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

Rapport de certification ANSSI-CC-2011/82

ID One ePass v2.2 en configuration BAP et AA sur composant ST23YR18A

Paris, le 23 juillet 2011

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

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-2011/72

Nom du produit

ID One ePass v2.2 en configuration BAP et AA sur composant ST23YR18A

Référence/version du produit

Code ROM : 075481
Code optionnel : 076842

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3

Développeurs

Oberthur Technologies
71-73, rue des Hautes Pâtures,
92726 Nanterre Cedex

STMicroelectronics
190 Avenue Célestin Coq, ZI de Rousset, BP2,
13106 Rousset Cedex
France

Commanditaire

Oberthur Technologies
71-73, rue des Hautes Pâtures,
92726 Nanterre Cedex

Centre d'évaluation

Serma Technologies
30 avenue Gustave Eiffel, 33608 Pessac, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

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 disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « ID One ePass v2.2 en configuration BAP et AA sur composant ST23YR18A » développé par Oberthur Technologies sur un composant STMicroelectronics.

Le produit évalué est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de permis de conduire électronique. Ce produit est destiné à vérifier l'authenticité du permis de conduire à l'aide d'un système d'inspection.
Ce microcontrôleur et son logiciel embarqué peuvent être intégrés sous forme de module ou d'*inlay*. Le produit final peut être un permis de conduire, une carte plastique, etc.

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité s'inspire du profil de protection [PP BAC]. Le commanditaire a considéré que la problématique de sécurité du produit « permis de conduire » était proche de celle du passeport et que l'utilisation du [PP BAC] était pertinente pour l'établissement de cette cible de sécurité.

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments listés dans [GUIDES]. En réponse à la commande GET DATA de valeur DF52 les 17 premiers octets doivent être DF52 0C 5A 01 00 075681 303736383432 dont le détail est le suivant :

- rappel des données du GET DATA : **DF 52**;
- information sur la taille de la réponse : **0C** ;
- numéro du masque : **5A** ;
- version du masque : **01** ;
- *« LDS configuration »* : **00** ;
- code SAAAAR du ROM code : **075481** ;
- code SAAAAR du code optionnel (Codop) : **303736383432**[1].

[1] code ASCII du code SAAAAR 076842 attendu.

La TOE peut aussi être identifiée comme suit :

Configuration		Source
Nom commercial de la TOE	ePass v2.2 on ST23YR18 in BAP configuration with Active Authentication	Oberthur Technologies
Label PVCS du ROM code	Epass_YR18_015	
Code SAAAAR du ROM code	075481	
Label PVCS du Codop	Epass_YR18_016	
Code SAAAAR du Codop	076842	
Identification du circuit integré	ST23YR18A	STMicroelectronics
Référence du masque (label IC)	RVS	

1.2.3. Services de sécurité

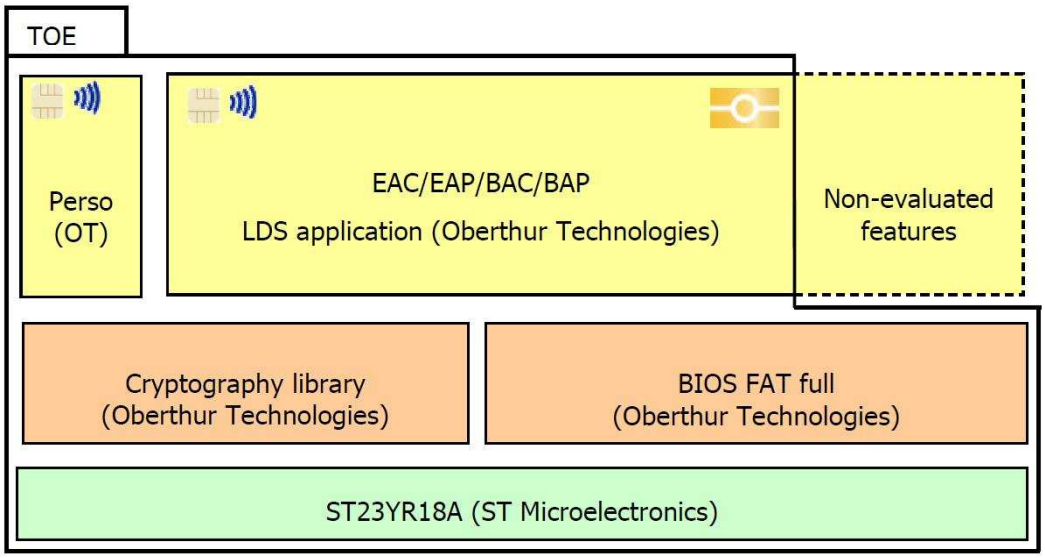
Les principaux services de sécurité fournis par le produit sont :
- le contrôle d'accès en lecture et en écriture ;
- le mécanisme BAP ;
- le mécanisme de « *secure messaging* » ;
- l'authentification de l'agent de personnalisation ;
- l'authentification active[1] (si activée) ;
- la protection physique.

1.2.4. Architecture

Le produit est une carte à puce fermée constituée des éléments suivants :
- un microcontrôleur (ST23YR18A de STMicroelectronics) ;
- une application native « *BIOS FAT full* » donnant l'accès aux fonctionnalités du microcontrôleur ;
- une librairie cryptographique dédiée ;
- une application de personnalisation *Perso* ;
- l'application LDS[2] supportant les mécanismes EAC, EAP, BAC et BAP et dont certaines fonctionnalités ne font pas partie de la TOE.

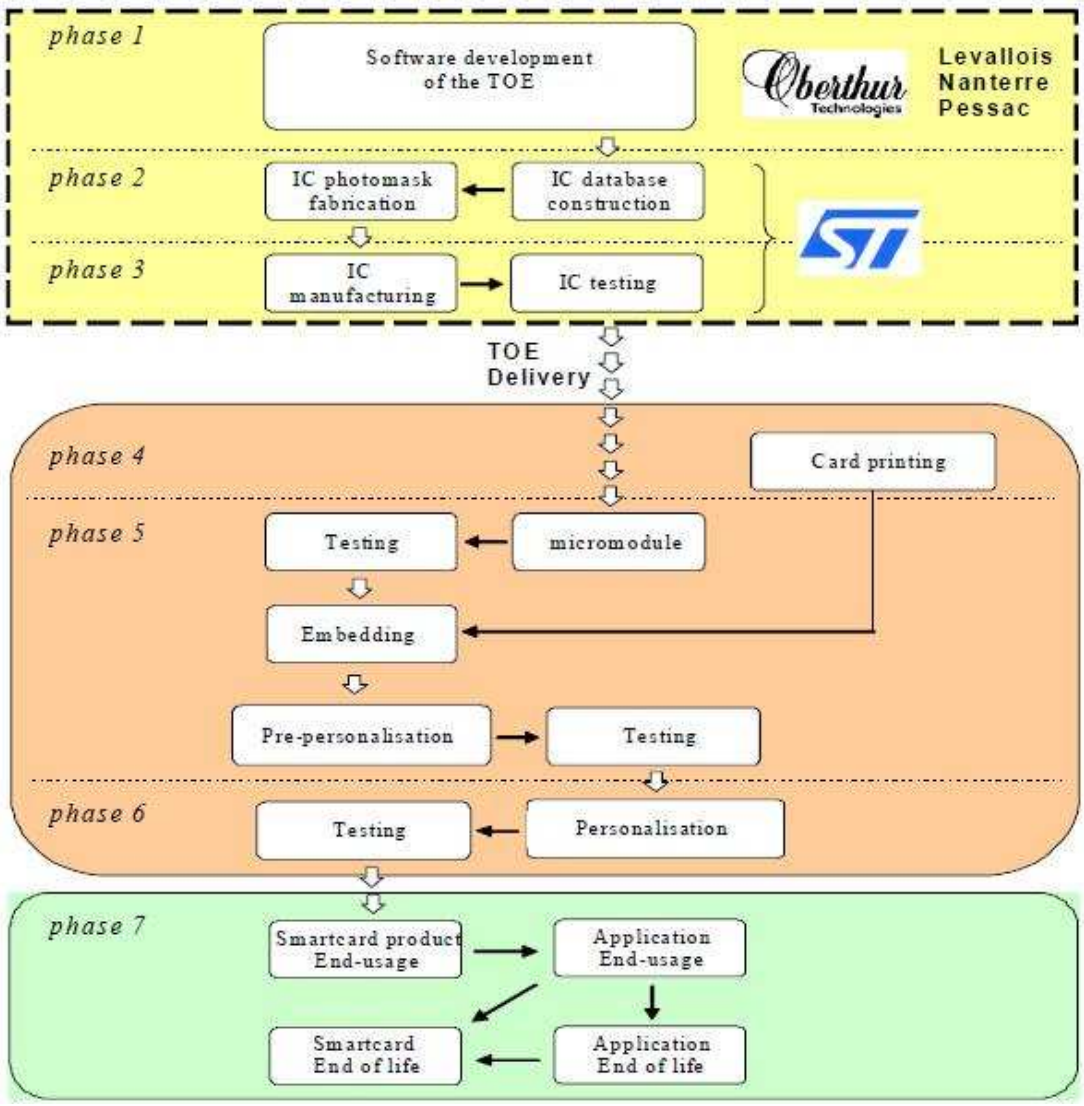
[1] *Active authenticate*
[2] *Logical Data Structure*

La figure suivante représente cette architecture :



1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :



Les composants logiciels du produit ont été développés sur les site suivants :

Oberthur Technologies – Site de Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies – Site de Levallois

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies – Site de Pessac
Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus – Porte 2
33600 Pessac
France

Le microcontrôleur a été développé et fabriqué par STMicroelectronics sur ses sites (voir [ANSSI-CC-2010/03]).
Les « administrateurs du produit » sont les nations ou organisations émettrices du document électronique.
Les « utilisateurs du produit » sont les systèmes d'inspection pendant la phase d'utilisation.

1.2.6. Configuration évaluée

Le certificat porte sur le produit présenté au chapitre 1.2.1 en configuration fermée.
L'évaluation n'a porté que sur la configuration BAP avec le mécanisme d'*active authenticate* activé.

2. L'évaluation

2.1. Référentiels d'évaluation

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

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [CC AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « ST23YR18A » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP0035]. Ce microcontrôleur a été certifié le 19 avril 2010 sous la référence [ANSSI-CC-2010/03].
Le niveau de résistance du microcontrôleur a été confirmé en juin 2011 dans le cadre du processus de surveillance, voir [SUR_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 23 juin 2011, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était en dehors du périmètre de l'évaluation et n'a pas été analysé. Le générateur d'aléas utilisé par le produit final a cependant été évalué dans le cadre de l'évaluation du microcontrôleur (voir [ANSSI-CC-2010/03]).

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.

Ce certificat atteste que le produit « ID One ePass v2.2 en configuration BAP et AA sur composant ST23YR18A » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2, ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 et ATE_DPT.3.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat 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 :

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

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], 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 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**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal 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	**5**	Development tools 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_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation
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**	**2**	**3**	3	**4**	**3**	Testing modular 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 Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cayenne security target BAP, version 2, référence FQR 110 5572, 26 avril 2011. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Cayenne BAP Security Target Lite, version 1, référence FQR 110 6069, 2011.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – Cayenne Project, référence : CAYENNE_ETR_v1.0 / 1.0, 23 juin 2011.
[CONF]	Configuration List, version 1, référence développeur FQR : 110 5602.
[GUIDES]	Guide d'administration du produit : - CAYENNE Administration and Personalization Guidance Document, version 3, référence FQR 110 5617 ; Guide d'utilisation du produit : - CAYENNE GUIDANCE, version 1, référence FQR 110 5622.
[ANSSI-CC-2010/03]	Microcontrôleurs sécurisés ST23YR18A. *Certifié par l'ANSSI le 19 avril 2010 sous la référence ANSSI-CC-2010/03*.
[SUR_IC]	Surveillance des produits « Microcontrôleurs sécurisés ST23YR18A », juin 2011 éditée par l'ANSSI.
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[PP BAC]	Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.10, 25 Mars 2009. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0055-2009.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure 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, 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 IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[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.
[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 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.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.