Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Certification Report ANSSI-CC-PP-2010/05

(U)SIM Java Card Platform Protection Profile / SCWS Configuration

(ref. PU-2009-RT-79, version 2.0.2)

Paris, 12th July 2010

Courtesy Translation

SÉCURITÉ CERTIFICATION

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-2010/05

Protection profile name

(U)SIM Java Card Platform Protection Profile
Basic and SCWS Configurations
(SCWS configuration)

Protection profile reference and version

Ref. PU-2009-RT-79 / version 2.0.2

Protection profile conformity

[PP JCS_O], version 2.6
Java Card System - Open Configuration Protection Profil

Evaluation criteria and version

Common Criteria version 3.1, révision 3

Evaluation level imposed by the PP

EAL 4 augmented
ALC_DVS.2, AVA_VAN.5

Writer

Trusted Labs S.A.S.
5 rue du Bailliage, 78000 Versailles, France

Sponsor

Société Française du Radiotéléphone (SFR)
1 place Carpeaux, Tour Séquoia, 92915 Paris La Défense, France

Evaluation facility

THALES - CEACI (T3S – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France
Tél : +33 (0)5 62 88 28 01 or 18, mél : nathalie.feyt@thalesgroup.com

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, modified. 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: (U)SIM Java Card Platform Protection Profile - SCWS Configuration
Reference, version: PU-2009-RT-79, version 2.0.2
Date: 17th June 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 (TOE) is the (U)SIM Java Card ™ platform embedded in a (U)SIM card intended to be plugged in a mobile phone or other mobile devices.

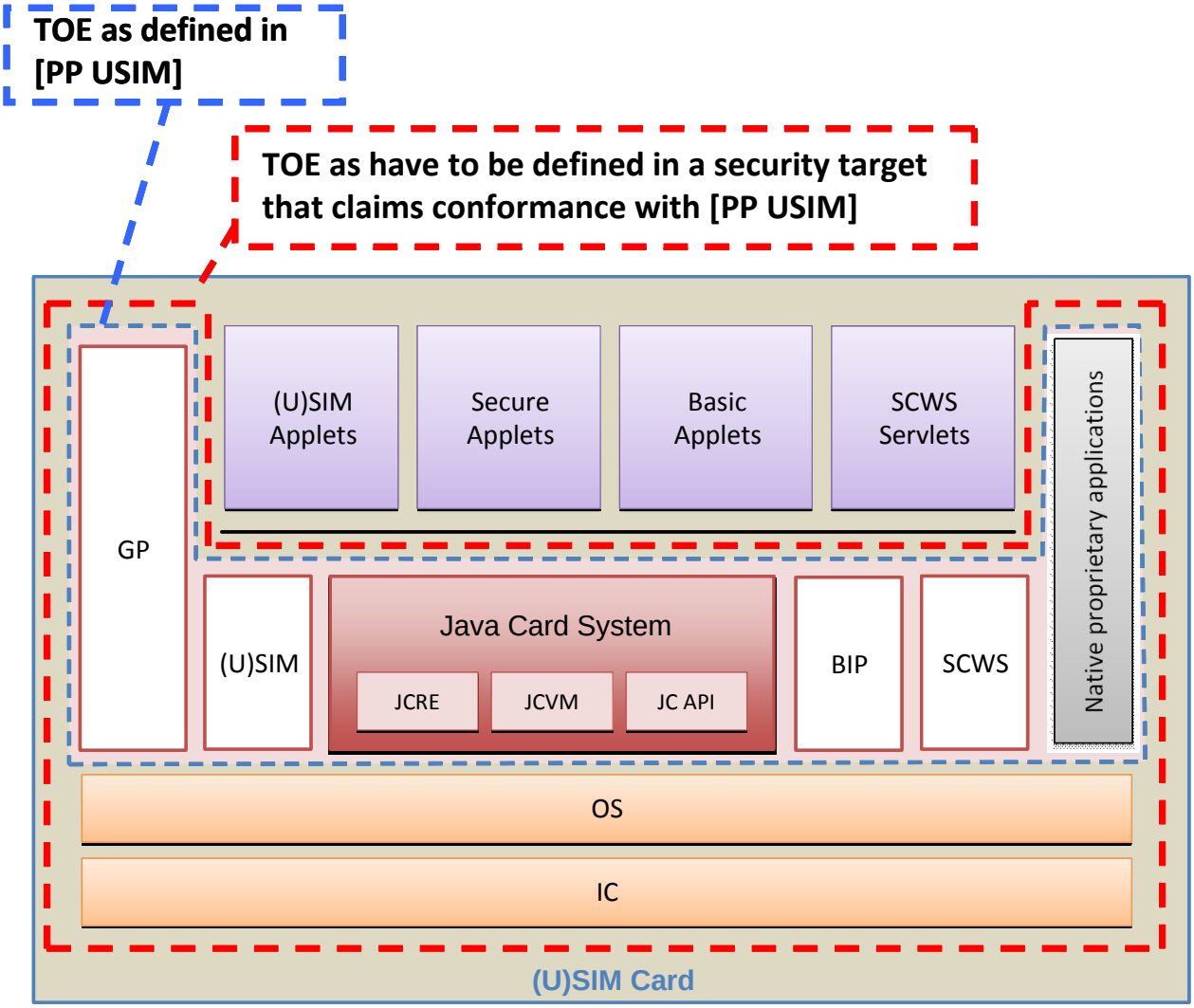
Usage of this Protection Profile will permit the certification according to the Common Criteria, and up to EAL4+ level, security applications loaded on a (U)SIM Java Card open platform previously certified. Those security applications will be able to coexist on the certified card with non security application (those last applications will not be certified, nevertheless they will have to be compliant with the platform constraints). As the considered cards are open, applet loading could be realized after the card issuance to the end users of the mobile devices (operational use phase).

This Protection Profile focuses on the security requirements for the (U)SIM Java Card platform. The IC and the OS are considered in this PP as the environment of the (U)SIM Java Card platform, covered by environmental security objectives. Nevertheless, any (U)SIM smart card evaluation according to this PP shall comprehend the whole in the TOE : IC, OS, all native code, (U)SIM Java Card platform and pre-loaded applet should also be included in the TOE described in the security target which claim conformance with this PP, see chapter 3.2 for further details.

The TOE defined in [PP USIM] in Basic configuration is composed of the following elements:

- A Java Card System, conformant with the protection profile [PP JCS_O], which manages and executes Java Card applications (applets). It also provides APIs to develop applets on top of it, in accordance with Java Card specifications;
- GlobalPlatform (GP) packages, which provides to the applications hosted on the card a standardized interface in order to communicate with the external world and which also permit to manage applications in a secure way;
- (U)SIM APIs, which permits data exchange between (U)SIM applications and the mobile network, including applications downloading are enforced through a communication channel based on SMS[1] or BIP technology (security services provided by this element are not forced to be evaluated in a evaluation conformant to [PP USIM]);
- The BIP[2] technology which permits Over-The-Air (OTA) data exchange between (U)SIM card on a mobile phone and remote servers (security services provided by this element are not forced to be evaluated in a evaluation conformant to [PP USIM]);
- A Smart Card Web Server (SCWS) which enables the end-user to access the (U)SIM contents and applications through a web browser of its mobile phone;
- Native applications, if existing, running on the OS of the card (those applications don't provide any security function to be evaluated according to [PP USIM]).

[1] Short Message Service
[2] Bearer Independent Protocol


TOE as defined in [PP USIM]
TOE as have to be defined in a security target that claims conformance with [PP USIM]
GP
(U)SIM Applets
Secure Applets
Basic Applets
SCWS Servlets
Native proprietary applications
(U)SIM
Java Card System
JCRE
JCVM
JC API
BIP
SCWS
OS
IC
(U)SIM Card

1.4. Functional requirements

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

- Enforced proof of origin (FCO_NRO.2) ;
- Cryptographic operation (FCS_COP.1) ;
- Subset access control (FDP_ACC.1) ;
- Security attribute based access control (FDP_ACF.1) ;
- Complete information flow control (FDP_IFC.2) ;
- Simple security attributes (FDP_IFF.1) ;
- Import of user data with security attributes (FDP_ITC.2) ;
- Basic rollback (FDP_ROL.1) ;
- Data exchange integrity (FDP_UIT.1) ;
- Timing of authentication (FIA_UAU.1) ;
- Single-use authentication mechanisms (FIA_UAU.4) ;
- Timing of identification (FIA_UID.1) ;
- Management of security attributes (FMT_MSA.1) ;
- Static attribute initialisation (FMT_MSA.3) ;
- Specification of management functions (FMT_SMF.1) ;
- Security roles (FMT_SMR.1) ;
- Failure with preservation of secure state (FPT_FLS.1) ;
- Replay detection (FPT_RPL.1) ;
- Inter-TSF basic TSF data consistency (FPT_TDC.1) ;
- Inter-TSF trusted channel (FTP_ITC.1) ;
- Trusted path (FTP_TRP.1).

A security target conformant to [PP USIM] will also have to identified the following security functional requirements from [PP JCS_O] :

- Security alarms (FAU_ARP.1) ;
- Enforced proof of origin (FCO_NRO.2) ;
- Cryptographic key generation (FCS_CKM.1) ;
- Cryptographic key distribution (FCS_CKM.2) ;
- Cryptographic key access (FCS_CKM.3) ;
- Cryptographic key destruction (FCS_CKM.4) ;
- Cryptographic operation (FCS_COP.1) ;
- Complete access control (FDP_ACC.2) ;
- Security attribute based access control (FDP_ACF.1) ;
- Subset information flow control (FDP_IFC.1) ;
- Complete information flow control (FDP_IFC.2) ;
- Simple security attributes (FDP_IFF.1) ;
- Import of user data with security attributes (FDP_ITC.2) ;

- Subset residual information protection (FDP_RIP.1) ;
- Basic rollback (FDP_ROL.1) ;
- Stored data integrity monitoring and action (FDP_SDI.2) ;
- Data exchange integrity (FDP_UIT.1) ;
- User attribute definition (FIA_ATD.1) ;
- Timing of identification (FIA_UID.1) ;
- User identification before any action (FIA_UID.2) ;
- User-subject binding (FIA_USB.1) ;
- Management of TSF data (FMT_MTD.1) ;
- Secure TSF data (FMT_MTD.3) ;
- Management of security attributes (FMT_MSA.1) ;
- Secure security attributes (FMT_MSA.2) ;
- Static attribute initialisation (FMT_MSA.3) ;
- Revocation (FMT_REV.1) ;
- Specification of Management Functions (FMT_SMF.1) ;
- Security roles (FMT_SMR.1) ;
- Unobservability (FPR_UNO.1) ;
- Failure with preservation of secure state (FPT_FLS.1) ;
- Automated recovery without undue loss (FPT_RCV.3) ;
- Inter-TSF basic TSF data consistency (FPT_TDC.1) ;
- Inter-TSF trusted channel (FTP_ITC.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[1] with the following assurance requirements:**

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] 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 version 3.1, revision 3** [CC] and the evaluation methodology defined within the CEM [CEM].

2.2. Sponsor

Société Française du Radiotéléphone (SFR)

1 place Carpeaux
Tour Séquoia
92915 Paris La Défense
France

2.3. Evaluation facility

THALES - CEACI (T3S – CNES)

18 avenue Edouard Belin
BPI 1414
31401 Toulouse Cedex 9
France

Phone : +33 (0)5 62 88 28 01 or 18

Adresse électronique : nathalie.feyt@thalesgroup.com

2.4. Evaluation tasks

The evaluation technical report [ETR], delivered to ANSSI the 5th July 2010, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks listed below are "**pass**".

Components	Descriptions
APE_CCL.1	Conformance claims
APE_ECD.1	Extended components definition
APE_INT.1	Protection profile introduction
APE_OBJ.2	Security objectives
APE_REQ.2	Derived security requirements
APE_SPD.1	Security problem definition

Tableau 2 - PP evaluation

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

[PP USIM] is conformant to [PP JCS_O] as a Java Card system is included in the TOE described in [PP USIM]. For a better readability of this PP, all elements of [PP JCS_O] that have to be reproduce from it in a security target that claims conformance to [PP USIM] are note explicitly listed in [PP USIM] (nevertheless guidance for the redaction are available in this PP).
Thus, the writer of a security target conformant to [PP USIM] will have to reproduce in the security target:

- all threats from [PP JCS_O], except T.PHYSICAL ;
- all assumption from [PP JCS_O] ;
- all organisational security policies from [PP JCS_O] ;
- all objectives on the TOE from [PP JCS_O].
- all objectives for the operational environment from [PP JCS_O], except the following :
  - OE.CARD-MANAGEMENT ;
  - OE.SCP.SUPPORT ;
  - OE.SCP.IC ;
  - OE.SCP.RECOVERY.
- all security functional requirement from [PP JCS_O].

Any evaluation that wants to claim conformance to the [PP USIM] shall include in its TOE, the operating system (OS) and the IC, according to the representation of chapter 1.3.
Thus, a security target conformant to [PP USIM] will have

- to describe the security objective for the operational environment OE.SCP.SUPPORT from [PP USIM] as security objective on the TOE ;
- to describe the following security objectives for the operational environment from [PP JCS_O] as security objectives on the TOE :
  - OE.SCP.IC ;
  - OE.SCP.RECOVERY ;
- to identify the security functional requirements related to the IC and OS derived from the correspondent security objectives.

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 2010 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable, for smart cards and similar devices, up to ITSEC E6 High 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, 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

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 Developmentt	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	**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
	ALC_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 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**	1	**3**	3	**4**	**1**	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**	Independent testing: sample
AVA Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Focused 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 3.0, 8th January 2010, Management Committee.
[PP USIM]	(U)SIM Java Card Platform Protection Profile – Basic and SCWS Configurations, ref. PU-2009-RT-79, version 2.0.2.
[PP JCS_O]	Java Card System - Open Configuration Protection Profile, version 2.6, 19th April 2010. *Certified by ANSSI under the reference ANSSI-CC-PP-2010/03.*
[ETR]	Protection Profile evaluation detailed technical report - Project: USIM, ref. USI_APE, révision 6.0.