PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/43

JCLX80jTOP20ID smart card: Java Trusted Open Platform on SLE66CLX800PE microcontroller

Paris, 19th of December 2008

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.gouv.fr

Certification report reference

DCSSI-2008/43

Product name

JCLX80jTOP20ID smart card: Java Trusted Open Platform on SLE66CLX800PE microcontroller

Product reference

IFXv#27_0.1, software revision v1.4

Protection profile conformity

None

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 5 augmented

ALC_DVS.2, AVA_VLA.4

Developer(s)

Trusted Logic SA

5, rue du Bailliage 78000 Versailles – France

Sponsor

Trusted Logic SA

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 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 "JCLX80jTOP20ID smart card: Java Trusted Open Platform on SLE66CLX800PE microcontroller, IFXv#27_0.1, software revision v1.4" developed by Trusted Logic SA.

It is a dual-mode (contact/contactless) smart card comprising a platform compliant with Java Card 2.2.1 and VISA GlobalPlatform 2.1.1–Configuration 2 standards and which platform is embedded on Infineon Technologies' SLE66CLX800PE microcontroller. The patch v1.4 is loaded on EEPROM (Electrically Erasable Programmable Read Only Memory).

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.

This security target has been inspired from [JCSPP][1]. However, as Remote Method Invocation and the use of several logical channels are not included in the evaluation scope, the conformance to that PP is not claimed.

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:

Items	***Configuration***	***Origin***
Commercial name	JCLX80jTOP20ID	Trusted Logic
TOE reference (internal label)	jTOP v#27.01_1.4	Trusted Logic
TOE reference (IC label)	SLE66CLX800PE	Infineon
OS reference	IFXv#27_0.1, with software revision v1.4	Trusted Logic
IC identifier	SLE66CLX800PE-m1581-e13/a14	Infineon

1 **[JCSPP] Java Card System Standard 2.2.1 Configuration Protection Profile**
Version 1.0b, August 2003, registered and certified by the French Certification Body (DCSSI) under the reference PP/0305.

TOE samples have been provided for evaluation. The TOE can be uniquely identified through the ATR returned upon reset:

- 3B FE 18 00 00 80 31 FE 45 80 31 80 66 40 90 A4 56 1B 14 83 XX 90 00 where the historical bytes allow identifying:
  - the IC Manufacturer: 40 90;
  - the chip type: A4;
  - the mask type: 56;
  - the mask version: 1B (version 27 of jTOP);
  - the mask revision: 14 (1.4 is the current software revision version).

The last byte of the ATR preceding the status word is variable as it corresponds to the current life-cycle state of the card (in the GlobalPlatform coding, from OP_READY to TERMINATED).

This information allows tracing back to all items constituting the TOE (IC, hardmask and software patch). It allows properly and uniquely identifying the TOE. This could be checked on successive versions of the TOE.

1.2.2. Security services

The product provides mainly the following security services:

- Card Management
  - Issuer Security Domain
    - OPEN
    - Card Content Management
      - Card Content Loading
      - Card Content Installation
      - Card Content Deletion
    - Life Cycle Management
    - Administration Commands Control
  - Secure Channels
    - Host Authentication
    - Message Integrity and Authentication
    - Message Data Confidentiality
    - Secure Channel Termination
  - Secure Channel Key Management
    - Session Key Generation
    - ISD Key Loading and Replacement
  - Cardholder Verification Management
    - Global CVM
- Runtime Environment
  - Application Reference Monitors
    - Java Card Firewall
    - Defensive Java Card Virtual Machine
  - Security countermeasures
    - Card Muting
    - Card Locking
    - Card Termination
  - Life Cycle Management
    - Clearing sensitive information

        - Booting Tests
    - Integrity
        - Atomic Transactions
    - Service Availability
        - Resource Quotas
    - Cryptography
        - Signature Generation and Verification
        - Encryption and Decryption
        - Message Digest Generation
        - Random Number Generation
    - Key Management
        - Key Generation
        - Key Agreement
        - Key Encryption
        - Key Integrity
        - Key Destruction
    - Cardholder Authentication
        - Cardholder Verification
        - PIN Value Integrity
- Integrated Circuit TSFs
    - Operating State Checking
    - Phase Management
    - Protection Against Snooping
    - Hardware Data Encryption
    - True Random Number Generation
    - Hardware Self Test
    - Notification of Physical Attack
    - Memory Management Unit
    - Cryptographic Support

1.2.3. Architecture

The TOE is a composite product, a complete smart card comprising embedded software including:

- Operating System;
- Java Card System (JCVM, JCRE and JCAPI) 2.2.1;
- VISA GlobalPlatform 2.1.1, configuration 2 functionalities.

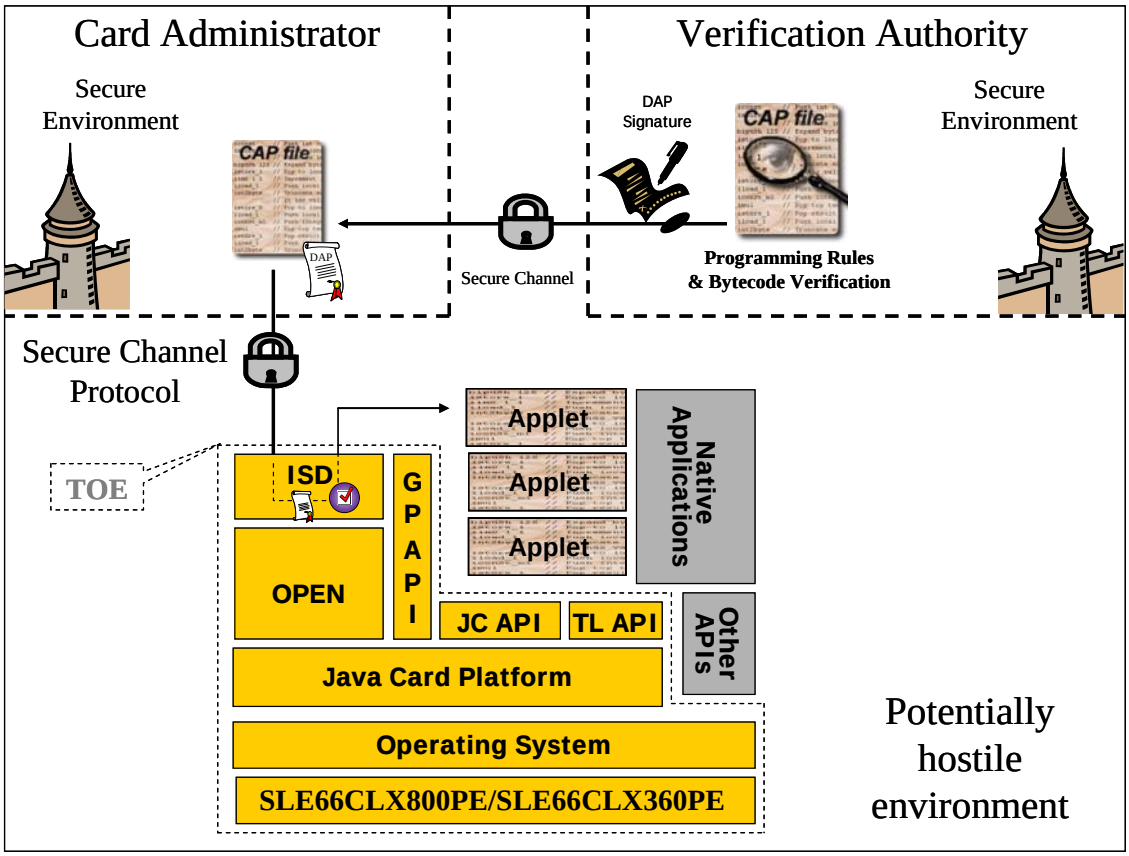
The TOE is embedded on the SLE66CLX800PE-m1581-e13/a14 microcontroller, which was certified on May the 27th 2008 under the reference BSI-DSZ-CC-0482[1].

[1] This certificate also includes the SLE66CLX360PE-m1587-e13/a14 microcontroller (which differs on its memory size).

This composition transforms the card into a secure open platform device for hosting Java Card applications.

The different operations involved in the management of those applications are performed in accordance with VISA GlobalPlatform 2.1.1 specifications, Configuration 2. Management operations include the downloading, installation, removal, and selection for execution of Java Card applications, life-cycle management of both the card and the application, and sharing of a global common PIN among all the applications installed on the card.

The following picture sums up the product architecture:



The following items are within the scope of the evaluation:

- Java Card 2.2.1 functionalities except logical channels and RMI ;
- VISA GlobalPlatform 2.1.1, configuration 2 functionalities ;
- additional proprietary Java Card APIs (util, security) ;
- The TOE life cycle perimeter includes only the design and development phases of the embedded software, the design and construction of the IC being covered by the IC evaluation.

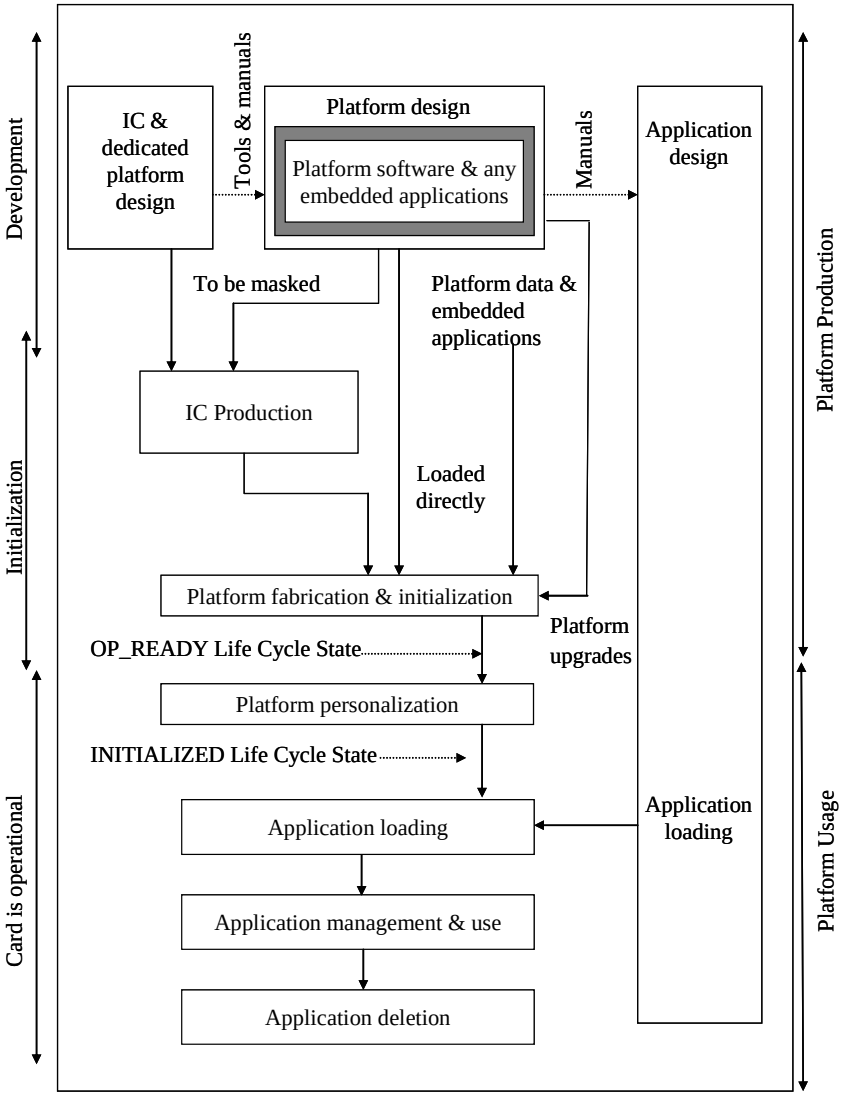
The following items are out of the scope of the evaluation:

- RMI ;
- logical channels ;
- additional proprietary Java Card APIs (iso7816, math, sim) ;
- any native application that may be embedded on the product;
- any Java card applet that may be loaded onto the platform.

1.2.4. Life cycle

As indicated before, the evaluated TOE life cycle states include only the design and development phases of the embedded software, the design and construction of the IC being covered by the IC evaluation. In the following picture, which represents the whole life-cycle of the product, this is represented by the “Platform design” bloc.

The initialization and personalization phases of the platform are out of the scope of the evaluation. Security functions of the TOE are evaluated in the usage phase (SECURED state in the GlobalPlatform life-cycle).



The product has been developed in the following site:

Trusted Logic SA

5 rue du Bailliage
78000 Versailles
France

In the evaluation context, the Card Administrator has been considered as “product administrator”. This role is defined in [ST] and reminded in [ADM] in the *Definitions* chapter.

In particular, the Card Administrator is the representative of the Card Issuer and has ultimate control of the smart card’s content and life cycle management. During the platform initialization phase, this role is embodied by the Card Enabler. During the platform usage phase, the Card Administrator can lock, unlock or terminate the smart card, download new applets on it, modify the static keys of the ISD or retrieve administration information from the smart card. The Card Administrator always acts on behalf of the Card Issuer.

Besides, still in the evaluation context, the Application Developers have been considered as “product users”, their responsabilities are detailed in [USR].

1.2.5. Evaluated configuration

The certificate applies to the only Java Card platform, as described above in 1.2.3 Architecture chapter, and when configured as required by the personalization guide (cf. [GUIDES]).

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's own evaluation methods consistent with [AIS 34], 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 from the integration of the software in the microcontroller already certified.

Therefore, the results of the evaluation of the microcontroller at EAL4 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [PP0002] protection profile, have been used.

The evaluation technical report [ETR], delivered to DCSSI on the 9th December 2008 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 been analysed by DCSSI. The results are stated in the cryptographic analysis report [ANA-CRY], they lead to the following conclusion: some of the mecanisms analysed do not reach the "standard" level as defined in DCSSI cryptographic referential [REF-CRY].

The analysis has identified some theoretical weaknesses existing in some examined mecanisms. However, the results have been taken into account in the independent evaluator vulnerability analysis but do not allowed to bring to light exploitable vulnerablities for the aimed VLA level.

2.4. Random number generator analysis

The evaluated product provides two random number generators (SMRNG and APRNG in short).

Both use the TRNG (True Randon Number Generator) provided by the IC. This TRNG has been evaluated "AIS 31 class P2 level High" when it is used with respect of specific recommendations described in [AN_RNG] in chapter 2.

The SMRNG is intended for the needs of the only operating system. The SMRNG outputs data are note available neither to the applications, nor to the end user of the card, and are not used for cryptographic applications. The DCSSI therefore stopped the SMRNG's analysis at this discovery.

The APRNG is intended for the purpose of applications. More precisely, the random data generated, a combination of TRNG and of a cryptographic post-treatment, are used for:

- generating keys;
- the padding in some protocol;
- producing random data for class RandomData (JavaCard API).

The APRNG has been analysed by DCSSI, it reaches its "standard" robutness level.

Indeed, this analysis did not show any flawed statistic bias for a direct use of the generated numbers. This does not imply that the generated numbers are really random but ensures that the generator is exempt of major conception flaws. As stated in the document [REF-CRY], DCSSI reminds that for a cryptographic use, the hardware-generated numbers shall be reprocessed by a cryptographic algorithm, even if the analysed random number generator did not show any weakness.

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 "JCLX80jTOP20ID smart card: Java Trusted Open Platform on SLE66CLX800PE microcontroller, IFXv#27_0.1, software revision v1.4" submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 5 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].

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:

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

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[1], 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 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, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

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 5+	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	**3**	Development tools 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	**1**	Installation, generation and start-up procedures
ADV Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**3**	Semiformal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**3**	Semiformal high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**	**1**	Modularity
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**2**	Semiformal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**3**	Formal 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**	**2**	Standardised life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
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	**1**	Covert channel analysis
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Analysis and testing of 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: • JCLX80jTOP20ID/JCLX36jTOP20ID - Security Target - version 1.8 (Developer's reference is CP-2006-RT-389) For the needs of publication, the following security target has been provided and validated in the evaluation: • JCLX80jTOP20ID/JCLX36jTOP20ID - Security Target Lite - version 1.4 (Developer's reference is CP-2007-RT-075)
[ETR]	Evaluation technical report : • Evaluation Technical Report - ALCAZAR project, ALCAZAR_ETR_v1.1 For the needs of composite evaluation with this microcontroller, a technical report for composition has been validated: • ETR-LITE FOR COMPOSITION (ETR-LITE), v1.0, 2008.03.11, (Developer's reference is 0482_ETRcomp_080311_v1) o SLE66CLX800PE / m1581-e13/a14 o SLE66CLX800PEM / m1580-e13/a14 o SLE66CLX800PES / m1582-e13/a14 o SLE66CX800PE / m1599-e13/a14 o SLE66CLX360PE / m1587-e13/a14 o SLE66CLX360PEM / m1588-e13/a14 o SLE66CLX360PES / m1589-e13/a14 o SLE66CLX180PE / m2080-a14 o SLE66CLX180PEM / m2081-a14 o SLE66CLX120PE / m2082-a14 o SLE66CLX120PEM / m2083-a14 o all optional with RSA2048 V1.5 and ECC V1.1 Certification ID: 8103819623 / BSI-DSZ-CC-0482
[ANA-CRY]	Cotation de mécanismes cryptographiques, 847/SGDN/DCSSI/SDS/Crypto, 18/04/2008
[CONF]	Software configuration management plan (reference [ACM] in [RTE]): • JCLX80jTOP20ID Software Configuration Management Plan - version 1.2 (Developer's reference is CP-2007-RT-017) Configuration list (reference [LIS] in [RTE]) : • Configuration list - version 0.5 (Developer's reference is CVS-Files-Versions.txt /CVS-Repositories-Architectures.txt / SVN-Files-Versions.txt)

[GUIDES]	Administration guidance: • JCLX80jTOP20ID Administration Guide, version 1.2 (Developer's reference is CP-2007-RT-165) User guidance: • JCLX80jTOP20ID Common Criteria User Guide, version 1.1, (Developer's reference is CP-2007-RT-166)
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0002-2001.
[AN_RNG]	Application Note : Security & Chip Card Ics SLE 66CxxxP and SLE 66CxxxPE Testing the Random Number Generator non-AIS-31 and AIS-31 compliant, version 11.2004 (Developer's reference is CAN_SLE66CxxxP_PE_RNG_2004_11)

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, 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, 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.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.10, 14th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR

[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, Bundesamt für Sicherheit in der Informationstechnik
[AIS31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25/09/2001, Bundesamt für Sicherheit in der Informationstechnik