PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2008/15

Microcontrôleur CXD9916H3 / MB94RS403 & HAL Library pour carte sans-contact FeliCa

Paris, le 26 mai 2008

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.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

DCSSI-2008/15

Nom du produit

Microcontrôleur CXD9916H3 / MB94RS403 & HAL Library pour carte sans-contact FeliCa

Référence/version du produit

Microcontrôleur référence : CXD9916H3/MB94RS403 Version FR01 0001

Librairie logicielle : HAL Library Version 01

Conformité à un profil de protection

BSI-PP-0002-2001

Smart card IC Platform Protection Profile Version 1.0 July 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

Fujitsu Microelectronics Limited

1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, 211-8588, Japon

Commanditaire

Fujitsu Microelectronics Limited

1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, 211-8588, Japon

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

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 CXD9916H3 / MB94RS403 avec sa librairie logicielle HAL, développé par Fujitsu Microelectronics Limited.

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

Ce microcontrôleur est particulièrement destiné à être utilisé dans les cartes à puce sans-contact de type Felica (communication, transport et finance). Il est conforme à la norme ISO/IEC18092 « Passive Communication Mode of Contactless communication interface (212/424 kbps) ».

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 [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 :

- microcontrôleur référence : CXD9916H3/MB94RS403 Version FR01 0001 ;
- librairie logicielle : HAL Library Version 01.

Le produit est physiquement identifié par des caractères et des codes d'identification dessinés sur la couche de métal supérieure. La bibliothèque logicielle HAL comporte également une commande renvoyant les données d'identification. Ces données sont détaillées dans le rapport technique d'évaluation pour la composition (cf. [RTE]).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- générateur de nombres aléatoires déterministes (DRNG) 64 bits ;
- coprocesseur DES conforme au FIPS46-3, supportant les modes ECB ou CBC pour le chiffrement et le déchiffrement ;
- détection de fonctionnement en dehors des plages prévues de température, fréquence et tension ;

- détection et protection contre les intrusions physiques : grille active de protection contre le « probing » et les manipulations physiques, protection contre les fuites en canaux auxiliaires ;
- tests du microcontrôleur ;
- écriture des données d'identifications et de pré-personnalisation en mémoire FRAM ;
- contrôle d'accès aux mémoires ;
- brouillage des mémoires ;
- contrôle d'intégrité des mémoires FRAM.

1.2.3. Architecture

Le produit CXD9916H3 / MB94RS403 est constitué des éléments suivants :

- une partie matérielle composée :
  - d'un processeur 8-bits CISC F^2MC-8FX ;
  - de mémoires : 4Ko de mémoire FRAM (avec contrôle d'intégrité), 56KB de mémoire ROM, 3KB de mémoire RAM ;
  - de modules de sécurité : contrôle d'accès aux mémoires, contrôle d'intégrité des mémoires, détecteurs de sécurité (température, voltage, fréquence, probing) ;
  - de modules fonctionnels : gestion des entrées/sorties en mode sans contact « ISO/IEC 18092 Passive Communication Mode (212/424 kbps) », support à la génération de nombres aléatoires, co-processeurs DES.
- une partie « logiciels dédiés » en ROM intégrant :
  - une bibliothèque HAL (Hardware Abstraction Layer), incluant la génération déterministe de nombres aléatoires de 64 bits (conforme au standard ANSIX9.42-2001 Annex C.2) ;
  - des logiciels dédiés de tests du microcontrôleur.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

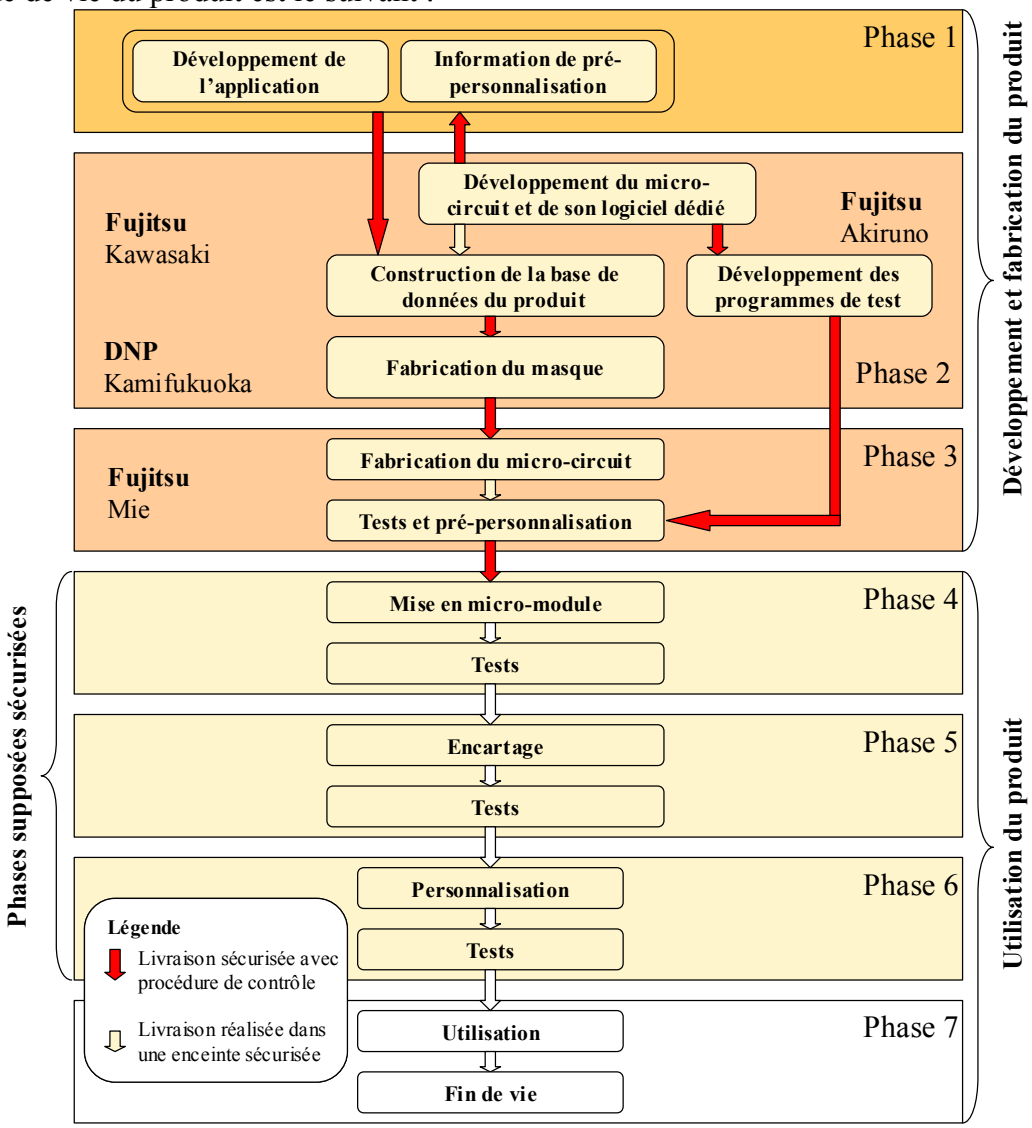

Figure 1 - Cycle de vie du produit

Le design du produit est réalisé par :

Fujitsu Microelectronics Limited - Kawasaki R&D Facilities

1-1, Kamikodanaka 4-chome, Nakahara-ku,
Kawasaki, 211-8588,
Japon

Le développement du programme de test est réalisé par :

Fujitsu Microelectronics Limited - Akiruno Technology Center

50 Fuchigami, Akiruno,
Tokyo, 197-0833,
Japon

Les réticules du microcontrôleur sont fabriqués par :

Dai Nippon Printing Limited - Kamifukuoka plant

2-2-1, Fukuoka, Kamifukuoka-shi,
Saitama, 356-8507,
Japon

Le produit est fabriqué et testé par :

Fujitsu Microelectronics Limited - Mie plant

1500, Mizono, Todo-cho, Kuwana-shi,
Mie, 511-0192,
Japon

Le microcontrôleur comporte deux modes d'utilisation :

- un mode « Test », dans lequel le fonctionnement du microcontrôleur est testé à l'aide d'un système de test externe. Cette étape est réalisée dans l'enceinte sécurisée du site du développeur. Les données de personnalisation sont chargées en FRAM. 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.

1.2.5. Configuration évaluée

Ce rapport de certification porte sur le microcontrôleur et le logiciel identifié en §1.2.1 et décrit en §1.2.3. Tout autre logiciel utilisé pour les besoins de l'évaluation ne fait pas partie de la certification.
Au regard du cycle de vie, le produit évalué est celui qui sort de fabrication (phase 3).

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 [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

L'évaluation s'appuie sur les résultats d'évaluation du produit « IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library » certifié le 14 décembre 2006 sous la référence 2006/29 (cf. [2006/29]).

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 21 mai 2008, 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 déterministe qui peut être utilisé par le logiciel embarqué.
Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS 20] par le centre d'évaluation et sa conformité au référentiel cryptographique de la DCSSI (cf. [REF-CRY]) a également été vérifiée.
Le générateur atteint le niveau « standard » selon le référentiel cryptographique de la DCSSI (cf. [REF-CRY]), et atteint la classe de fonctionnalité K3 avec une résistance des mécanismes « élevé » selon la méthodologie [AIS 20].

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 « Microcontrôleur CXD9916H3 / MB94RS403 & HAL Library pour carte sans-contact FeliCa » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 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 CXD9916H3 / MB94RS403 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 fondant 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] au chapitre 4.2 et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

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, la Grèce, 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, 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**	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

[2006/29]	Rapport de certification 2006/29 - IC Platform of FeliCa Contactless Smartcard CXD9861/ MB94RS402 with HAL-API & DRNG Library, 14 décembre 2006, DCSSI.
[ST]	Cible de sécurité de référence pour l'évaluation : - IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 - Security Target, Référence : MB94RS403_ST_E02_V6, May 20th, 2008 Fujitsu Microelectronics Limited Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 - Security Target (Public Version), Référence : MB94RS403_STlite_E02_V2, May 20th, 2008 Fujitsu Microelectronics Limited
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - Project: TORNADO MINI, Référence : TORM_ETR_V4.0 CEACI Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ETR LITE for composition TORNADO MINI - Smartcard Integrated Circuit "CXD9916H3/MB94RS403" / FR01 - HAL Library Version 01, Référence : TORM_ETR_Lite_V1.0 CEACI
[CONF]	La liste de configuration est constituée des éléments suivants : - HAL configuration list V5L15, Référence : Tornado_HAL_CM_list_V5L15, Fujitsu Microelectronics Limited - Hardware configuration item lists 09/04/08, Référence : 20080404_CIL, Fujitsu Microelectronics Limited - MB94RS403 Configuration lists for CC document, 2008/5/20, version 14 Fujitsu Microelectronics Limited
[GUIDES]	Les guides du produit sont : - CXD9916H3/MB94RS403 LSI Specification, Référence : MB94RS403_USR_E05_V3, Nov. 20, 2007, Fujitsu Microelectronics Limited - MB94RS403 HAL Library Specification, Référence : MB94RS403_USR_E04_V3, March 27, 2008 Fujitsu Microelectronics Limited

	- MB94RS403 Security Recommendation Guidance, Référence : MB94RS403_SRG_E01_V1, May 12, 2008, Fujitsu Microelectronics Limited
[PP0002]	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.*

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, version 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)
[AIS 20]	Functionality classes and evaluation methodology for deterministic random number generators, AIS 20, Version 1,02/12/1999, Bundesamt für Sicherheit in der Informationstechnik