PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Certification report 2005/52

jTOP® ePassport

-

Integrated Circuit SLE66CLX641P masked by the application jTOP® ePassport version 8.05

Paris, December 19th 2005

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.

Synthesis

Certification report 2005/52

Product: jTOP® ePassport Integrated Circuit SLE66CLX641P masked by the application jTOP® ePassport version 8.05

Developers: Trusted Logic, Infineon Technologies

Common Criteria version 2.2

EAL4 Augmented
(ADV_IMP.2, ALC_DVS.2)

Evaluation sponsor: Trusted Logic

Evaluation facility: Serma Technologies

The following augmentations are not recognized within the framework of the CC RA:
ADV_IMP.2, ALC_DVS.2

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 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 procedures have been published and are available in French on the following Internet site:

www.ssi.gouv.fr

Recognition Agreement of the certificates

The European Recognition Agreement made by SOG-IS in 1999 allows recognition, between Signatory States of the agreement[1], of the certificates delivered by the respective certification bodies. The mutual 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:

The Direction Centrale de la Sécurité des Systèmes d'Information has also signed recognition agreements with other certification bodies from countries that are not members of the European Union. Those agreements can feature that the certificates delivered by France are recognized by the Signatory States. They also can feature that the certificated delivered by each Party are recognized by all signatory parties. (Article 9 of decree number 2002-535).
Thus, the Common Criteria Recognition Arrangement allows the recognition, by all 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 In April 999, the signatory countries of the SOG-IS agreement are: United Kingdom, Germany, France, Spain, Italy, Switzerland, Netherlands, Finland, Norway, Sweden and Portugal.
2 In May 2005, the countries releasing certificates that have signed the agreement are : France, Germany, United Kingdom, United States, Canada, Australia-New Zealand and Japan ; the countries not releasing certificates that have signed the agreement are: Austria, Spain, Finland, Greece, Hungary, Israel, Italy, Norway, Netherlands, Sweden,Turkey, Tcheque Republic, Singapore and India.

Contents

1. THE EVALUATED PRODUCT 6

1.1. PRODUCT IDENTIFICATION 6
1.2. THE DEVELOPER 6
1.3. EVALUATED PRODUCT DESCRIPTION 6
1.3.1. Architecture 6
1.3.2. Life cycle 8
1.3.3. Evaluated product scope 8

2. THE EVALUATION 9

2.1. CONTEXT 9
2.2. EVALUATION REFERENTIAL 9
2.3. EVALUATION SPONSOR 9
2.4. EVALUATION FACILITY 9
2.5. EVALUATION TECHNICAL REPORT 10
2.6. SECURITY TARGET EVALUATION 10
2.7. PRODUCT EVALUATION 10
2.7.1. Evaluation tasks 10
2.7.2. Development environment evaluation 11
2.7.3. Product development 11
2.7.4. Delivery and installation procedure evaluation 12
2.7.5. Guidance documentation evaluation 13
2.7.6. Functional test evaluation 13
2.7.7. Vulnerability assessment 14
2.7.8. Cryptographic mechanism analysis 14

3. THE CERTIFICATION 15

3.1. CONCLUSIONS 15
3.2. USAGE RESTRICTIONS 15
3.3. EUROPEAN RECOGNITION (SOG-IS) 16
3.4. INTERNATIONAL RECOGNITION (CC RA) 16

APPENDIX 1. SITE VISIT REPORT CONCERNING THE DEVELOPMENT ENVIRONMENT 17

APPENDIX 2. PREDEFINED EVALUATION ASSURANCE LEVEL 18

APPENDIX 3. REFERENCES ABOUT THE EVALUTED PRODUCT 19

APPENDIX 4. REFERENCES ABOUT CERTIFICATION 21

1. The Evaluated Product

1.1. Product identification

The evaluated product is the jTOP® ePassport application, version 8.05, developed by Trusted Logic S.A., masked on the SLE66CLX641P integrated circuit developed by Infineon Technologies AG (reference m1522-all with the RSA2048 v1.3 library).

1.2. The developer

The embedded software is developed by the company:

Trusted Logic S.A.

5, rue du Bailliage

78000 Versailles

France

The integrated circuit and its RSA library are developed and manufactured by the company:

Infineon Technologies AG

St.-Martin-Straße 76,

81609 München

Germany

1.3. Evaluated product description

The evaluated product is a contactless smart-card implementing the ePassport features according to the specifications from the International Civil Aviation Organization (cf. ICAO). This product is a contactless-interface chip featuring embedded software enabling:

- to store passport bearer's signed data (issuing state or organization, passport number, expire date, bearer's name, nationality, birth date, sex, other optional data) a bearer's biometric data (face portrait), optional authentication data and several other pieces of data for managing the document security;
- to check passport's authenticity and to identify its bearer during a boarder control with the support of an inspection system.

The chip and its embedded software are intended to be inserted into the cover page of traditional passport booklets.

1.3.1. Architecture

The product is an MRTD (Machine Readable Travel Document) built from hardware (the SLE66CLX641P chip) and software including:

- a runtime environment enabling to execute Java Card™ applications. This environment is compliant with Java Card™ (cf. [JCP]);
- a GlobalPlatform layer providing application installation and configuration services, application selection for execution, and isolation between different application execution contexts. It also offers life cycle management services of the smart card and other administrative operations. This layer (including the functional blocks "OPEN" and "Issuer Security Domain") is compliant with VISA GlobalPlatform specifications (cf. [VGP]).
- The electronic passport application itself (LDS) compliant with the International Civil Aviation Organization (cf. [ICAO]).

This architecture is summarized in the following figure:

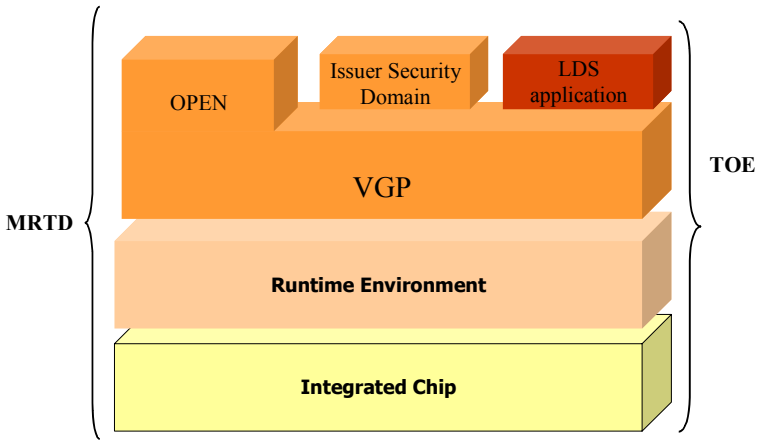

Figure 1: Product Architecture

1.3.2. Life cycle

The life cycle of the product is the following:

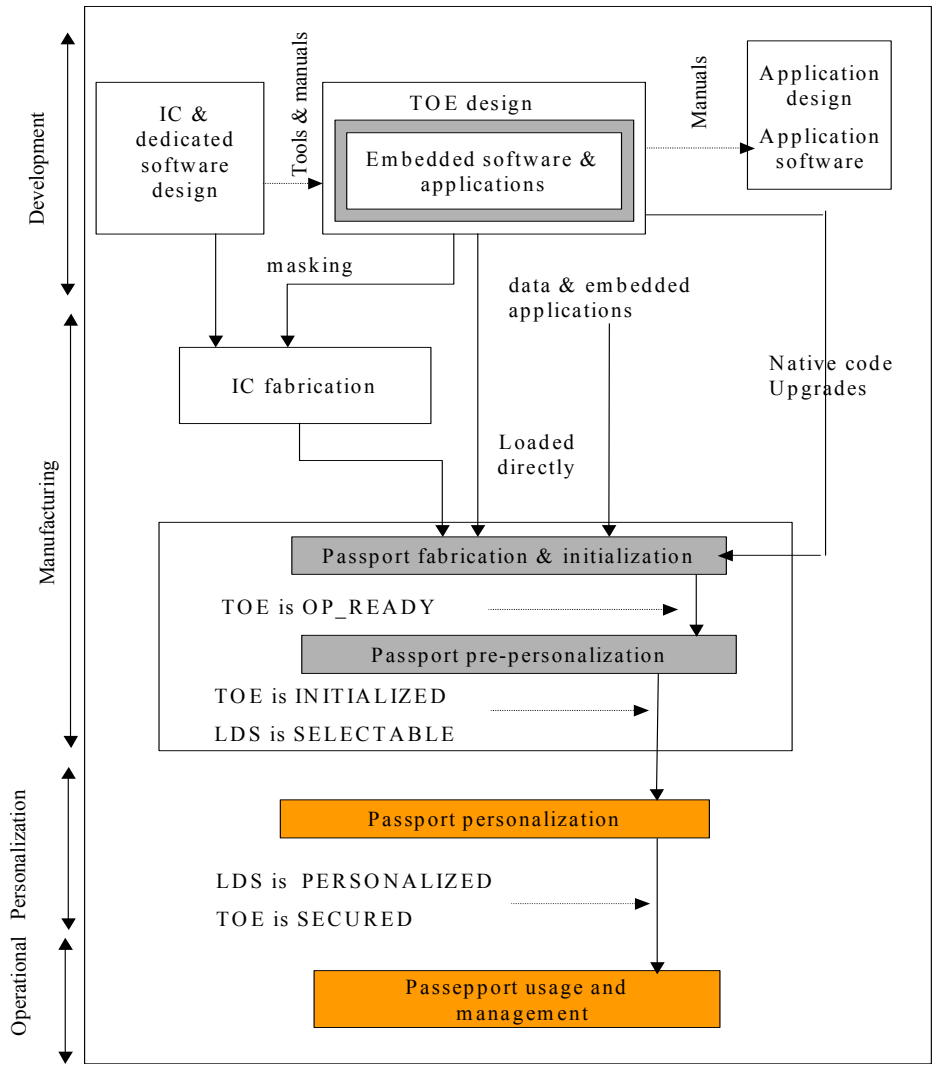

Figure 2 –Life-cycle

1.3.3. Evaluated product scope

The evaluated product includes the whole smart card, that is, the chip and its embedded software as described in paragraph 1.3.1. The inspection systems enabling to send request to the card is out of the evaluation scope.

Regarding the life cycle, the evaluated produce is the product issued from the fabrication, initialization and pre-personalization phases (“Manufacturing” phase), that is to say, the product in the personalization and operational phases (highlighted in orange in Figure 2).

2. The Evaluation

2.1. Context

The evaluation has been conducted according to the composition scheme defined in [COMP]. This scheme consists to evaluate a masked component by evaluating, on one hand, the chip, and on the other hand, the embedded software, and finally verifying that no weakness is introduced by the integration of both parts.

This evaluation has been based upon the results of the SLE66CLX641P chip evaluation at the EAL5 level augmented with the ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 components, according to the [PP-BSI] protection profile. This chip has been certified in Germany, on November 9th, 2005, under the BSI-DSZ-CC-0338-2005 reference (cf. [CERT-IC]).

Thus, some of the current evaluation verdicts are based on the results of the related evaluation works but also on the surveillance works performed for the certificates released on other product of the same family.

2.2. Evaluation referential

The evaluation has been conducted in accordance with the Common Criteria standard [CC], the evaluation methodology defined within the CEM [CEM], and the following list of interpretation:

2.3. Evaluation sponsor

Trusted Logic S.A.

5, rue du Bailliage

78000 Versailles

France

2.4. Evaluation facility

Serma Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Tel.: +33 (0)5 57 26 08 64

Email: m.dus@serma.com

2.5. Evaluation technical report

The evaluation took place from March to December 2005.

The Evaluation Technical Report [ETR] describes the evaluator activities and presents the obtained results. The following paragraphs summarize the main evaluation results.

2.6. Security target evaluation

The security target [ST] defines the evaluated product and its operational environment. This security target has been inspired from the [MRTD-PP] Protection Profile, which was being developed during the evaluation of this product.

For the security target evaluation tasks, the evaluator has issued the following verdicts:

ASE class: Security target evaluation		**Verdicts**
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

2.7. Product evaluation

2.7.1. Evaluation tasks

The evaluation tasks have been performed in compliance to Common Criteria [CC] and its methodology [CEM] at level EAL4[1] augmented. The following table details the selected EAL4 augmentations:

Assurance Components	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ ALC_DVS.2	Sufficiency of security measures

[1]Appendix 2 : Table of the different evaluation assurance levels (EAL – Evaluation Assurance Level) predefined in the Common Criteria [CC].

2.7.2. Development environment evaluation

The embedded software is developed on the site:

Trusted Logic S.A.

5, rue du Bailliage

78000 Versailles

France

The security measures assessed by the evaluator provide guaranty to maintain the confidentiality and the integrity of the evaluated product and its related documentation during the development phase.

The evaluator has analyzed the configuration management plan provided by the developer that describes the use of the configuration management system. This system can generate in particular the configuration list [CONF] that identifies all the product components managed by the system.

The generation procedures also provide assurance that the appropriate components are used to generate the evaluated product.

A verification of the procedure enforcement has been done during an audit from the evaluator at Versailles' site (cf. Appendix 1).

The chip development and manufacturing environment has been reviewed in the framework of the chip evaluation (cf. [CERT-IC]).

For the development environment related evaluation tasks, the evaluator has issued the following verdicts:

ACM class: Configuration Management		**Verdicts**
ACM_AUT.1	Partial CM automation	Pass
ACM_CAP.4	Generation support and acceptance procedures	Pass
ACM_SCP.2	Problem tracking CM coverage	Pass
ALC class: Life cycle support		**Verdicts**
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

2.7.3. Product development

The development documentation analysis has provided the evaluator assurance that the functional requirements which are identified in the security target and listed here below, are correctly and completely refined in the following product representation levels: functional specifications (FSP), high level design (HLD), low level design (LLD) and implementation (IMP)

The functional requirements which are identified in the security target are the following:

- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Subset access control (FDP_ACC.1)
- Security attributes based access control (FDP_ACF.1)
- Export of user data without security attributes (FDP_ETC.1)
- Subset information flow control (FDP_IFC.1)
- Import of user data without security attributes (FDP_ITC.1)
- Basic internal transfer protection (FDP_ITT.1)
- Basic rollback (FDP_ROL.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Basic data exchange confidentiality (FDP_UCT.1)
- Timing of identification (FIA_UID.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Specification of management functions (FMT_SMF.1)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Inter-TSF detection of modification (FPT_ITI.1)
- Resistance to physical attack (FPT_PHP.3)
- TSF domain separation (FPT_SEP.1)
- TSF testing (FPT_TST.1)
- Limited fault tolerance (FRU_FLT.2)
- Inter-TSF trusted channel (FTP_ITC.1)

Explicitly stated security requirements :
- Limited capabilities (FMT_LIM.1)
- Limited availability (FMT_LIM.2)

For the product development evaluation tasks, the evaluator has issued the following verdicts:

ADV class: Development		**Verdicts**
ADV_SPM.1	Informal TOE security policy model	Pass
ADV_FSP.2	Fully defined external interfaces	Pass
ADV_HLD.2	Security enforcing high-level design	Pass
ADV_LLD.1	Descriptive low-level design	Pass
ADV_IMP.2	Implementation of the TSF	Pass
ADV_RCR.1	Informal correspondence demonstration	Pass

2.7.4. Delivery and installation procedure evaluation

The evaluator has analyzed the procedures for delivering Trusted Logic's mask to Infineon for manufacturing, as well as the product initialization guides.

These procedures enable to ensure the delivery origin and to detect any product modification that may occur during the delivery procedure. Product delivery to the clients after product manufacturing as well as the pre-personalization are carried out under the responsibility of Infineon AG, and the associated procedures has been analyzed during the chip evaluation (cf. [CERT-IC]).

Product installation corresponds to the product initialization phase, until its life cycle is moved to the OP_READY state (cf. 1.3.2 Life Cycle), that is, until the product is in a state enabling to be pre-personalized. The analyzed procedures [INSTALL] enable to obtain the evaluated product configuration.

For the delivery and installation procedure evaluation tasks, the evaluator has issued the following verdicts:

ADO class: Delivery and Operation		Verdicts
ADO_DEL.2	Detection of modification	Pass
ADO_IGS.1	Installation, generation, and start-up procedures	Pass

2.7.5. Guidance documentation evaluation

For the evaluation purposes, the administration roles are:

- The passport administrator roles involved during the initialization phase: they are responsible for personalizing the passport according to the rules settle in the issuing state, and notably for configuring the application (LDS) and for loading the cryptography key for authenticating the personalization agent.
- The Personalization Agent: he/she behaves according to the rules set forth in the issuing state for validating the identity of the future passport bearer, validating the biographical data of the future passport bearer, storing the biometrical data of the future passport bearer, electronically signing this data and integrating it into the passport.
- The passport administrator in its operational phase: they are responsible for managing the smart card life cycle. This role may be successively embodied by an actor playing one of the previously identified roles.

For the evaluation purposes, the user roles are:

- The General Inspection System: this is the system enabling to communicate with the passport and to perform the operation required for border control.
- The Border Officer: he/she is the responsible for performing the border controls using the General Inspection System.
- The Passport Bearer.

The evaluator has analyzed the administration and user guidance [GUIDES] to provide assurance that the evaluated product could be used in a secured manner.

For the guidance documentation evaluation tasks, the evaluator has issued the following verdicts:

AGD class: Guidance		Verdicts
AGD_ADM.1	Administrator guidance	Pass
AGD_USR.1	User guidance	Pass

2.7.6. Functional test evaluation

The evaluator has analyzed the documentation of the tests performed by the developer in order to provide assurance that all the product functionalities listed in the security target have been properly tested.

The evaluator has also carried out independent functional tests to provide assurance of the correct operation of the evaluated product.
The evaluator has performed his independent functional tests on the following platform: smart cards identified in §1.1 in the two most representative life cycle states of the certified product, namely, before being personalized and after personalization. A chip emulator has been also used.

For the functional test evaluation tasks, the evaluator has issued the following verdicts:

ATE class: Tests		**Verdicts**
ATE_COV.2	Analysis of coverage	Pass
ATE_DPT.1	Testing: high-level design	Pass
ATE_FUN.1	Functional testing	Pass
ATE_IND.2	Independent testing - sample	Pass

2.7.7. Vulnerability assessment

The evaluator has checked that the documentation delivered with the product [INSTALL][GUIDES] is clear enough to avoid any misuse or operational mistake that could lead to a non secured state of the product.

No security function has required an intrinsic resistance level assessment.

Relying on the developer vulnerability analysis and all the information provided in the evaluation frame, the evaluator has performed its own independent analysis to assess the potential vulnerabilities of the product. This analysis was completed by tests performed on platform: smart cards identified in §1.1 in the two most representative life cycle states of the certified product, namely, before being personalized and after personalization. A chip emulator has been also used.

The analysis conducted by the evaluator does not point the existence of exploitable vulnerabilities for the targeted security level. The product is thus resistant to attacker possessing ***VLA.2*** attack potential.

For the vulnerability assessment tasks, the evaluator has issued the following verdicts:

AVA class: Vulnerability assurance		**Verdicts**
AVA_MSU.2	Validation of analysis	Pass
AVA_SOF.1	Strength of TOE security function evaluation	Pass
AVA_VLA.2	Independent Vulnerability Analysis	Pass

2.7.8. Cryptographic mechanism analysis

No analysis of the cryptographic mechanism resistance has been performed by the DCSSI.

3. The Certification

3.1. Conclusions

The whole tasks performed by the ITSEF and described in the evaluation technical report [ETR] enable the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the copies of the products or systems submitted for evaluation fulfill the security features specified in its security target [ST]. It also certifies that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (Art. 8 of decree 202-535).

3.2. Usage restrictions

The evaluation conclusions are valid only for the product identified in chapter 1 of the current certification report.

The user of the certified product shall respect the operational environmental security objectives summarized hereafter and the recommendations within the user guidance [INSTALL], [GUIDES]:

- The Passport Manufacturer and Administrator shall not perform operations that could downgrade the passport security level. All the cryptography keys enabling a user to embody the Passport Administration role shall be kept secret and protected by a secure environment ensuring their confidentiality and integrity. This concerns the administration keys (ISD key), the Basic Access Control key (BAC key); the Active Authentication key, as well as the document signing key used to sign the passport data.
- The Passport Issuing State shall ensure that any user embodying the Personalization Agent role shall (i) validate that the candidate passport bearer (in the sequel: the candidate) is the genuine intended owner of the passport, and check that candidate biographical data required for personalizing the passport is correct (ii) store the candidate's biometric reference data, that is, his/her portrait, (iii) personalize the passport for the candidate enforcing the required physical and logical security measures (including electronically signing the candidate data in the passport). The Personalization Agent shall generate 112 bits cryptographic keys according to the algorithm for deriving BAC keys specified in Appendix E of the [ICAO] document relative to PKI.
- The Issuing State or Organization shall:
    1. Generate a cryptographically sure Country Signing Key Pair;
    2. Ensure the secrecy of the private key of its Country Signing Key Pair and sign the Document Signer Certificate in a secure operational environment;
    3. Distribute a Country Signing Certificate containing the public key of its Country Signing Key Pair to the host state or organizations. This certificate ensures the integrity and authenticity of its public signature key.

  The Issuing State or Organization shall also:
    1. Generate a cryptographically sure Document Signer Key Pair;
    2. Ensure the secrecy of the private key of its Document Signer Key Pair and sign the genuine passport security data in a secure operational environment;

3. Distribute a Document Signer Certificate containing the public key of its Document Signer Key Pair to the host state or organizations, keeping its integrity and authenticity by using the key infrastructure described in [MRTD].

- The Issuing State or Organization shall also:
  1. Generate a cryptographically sure Active Authentication Key Pair for the passport;
  2. Sign the public key of the Active Authentication Key Pair and store it into the passport.
- The host state or organization's Inspection System shall use the passport for verifying the identity of the passport bearer and the authenticity of the passport. The Inspection System is a trusted terminal which does not use its privileges neither for disclosing the passport data nor for tracing the use of the passport.
- The Inspection System shall verify the signature of the signed date on the passport before using them for identifying its bearer. The states and organizations shall preserve the authenticity and the availability of the Country Signing Certificates and Document Signer Certificates for the Inspection Systems (the public key of the Country Signing Key Pair may be read out from the passport) itself.
- The Inspection Systems and the host states and organizations shall ensure the confidentiality and the integrity of the data read out from the passport. The Inspection System shall implement the terminal side of the BAC protocol.
- The host states and organizations and the Inspection System itself shall check the passport authenticity using the Active Authentication mechanism, provided that the Inspection System supports this mechanism.
- The Passport Manufacturer shall ensure the quality and integrity of the manufacturing process. This role is also responsible for the de-activation of any test, debug or patch mechanism present in the passport when it reaches the OP_READY life cycle state (just before the pre-personalization phase). The different roles involved in the passport manufacturing, (Manufacturer, Passport Administrator in charge of initializing the passport) shall use the security procedures ensuring the confidentiality and integrity of the code and test data embedded on the passport until its delivery to the final user (in order to prevent any copy, modification, steel or non authorized usage). In particular, the product shall be protected by appropriate measures when it is delivered from one actor to another.

3.3. European Recognition (SOG-IS)

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

3.4. International Recognition (CC RA)

This certificate is released in accordance with the provisions of the CC RA [CC RA]. However, the following augmentations are not mutually recognized in accordance with provisions of the CC RA [CC RA]: ADV_IMP.2, ALC_DVS.2.

Appendix 1. Site visit report concerning the development environment

The development site of Trusted Logic, located at *5 rue du Bailliage, 78000, Versailles, France*, has been visited by the evaluator on March 24th and 25th, 2005 and September 23rd, 2005 in order to verify the application of the procedures related to the configuration management, life cycle support and delivery, for the jTOP® e-Passport v8.05 product.

The procedures have been provided and analyzed in the following evaluation framework:

- ACM_AUT.1 and ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

A visit report [Visit] has been released by the evaluator.

Appendix 2. Predefined Evaluation Assurance Level

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 3. References about the evaluted product

[CERTIF-IC]	Certification Report – Infineon Smart Card IC (Security controller), SLE66CLX640P/m1523-a11 and SLE66CLX641P/m1522-a11 both with RSA2048 v1.3 and specific IC dedicated software, Reference: BSI-DSZ-CC-0338-2005, 9 november 2005, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[CONF]	jTOP v#8.05 e-Passport - Configuration Management Plan, Reference: DR-2005-NT-165-1.2 Trusted Logic
[GUIDES]	• jTOP v#8.05 - Administration Guide, Reference : CP-2005-RT-136-1.2 Trusted Logic • jTOP v#8.05 e-Passport - User Guide, Reference: CP-2005-RT-137-1.1 Trusted Logic
[ICAO]	• PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 1st 2004, International Civil Aviation Organization, • Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, May 18th 2004, International Civil Aviation Organization, • Machine Readable Travel Documents, supplement 9303, version 3.0, 12 June 2005
[INSTALL]	jTOP v#8.05 e-Passport – Card Initialization Phase, Reference : CP-2003-RT-52-3.0, Trusted Logic
[JCP]	• Card 2.1.1 Runtime Environment Specification, Revision 1.0, May 18th 2000, Sun Microsystems, • Java Card 2.1.1 Virtual Machine Specification, Revision 1.0, May 18th 2000, Sun Microsystems • Java Card 2.1.1 Application Programming Interface, Revision 1.0, May 18th 2000, Sun Microsystems.
[MRTD-PP]	Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Basic Access Control, Reference: BSI-PP-0017 Version 1.0, 18 August 2005, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[PP-BSI]	Smartcard IC Platform Protection Profile

	Reference: BSI-0002-2001, version 1.0, July 2002, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[RTE]	Evaluation Technical Report - jTOP v#8.05 e-Passport (EAL4+ evaluation), Reference: COCOON_ETR_V1.0, Serma Technologies
[ST]	Evaluation Security Target : • JTOP e-Passport Security Target, Reference: CP-2005-RT-75/1.10, Trusted Logic. For the sake of international recognition agreement, the following lite security target has been provided: • JTOP e-Passport Security Target Lite, Reference: PU-2005-RT-624/1.0, Trusted Logic
[VGP]	• GlobalPlatform Card Specification, Version 2.0.1', 7 April 2000 • VISA GlobalPlatform 2.0.1' Card Implementation Requirements, Configuration 2 – Compact with PK, Version 1.0, February 2000, • VISA GlobalPlatform 2.0.1' Card Implementation Requirements, Configuration 2 – Compact with PK, Errata 2.0, June 2003
[Visite]	Evaluation report - Classes ACM, ADO, ALC – Annexe A, Reference: COCOON_ACM-ALC-ADO_v1.1, Serma Technologies

Appendix 4. References about certification

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 de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[COMP]	Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation: Recommended best practice, Version 1.2, March 2002.
[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.

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