PREMIER MINISTRE

General Secretariat for Defence and National Security

French Network and Information Security Agency

Certification Report ANSSI-CC-PP-2010/02

Secure Access Module for Electronic Money system Protection Profile

(reference SFPMEI-CC-PP-SAM, version 1.5 dated from 4 February 2010)

Paris, the 17 February 2010

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 et de la sécurité 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-2010/02

Protection profile name

Secure Access Module for Electronic Money system Protection Profile

Protection profile reference

Reference SFPMEI-CC-PP-SAM / version 1.5 dated from 4 February 2010

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

Trusted Labs SAS

5 rue du Bailliage, 78000 Versailles, France

Sponsors

BMS

153 rue Saint-Honoré, 75001 Paris, France

SFPMEI

168 rue de Rivoli, 75001 Paris, France

Evaluation facility

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mail : e.francois@serma.com

Recognition arrangements

CCRA

SOG-IS

Recognition until the 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.

Contents

1. Presentation of the protection profile

1.1. Protection profile identification

Title: Secure Access Module for Electronic Money system Protection Profile.
Reference: SFPMEI-CC-PP-SAM, version 1.5.
Date: 4 February 2010.

1.2. Writer

This protection profile has been written by:

Trusted Labs S.A.S.

5 rue du Bailliage
78000 Versailles
France

1.3. Protection profile description

The target of evaluation defined in the protection profile [PP] is a Secure Access Module (SAM). It comprises an integrated circuit (which moreover shall be certified in accordance with the protection profile [PP-0035]), with contact interface, and all the embedded software necessary to the implementation of the SAM functionnalities.

The SAM is included in a purchase device which is either a physical device installed at the merchant (a terminal), or a server. The purchase device is used to accept payment from an electronic purse. The SAM shall provide the necessary security for the electronic money payment, the quickload and the collect transactions.

The target of evaluation described in the protection profile shall be able to:
- store its amount of electronic money;
- receive an amount of electronic money from an electronic purse, via a credit operation, after debit of the electronic purse;
- deliver stored electronic money to an acquirer device via a collect transaction;
- execute quickload transactions;
- update SAM parameters.

The target of evaluation shall provide offline electronic money payment transactions capabilities thus requiring the following security mechanisms to prevent from fraud:
- integrity protection of electronic money during collect, quickload and payment transactions;
- integrity and confidentiality protection of cryptographic keys when used or stored;
- mutual authentication between the target of evaluation and the electronic purse during quickload and payment transactions;
- signature of collect transactions.

1.4. Functional requirements

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

- Audit data generation (FAU_GEN.1)
- Audit review (FAU_SAR.1)
- Protected audit trail storage (FAU_STG.1)
- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)
- Security attribute based access control (FDP_ACF.1)
- Basic Data Authentication (FDP_DAU.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Import of user data without security attributes (FDP_ITC.1)
- Stored data integrity monitoring (FDP_SDI.1)
- TSF Generation of secrets (FIA_SOS.2)
- Timing of authentication (FIA_UAU.1)
- Unforgeable authentication (FIA_UAU.3)
- Single-use authentication mechanisms (FIA_UAU.4)
- Re-authenticating (FIA_UAU.6)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Inter-TSF confidentiality during transmission (FPT_ITC.1)
- Inter-TSF detection and modification (FPT_ITI.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance of physical attack (FPT_PHP.3)
- Function recovery (FPT_RCV.4)
- Replay detection (FPT_RPL.1)

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 with the following assurance requirements[1]:**

Components	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] **Erreur ! Source du renvoi introuvable.**: 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. Sponsors

BMS

153 rue Saint-Honoré
75001 Paris
France

SFPMEI

168 rue de Rivoli
75001 Paris
France

2.3. Evaluation facility

SERMA Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Phone : +33 (0)5 57 26 08 75

Mail: e.francois@serma.com

2.4. Evaluation tasks

The evaluation technical report [ETR], delivered to ANSSI the 12 January 2010, 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. 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:

3.3. 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

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 4+	Name of the component
ADV Development	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_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guidance	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Life-cycle support	ALC_CMC		**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
ST Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components 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 specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**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**	Independent testing - sample
AVA Vulnerability assessment	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.
[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-0035]	Security IC Platform Protection Profile, Reference: BSI-PP-0035, version 1.0 dated from 15/06/2007 *Certified by the BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-CC-PP-0035-2007.*
[PP]	SAM for EM system Protection Profile, Reference: SFPMEI-CC-PP-EP, version 1.5 dated from 04/02/2010, Trusted Labs SAS
[RTE]	Electronic Purse and Secure Access Module for EM system Protection Profiles Evaluation Report, Reference: MONEO_APE_v1.2, version 1.2, Serma Technologies