Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2018/50

IDMotion V2 Multos Virtual Machine

OS Multos V4.5.2, AMD version 0151v001

Paris, le 14 décembre 2018

Le directeur général de l'agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGNAL 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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), 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 et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2018/50

Nom du produit

IDMotion V2 Multos Virtual Machine

Référence/version du produit

OS version Multos V4.5.2

AMD version 0151v001

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 7

Développeurs :

Gemalto

La Vigie, Avenue du jujubier, ZI Athélia IV, BP 90- 13702 La Ciotat

Trusted Labs

6, rue de la Verrerie – CS20001, 92197 Meudon Cedex

Infineon Technologies AG

Am Campeon 1-12, 85579 Neubiberg

Commanditaire

Gemalto

La Vigie, Avenue du jujubier, ZI Athélia IV, BP 90- 13702 La Ciotat

Centre d'évaluation

THALES (TCS – CNES)

290 allée du Lac, 31670 Labège, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2

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 modifié. Ce décret indique que :

- L'agence nationale 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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 6
1.2.4. Identification du produit 8
1.2.5. Cycle de vie 8
1.2.6. Configuration évaluée 8

2. L'EVALUATION 9

2.1. REFERENTIELS D'EVALUATION 9
2.2. TRAVAUX D'EVALUATION 9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 9
2.4. ANALYSE DU GENERATEUR D'ALEAS 9

3. LA CERTIFICATION 10

3.1. CONCLUSION 10
3.2. RESTRICTIONS D'USAGE 10
3.3. RECONNAISSANCE DU CERTIFICAT 11
3.3.1. Reconnaissance européenne (SOG-IS) 11
3.3.2. Reconnaissance internationale critères communs (CCRA) 11

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 12

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 13

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 14

1. Le produit

1.1. Présentation du produit

Le produit évalué est la machine virtuelle « IDMotion V2 Multos Virtual Machine » de la plateforme « IDMotion V2 masquée sur le composant IFX_CCI_000014h, OS version Multos V4.5.2, AMD version 0151v001 », développée par *GEMALTO*, *TRUSTED LABS* et *INFINEON TECHNOLOGIES AG*.
La plateforme a déjà fait l'objet d'une certification au niveau EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5 (voir détails en section 2.2).

Le produit évalué est de type « carte à puce » avec et sans contact. Il est conçu de façon à ce que plusieurs applications puissent être chargées et exécutées de façon sécurisée sur la carte à puce. Ces applications sont écrites dans un langage, indépendant du composant sous-jacent, nommé MEL[1]. Les applications en langage MEL sont interprétées par le système d'exploitation Multos.

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- l'exécution sécurisée des instructions MEL et des primitives ;
- la gestion des effets mémoires lors de l'ouverture, la création, le chargement, la suppression et la sélection/désélection des applications ;
- l'interaction sécurisée entre les applications (à travers le mécanisme de délégation).

1.2.3. Architecture

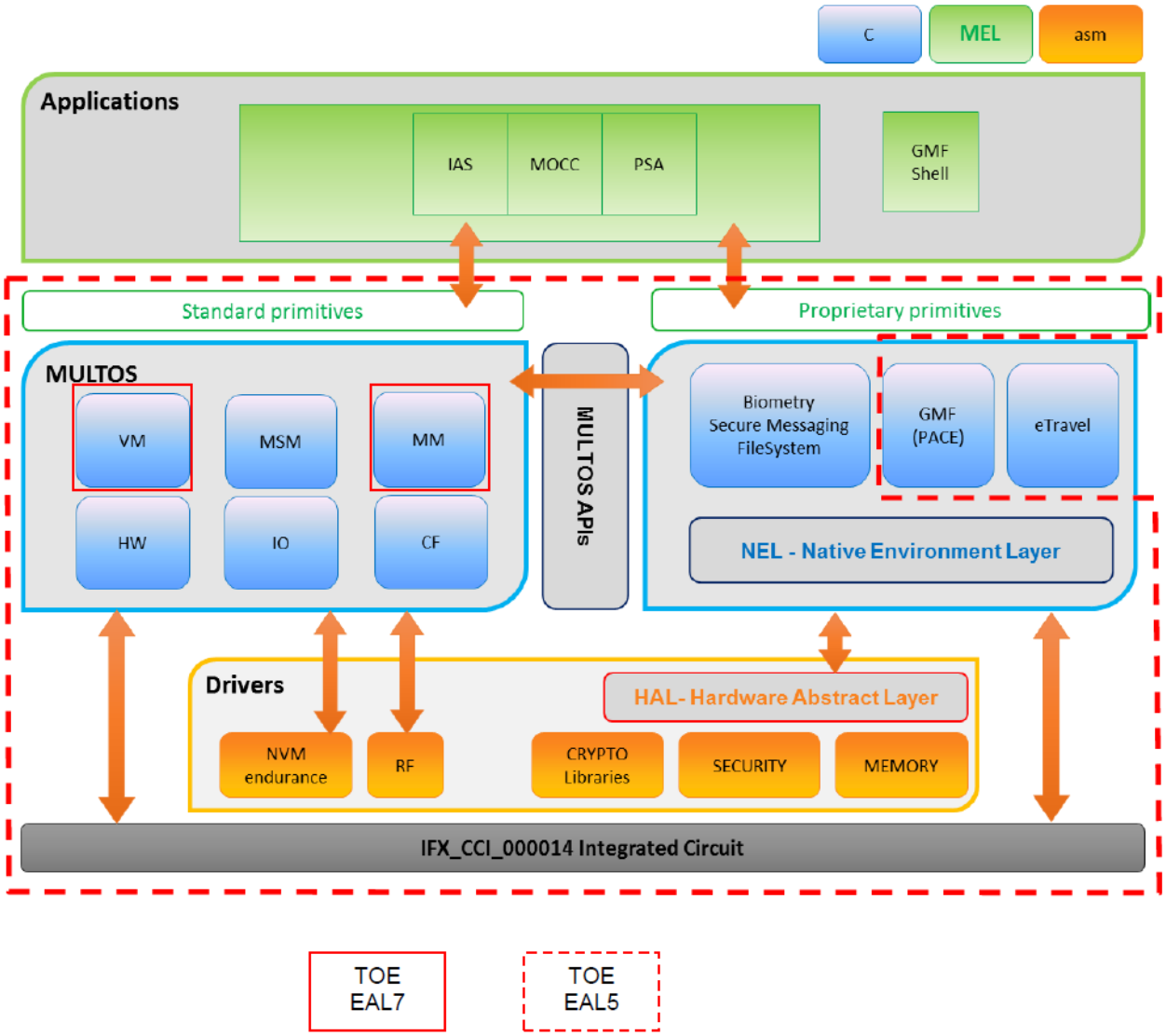
La carte « IDMotion V2 avec OS MULTOS v4.5.2 » est constituée des éléments suivants :
- du microcontrôleur IFX_CCI_000014h précédemment certifié (voir [CER-IC]) ;
- de la plateforme « IDMotion v2 avec OS MULTOS v4.5.2 » certifié au niveau EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5 (voir [CER-PLF]).

La TOE[2] soumise à l'évaluation au niveau EAL 7 est restreinte à :
- l'*Abstract Application Machine subsystem* (AM inclus dans la VM), qui permet l'interprétation des applications Multos ;
- l'*Application Memory Manager subsystem* (MM) qui gère l'espace mémoire dédié à chaque application.

L'architecture du produit est illustrée par la figure ci-après, où il est précisé :

[1] *Multos Executable Language* - langage exécutable Multos.
[2] *Target of evaluation* - cible d'évaluation.

- par un encadré rouge la présente TOE (évaluée au niveau EAL7).
- par des pointillés rouges la TOE qui a été certifiée précédemment, voir [CER-PLF].



VM: *Virtual Machine*
MSM: *Multos Security Manager*
MM: *Application Memory Manager Subsystem*
CF: *Cryptographic Functions subsystem*
IO: *I/O Communications subsystem*
HW: *Hardware Services subsystem*
NVM: *Non Volatile Memory*

Figure 1 : Architecture du produit

1.2.4. Identification du produit

Les éléments constitutifs de la carte « IDMotion V2 avec OS MULTOS v4.5.2 », dont sa machine virtuelle, sont identifiés dans la liste de configuration [CONF].

La version certifiée de la carte « IDMotion V2 avec OS MULTOS v4.5.2 » est identifiable par les éléments du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 2 « introduction ».

Configuration de la TOE	Données lues	Origine
OS version Multos V4.5.2	000452	*GEMALTO*
Version du code correctif (AMD) IDMotion V2	0151001	
Build number 1.1.42	00010001002A	
Identifiant de la plateforme	16	
Donnée d'identification du circuit intégré IFX_CCI_000014	00 00 14	*INFINEON TECHNOLOGIES AG*

Tableau 1 : Identification du carte « IDMotion V2 avec OS MULTOS v4.5.2 »

1.2.5. Cycle de vie

Le cycle de vie de la carte « IDMotion V2 avec OS MULTOS v4.5.2 » détaillé au chapitre « *2.5.4 Smartcard Product Life Cycle* » de la cible de sécurité [ST], est celui d'une carte à l'exception du point de livraison qui s'effectue à la fin de la phase 5.

1.2.6. Configuration évaluée

Le certificat porte uniquement sur les fonctionnalités offertes par la machine virtuelle de la plateforme « IDMotion V2 avec OS MULTOS v4.5.2 » identifiée dans la section 1.2.4.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément **aux Critères Communs version 3.1 révision 5** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].
Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation de la « plateforme IDMotion V2 masquée sur le composant IFX_CCI_000014h, OS version Multos V4.5.2, AMD version 0151v001 » certifiée le 30/08/2018 sous la référence ANSSI-CC-2018/35, voir [CER-PLF].

Cette évaluation a consisté à évaluer la machine virtuelle « IDMotion V2 Multos Virtual Machine » de la plateforme, selon les plus hautes exigences des Critères Communs : les composants du niveau EAL7, qui nécessitent la mise en œuvre de méthodes formelles.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 23/11/2018, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).
Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

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 la machine virtuelle « IDMotion V2 Multos Virtual Machine » soumise à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 7.

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, tels que spécifiés dans la cible de sécurité [ST], 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 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. 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 EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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 7	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	6	Complete semi-formal functional specification with additional formal specification
	ADV_IMP				1	1	2	2	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	Minimally complex internals
	ADV_SPM						1	1	1	Formal TOE security policy model
	ADV_TDS		1	2	3	4	5	6	6	Complete semiformal modular design with formal high-level design presentation
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	5	Advanced support
	ALC_CMS	1	2	3	4	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	2	Measurable life-cycle model
	ALC_TAT				1	2	3	3	3	Compliance with implementation standards - all parts
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	3	Rigorous analysis of coverage
	ATE_DPT			1	1	3	3	4	4	Testing: implementation representation
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	3	Independent testing - complete
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - IDMotion V2: MULTOS Virtual Machine Security Target, référence ST_D1430933_IDMotionV2_VM_EAL7_v1.1, version 1.1, 13 novembre 2018. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - IDMotion V2 Virtual Machine Security Target Public Version, référence ST_D1430933_IDMotionV2_VM_EAL7_Lite, version 1.2.
[RTE]	Evaluation Technical Report – BOLERO_D, référence BOLD_EAL7_ETR_1, version 4.0, 23/11/2018.
[CONF]	Liste de configuration du produit : - LIS__ceryneia.CC-delivery_004 / 004, 28 février 2018 ; - LIS__cceryneia.Ccdoc-Labo-delivery_001 / 001, 28 juin 2018.
[GUIDES]	- Multos Enablement, référence MAO-DOC-TEC-101, version 1.2 ; - Multos GLDA, Guide to Loading and Deleting, reference MAO-DOC-TEC-008, version 2.28 ; - Multos MDRM, Multos Developer's Reference Manual, référence MAO-DOC-TEC-006, version 1.54 ; - [SEC_GUID] Security Guidance for MULTOS Application Developers, référence MI-MA-0031, version 1.6 ; - Multos GALU, Guide to Generating Application Load Units, référence MAO-DOC-TEC-009, version 2.9 ; - Mask Verification Procedure, référence MI-PR-0012, version 1.1.
[CER-IC]	Certification Report BSI-DSZ-CC-0945-2017 for IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch and IFX_CCI_00001Dh design step H13 including optional software libraries and dedicated firmware from Infineon Technologies AG. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 10 juillet 2017.*
[CER-PLF]	Rapport de certification ANSSI-CC-2018/35, Plateforme ouverte IDMotion V2 masquée sur le composant IFX_CCI_000014h, OS Multos V4.5.2, AMD version 0151v001. *Certifié par l'ANSSI le 30 août 2018*.
[PP/0010]	Protection Profile Smart Card Integrated Circuit With Multi-Application Secure Platform, version 2.0, novembre 2000. *Certifié par l'ANSSI sous la référence PP/0010.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.