class FPT	**Protection of the TSF**
Fail secure	
FPT_FLS.1	*Failure with preservation of secure state* Le produit doit préserver un état sûr dans le cas de défaillances identifiées.
TSF physical protection	
FPT_PHP.3	*Resistance to physical attack* Le produit doit empêcher ou résister à certaines intrusion physique (spécifiées dans la cible de sécurité [ST]) sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
Domain separation	
FPT_SEP.1	*TSF domain separation* Le produit doit offrir un domaine protégé et distinct pour les fonctions de sécurité du produit et procurer une séparation entre sujets.
Inter-TSF TSF data consistency	
FPT_TDC.1	*Inter-TSF basic TSF data consistency* Le produit doit offrir la capacité de garantir la cohérence des attributs lors des échanges avec un autre produit de confiance.
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.
Class FTP	**Trusted path/channels**
Inter-TSF trusted channel	
FTP_ITC.1	*Inter-TSF trusted channel* Le produit doit offrir un canal de communication de confiance entre lui-même et un autre produit TI de confiance.

Appendix 5. Predefined Evaluation Assurance Levels IS 15408 or CC

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Appendix 6. References about the evaluted product

[322P-B14]	Rapport de certification Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, a27 and b14 Référence BSI-DSZ-CC-0223-2003 Août 2003 Bundesamt für Sicherheit in der Informationstechnik
[ACM]	Configuration Management Plan Référence MRD11SCM023011 Version1.1 Schlumberger Systèmes
[ADM]	Administrator Manual Référence MRD11GUI023007 Version 1.4 Schlumberger Systèmes
[Audit]	Classes ALC ACM ADO evaluation report Version 2.0 Juillet 2003 Serma Technologies
[DEL]	Delivery and Operation Reference MRD11DEL023012 Version 1.2 Schlumberger Systèmes
[EC 1360/2002]	Règlement numéro 1360/2002 de la Commision des Communautés Européennes du 13 juin 2002 et publié le 5 août 2002, concernant l'appareil de contrôle dans le domaine des transports par route
[EC/A1B]	Annexe 1B du règlement 1360/2002 Exigences applicables à la construction, aux essais, à l'installation et à l'inspection
[HLD]	High Level Design Référence MRD11HLD023014 Version 1.1 Schlumberger Systèmes
[IGS]	Les guides pour l'installation, la génération et l'initialisation sont : ▪ Pre-personnalization procedure Référence MRD11IGS023013 Version 1.3 Schlumberger Systèmes ▪ Initialization procedure for Cyberflex Palmera

	Référence MITPRO023022 Version 1.0 Schlumberger Systèmes
[JIL-Comp]	Les guides pour la composition sont : ▪ ETR-lite for composition version 1.0 mars 2002 Joint Interpretation Library ▪ ETR-lite for composition : Annex A, Composite smartcard evaluation : Recommended best practice version 1.2 mars 2002 Joint Interpretation Library
[JIL-Tacho]	Security Evaluation and Certification of Digital Tachographs Version 1.12 Joint Interpretation Library
[LGC]	Configuration List Référence MRD11LIS0330071 Version 1.0 Schlumberger Systèmes
[LLD]	Low Level Design Référence MRD11LLD023015 Version 1.1 Schlumberger Systèmes
[PP/9806]	Smart Card Integrated Circuit Protection Profile Version 2.0 Septembre 1998
[PP/9911]	Smart Card Integrated Circuit with Embedded software Protection Profile Version 2.0 Juin 1999
[RTE]	Evaluation Technical Report Version Juillet 2003 Serma Technologies
[SSVG]	Profil de protection «Smartcard Integrated Circuit Protection Profile v2.0» Référence BSI-PP-0002 Bundesamt für Sicherheit in der Informationstechnik
[ST]	Security Target Référence MRD11STT023001

	Version 1.5 Schlumberger Systèmes
[USR]	User Manual Référence MRD11GUI023008 Version 1.3 Schlumberger Systèmes

Appendix 7. References about certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
Décret 2001-272 du 30 mars 2001- Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.	
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, august 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[IS 15408]	Norme ISO/IEC 15408 :1999, comportant 3 documents : ▪ IS 15408–1: (Part 1) Introduction and general model ; ▪ IS 15408–2: (Part 2) Security functional requirements ; ▪ IS 15408–3: (Part 3) Security assurance requirements ;
[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.
[MQ]	Manuel qualité du centre de certification Référence SGDN/DCSSI/SDR/MQ.01 Version 1.0 SGDN/DCSSI
[CER/P/01]	Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information Référence CER/P/01.1 Version 1 SGDN/DCSSI

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
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr