PREMIER MINISTRE

Secretariat General for National Defence

French Network and Information Security Agency

Certification Report ANSSI-CC-PP-2009/02

Protection Profile
Embedded Software for Smart Secure Devices
Basic and Extended Configurations
(reference ANSSI-CC-PP-ESforSSD, version 1.0, 27 November 2009)

Paris, 1st December 2009

Courtesy Translation

Warning

This report testifies that the protection profile evaluated fulfill the evaluation criteria.
A protection profile is a public document which defined for a special product category a set of requirements and security objectives independently of the technology and the implementation. The products defined from this protection profile satisfied the security needs from a common group of users.

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.anssi@ssi.gouv.fr

Certification report reference

ANSSI-CC-PP-2009/02

Protection profile name

Protection profile
Embedded Software for Smart Secure Devices
Basic and Extended Configurations

Protection profile reference

ANSSI-CC-PP-ESforSSD,
version 1.0, 27 November 2009

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level imposed by the PP

EAL 4 augmented
ALC_DVS.2, AVA_VAN.5

Writer(s)

Trusted Labs SAS
5 rue du Bailliage, 78000 Versailles, France

Sponsor

ANSSI
51, boulevard de la Tour-Maubourg, 75700 Paris 07 SP, France

Evaluation facility

CEA - LETI
17 rue des martyrs, 38054 Grenoble Cedex 9, France
Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr

Recognition arrangements

CCRA

SOG-IS

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. Presentation of the protection profile

1.1. Protection profile identification

This [PP] is a unique document gathering two protection profiles in the form of two configurations, each being identified in a unique way:

- ANSSI-CC-PP-ESforSSD_Basic for the Basic configuration ;
- ANSSI-CC-PP-ESforSSD_Extended for the Extended configuration ;

The document is organised so as to easily identify the elements that are specific to each configuration, as the chapters, the figures or the tables: they are tagged with the configuration identifier (ANSSI-CC-PP-ESforSSD_Basic or ANSSI-CC-PP-ESforSSD_Extended); elements that are common to both configurations do not hold any label.

Both tables below recapitulate the characteristics for each configuration:

Title	Protection profile Embedded Software for Smart Secure Devices Basic Configuration
Configuration identifier	ANSSI-CC-PP-ESforSSD_Basic
Document's reference	ANSSI-CC-PP-ESforSSD
Document's version	1.0
Document's date	27 November 2009
CC version	CCv3.1r3
Editor	Trusted Labs SAS
Sponsor	ANSSI

Title	Protection profile Embedded Software for Smart Secure Devices Extended Configuration
Configuration identifier	ANSSI-CC-PP-ESforSSD_Extended
Document's reference	ANSSI-CC-PP-ESforSSD
Document's version	1.0
Document's date	27 November 2009
CC version	CCv3.1r3
Writer	Trusted Labs SAS
Sponsor	ANSSI

1.2. Writer

This protection profile has been written by:

Trusted Labs SAS

5 rue du Bailliage, 78000 Versailles, France

1.3. Protection profile description

This [PP] replaces the Protection Profile "Smart Card Integrated Circuit with Embedded Software" [PP 9911] certified by French Scheme ANSSI in 1999. It meets current needs and technological trends in smart secure devices, e.g. smartcards. Joint work with actors from the smartcard industry and with specialized evaluation laboratories has been carried out in order to have the most accurate inputs and actual constraints.

This [PP] applies to smart secure devices composed of a Security Integrated Circuit and of Embedded Software running on top of this IC. The Security IC provides processing units, security components, random number generator, I/O ports, volatile and non-volatile memories. The Embedded Software implements Operating System functionalities such as secure boot, memory management, life cycle management and, potentially, applicative behaviour.

The products targeted by this [PP] are of two kinds:

- "Integrated products" where the Embedded Software consists of native code that implements both OS and applicative behaviour without demarcation between them;
- "Layered products" where the Embedded Software consists of an "OS Layer", potentially with integrated applicative behaviour, and an "Application Layer" on top of it. The OS provides a separation mechanism between itself and the Application Layer as well as services to the Application Layer.

This [PP] focuses on the security requirements for the OS, which constitutes the TOE; the Security IC is considered as the environment of the OS, covered by security objectives. Nevertheless, any smart secure device evaluation against this [PP] shall comprehend the whole product including both the Security IC and the OS: the security target of the product shall enforce the security objectives for the IC stated in this [PP] by means of security requirements for the IC.

The evaluation of the product may be "composite" according with security assurance requirements in [COMP][1], provided the IC has been evaluated separately. This [PP] does not require any formal compliance to a specific hardware Protection Profile for the IC evaluation but those ICs evaluated against [PP0035] fully meet the objectives. However, composition with an already certified IC is not mandatory. In the case where the IC has not been certified, the product evaluation shall address both the IC and the OS at the same time. Requirements on vulnerability assessment stated in [CC AP] document apply in both cases.

[1] The Security Assurance Requirements in [COMP] come in addition to the EAL specified in this Protection Profile, especially the requirements related to the recommendations from the Security IC evaluation.

This [PP] defines two TOE configurations, Basic and Extended, that map to the kinds of products identified above:

- Basic TOE: There is no separation between the OS and the applications. The Basic TOE implements security features for its own purposes (cf. section 2.4.1 of the [PP]). This configuration corresponds to integrated products;
- Extended TOE: The OS implements a separation mechanism between itself and the Application Layer. The Extended TOE implements security features for its own purposes and potentially for the Application Layer (cf. section 2.4.2 of the [PP]). This configuration corresponds to layered products.

Each TOE configuration gives rise to a [PP] configuration, with unique identification:

- "ANSSI-CC-PP-ESforSSD_Basic" addresses integrated products with Basic TOE where the OS and the applicative behaviour are not separated;
- "ANSSI-CC-PP-ESforSSD_Extended" addresses layered products with Extended TOE where the OS provides a separation mechanism between itself and the Application Layer that runs on top of it.

This [PP] requires "demonstrable" conformance.

Security Targets or Protection Profiles conformant to this [PP] can enlarge the perimeter of the chosen TOE configuration with additional functionalities like, for instance, authentication mechanisms, post-delivery loading of code and data, secure communication protocols[1].

1.4. Functional requirements

The **security functional requirements** which are identified in this protection profile are the following:

- For the TOE in Basic configuration:
  - Regarding atomicity functionality:
    - *FDP_ACC.1/Atomicity Subset access control ;*
    - *FDP_ROL.1/Atomicity Basic rollback ;*
  - Regarding confidentiality functionality:
    - *FDP_ACC.1/Confidentiality Subset access control ;*
    - *FDP_ACF.1/Confidentiality Security attribute based access control ;*
    - *FDP_RIP.1/Confidentiality Subset residual information protection ;*
    - *FDP_UCT.1/Confidentiality Basic data exchange confidentiality ;*
    - *FMT_MSA.1/Confidentiality Management of security attributes ;*
    - *FMT_MSA.3/Confidentiality Static attribute initialisation ;*
    - *FPR_UNO.1/Confidentiality Unobservability ;*
    - *FPT_ITC.1/Confidentiality Inter-TSF confidentiality during transmission ;*
  - Regarding cryptography functionality:
    - *FCS_CKM.4 Cryptographic key destruction ;*
    - *FCS_COP.1 Cryptographic operation ;*

[1] This Protection Profile has been designed to ease composite evaluations with applicative Protection Profiles like "Electronic Purse" Protection Profile [PPEP] and "Java Card System" Protection Profiles [PPJCS].

  - Regarding integrity functionality:
    - *FDP_ACC.1/Integrity Subset access control ;*
    - *FDP_ACF.1/Integrity Security attribute based access control ;*
    - *FDP_SDI.2/Integrity Stored data integrity monitoring and action ;*
    - *FDP_UIT.1/Integrity Data exchange integrity ;*
    - *FMT_MSA.1/Integrity Management of security attributes ;*
    - *FMT_MSA.3/Integrity Static attribute initialisation ;*
    - *FPT_ITI.1/Integrity Inter-TSF detection of modification ;*
  - Regarding life cycle functionality:
    - *FDP_ACC.1/Life_cycle Subset access control ;*
    - *FDP_ACF.1/Life_cycle Security attribute based access control ;*
    - *FMT_MSA.1/Life_cycle Management of security attributes ;*
    - *FMT_MSA.3/Life_cycle Static attribute initialisation ;*
  - Regarding monitoring functionality:
    - *FAU_ARP.1/Monitoring Security alarms ;*
    - *FAU_SAA.1/Monitoring Potential violation analysis ;*
  - Regarding operate functionality:
    - *FMT_MOF.1/Operate Management of security functions behaviour ;*
    - *FMT_MTD.1/Operate Management of TSF data ;*
    - *FPT_FLS.1/Operate Failure with preservation of secure state ;*
    - *FPT_TST.1/Operate TSF testing ;*
  - Regarding random numbers functionality:
    - *FIA_SOS.2/RND TSF Generation of secrets ;*
  - Regarding roles functionality:
    - *FIA_UID.1 Timing of identification ;*
    - *FMT_SMR.1 Security roles ;*
- For the TOE in Extended configuration:
  - Regarding separation functionality:
    - *FDP_IFC.1/Separation Subset information flow control ;*
    - *FDP_IFF.1/Separation Simple security attributes ;*
    - *FMT_MSA.3/Separation Static attribute initialisation ;*
    - *FMT_MSA.1/Separation Management of security attributes ;*

All these security functional requirements are extracted from Common Criteria part 2 [CC].

1.5. Assurance requirements

The assurance requirements required for this protection profile is **EAL 4 augmented[1] with the following assurance requirements:**

Composants	Descriptions
ALC_DVS.2	Sufficiency of security measures
AVA_VAN.5	Advanced methodical vulnerability analysis

Tableau 1 - Augmentations

All these security assurance requirements are extracted from Common Criteria part 3 [CC].

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

2. Evaluation

2.1. Evaluation referential

The evaluation has been conducted in accordance with the **Common Criteria standard version 3.1** [CC] and the evaluation methodology defined within the CEM [CEM].

2.2. Sponsor

ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP
France

2.3. Evaluation facility

CEA - LETI

17 rue des martyrs
38054 Grenoble Cedex 9
France

Téléphone : +33 (0)4 38 78 40 87

Adresse électronique : cesti.leti@cea.fr

2.4. Evaluation tasks

The evaluation technical report [ETR], delivered to ANSSI on 15 September 2009, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

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.

3.2. Warnings and usage restrictions

As mentioned above (see 1.3 Protection profile description), the writer of a security target, claiming conformance to this [PP], shall specify security objectives for the underlying component corresponding to the security objectives for the component stated in this [PP]. This principle is a part of a set of principles which were adopted for this [PP], and which are detailed in the [PP], in particular in the chapter 4 Underlying security model.

3.3. European recognition (SOG-IS)

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

3.4. 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, Switzerland and United Kingdom.
2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, 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**	1	**3**	3	**4**	**1**	Testing: basic design
	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. References

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CPP/P/01]	Procedure CPP/P/01 – Protection profiles certification, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[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 AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009, or current applicable version.
[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.
[PP]	Protection Profile object of this Certification Report: Protection Profile - Embedded Software for Smart Secure Devices - Basic and Extended Configurations Reference ANSSI-CC-PP-ESforSSD, version 1.0, 27 November 2009
[PP 9911]	Protection Profile certified by ANSSI: Smart Card Integrated Circuit with Embedded Software Protection Profile, Version 2.0, June 1999
[PP0035]	Protection Profile certified by BSI: Security IC Platform Protection Profile, Version 1.0, June 2007
[ETR]	PROJECT PP-09x - Rapport de tâche APE Reference: LETI.CESTI.P9x.RAP.001 - v1.2 - 15/09/09