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-2020/52

IAS ECC v2, version 1.3 in configuration #3 on ID-One Cosmo v8.2 open platform

Paris, le 9 juillet 2020

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

Guillaume POUPARD
[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 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-2020/52

Nom du produit

IAS ECC v2, version 1.3 in configuration #3 on ID-One Cosmo v8.2 open platform

Référence/version du produit

Identification de l'applet : F0 02 02 13

Identification du matériel de la plateforme : 09 11 21

Identification du patch : 09 42 22

Conformité à un profil de protection

Protection profiles for secure signature creation device

Part 2 : Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-01 ;
Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012 ;
Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012.

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Idemia	NXP Semiconductors GmbH
2 place Samuel de Champlain, **92400 Courbevoie, France**	**Troplowitzstrasse 20,** **22529 Hamburg, Allemagne**

Commanditaire

Idemia

2 place Samuel de Champlain,
92400 Courbevoie, France

Centre d'évaluation

CEA - LETI

17 avenue des martyrs, 38054 Grenoble Cedex 9, 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 directeur général de l'Agence national de la sécurité des systèmes d'information 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 « IAS ECC v2, version 1.3 in configuration #3 on ID-One Cosmo v8.2 open platform, identification de l'*applet* : F0 02 02 13, identification du matériel : 09 11 21, identification du patch : 09 42 22 » développée par *IDEMIA* et masquée sur le composant NXP P60D145 développé par *NXP SEMICONDUCTORS GMBH*.

Ce produit est une carte à puce constituée d'un logiciel conforme au standard IAS ECC v2 et d'un microcontrôleur sécurisé. Il est destiné à être utilisé comme dispositif sécurisé de création de signature ou de sceau électronique (SSCD[1]). Il peut être utilisé dans différents types de documents (carte d'identité, permis de conduire, carte d'entreprise, passeport, etc.) disposant d'interfaces avec et/ou sans contact.

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.

Cette cible de sécurité est strictement conforme au profil de protection [PP-SSCD-Part2], [PP-SSCD-Part3] et [PP-SSCD-Part4].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la création de signature ou de sceau électronique dans un environnement où la sécurité repose sur des mesures organisationnelles ;
- la génération des clés de signature (c'est-à-dire la génération de la donnée de création de signature (SCD[2]) et de la donnée de vérification de signature (SVD[3]) associée) ;
- l'import des clés de signature (c'est-à-dire de la SCD et, optionnellement, de la SVD associée) ;
- l'établissement d'un canal de confiance pour l'import de la SCD dans un environnement non protégé ;
- l'export de la SVD pour la création de certificat électronique à travers un canal de confiance ;
- l'authentification du porteur de carte basée sur la vérification d'un code PIN ou de données biométriques, appelés indistinctement donnée d'authentification de référence (RAD[4]) ;
- le déblocage de la RAD.

Les principaux services de sécurité de la plateforme sont décrits dans [CER-PTF].

[1] *Secure Signature Creation Device*
[2] *Signature Creation Data*
[3] *Signature Verification Data*
[4] *Reference Authentication Data*

1.2.3. Architecture

Le produit est constitué :
- du microcontrôleur « NXP P60D145 » certifié sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte « ID-One Cosmo V8.2 » certifiée sous la référence [CER-PTF] ;
- de l'application «IAS ECC v2 version 1.3 » en configuration #3.

Des applications peuvent être chargées sur la plateforme *Java Card* ouverte, à côté de l'application « IAS ECC v2, version 1.3 ». Il s'agit soit des applications identifiées dans le certificat de la plateforme [CER-PTF], soit d'applications inconnues à condition que leur chargement respecte les [GUIDES]. La conformité aux prescriptions du document [OPEN] pour le chargement d'applications a été prise en compte lors de l'évaluation de la plateforme [CER-PTF].

1.2.4. 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 du tableau ci-après, détaillés dans la cible de sécurité [ST] et dans les [GUIDES].

Eléments de configuration		**Origine**
Nom de la TOE	IAS ECC v2, version 1.3 in configuration #3 on ID-One Cosmo v8.2 open platform	*IDEMIA*
Identification de l'application	« F0 02 02 13 »	
Identification du matériel de la plateforme	« 09 11 21 »	
Identification du *patch*	« 09 42 22 »	

Ces éléments peuvent être vérifiés par les méthodes décrites dans les [GUIDES], notamment :
- l'identification de l'*applet* par l'envoi de la commande GET DATA avec le tag « DF67 » ;
- l'identification de la plateforme et du composant comme décrit dans [CER-PTF].

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au paragraphe 3.5 de [ST]. Il est composé des phases listées dans le tableau suivant, pouvant être regroupées en trois étapes :
- le développement (phases 1 à 3) ;
- la production (phases 4 et 5) ;
- l'état opérationnel (phases 6 et 7).

Le point de livraison de la TOE est en sortie de la phase 3. Après cette phase la TOE est considérée comme auto-protégée.

Phases	Tâches	Classes d'assurance	Acteurs ou Sites
1	Développement des parties logicielles	ALC	*IDEMIA* (Courbevoie et Pessac) Sites de [CER-PTF]
2	Développement du microcontrôleur	ALC	Sites de [CER-IC]
3	Fabrication	ALC	Sites de [CER-PTF] et [CER-IC]
Point de livraison de la TOE			
4	*Packaging* et initialisation	AGD_PRE	Agent de fabrication
5	Pré-personnalisation	AGD_PRE	Agent de fabrication
6	Personnalisation	AGD_PRE	Agent personnalisateur
7	Utilisation	AGD_OPE	Utilisateur final

Le produit a été développé sur les sites suivants (voir [SITES]) :

***IDEMIA* – Courbevoie** [CRB] 2, place Samuel de Champlain 92400 Courbevoie, France	***IDEMIA* – Pessac** [PSC] Bâtiment Elnath, 11 avenue de Canteranne, 33600 Pessac, France

Les sites intervenant dans le cycle de vie de la plateforme et du composant sont listés respectivement dans [CER-PTF] et [CER-IC].

1.2.6. Configuration évaluée

Le certificat porte sur le produit identifié au paragraphe 1.2.4 et configuré comme suit :

- l'application « IAS ECC v2 » est instanciée sur la plateforme *Java Card* ouverte couverte par le certificat [CER-PTF] ;
- les recommandations des [GUIDES] sont strictement appliquées pendant les phases de « Pré-personnalisation » et « Personnalisation » afin de personnaliser l'application en configuration #3.

La configuration ouverte du produit a été évaluée conformément à [OPEN] dans le cadre de la certification de la plateforme [CER-PTF]. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées dans [CER-PTF] ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

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 en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur la plateforme déjà certifiée par ailleurs (voir [CER-PTF]).

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la « Plateforme ID-One Cosmo v8.2 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5. Cette plateforme a été certifiée le 16 juin 2020 sous la référence ANSSI-CC-2020/26 (voir [CER-PTF]).

L'évaluation s'appuie sur les résultats d'évaluation du produit « IAS ECC v2, version 1.3 en configuration #3 sur la plateforme ID-One Cosmo v8.2 » certifié sous le 17 septembre 2019 sous la référence ANSSI-CC-2019/35 (voir [CER-IAS]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 16 juin 2020, 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 a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations données dans le document [AGD_QUA] doivent être respectées.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [RTE]. Ces 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.

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 (voir [CER-PTF]).
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 le produit « IAS ECC v2, version 1.3 in configuration #3 on ID-One Cosmo v8.2 open platform, identification de l'*applet* : F0 02 02 13, identification du matériel : 09 11 21, identification du patch : 09 42 22 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

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], notamment en ce qui concerne la vérification et le chargement d'applications, qui doivent être effectués conformément aux résultats de l'évaluation de la plateforme (voir [CER-PTF]).

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].

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

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 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 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 5+	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	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	**1**	Implementation representation of the TSF
	ADV_INT					2	3	3	**2**	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**4**	Semiformal modular design
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	**4**	Production support, acceptance procedures and automation
	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	**1**	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	**2**	Compliance with implementation standards
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	**2**	Analysis of coverage
	ATE_DPT			1	1	3	3	4	**3**	Testing: modular 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_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 : - Clytemnestre-R in Configuration #1 IAS ECC V2 Security Target, référence 110 8966, version 5.0 du 21 avril 2020, *IDEMIA*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - IAS ECC V2, version 1.3 in configuration #1 on ID-One Cosmo v8.2 - Public Security Target, référence 110 9186, version 3 du 21 avril 2020, *IDEMIA*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report CLYTEMNESTRE-R2, référence LETI.CESTI.CLR.ETR.001, version 2.1 du 16 juin 2020, *CEA-LETI.*
[ANA-CRY]	Cotation des mécanismes cryptographiques CLYTEMNESTRE-R, référence LETI.CESTI.CLR.RT.008-V1.0, version 1.0 du 16 mai 2019, *CEA-LETI.*
[CONF]	Liste de configuration du produit : - CLYTEMNESTRE_R CONFIGURATION LIST, référence 110 9083, version 4 du 12 juin 2020, *IDEMIA*.
[GUIDES]	Guide d'installation du produit : - [AGD_PRE] CLYTEMNESTRE- R ADV_PRE, référence FQR 110 8968, version 2 du 11 avril 2019, *IDEMIA*. Guide d'administration du produit : - [AGD_OPE] CLYTEMNESTRE – R ADV_OPE, référence FQR 110 8969, version 3 du 5 août 2019, *IDEMIA*. Guide d'utilisation du produit : - [AGD_QUA] CLYTEMNESTRE Recommandations pour la compatibilité avec le référentiel de qualification renforcée, référence 110 9078, version 1 du 4 janvier 2019, *IDEMIA*. Guides d'installation, d'administration et de développement d'applications sécurisées sur la plateforme : - [AGD_PPRE] ID-One Cosmo V8.2 Pre-Perso Guide, référence FQR 110 8875 version 9 du 2 juin 2020, *IDEMIA* ; - [AGD_POPE] ID-One Cosmo V8.2 Reference Guide, référence FQR 110 8885, version 8 du 2 juin 2020, *IDEMIA* ; - [AGD_PDEV] ID-One Cosmo V8.2 on P60D145 - Applet Security Recommandations, référence FQR 110 8963, version 4 du 18 mars 2019, *IDEMIA* ;

	- [AGD_PALP] ID-One Cosmo V8.1-n Application Loading Protection Guidance, référence FQR 110 8001, version 1 du 11 octobre 2016, *IDEMIA*.
[CER-IC]	Certification Report BSI-DSZ-CC-1059-2018 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH, 18 mai 2018. Certification Report BSI-DSZ-CC-1059-V3-2019 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH, 29 novembre 2019.
[CER-PTF]	Rapport de certification ANSSI-CC-2020/26, Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145, 16 juin 2020.
[CER-IAS]	Rapport de certification ANSSI-CC-2019/35, IAS ECC V2, version 1.3 en configuration #3 sur la plateforme ID-One Cosmo v8.2, 17 septembre 2019.
[SITES]	Rapports d'analyse documentaire : - IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence IDEMIA R&D site 2018_GEN_v1.0, 29 novembre 2018 ; - IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence IDEMIA R&D site 2018_GEN_v1.1, 19 juin 2019. Rapports d'audit de site pour la réutilisation : - [CRB] Site Technical Audit Report CRB, référence IDEMIA R&D site 2018_CRB_STAR_v1.3, 26 juin 2019 ; - [PSC] Site Technical Audit Report PSC, référence IDEMIA R&D site 2018_PSC_STAR_v1.2, 18 décembre 2019.
[PP-SSCD-Part2]	Protection profiles for secure signature creation device – Part 2: Device with key generation, référence : prEN 14169-2:2012, version 2.0.1 datée du 23 janvier 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.*
[PP-SSCD-Part3]	Protection profiles for secure signature creation device – Part 3: Device with key import, référence : prEN 14169-3:2012, version 1.0.2 datée du 24 juillet 2012. *Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.*

[PP-SSCD-Part4]	Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, référence : prEN 14169-4:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.*
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*

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 3.0, avril 2019.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5.1, mai 2018.
[OPEN]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 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.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.

	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), 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.