Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2007/01

Microcontrôleur sécurisé ATMEL AT90SC6408RFT rev. E

Paris, le 15 janvier 2007

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ Ti 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 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

2007/01

Nom du produit

Microcontrôleur sécurisé ATMEL AT90SC6408RFT rev. E

Référence/version du produit

AT90SC6408RFT, référence AT58848 révision E

Conformité à un profil de protection

PP/9806

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeur(s)

ATMEL Smart Card ICs

Maxwell Building - Scottish Enterprise technology Park
East Kilbride, G75 0QR - Ecosse, Royaume-Uni

Commanditaire

ATMEL Smart Card ICs

Maxwell Building - Scottish Enterprise technology Park
East Kilbride, G75 0QR - Ecosse, Royaume-Uni

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France
Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr

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 AT90SC6408RFT, référence AT58848 révision E.

Ce microcontrôleur appartient à la famille de produits AVR ASL4 développée par Atmel SmartCard Ics.

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 au profil de protection [PP9806].

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 :

- Nom du produit : AT90SC6408RFT, et son numéro d'identification : AT58848. Cette information peut être vérifiée en utilisant le registre de numéro de série SN_0, qui contient la donnée hexadécimale 0x26 (voir [GUIDES], document « AT90SC6408RFT Datasheet » section 21.1.1.).
- Silicium révision E. Contrairement aux spécifications décrites dans le document « AT90SC6408RFT Datasheet », cette information ne peut pas être vérifiée en utilisant le numéro de série SN_1. ATMEL propose donc le processus suivant : les clients contactent ATMEL avec l'information « batch number » (Registre SN_2 à SN_8). ATMEL enverra alors les données d'identification (révision silicium).
- Le produit lui-même peut être physiquement identifié par ses numéros de réticules identifiés dans le document « Patern and mask list » (cf. [CONF]), et visibles au microscope sur la surface métallique du produit.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- procédure d'entrée en mode « test » ;
- protection du contenu des mémoires en mode « test » ;
- désactivation du mode « test » ;
- test du produit ;

- détection des erreurs ;
- pare-feu ;
- audit d'évènements ;
- actions associées aux évènements ;
- non observabilité ;
- cryptographie ;
- procédure d'entrée en mode « diagnostic » ;
- protection du contenu des mémoires en mode « diagnostic ».

1.2.3. Architecture

Le microcontrôleur AT90SC6408RFT est constitué des éléments suivants :

- processeur AVR Risc ;
- 64ko de mémoire ROM pour le stockage des programmes ;
- 8ko de mémoire EEPROM pour le stockage des programmes et des données avec 64 octets d'OTP (mémoire inscriptible, non effaçable en mode « utilisateurs », pour stocker les données sensibles par exemple, ou servir de verrous sur les phases du cycle de vie notamment) et 192 octets accessibles par bit, une pompe de charge et ses oscillateurs ;
- 1ko de mémoire RAM statique utilisateur ;
- un accélérateur de calcul de checksum 32 bits (support à la détection d'erreurs sur les données ou programmes en mémoire) ;
- un périphérique CRC-16/32 (support à la détection d'erreurs sur les données ou programmes en mémoire) ;
- un générateur de nombres aléatoires ;
- un accélérateur de calcul cryptographique DES/3DES ;
- des détecteurs tension, fréquence, température et lumière ultraviolette ;
- un firewall protégeant l'accès à toutes les mémoires et tous les périphériques ;
- un régulateur de tension (le microcontrôleur fonctionne dans une gamme de tension de 3.0V à 5.0V) ;
- 3 Timers ;
- 1 port série avec une interface et un contrôleur conforme au standard ISO7816 ;
- 1 port RF, avec une interface et un contrôleur en mode sans contact conforme au standard ISO/IEC 14443 type A et B ;
- une structure de test dédiée, sciée lors de la mise en micro-module et accessible uniquement en mode test pour les tests de production.

1.2.4. Cycle de vie

Le cycle de vie du produit, inspiré du cycle de vie décrit dans le PP/9806 (cf. [PP9806]), est le suivant :

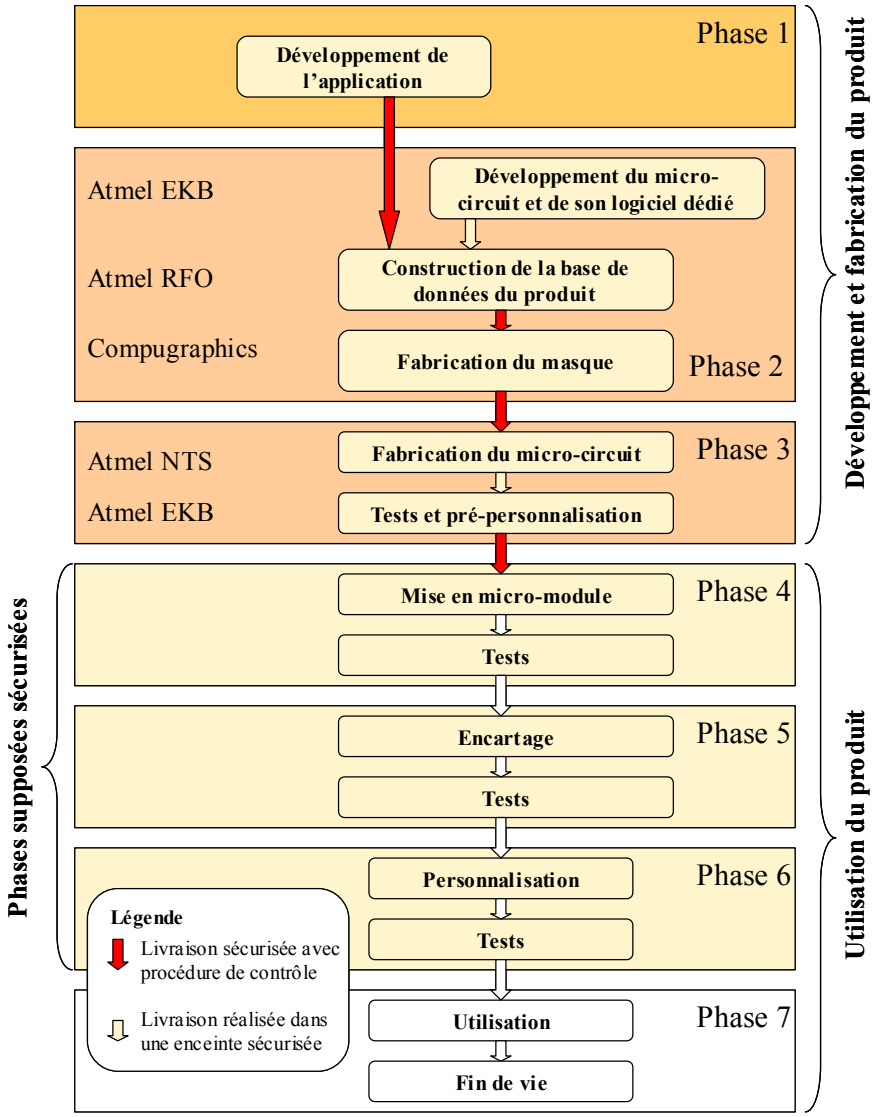

Figure 1 - Cycle de vie du produit

Le micro-circuit est développé et testé par :

Atmel East Kilbride

Maxwell Building
Scottish Enterprise technology Park
East Kilbride, G75 0QR
Ecosse, Royaume-Uni.

La base de données de fabrication du masque du micro-circuit est réalisée par :

Atmel Rousset

Z.I. Rousset Peynier
13106 Rousset Cedex
France.

Les réticules du micro-circuit sont fabriqués par :

Compugraphics International Ltd

Newark Road North
Eastfield industrial Estate
Glenrothes
Fife, KY7 4NT
Ecosse, Royaume-Uni.

Le microcontrôleur est fabriqué par :

Atmel North Tyneside

Middle Engine Lane
Silverlink business Park
North Tyneside, NE28 9N2
Royaume Uni

Le microcontrôleur comporte trois modes d'utilisation :

- un mode « Test », dans lequel le microcontrôleur fonctionne sous le contrôle d'un logiciel de test écrit en mémoire EEPROM à l'aide d'une interface de test et utilisé sous le contrôle d'un système de test externe. Ce mode requiert une authentification de l'administrateur. Il n'est utilisable que par le personnel autorisé de l'équipe du développement et dans un environnement sécurisé. Après la phase de test, le mode « test » est inhibé de façon irréversible par découpage du « wafer ». L'interface de test n'est alors plus accessible ;
- un mode « utilisateur », dans lequel le microcontrôleur fonctionne sous le contrôle du logiciel embarqué de la carte à puce. Les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans ce mode ;
- un mode « diagnostic », utilisé lors du retour de pièces défectueuses et permettant d'effectuer des tests à l'aide d'une interface de test utilisée sous le contrôle d'un système de test externe. Lors de l'activation de ce mode, le contenu des mémoires est effacé. Ce mode n'est utilisable que par le personnel autorisé de l'équipe du développement et dans un environnement sécurisé.

1.2.5. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur seul.
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 AT90SC6408RFT a été fourni au centre d'évaluation avec un système d'exploitation logiciel dédié, 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 ATMEL AT90SC320288RCT/AT90SC144144CT rev. G certifié en date du 16 novembre 2006 sous la référence 2006/20 (cf. [2006/20]).

Le rapport technique d'évaluation [RTE], délivré à la DCSSI le 22 décembre 2006, 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.

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 produit « AT90SC6408RFT, référence AT58848 révision E » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 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 AT90SC6408RFT 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 :

- 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 :

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

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[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 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 4+	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	**2**	Problem tracking 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**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal 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**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-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		
	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

[2006/20]	Rapport de certification 2006/20 - Microcontrôleur sécurisé ATMEL AT90SC320288RCT/AT90SC144144CT rev. G, 16 novembre 2006, SGDN/DCSSI
[ST]	Cible de sécuritéde référence pour l'évaluation : - Twister Security Target, Référence : Twister_ST_V1.3_12Dec06 ATMEL Smart Card ICs Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - AT90SC6408RFT Security Target Lite, Référence : TPG0141A_15Dec06 ATMEL Smart Card ICs
[RTE]	Rapport technique d'évaluation : - TWISTER Project - Evaluation Technical Report, Référence : LETI.CESTI.TWI.RTE.001 version 1.1 CESTI LETI Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validée : - TWISTER Project - Evaluation Technical Report Lite, Référence : LETI.CESTI.TWI.RTE.002 version 1.2 CESTI LETI
[CONF]	Liste de configuration du design : - Twister Design Configuration List, Référence : Twister_DCL_V1.1 ATMEL Smart Card ICs Liste de configuration de la fabrication : - Twister Manufacturing Configuration List, Référence : Twister_MCL_V1.1 ATMEL Smart Card ICs Liste des patterns et des masques : - Twister Pattern Mask List, Référence : Twister_PML_V1.1 ATMEL Smart Card ICs Liste des fournitures ATMEL : - Twister deliverables list, Référence : Twister Rev E _ EDL_15Dec06 ATMEL Smart Card ICs
[GUIDES]	Un document générique sert d'interface pour toute la documentation d'utilisation : - AT90SC CC AGD Interface, Référence : AT90SC_GUID_V1.4_05Jul05 ATMEL Smart Card ICs Les documents associés sont :

	- AT90SC6408RFT Datasheet, Référence : TPR0184AX_12Apr06 ATMEL Smart Card ICs - AT90SC Addressing Modes and Instruction Set, Référence : 1323C-03May04 ATMEL Smart Card ICs - Security Recommendations for AT90SC ASL4 Products, Référence : TPR0066G-05Jul05 ATMEL Smart Card ICs - Secured Hardware DES/TDES on AT90SC ASL4 Products, Référence : TPR0063FX-29Sep06 ATMEL Smart Card ICs - Generating unpredictable random numbers on the AT90SC family devices, Référence : 1573CX_SMIC_21mar03 ATMEL Smart Card ICs - Using the supervisor and user modes on the AT90SC ASL4 products, Référence : TPR0095A-11Mar03 ATMEL Smart Card ICs - Checksum Accelerator use on the AT90SC ASL4 products, Référence : TPR0065A-02Jul02 ATMEL Smart Card Ics - Wafer Saw Recommendations, Référence : TPG0079A_13Jun05 ATMEL Smart Card ICs
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certifié sous la référence PP/9806.*

Annexe 3. Certification references

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