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 DCSSI-2008/36

Microcontrôleur sécurisé ATMEL AT91SC464384RCU (AT58U21) rév. B

Paris, le 17 décembre 2008

Le Directeur central 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 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.gouv.fr

Référence du rapport de certification

DCSSI-2008/36

Nom du produit

Microcontrôleur sécurisé ATMEL AT91SC464384RCU

Référence / Version du produit

AT58U21 / Rév. B

Conformité à un profil de protection

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 4 augmenté

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

Développeur

ATMEL Secure Microcontroller Solutions

Maxwell Building - Scottish Enterprise technology Park

East Kilbride, G75 0QR - Ecosse, Royaume-Uni

Commanditaire

ATMEL Secure Microcontroller Solutions

Maxwell Building - Scottish Enterprise technology Park

East Kilbride, G75 0QR - Ecosse, Royaume-Uni

Centre d'évaluation

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Tél : +33 (0)5 61 28 16 51, mél : ceaci@cnes.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

La certification concerne le produit de type microcontrôleur sécurisé 32 bits portant la référence commerciale AT91SC464384RCU, issu de la famille AT91SC des composants pour cartes à puce. Il correspond à la puce de référence ATMEL interne AT58U21, en révision B, basée sur le cœur ARM SC100.

De manière générale, un 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, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

Les microcontrôleurs AT91SC464384RCU sont plutôt destinés à des cartes à puce supportant des applications de types bancaire, transactions sécurisées, télévision à péage ou contrôle d'accès, etc.

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.

La cible de sécurité déclare une conformité au profil de protection BSI-PP-002-2001 [BSI_PP] et s'inspire du document [BSI_AUG] pour définir certaines augmentations.

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 : AT91SC464384RCU, puce dont le numéro d'identification est : AT58U21. Cette information peut être vérifiée logiquement en comparant la valeur du registre IDREG à celle fournie dans les guides (cf. [GUIDES], « AT91SC464384RCU Technical Data Sheet » section 20.1.2).
- Silicium révision B. Cette information peut être vérifiée par une lecture d'un octet du registre de numéro de série SN_0 (cf. [GUIDES], « AT91SC464384RCU Technical Data Sheet » section 20.1.2).
- Le produit lui-même peut partiellement être physiquement identifié. Si l'identifiant « AT58U21 » est visible, la révision « rev B » et les numéros de réticules identifiés dans le document « Patern and mask list » (cf. [CONF]) sont cependant cachés derrière la grille de protection « Active Shield ».

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit évalué sont :

- identification unique du produit ;
- détection et contrôle des conditions environnementales (contre des attaques par injection de fautes) ;
- protection contre la fuite d'informations (contre des attaques par canaux auxiliaires) ;
- générateur physique de nombres aléatoires ;
- support cryptographique (triple DES) ;
- contrôle d'accès aux mémoires ;
- test du produit et contrôle d'accès au mode test.

1.2.3. Architecture

Le microcontrôleur AT91SC464384RCU est constitué des éléments hardware évalués suivants :

- processeur 32-bit ARM SC100 Enhanced RISC Architecture ;
- 384Ko de EEPROM interne, incluant 128 octets OTP et 384 octets accessibles par bit ;
- 464Ko de ROM ;
- 18Ko de RAM (dont 2Ko de RAM partagée) ;
- bus de données 32 bits pour instructions et données ;
- unité de protection mémoire (MPU) ;
- pare-feu ;
- oscillateur interne à fréquence variable (VFO) ;
- générateur hardware de nombre aléatoire (RNG) ;
- module harware DES/TDES incluant des mécanismes contre des attaques par canaux auxiliaires ;
- détecteurs de tension, fréquence, température et lumière ;
- protection contre les attaques physiques, incluant la grille de protection (Active Shield) ;
- moteurs CRC16 et CRC32 ;
- interfaces ISO7816 et SWP.

Les éléments du microcontrôleur AT91SC464384RCU ci-dessous n'ont pas été inclus par Atmel (cf. [ST]) ou non pas été testés par le CESTI dans le cadre de l'évaluation :

- la bibliothèque logicielle « Toolbox 02.03.12.01» chargée en ROM, fournissant une implémentation rapide de fonctions cryptographiques (RSA, SHA-1, etc.) basée sur l'accélérateur cryptographique AdvX, n'a pas été définie au sein de la TOE ;
- l'accélérateur cryptographique hardware « AdvX », offrant des primitives arithmétiques dédiées à des fonctionnalités cryptographiques à clé publique telles que RSA, DSA, génération de clé, ECC. Il n'était pas possible d'introduire l'AdvX dans la TOE puisque la Toolbox en était exclue ;
- bien que l'accélérateur Java du microcontrôleur AT91SC464384RCU ait été défini au sein de la TOE dans la cible de sécurité, celui-ci n'a pas été testé par le CESTI. L'évaluateur a jugé qu'il était plus approprié de considérer cette tâche (dont le verdict dépendra de l'OS et de l'application embarquée) lors d'une évaluation composite ;

- quant au module hardware DES/TDES, seul le triple DES (TDES) a été évalué (cf. le rapport ETR Lite [RTE]).

1.2.4. Cycle de vie

Le cycle de vie du produit est constitué de plusieurs phases qui s'opèrent sur différents sites du développeur.

Les entités impliquées dans le développement sont les suivantes :

- **Atmel East Kilbride (ATMEL EKB)**
  Maxwell Building
  Scottish Enterprise technology Park
  East Kilbride, G75 0QR
  Ecosse, Royaume-Uni

- **Atmel Rousset (ATMEL RFO)**
  Z.I. Rousset Peynier
  13106 Rousset Cedex
  France

- **Compugraphics**
  Newark Road North
  Eastfield Industrial Estate
  Glenrothes
  Fife KY7 4NT
  Ecosse

Les phases du processus de développement du produit qui s'inscrivent dans la cible d'évaluation peuvent être décrites comme suit :

Phase 1 :
- développement de l'application par le client.

Phase 2 :
- conception du circuit intégré et du logiciel dédié : ATMEL RFO ;
- gestion du code client : ATMEL EKB ;
- préparation des données pour les masques : ATMEL RFO ;
- fabrication des masques: COMPUGRAPHICS.

Phase 3 :
- fabrication du micro-circuit : ATMEL RFO FAB7 ;
- test paramétrique et réveil mémoire (P1) : ATMEL RFO ;
- test fonctionnel (P2/P3) : ATMEL EKB ;
- polissage et sciage des galettes de silicium : ATMEL EKB.

Les interactions entre ces phases de développement conduisent au transfert de biens sensibles, logiques (données de conception, code source) ou physiques (échantillons de produit en cours de développement).

Les livraisons suivantes doivent alors être sécurisées :
- logiciel dédié et guide au développeur de l'application ;
- code du logiciel embarqué au fabricant du microcontrôleur ;
- données requises par le fabricant des masques ;
- masques au fabricant du microcontrôleur ;
- microcontrôleur à l'entité qui réalise l'encapsulation.

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. 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.

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 4 dédiée à l'encapsulation de la puce dans un package tel qu'un micromodule par exemple.

Pour les besoins de l'évaluation, le microcontrôleur AT91SC464384RCU utilisé était un DIL avec la puce en face arrière portant la référence « AT58U21 BA silicon Rev B rom Engi A ». Ce microcontrôleur a été fourni au centre d'évaluation avec un système d'exploitation dédié aux tests dans un mode dit fermé[1] avec la référence « CCOS-SMFC EMVco Rev 2.2 ». L'évaluateur a pu néanmoins proposer ses propres fonctions, développées par la suite par Atmel, afin de réaliser des tests particuliers.

[1] Mode ne permettant pas à l'évaluateur 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].

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 [AIS 34], ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 12 août 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ». Suite à la levée d'une ambiguïté entre la cible de sécurité et le RTE concernant l'inclusion de l'interface SWP au sein de la cible d'évaluation et conformément à la demande de la DCSSI, l'évaluateur a fourni en complément du RTE [RTE] une analyse de la conception de cette interface SWP et l'a également testée conduisant à des résulats (cf. ETR_Lite du 14 novembre 2008 [RTE]) ne remettant pas en cause le verdict du RTE [RTE].

2.3. Analyse de la résistance des mécanismes cryptographiques

Le produit évalué offre des services cryptographiques identifiés §1.2.3 mais qui ne peuvent cependant pas être analysés d'un point de vue cryptographique car ils ne concourent pas à la sécurité propre du produit ; leur résistance dépend de leur emploi par l'application embarquée sur le microcontrôleur.

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 microcontrôleur sécurisé ATMEL AT91SC464384RCU de référence AT58U21 en révision B, soumis à l'évaluation (cf. §1.2 pour la configuration évaluée), répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants d'assurance ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4.

En particulier au regard d'une future composition (cf. §1.1), le microcontrôleur évalué est déclaré résistant à des attaques de haut niveau (VLA.4) seulement si les recommandations fournies dans les guides de sécurité associés à ce microcontrôleur [GUIDES] sont suivies par le développeur de logiciel embarqué.

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 AT91SC464384RCU 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 :

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[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, 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, la République de Corée, 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**	Validation of analysis
	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

[ST]	Cible de sécurité de référence pour l'évaluation : - LIGHTBIRD Security Target, Référence : LIGHTBIRD_ST_V1.3 (23 Jun 08), ATMEL
[RTE]	Le rapport technique d'évaluation : - ETR LIGHTBIRD, Référence: LIG_ETR_V1.0 (12 Aug 08) CEACI Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ETR Lite LIGHTBIRD, Référence: LIG_ETR_Lite_V4.0 (14 Nov 08) CEACI
[CONF]	- Lightbird Design Configuration List, Référence : Lightbird_DCL_V1.1 (7 May 08), ATMEL - Lightbird Manufacturing Configuration List, Référence : Lightbird_MCL_V1.1 (01 Apr 08), ATMEL - Lightbird Pattern and mask list, Référence : Lightbird_PML_V1.3 (7 May 08), ATMEL - Lightbird Development Tools Configuration List, Référence : Lightbird_DTCL_V1.0, ATMEL - Lightbird Configuration Management Plan, Référence : Lightbird_CMP_V1.0 (20 Feb 08), ATMEL - Lightbird CC Configuration Management (ACM Interface Document), Référence : Lightbird_ACM_V1.0 (16 Feb 08), ATMEL - Lightbird CC Delivery and Operation (ADO Interface Document) Référence : Lightbird_ADO_V1.0 (16 Feb 08),

	ATMEL
[GUIDES]	- AT91SC464384RCU Technical Datasheet, Référence : TPR0284BX (15 Jan 08), ATMEL - Security Recommendations for AT91SC464384RCU products, Référence : TPR0330CX, ATMEL - AdvX™ for AT91SC and AT91SO families datasheets, Référence : TPR0204AX (13 Apr 06), ATMEL - Secured Hardware DES/TDES on the AT91SC Products, Référence : TPR0353AX (18 Jan 08), ATMEL - Generating Unpredictable Random Numbers on the AT91SC464384RCU Product, Référence : TPR0331AX (28 Aug 07) ATMEL - ARM Developer Suite Assembler Guide, Référence : ARM DUI 0068B V1.2 ARM - ARM Developer Suite Compilers and Libraries Guide, Référence : ARM DUI 0067D V1.2 ARM - ARM Developer Suite Developer Guide, Référence : ARM DUI 0056D Rev D ARM - ARM Architecture reference manual, Référence : ARM DDI 0100E Rev E, ARM - SC100 technical reference manual, Référence : ARM DDI 0207A Rev A, ARM - Lightbird CC guidance documents (AGD interface document), Référence : Lightbird_AGD_V1.0 (09 Jun 08),

	ATMEL
[BSI_PP]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.*
[BSI_AUG]	Smartcard Integrated Circuit Platform Augmentations, version 1.0, mars 2002. *Développé par Atmel, Hitachi Europe, Infineon Technologies et Philips Semiconductors et édité par le BSI (Bundesamt für Sicherheit in der Informationstechnik).*

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, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2007-04-001 version 2.3, revision 1, April 2007.
[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 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.

[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik)