PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2007/07

Microcontrôleur sécurisé ST19NA18C

Paris, le 28 mars 2007

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), 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 nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr

Référence du rapport de certification

2007/07

Nom du produit

Microcontrôleur sécurisé ST19NA18C

Référence/version du produit

ST19NA18 revision C microcontroller (dedicated software ZSC, maskset K7L0A)

Conformité à un profil de protection

PP/9806 – PP BSI-PP-002-2001

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeur(s)

STMicroelectronics

Smartcard IC division, ZI de Rousset, BP2, 13106 Rousset Cedex, France

Commanditaire

STMicroelectronics

Smartcard IC division, ZI de Rousset, BP2, 13106 Rousset Cedex, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 64, mél : m.dus@serma.com

Accords de reconnaissance applicables

CCRA

SOG-IS

IT Security Certified

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 le microcontrôleur sécurisé ST19NA18 en révision C développé par STMicroelectronics. Le microcontrôleur inclut une partie logicielle en ROM intégrant des logiciels de tests du microcontrôleur (autotest) et des bibliothèques (gestion du système, services cryptographiques).

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
Cette cible de sécurité est conforme aux profils de protection [PP9806] et [PP0002].

1.2.1. 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 suivants, visibles au microscope sur les puces :

- identification de la puce (maskset) : K7L0A ;
- référence du logiciel dédié : ZSC ;
- référence du logiciel embarqué : dépendant de l'application masquée en ROM ;
- identification du site de fabrication : STMicroelectronics_4 (Rousset).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- initialisation de la plate-forme matérielle et des attributs ;
- gestion sécurisée du cycle de vie ;
- intégrité logique du produit (dont l'intégrité des mémoires) ;
- tests des fonctions de sécurité ;
- authentification de l'administrateur ;
- stockage et firewall de contrôle d'accès ;
- détection des attaques (dont les attaques par injections de fautes) ;
- réactions aux événements de sécurité ;
- non-observabilité ;
- support au chiffrement cryptographique à clés symétriques ;
- support au chiffrement cryptographique à clés asymétriques ;
- génération de nombres aléatoires.

1.2.3. Architecture

Le microcontrôleur ST19NA18C est constitué des éléments suivants :

- une partie matérielle composée :
  - d'un processeur 8-bits ;
  - de mémoires : 18KB de mémoire EEPROM (avec contrôle d'intégrité) pour le stockage des programmes et des données, 128KB de mémoire ROM pour le stockage des programmes utilisateurs, 4KB de mémoire RAM et 32KB de mémoire ROM pour le stockage des logiciels dédiés (logiciel de test et bibliothèque cryptographique) ;
  - de modules de sécurité : contrôle logique d'accès aux mémoires (SMACL), générateur d'horloge, contrôle de la sécurité, gestion de l'alimentation, contrôle d'intégrité des mémoires, détection de fautes ;
  - de modules fonctionnels : 3 compteurs 8-bits, gestion des entrées/sorties en mode contact (IART ISO 7816-3), générateurs de nombres aléatoires (TRNG), co-processeurs DES et RSA.
- une partie « logiciels dédiés » en ROM intégrant :
  - des logiciels de tests du microcontrôleur («autotest») ;
  - des utilitaires pour la gestion du système et de l'interface hardware/software ;
  - des services cryptographiques DES (implémentation E-DES), AES (implémentation E-AES) et RSA inclus dans la cible de sécurité du produit.

1.2.4. Cycle de vie

Le cycle de vie du développement est résumé dans le schéma suivant :

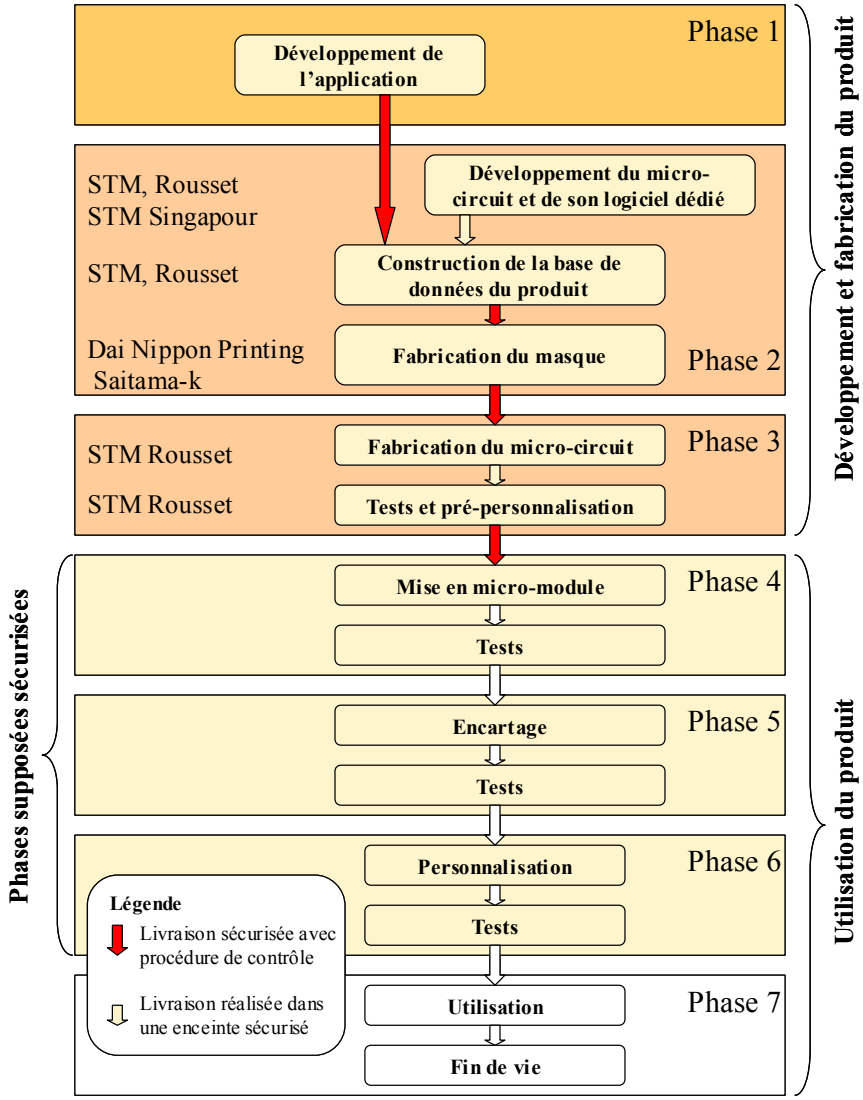

Figure 1 - Cycle de vie standard d'une carte à puce

Le produit est développé, intégré (préparation de la base de données du produit), fabriqué et testé par :

STMicroelectronics

Smartcard IC division
ZI de Rousset, BP2
13106 Rousset Cedex
France

Une partie du développement du produit est réalisée par :

STMicroelectronics

5A Serangoon North Avenue 5,
Singapore 554574
Singapour

Les réticules du produit sont fabriqués par :

DAI NIPPON PRINTING CO., LTD

2-2-1, Fukuoka, kamifukuoka-shi,
Saitama-Ken, 356-8507
Japon

Le produit comporte lui-même une gestion de son cycle de vie fonctionnel, prenant la forme de trois configurations d'utilisation :

- configuration «Test» : à la fin de sa fabrication, le microcontrôleur est testé à l'aide du logiciel de test présent en ROM. Les données de pré-personnalisation peuvent être chargées en EEPROM. Ce mode est ensuite bloqué de manière irréversible lors du passage en configuration «Issuer» ;
- configuration «Issuer» : mode utilisé lors des phases d'encartage et de personnalisation du microcontrôleur. Certains tests internes du microcontrôleur sont encore disponibles. Les données de personnalisation peuvent être chargées en EEPROM. Ce mode est ensuite bloqué de manière irréversible lors du passage en configuration «User» ;
- configuration «User» : mode final d'utilisation du microcontrôleur qui fonctionne alors sous le contrôle du logiciel embarqué de la carte à puce. Le logiciel de test n'est plus accessible. Les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans cette configuration.

1.2.5. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur et à son logiciel dédié identifié au §1.1.
Toute application, éventuellement embarquée pour les besoins de l'évaluation, ne fait pas partie du périmètre d'évaluation.
En regard du cycle de vie, le produit évalué est celui qui sort de la phase de fabrication, tests et pré-personnalisation (phase 3).
Pour les besoins de l'évaluation, le microcontrôleur ST19NA18C a été fourni au centre d'évaluation avec un système d'exploitation logiciel dédié (Card Manager), dans un mode dit « ouvert[1] ».

[1] Mode permettant de charger et d'exécuter du code natif en EEPROM et de déconnecter les mécanismes sécuritaires paramétrables.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par la DCSSI et compatibles avec le document [AIS34] ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CCIC] et [CCAP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation du microcontrôleur sécurisé ST19NR66B certifié en 2006 sous la référence 2006/27 (cf. [2006/27]).

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 19 mars 2007, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

2.4. Analyse du générateur d'aléas

Le produit évalué offre un générateur d'aléas qui peut être utilisé par le logiciel embarqué.
Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS31] et [FIPS 140] par le centre d'évaluation.
Le générateur est de classe « P2 – *SOF-high* » selon l'[AIS31], et atteint le niveau « Level 3[1] » selon la [FIPS 140].

[1] Seul le sous-ensemble du [FIPS 140] relatif aux générateurs de nombres aléatoires a été évalué et uniquement au travers des tests statistiques spécifiés dans cette norme.

3. La certification

3.1. Conclusion

L'évaluation, identifiée au chapitre 2 et décrite dans le rapport technique d'évaluation [RTE], a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises par 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 microcontrôleur sécurisé ST19NA18C soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté.

3.2. Restrictions d'usage

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

Ce certificat donne une appréciation de la résistance du produit ST19NA18C à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

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

- des procédures sécuritaires doivent être utilisées lors de la distribution du produit aux utilisateurs afin de maintenir la confidentialité et l'intégrité du produit et de ses données de fabrication et de test (pour prévenir toute copie, modification, conservation, vol ou usage non autorisés) ;
- la communication entre un produit développé sur le microcontrôleur sécurisé et d'autres produits doit être sécurisée (en termes de protocole et de procédure) ;
- le système (terminal, communication,…) doit garantir la confidentialité et l'intégrité des données sensibles qu'il stocke ou qu'il traite.

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 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat 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 Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, la Corée du Sud, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Nouvelle-Zélande, la Norvège, les Pays-Bas, 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 5+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**3**	Development tools CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**3**	Semiformal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**3**	Semiformal high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**	**1**	Modularity
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**2**	Semiformal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**3**	Formal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**2**	Standardised life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**2**	Testing: low-level 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_CCA					**1**	**2**	2	**1**	Covert channel analysis
	AVA_MSU			**1**	**2**	2	**3**	3	**3**	Analysis and testing of insecure states
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**4**	Highly resistant

Annexe 2. Références documentaires du produit évalué

[2006/27]	Rapport de certification 2006/27 - Microcontrôleur sécurisé ST19NR66B, 8 décembre 2006, SGDN/DCSSI
[ST]	Cible de sécurité de référence pour l'évaluation : - ST19NA18 Security Target, Référence : SMD_ST19NA18_ST_06_001 V01.00 STMicroelectronics Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST19NA18 Security Target – Public version, Référence : SMD_ST19NA18_ST_07_001 V01.01 STMicroelectronics
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – ST19NA18C – (EAL5+ evaluation), Référence : YQM_ETR_NA18C_v1.2 Serma Technologies Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validée : - ETR Lite for Composition, ST19NA18C (EAL5+ evaluation) Référence : YQUEM_ETR lite ST19NA18C_v1.1 Serma Technologies
[CONF]	Liste de configuration du produit : - Configuration List ST19NA18C PRODUCT, Référence : SCP_ST19NA18C_CFGL_06_001 V01.03 STMicroelectronics Liste de la documentation : - Yquem evaluation –Documentation report (ST19NA18C), Référence : SMD_NA18_DR_06_001 V01.04 STMicroelectronics
[GUIDES]	Les guides sont constitués des documents suivants : - ST19NA18 Smartcard MCU with MAP, IART, High Speed CPU Clock & 18 KBytes High Density EEPROM, Référence : DS_19NA18/0702 Rev. 9 STMicroelectronics - ST19NA18 - Security Application Manual, Référence : APM_19NA18_SECU/0702 Rev. 1 STMicroelectronics - ST19W - System ROM –Issuer configuration - user manual, Référence : UM_19W_SR_I/0306VP2 STMicroelectronics ST19W - System ROM - Issuer configuration - user manual

	addendum, Référence : AD_UM_19W_SR_I/0308V1.1 STMicroelectronics - ST19W - System ROM –Issuer configuration - user manual addendum 2, Référence : AD2_UM_19W_SR_I/0702V1.0 STMicroelectronics - ST19N System Library V2 User Manual, Référence : Um_19N_SysLibV2/0610 Rev 3 STMicroelectronics - ST19X, ST19W and 19N EDES Library User Manual, Référence : UM_19X_EDESLIB/0605 Rev 2 STMicroelectronics - ST19N - Fast Cryptographic Library FastLIB4 – User Manual, Référence : UM_19N_FASTLIB4/0605 Rev 3 STMicroelectronics - Information Note, Référence : SE_IN_06_004 V1.01 STMicroelectronics - ST19W and ST19N AES Library - User Manual, Référence : UM_19W_19N_AES/0610 Rev 2 STMicroelectronics - AIS31 Compliant Random Numbers on ST19N Products - User Manual, Référence : UM_19N_AIS31_CRN/0702 V1 STMicroelectronics
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certifié sous la référence PP/9806.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié sous la référence BSI-PP-0002-2001.*

Annexe 3. Références liées à la certification

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.	
[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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[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.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004 Bundesamt für Sicherheit in der Informationstechnik
[AIS31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, Bundesamt für Sicherheit in der Informationstechnik

[FIPS 140]	Security Requirements for Cryptographic Modules Référence : FIPS PUB-140-2:1999 NIST.