PREMIER MINISTRE

Secretariat General for National Defence

French Network and Information Security Agency

Certification Report ANSSI-2009/21

TL ICAO LDS Smart Card

Paris, 17 july 2009

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 ANSSI (French Network and Information Security Agency), 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
Agence nationale 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.gouv.fr

Certification report reference

ANSSI-2009/21

Product name

TL ICAO LDS smart card: electronic passport applet loaded on JCLX80jTOP20ID platform masked on SLE66CLX800PE component

Product reference

Version 2.0

Protection profile conformity

[PP EAC]

Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 4 augmented

ALC_DVS.2, AVA_VAN.5

Developer(s)

Trusted Logic	Infineon Technologies AG
5 rue du Bailliage, 78000 VERSAILLES, FRANCE	**AIM CC SM PS - Am Campeon 1-12 - 85579 Neubiberg, GERMANY**

Sponsor

Trusted Logic

5 rue du Bailliage, 78000 VERSAILLES, 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 French Network and Information Security Agency 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 sponsors 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 TL ICAO LDS smart card**,** version 2.0, developed by Trusted Logic. It is composed of an electronic passport applet loaded on the JCLX80jTOP20ID Trusted Logic Platform, this later one being masked on the component SLE66CLX800PE developed by Infineon technologies AG.

The Target Of Evaluation (TOE) is the result of a double composition:

- The first composition is between the JCLX80jTOP20ID platform (Operating System and Java Card Open Platform) and the component SLE66CLX800PE from Infineon Technologies, that corresponds to the smart card "JCLX80jTOP20ID smart card: Java Trusted Open Platform on SLE66CLX800PE microcontroller" certified under [DCSSI-2008_43] reference (named "host" in the rest of the document);
- The second composition is between the electronic passport applet and the preceding product mentioned above, that corresponds to the certified product here.

This product implements the features of an electronic travel document following the ICAO specifications (cf. [ICAO]) and the protection profile Extended Access Control (cf. [PP EAC]).

1.2. Evaluated product description

The Security Target [ST] defines the evaluated product, the security features under evaluation and its running environment.

This Security target is compliant with the protection profile [PP EAC]. It is a demonstrable compliance: the argumentation is given in [ST] section §2.1 PP Claims.

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 the following elements:

Configuration Items		Origin
TOE name	TL ICAO LDS	Trusted Logic
TOE version	V2.0	
Platform name	jTop ID Platform[a]	
ROM reference (CM Label)	IFXv#27	
Patch reference (CM Label)	V1.6	
IC name	SLE66CLX800PE/360PE	Infineon Technologies AG
IC complete reference	SLE66CLX800PE-m1581-e13/a14 & SLE66CLX360PE-m1587-e13/a14	

a. The platform is also called JCLX80jTOP20ID (see [ETR_PF])

The Platform part of the TOE is identified through data returned by the power up (ATR for *Answer To Reset*):

- 3B FE 18 00 00 80 31 FE 45 80 31 80 66 40 90 A4 56 1B 16 83 XX 90 00 in which, historical bytes identify :
  - The component manufacturer: 40 90 ;
  - The type of the component: A4 ;
  - The type of the mask: 56;
  - The mask version: 1B (jTOP v27) ;
  - The mask revision: 16 (1.6 is the current patch version number).

The last byte 'XX' preceding the status word is a non-fixed state word. It depends of the current card life cycle state (from GlobalPlatform implementation may vary between OP_READY and TERMINATED).

The applet part of the TOE is identified thanks to the *tag* 53 sent when the LDS applet is selected:

- 6F 15 84 07 A0 00 00 02 47 10 01 A5 0A **53 08 01 07 01 01 02 00 82 95**

In the field of the *tag* 53 (composed of 8 bytes: **01 07 01 01 02 00 82 95**), we have:

- LDS specification version: 1.7;
- PKI specification version: 1.1;
- Applet version: 2.0;
- Applet generation date: October 22nd 2008.

This information (ATR and *tag* 53) allows the traceability of all the elements that compose the TOE (i.e. component, mask, patch and applet). They allow identifying correctly and in a unique way the TOE. This information has been verified on the TOE samples used during the evaluation.

1.2.2. Security services

The product provides mainly the following security services:

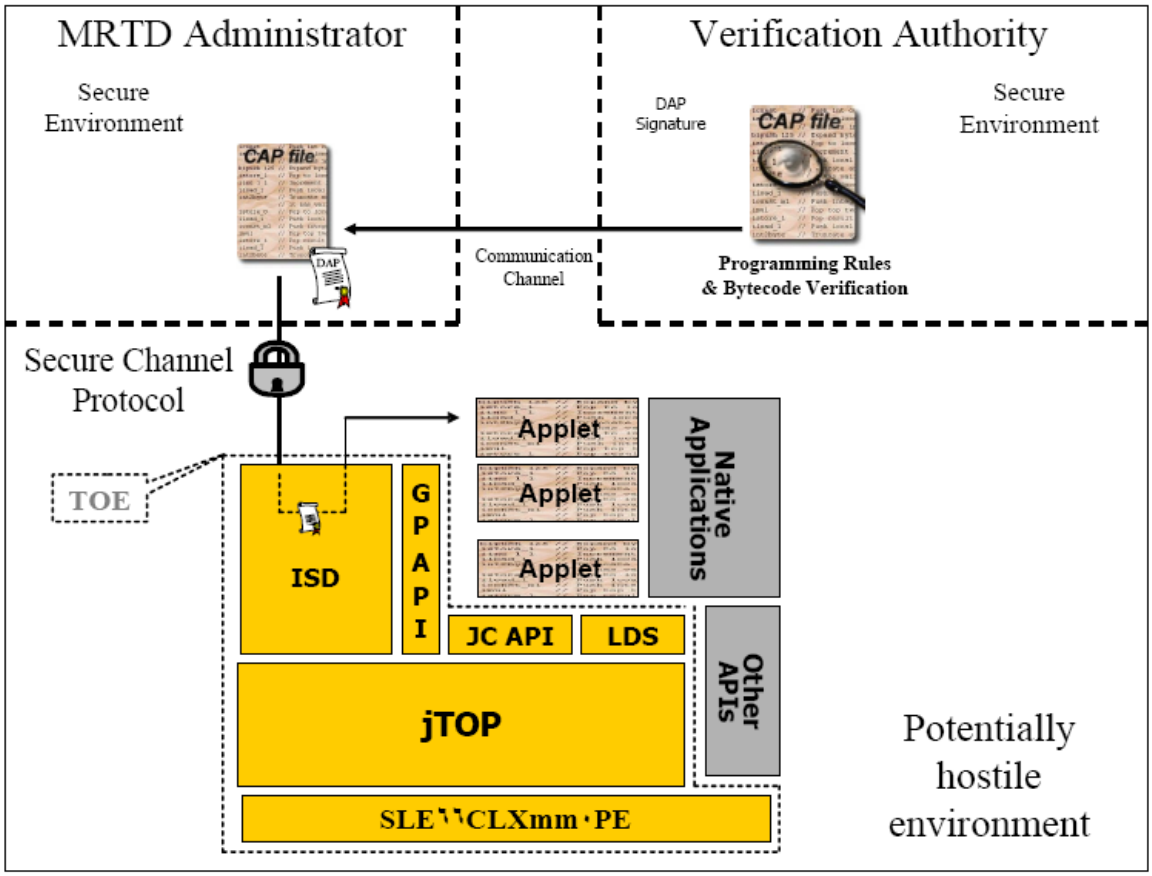
- The ones provided by the platform (see [DCSSI-2008_43]) :
- The one provided by the applet:
  - Secure channel with a personalization terminal ;
  - Secure Channel with an inspection system ;
  - Authentication protocol based on *Basic Access Control* (BAC) mechanism;
  - Chip Authentication Protocol ;
  - Active Authentication Protocol ;
  - Terminal Authentication Protocol ;
  - Personalization Authentication Protocol;
  - Files Access Control ;
  - MRTD Anonymity
  - ByteCode Integrity.

1.2.3. Architecture

The product consists of

- An electronic passport applet loaded in EEPROM ;
- A platform patch (v1.6), that is loaded in EEPROM ;
- A platform masked in ROM ;
- A chip.

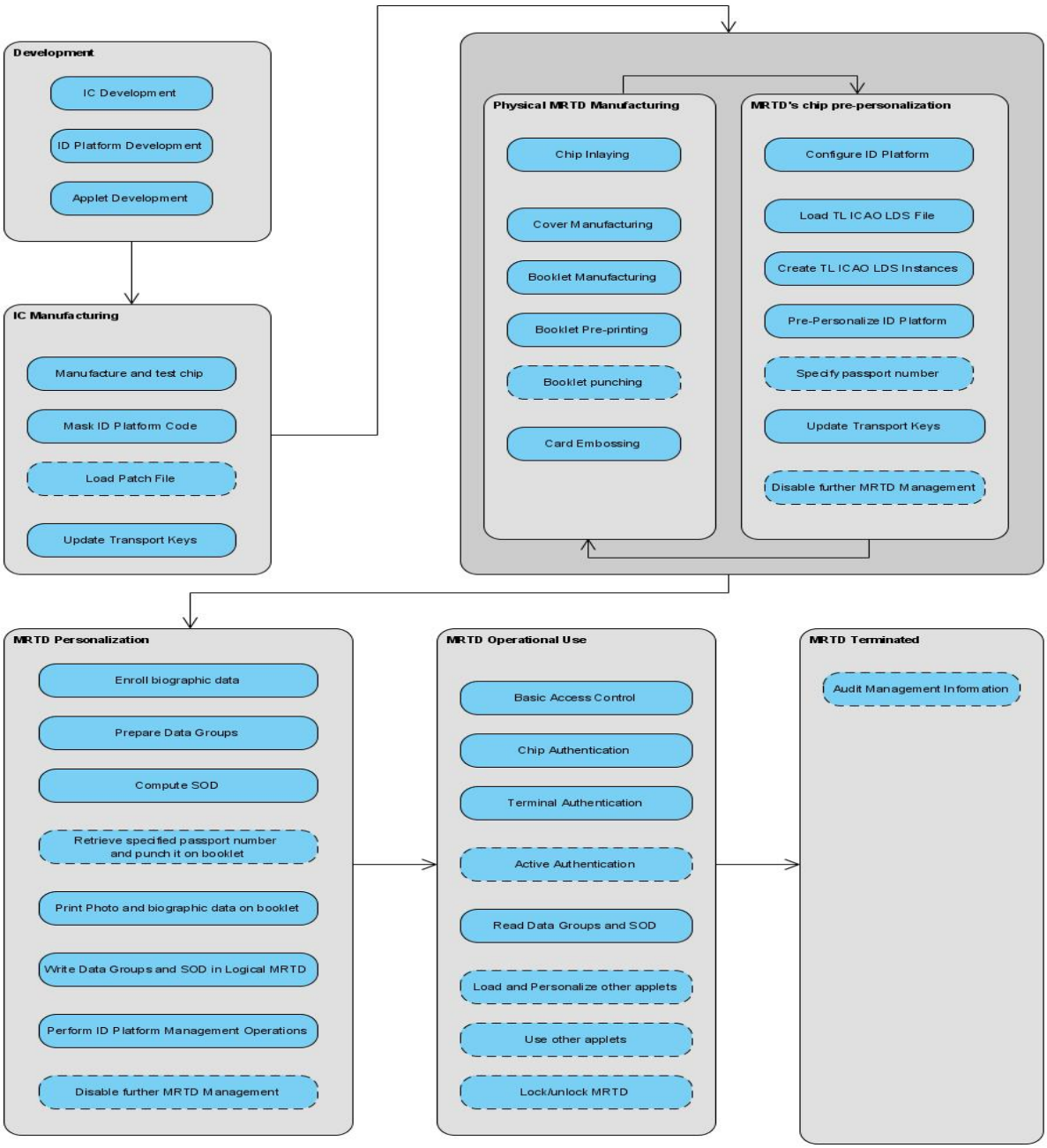
This architecture is illustrated as follows:



1.2.4. Life cycle

The product's life cycle is described in [ST] chapter §3.3.

The Application Note n°9 published by the DCSSI (see [DCSSI-NA-9]), and particularly the chapter related to life cycle, has been used. Therefore, the delivery of the TOE is fixed at the end of the IC Manufacturing instead of the end of the MRTD Manufacturing (delivery described in [PP EAC]). All the steps between these two points (see Physical MRTD Manufacturing and MRTD's pre-personalization in the next figure) are covered by the guides (see [GUIDE]).



NB: the blocks in dotted line represent optional actions.

The applet and the platform are developed on the following site:

Trusted Logic SA

5 rue du Bailliage
78000 VERSAILLES
FRANCE

The chip is developed on the following site:

INFINEON TECHNOLOGIES AG

AIM CC SM PS
Am Campeon 1-12
85579 Neubiberg
GERMANY

Users and administrators of the host ([DCSSI-2008_43]) are also users and administrators of the final product described in this document.

In other respects, for the evaluation, the evaluator has considered:

- National institutions that deliver the passport as product administrator ;
- Passport owner, customs officers and inspection system (during the use phase of the product) as product user.

1.2.5. Evaluated configuration

The evaluation covers both BAC and EAC mechanisms, which can be both performed based on RSA or ECC algorithm and on the Active Authentication protocol.

The Chip Authentication protocol can only be performed with the ECC algorithm. When activated, Active Authentication protocol can only be used with RSA CRT algorithm.

Moreover, since the product is composed of an open Java Card Platform, other applications can be loaded on the product. All configurations are in the scope of the evaluation.

The certificate covers the following configuration of the product:

- personalized state for the platform and the applet;
- GP INITIALIZED state for the card;
- SELECTABLE state for the applet.

Finally, for an electronic passport specific use case, the personalization agent has the capability to deactivate the card management features (in the Global Platform meaning) in order to let the platform behaves in a native mode (i.e. the Issuer Security Domain cannot be selected anymore).

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1** [CC], and with the Common Evaluation Methodology described in the CEM manual [CEM].

For the assurance components above EAL4 level, the in-house methods of the evaluation facility and validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] 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 by the integration of the applet in the host product ([DCSSI-2008_43]).

Thus, this evaluation uses the results of the evaluation, done by the same evaluator, of the host at EAL5 level augmented with ALC_DVS.2 and AVA_VLA.4.

The evaluation technical report [ETR], delivered to DCSSI on 31 March 2009, provides the details on the work performed by the evaluation facility and assesses that all evaluation tasks are marked as "**pass**".

2.3. Cryptographic mechanisms robustness analysis

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

2.4. Random number generator analysis

The random number generator is the one of the host (see [DCSSI-2008_43]).

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for 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 TL ICAO LDS: electronic passport applet loaded on the JCLX80jTOP20ID platform masked on the SLE66CLX800PE component, version 2.0, 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 security objectives for the operational environmental specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES]. In particular, he shall ensure that the certification authority verifies that any applet loaded on the platform, jointly with the electronic passport applet, respect anonymity required by the [PP EAC].

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is released 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, Spain, Sweden 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, Netherlands, New-Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedure
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Problem tracking CM coverage
	ADO_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well defined development tools
ASE Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**2**	Testing: security enforcing modules
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independant testing, sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	**2**	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - TL ICAO LDS EAC Security Target reference CP-2008-RT-432, version 1.3 Trusted logic For the needs of publication, the following security target has been provided and validated in the evaluation: - TL ICAO LDS EAC Security Target Lite reference PU-2009-RT-356, version 1.3 Trusted logic
[RTE]	Evaluation technical report : - Evaluation Technical Report - IRIS project reference IRIS_ETR_v1.0, version 1.0 Serma Technologies
[CONF]	Configuration list: - TF4C Software Configuration Management Plan reference CP-2007-RT-017, version 1.3 Trusted logic - TL ICAO LDS Software Configuration Management Plan reference CP-2008-RT-679, version 1.1 Trusted logic - Configuration List (IRIS files) reference IRIS_DELIVERY_SERMA_ALCCMS_200930330 Trusted logic
[GUIDES]	Preparation guide: - TL ICAO LDS Preparation Guide reference CP-2008-RT-727, version 1.3 Trusted logic User guidance: - TL ICAO LDS Operation Guide reference CP-2008-RT-740, version 1.1 Trusted logic
[PP BAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.0, 18 August 2005. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0017
[PP EAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control, version 1.2, 19 November 2007. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0026

[ICAO]	ICAO Doc 9303, Sixth Edition, 2007
[DCSSI-2008_43]	DCSSI certificate delivered on 19 Decembre 2008 for the product called "JCLX80jTOP20ID smart card: Java Trusted Open Platform on SLE66CLX800PE microcontroller"

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, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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.
[DCSSI-AN-9]	Application note E-passport : utilisation du profil de protection EAC référence NOTE/09.1, 2415/SGDN/DCSSI/SDR, 24 octobre 2008 SGDN/DCSSI