PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2008/13

ID-One EPass 64 v2.0 avec EAC RSA

Paris, le 16 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

Référence du rapport de certification

DCSSI-2008/13

Nom du produit

ID-One EPass 64 v2.0 avec EAC RSA

Référence/version du produit

Référence développeur de l'application : ePass 64k v2 (BAC AA EAC) v2.0 avec patch « Optional Code r3.0 for ID One ePass 64K » v3.0

Référence interne du microcontrôleur avec son masque ROM : P5CD080 UA/T0B16100

Conformité à un profil de protection

BSI-PP-0026 version 1.2

Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control

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

Développeurs

Oberthur Technologies

71-73, Rue des Hautes Pâtures – 92726 Nanterre Cedex, France

NXP Semiconductors GmbH

Box 54 02 40, D-22502 Hamburg, Allemagne

Commanditaire

Oberthur Technologies

71-73, Rue des Hautes Pâtures - 92726 Nanterre Cedex, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

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 l'application « ID-One ePass 64k v2.0 avec EAC RSA » développée par la société Oberthur Technologies, et embarquée sur le microcontrôleur P5CD080 (design step V0B) développé et fabriqué par la société NXP Semiconductors.

Le produit évalué est de type carte à puce sans contact avec antenne. Il implémente les fonctionnalités de document de voyage électronique conformément aux spécifications de l'Organisation de l'Aviation Civile Internationale (cf. [OACI]) et à l'Extended Access Control (cf [EAC]). Il s'agit d'un microcontrôleur à interface sans contact avec un logiciel embarqué destiné à vérifier l'authenticité du document de voyage et d'identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection, et permettant notamment :

- de protéger en intégrité les données stockées du futur porteur du document de voyage : nation ou organisation émettrice, n° de document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, photo du visage du porteur, données d'information optionnelles, données biométriques complémentaires du porteur, et diverses données permettant de gérer la sécurité du document ;
- d'authentifier le porteur du document de voyage et le système d'inspection (terminal de lecture des documents de voyage) préalablement à tout contrôle aux frontières, à l'aide du mécanisme « Basic Access Control » ;
- de protéger en intégrité et en confidentialité les données lues à l'aide du mécanisme « secure messaging » ;
- d'authentifier l'authenticité de la puce à l'aide du mécanisme « Active Authentication » (si activé) ;
- de réaliser une authentification forte de la puce et du système d'inspection préalablement à toute lecture des données biométriques.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels. Ils peuvent être intégrés sous forme de module, d'inlay ou de datapage. Le produit final peut être un passeport, une carte plastique, 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.
Cette cible de sécurité est conforme au profil de protection [PP EAC].

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 constituée des éléments suivants :

- nom et version du produit : ePass 64k v2 (BAC AA EAC) version 2.0 ;
- nom et version du patch : Optional Code r3.0 for ID One ePass 64K version 3.0.

Ces éléments sont identifiables à l'aide de la commande « READ BINARY » appliquée au fichier « EF.TOE_Identification », comme indiqué dans le guide d'administration (cf. [GUIDES]).

Les valeurs identifiables sont :
- code ROM du logiciel embarqué : 067511 ;
- code du patch embarqué : 067843 ;
- identifiant PP : 26 (pour l'EAC) ;
- identifiant du produit : 03.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- contrôle d'accès en lecture ;
- contrôle d'accès en écriture ;
- mécanisme BAC ;
- mécanisme « secure messaging » ;
- authentification de l'agent de personnalisation ;
- mécanisme « active authentication » ;
- mécanisme EAC à base de RSA ;
- auto-tests ;
- gestion de l'état ;
- protection physique.

Les services de sécurité offerts par le microcontrôleur sont :
- génération de nombres aléatoires ;
- coprocesseur triple DES ;
- coprocesseur AES ;
- contrôle des conditions de fonctionnement ;
- protection contre les modifications physiques ;
- protection logique ;
- protection du mode de contrôle ;
- contrôle d'accès aux mémoires ;
- fonctions spéciales de contrôle de l'accès aux registres.

1.2.3. Architecture

Le produit est constitué du microcontrôleur, du système d'exploitation embarqué, de la structure de fichiers (LDS) ainsi que des commandes de pré-personnalisation et personnalisation du document de voyage électronique (Base card). La figure suivante résume cette architecture :

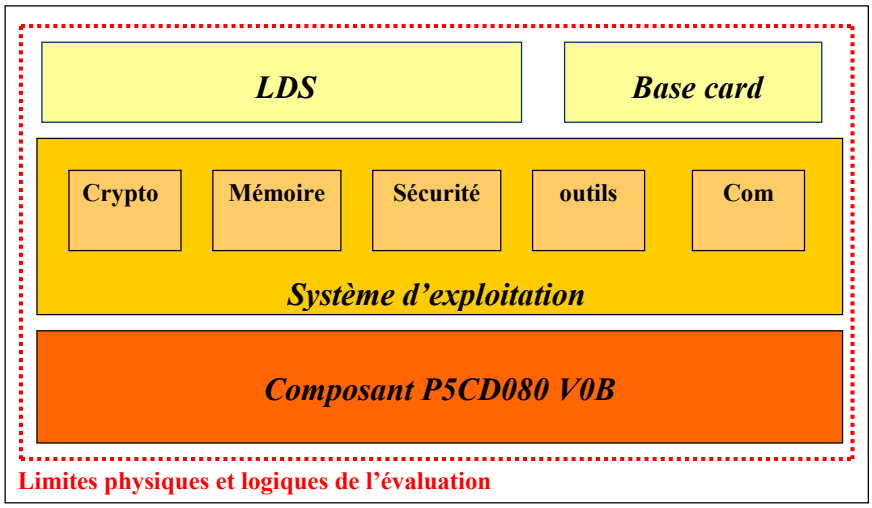

Figure 1 – Architecture du produit

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

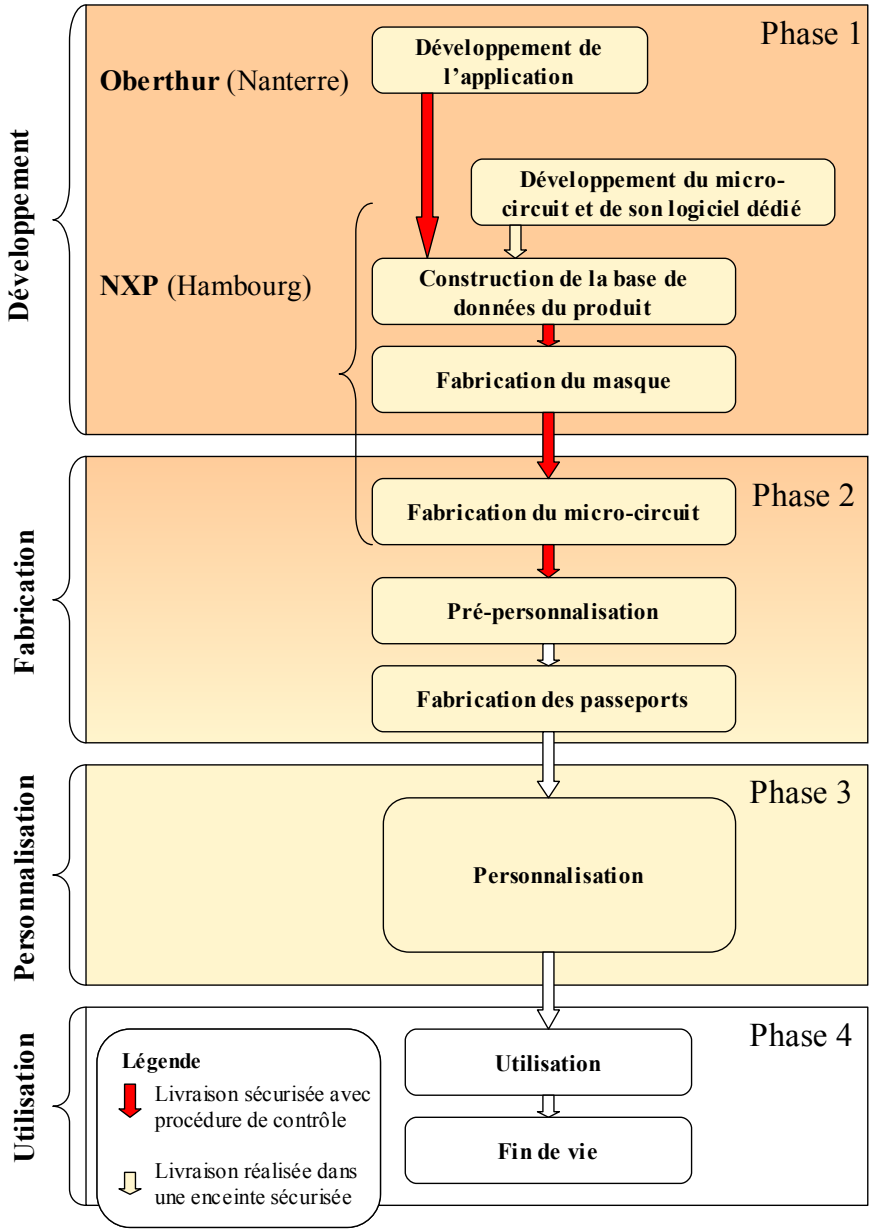

Figure 2 - Cycle de vie du produit

Le produit a été développé par Oberthur sur le site suivant :

Oberthur Technologies

71-73, Rue des Hautes Pâtures
92726 Nanterre Cedex,
France

Le microcontrôleur est développé et fabriqué par NXP Semiconductors sur le site suivant :

NXP Semiconductors

GmbHBox 54 02 40,
D-22502 Hamburg,
Allemagne

La phase de fabrication du document de voyage (pré-personnalisation) peut être réalisée par Oberthur Technologies ou par un sous-traitant. Cette phase qui n'est pas dans le périmètre d'évaluation est couverte par les guides (cf. [GUIDES]).

Le document de voyage contient un patch destiné à apporter des modifications à son comportement fonctionnel. Ce patch ne modifie aucune fonction de sécurité, ni ne réalise aucune contre-mesure sécuritaire. Par ailleurs, des mécanismes de contrôle présents dans la puce permettent de garantir que ce patch a été développé par Oberthur Technologies et n'a pas été modifié. Son chargement peut être réalisé soit par NXP dans l'enceinte de fabrication des microcontrôleurs, soit pendant la phase de fabrication du document de voyage (pré-personnalisation) en suivant la procédure décrite dans les guides (cf. [GUIDES]).
Les phases de mise en inlay et d'intégration de l'inlay dans le livret du document de voyage ne sont pas couvertes par l'évaluation, car il a été considéré qu'elles n'avaient pas d'impact sécuritaire, le produit étant protégé durant ces phases.

1.2.5. Configuration évaluée

Le produit évalué est une plate-forme e-Passport générique, qui peut être personnalisée sous différentes configurations. Ce rapport de certification porte sur la configuration incluant les mécanismes suivants :

- « Basic Access Control » ;
- « Extended Access Control » avec algorithme RSA;
- « Active Authentication ».

L'antenne et la phase de fabrication du document de voyage lui-même ne sont pas incluses dans le périmètre d'évaluation.

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 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 « P5CD080 V0B » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002]. Ce microcontrôleur a été certifié le 5 juillet 2007 sous la référence BSI-DSZ-CC-0410-2007.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 10 avril 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.

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 64 v2.0 avec EAC RSA » 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.

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 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 :

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

[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.

[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

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 :

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

[ST]	Cible de sécurité de référence pour l'évaluation : - Access World Security Target, Référence : 110 3851, édition : 1 Oberthur Technologies Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ID-One™ ePass 64 v2.0 with EAC RSA – Security Target Lite, Référence : 110 4054 édition 1 Oberthur Technologies
[RTE]	Evaluation Technical Report - Access World project, Référence : AccessWorld_ETR_v1.0 version 1.0 Serma Technologies
[CONF]	Access World configuration list, Référence : 110 4048 édition 1-AA Oberthur Technologies
[GUIDES]	Access World Administration and User Guidance Document, Référence : FQR 110 3860 édition 1-AD Oberthur Technologies
[OACI]	Doc 9303 Part 1 : Machine Readable Passports, volume 2 : Specifications for Electronically Enabled Passports with Biometric Identification Capability, référence : part 1, volume 2, Sixth Edition - 2006
[EAC]	Advanced Security Mechanisms for Machine readable travel documents – Extended Access control (EAC) – TR03110 – v1.11
[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.*
[PP EAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control, version 1.2 du 19 novembre 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0026*

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, Bundesamt für Sicherheit in der Informationstechnik