PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-PP 2010/05 du profil de protection pour plateforme (U)SIM Java Card en configuration SCWS (réf. PU-2009-RT-79, version 2.0.2)

Paris, le 12 juillet 2010,

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.
Un profil de protection est un document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

Toute correspondance relative à ce rapport doit être adressée au :

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

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-PP 2010/05

Nom du profil de protection

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

Référence/version du profil de protection

Ref PU-2009-RT-79 / version 2.0.2

Conformité à un profil de protection

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

Critères d'évaluation et version

Critères Communs version 3.1, révision 3

Niveau d'évaluation imposé par le PP

EAL 4 augmenté
ALC_DVS.2, AVA_VAN.5

Rédacteur

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

Commanditaire

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

Centre d'évaluation

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

Accords de reconnaissance applicables

CCRA **SOG-IS**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Table des matières

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : (U)SIM Java Card Platform Protection Profile - SCWS Configuration
Référence, version : PU-2009-RT-79, version 2.0.2
Date : 17 juin 2010

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Labs S.A.S.

5 rue du Bailliage
78000 Versailles
France

1.3. Description du profil de protection

La cible d'évaluation (TOE) définie dans ce PP correspond à une plateforme (U)SIM[1] Java Card ™ ouverte embarquée dans une carte (U)SIM destinée à être insérée dans un téléphone portable ou tout autre équipement téléphonique.

L'utilisation de ce profil de protection permettra la certification Critères Communs, jusqu'au niveau EAL4+, d'applications sécuritaires chargées sur des plateformes (U)SIM Java Card préalablement certifiées. Ces applications sécuritaires pourront coexister, dans ces cartes certifiées, avec des applications non sécuritaires (ces dernières ne seront pas certifiées, mais elles devront néanmoins satisfaire aux contraintes imposées par la plateforme). La plateforme considérée ici étant ouverte, le chargement de ces applications pourra être réalisé après que les cartes auront été mises à disposition des utilisateurs finaux des équipements mobiles (en phase opérationnelle).

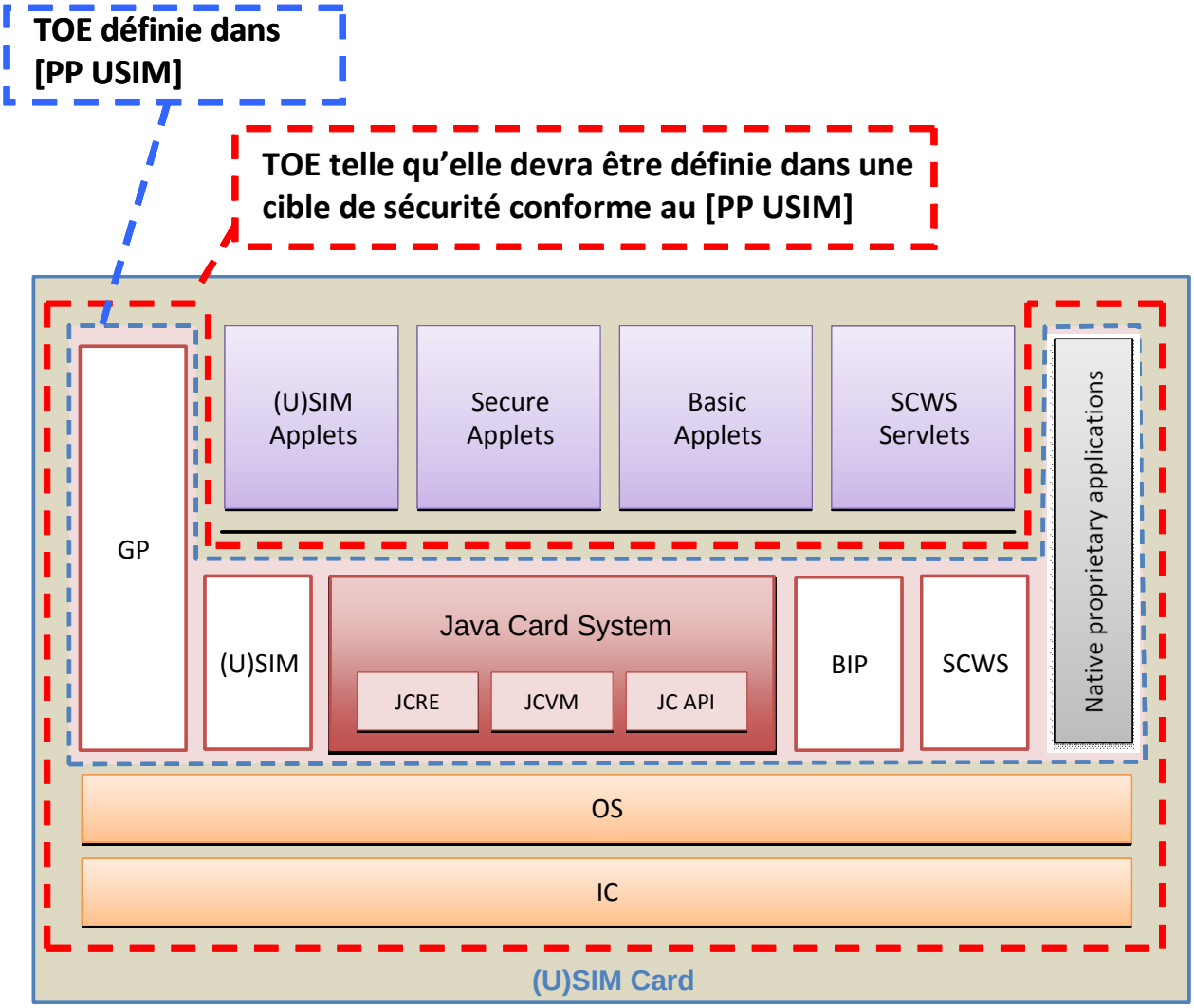
Ce profil de protection se concentre sur les exigences de sécurité de la plateforme (U)SIM Java Card. Le microcontrôleur (IC) et le système d'exploitation (OS) sont considérés dans ce PP en tant qu'environnement de la plateforme (U)SIM Java Card, c'est-à-dire couverts par des objectifs sur l'environnement du PP. Cependant, toute évaluation de carte selon ce PP devra inclure le tout dans la TOE : le microcontrôleur, le système d'exploitation, le code natif, a plateforme (U)SIM Java Card et toute application pré-chargée devront être inclus dans la TOE décrite dans la cible de sécurité qui réclame la conformité à ce PP, voir en 3.2 pour plus de détails.

[1] Universal Subscriber Identity Module

La TOE définie dans [PP USIM] en configuration SCWS est composée des éléments suivants :

- un système Java Card, conforme au profil de protection [PP JCS_O], qui permet la gestion et l'exécution d'applications Java Card (applets), et qui fournit une interface de programmation (API[1]) permettant de développer des applets destinées à être chargées sur le system Java Card conformément aux spécifications Java Card ;
- un paquetage GlobalPlatform (GP), qui fournit, aux applications accueillies par la carte, une interface standardisée permettant les communications avec le monde extérieur, en particulier pour le chargement d'applets, ainsi qu'une gestion sécurisée de ces applications ;
- une interface de programmation (API) (U)SIM qui permet l'échange de données entre les applications (U)SIM et le réseau mobile, dont notamment le téléchargement d'applications à partir de SMS[2] ou de la technologie BIP (les éventuels services de sécurité offerts par cet éléments ne correspondent pas à des fonctions de sécurité à évaluer au titre du [PP USIM]) ;
- la technologie BIP[3] qui permet l'échange de données "*Over The Air*" (OTA) entre les cartes (U)SIM d'un réseau mobile et des serveurs distants (les éventuels services de sécurité offerts par cet éléments ne correspondent pas à des fonctions de sécurité à évaluer au titre du [PP USIM]) ;
- un serveur Web SCWS (*Smart Card Web Server*) qui permet aux utilisateurs finaux d'accéder à la carte (U)SIM et à ses applications à travers un navigateur Web de son téléphone mobile ;
- les applications natives, si elles existent, qui s'exécutent sur l'OS de la carte (ces applications ne fournissent aucune fonction de sécurité à évaluer au titre du [PP USIM]).

[1] Application Programming Interface
[2] Short Message Service
[3] Bearer Independent Protocol


TOE définie dans [PP USIM]
TOE telle qu'elle devra être définie dans une cible de sécurité conforme au [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. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies par le profil de protection sont les suivantes :

- 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).

Une cible de sécurité conforme au [PP USIM] devra également décrire les exigences fonctionnelles de sécurité suivantes du [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).

Toutes les exigences fonctionnelles du profil de protection sont extraites de la partie 2 des Critères Communs [CC].

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL4 augmenté des composants d'assurance suivants**[1] :

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

Tableau 1 - Augmentations

Toutes les exigences d'assurance imposées par le profil de protection sont extraites de la partie 3 des Critères Communs [CC].

[1] Voir l'0 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Commanditaire

Société Française du Radiotéléphone (SFR)

1 place Carpeaux
Tour Séquoia
92915 Paris La Défense
France

2.3. Centre d'évaluation

THALES – CEACI (T3S – CNES)

18 avenue Edouard Belin
BPI 1414
31401 Toulouse Cedex 9
France

Téléphone : +33 (0)5 62 88 28 01 ou 18

Adresse électronique : nathalie.feyt@thalesgroup.com

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 5 juillet 2010, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives aux composants d'assurance ci-dessous sont à « **réussite** ».

Composants	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 - Evaluation du PP

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

3.2. Recommandations et limitations d'usage

Le [PP USIM] est conforme au [PP JCS_O]. La TOE décrite par le [PP USIM] doit inclure un système javacard ouvert conforme au [PP JCS_O]. Pour une meilleure lisibilité du PP, tous les éléments du [PP JCS_O] qui doivent être directement repris dans une cible de sécurité conforme au [PP USIM] ne sont pas explicitement identifiés dans ce PP (des guides pour la rédaction sont cependant disponibles dans ce PP).
Ainsi, le rédacteur d'une cible de sécurité conforme au [PP USIM] devra reprendre dans cette cible :

- toutes les menaces du [PP JCS_O], hormis T.PHYSICAL ;
- toutes les hypothèses du [PP JCS_O] ;
- toutes les politiques de sécurité organisationnelle (OSP) du [PP JCS_O] ;
- tous les objectifs sur la TOE du [PP JCS_O] ;
- tous les objectifs sur l'environnement opérationnel du [PP JCS_O] hormis :
  - OE.CARD-MANAGEMENT ;
  - OE.SCP.SUPPORT ;
  - OE.SCP.IC ;
  - OE.SCP.RECOVERY;
- toutes les exigences fonctionnelles de sécurité du [PP JCS_O].

Toute évaluation de produit selon le [PP USIM] devra inclure dans sa TOE le système d'exploitation (OS) et le microcircuit (IC) conformément à la figure du paragraphe 1.3.
Une cible de sécurité conforme à ce [PP USIM] devra donc :

- décliner l'objectif de sécurité sur l'environnement opérationnel OE.SCP.SUPPORT du [PP USIM] en tant qu'objectif de sécurité de la TOE ;
- décliner les objectifs de sécurité sur l'environnement opérationnel suivants du [PP JCS_O] en tant qu'objectifs de sécurité de la TOE :
  - OE.SCP.IC ;
  - OE.SCP.RECOVERY ;
- décliner les objectifs de sécurité relatifs au système d'exploitation et au microcircuit en exigences fonctionnelles de sécurité.

3.3. Reconnaissance européenne (SOG-IS)

Ce rapport de certification est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.4. Reconnaissance internationale (CC RA)

Ce rapport de certification est émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

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_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	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 procedures
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
	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 Evaluation de la cible de sécurité	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 Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Focused vulnerability analysis

Annexe 2. Références

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CPP/P/01]	Procédure CPP/P/01 Certification de profils de protection, 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, 8 Janvier 2010, Management Committee.
[PP USIM]	(U)SIM Java Card Platform Protection Profile – Basic and SCWS Configurations, réf. PU-2009-RT-79, version 2.0.2.
[PP JCS_O]	Java Card System - Open Configuration Protection Profile, version 2.6, 19 avril 2010. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03.*
[RTE]	Protection Profile evaluation detailed technical report - Project: USIM, réf. USI_APE, révision 6.0.