PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CC-2020/26-R01

Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145 (Codes SAAAAR : 091121, 094223 et 094742)

Paris, le 13 Novembre 2023

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

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2020/26-R01

Nom du produit

Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145

Référence/version du produit

Codes SAAAAR : 091121, 094223 et 094742

Conformité à un profil de protection

Java Card Protection Profile Open Configuration, version 3.0

Maintenu par l'ANSSI ANSSI-CC-PP-2010/03-M01 le 29 mai 2012

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

IDEMIA
2 place Samuel de Champlain 92400
Courbevoie, France

NXP SEMICONDUCTORS GMBH
Beiersdorfstraße 12,
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

Ce certificat est reconnu au niveau EAL2.

SOG-IS

PREFACE

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 nationale 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 MATIERES

1 Le produit 6
1.1 Présentation 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 7
1.2.4 Identification du produit 8
1.2.5 Cycle de vie 9
1.2.6 Configuration évaluée 10
2 L'évaluation 11
2.1 Référentiels d'évaluation 11
2.2 Travaux d'évaluation 11
2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI 11
2.4 Analyse du générateur d'aléa 11
3 La certification 12
3.1 Conclusion 12
3.2 Restrictions d'usage 12
3.4 Reconnaissance du certificat 13
3.4.1 Reconnaissance européenne (SOG-IS) 13
3.4.2 Reconnaissance internationale critères communs (CCRA) 13
ANNEXE A. Références documentaires du produit évalué 14
ANNEXE B. Références liées à la certification 15

1 Le produit

1.1 Présentation du produit

Le produit évalué est la « Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145, Codes SAAAAR : 091121, 094223 et 094742 » développé par IDEMIA embarquée sur le microcontrôleur NXP P60D145 développé et fabriqué par NXP SEMICONDUCTORS GMBH.

Le produit est une carte à puce qui dispose d'interfaces avec et sans contact. Il est destiné à héberger et exécuter une ou plusieurs applications, dites *applets* dans la terminologie *Java Card*. Ces applets peuvent revêtir un caractère sécuritaire différent (selon qu'elles soient « sensibles » ou « basiques ») et peuvent être chargées et instanciées avant ou après émission du produit. Les logiciels applicatifs ne sont pas inclus dans le périmètre de l'évaluation, mais ont été pris en compte au titre de [OPEN].

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 conforme au profil de protection [PP JCS-O]. La conformité est démontrable.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont détaillés dans la cible de sécurité [ST] aux chapitres 3.3 « *Major Security feature of the TOE* » et 10 « *TOE Summary Specification* ». Ils sont résumés ci-après :

- le chargement (avec vérification de signature DAP[1]), l'installation, « l'extradition[2] » et la suppression d'occurrences d'*applets* ou de *packages* par le *Card Manager* ;
- l'identification et l'authentification de l'utilisateur du produit ;
- la protection en confidentialité et en intégrité des données sensibles ;
- l'effacement sécurisé des données sensibles ;
- la mise à jour des données en mémoire persistante à travers un mécanisme de transactions atomiques ;
- des mécanismes de chiffrement, déchiffrement, signature et génération de nombres aléatoires ;
- la gestion des clés ;
- un mécanisme de pare-feu ;
- la gestion des exceptions ;
- la protection du chargement d'applications post-émission ;

l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

[1] *Data Authentication Pattern*

[2] « L'extradition » permet à plusieurs applications de partager un domaine de sécurité dédié.

1.2.3 *Architecture*

L'architecture du produit est décrite au chapitre 3 « *TOE Overview* » de la cible de sécurité [ST].

La cible de l'évaluation (TOE[3]) est constituée de :

- du microcontrôleur NXP P60D145 (P6022y VB), développé par NXP SEMICONDUCTORS GMBH et certifié sous la référence [CER_IC] ;
- des parties logicielles suivantes, constitutives de la plateforme « ID-One Cosmo V8.2 », développées par IDEMIA (à l'exception de l'algorithme de biométrie développé par la société ID3) et masquées en ROM :
  - un système d'exploitation composé :
    - d'une interface entre les composants matériels et les composants natifs, nommée BIOS[4],
    - de fonctionnalités cryptographiques,
    - d'une machine virtuelle *Java* (JVM[5]),
    - d'un environnement d'exécution *Java Card* (JCRE[6]),
    - des interfaces de programmation d'application (API[7]) : *Java Card* et *Global Platform* ;
  - un *dispatcher* nommé *Resident Application* et chargé de repartir les commandes envoyées à la carte vers les applications et modules correspondants ;
  - un gestionnaire d'applications (*Card Manager*) dont les fonctionnalités sont implémentées dans une *applet* dédiée du même nom ;
  - un algorithme de biométrie *Match-On-Card* (MOC) développé par la société ID3[8] et masqué en ROM ;
  - un mécanisme de chargement de *patch*s,
- du patch générique « *Optional Code generic DLATCH on Cosmo v8.2* » et du patch optionnel r2.0 LDS V10.1, développés par *IDEMIA*.

Le produit est aussi composé des éléments hors TOE suivants, développés par IDEMIA :

- de *patchs* logiciels optionnels chargés en EEPROM correspondants à des mises à jour des *applets* ;
- des applications masquées en ROM : SAC Server v1.1, CHV2.2 v2.2, IAS ECC V2 v2.0, LDS V10 v10.1, PIV 2.4 v2.4.1 et CPS2ter v2.

Les applications déjà chargées dans le produit sont toutes identifiées dans le document (voir tableau 1).
Bien que ces applications ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, ces applications ont été vérifiées conformément aux contraintes listées dans la cible de sécurité [ST] au chapitre 3.6 « *TOE Guidances* ».

[3] *Target Of Evaluation*.

[4] *Basic Input/Output System*.

[5] *Java Virtual Machine*.

[6] *Java Card Runtime Environment*.

[7] *Application Programming Interface*.

[8] Le site de développement de la société ID3, basé à Grenoble, n'a pas été audité.

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] aux chapitres 2.3 « *TOE Reference* » et 2.4 « *TOE Identification* ».

Eléments de configuration		Origine
Nom de la TOE	ID-One Cosmo v8.2 Platform	IDEMIA
Identification matérielle du produit	091121 (code SAAAR du produit)	
Identification des *patch*	094223 (*Optional Code Generic DLATCH on Cosmo v8.2*) 094742 (*Optional Code r2.0 LDS V10.1 on Cosmo v8.2*)	
Identification de la plateforme	6F 01	
Identification du composant	30 (NXP P60D145)	NXP SEMICONDUCTORS GMBH

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET DATA ou à la lecture de l'ATR, les méthodes et formats sont décrits dans les [GUIDES].

La principale différence entre le produit et la TOE correspond aux applications chargées en pré-émission et aux patchs optionnels pouvant être installés en pré-personnalisation.

Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après et dans la cible de sécurité [ST]. Ce tableau liste les applications et les paquetages (*packages*) inclus dans le produit, associés à leur nom et leur AID[9].

Nom de l'applet	AID (valeur en hexadécimal)	Nom du package
CHV2.2 v2.2	A000000077010808072000000000000003 A000000077010808072000000000000002 A000000077010808072000000000000001 A000000077010808072000000000000006 A000000077010808072000000000000005	Chv Cvm id3 Pw pw_fp
SAC Server v1.1	A000000077010800071000000000000015 A000000077010800071000000000000018	SAC *Applet Manager* SAC *Java Applet*
IAS ECC V2 v2.0	A000000077010800071000000000000B A000000077010800071000000000000D A000000077010800071000000000000013	*Server Applet Manager* IAS ECC API IAS *lihgt Add-On*
LDS V10 v10.1	A000000077010000071000000000000E A000000077010000071000000000000005	Ldslib Ldseac
PIV 2.4 v2.4.1	A000000077010000061000000000000024	PIV
CPS2ter v2	A000000077010800071000000000000C	CPS2ter

Tableau 1 - Applications du produit

[9] *Application Identifier.*

La commande GET STATUS permet à l'utilisateur du produit de vérifier quelles applications et quels *packages* sont installés dans le produit à sa disposition.

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 3.7 « *TOE Life cycle* » de la cible de sécurité [ST].

La phase 1 correspond à la conception et au développement de la plateforme, plus précisément :
- à la définition et l'écriture des données de l'utilisateur ;
- au développement du socle logiciel incluant l'algorithme de biométrie MOC ;
- au développement de patchs.

Les phases 2 et 3 correspondent respectivement au développement et à la fabrication du microcontrôleur et sont effectuées chez NXP SEMICONDUCTORS GMBH. La phase 3 inclut l'écriture en ROM du logiciel embarqué et en EEPROM de données de l'utilisateur et de *patchs* identifiés dans la cible de sécurité [ST]. Ces phases sont couvertes par l'évaluation du microcontrôleur [CER_IC].

La livraison de la TOE s'opère à la fin de la phase 3. Après cette phase, la TOE est considérée comme auto-protégée.

La phase 4 correspond au conditionnement (*packaging*) du produit, c'est-à-dire à l'intégration de la TOE au format final (par exemple, au format carte). Le produit est activé à partir de la phase 5. Cette phase supporte notamment :
- la configuration du logiciel embarqué de la plateforme (chargement de données de l'utilisateur et du code optionnel non chargé en phase 3) ;
- le *Card Content Management* géré par le *dispatcher* et le *Card Manager* (chargement, installation et suppression des fichiers de chargement, *Load Files* et des instances d'application) ;
- après cette phase, aucun *patch* ne peut être chargé, le mécanisme de chargement de *patch* est désactivé. Ces deux phases sont couvertes par le guide d'administration du produit [AGD_PRE].

La phase 6 correspond à la personnalisation du produit et la phase 7 correspond à la phase opérationnelle du produit. Ces phases sont couvertes par le guide d'utilisation du produit [AGD_OPE].

Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

Le produit permet le chargement d'applications en phase 3 (avant le point de livraison), en phase 5 (pré-émission) ou en phases 6 et 7 (post-émission) :
- le développement des applications masquées en ROM en phase 3 et identifiées dans la cible de sécurité [ST] a été réalisé sur les sites de Courbevoie et Pessac. Leur livraison et leur vérification ont été analysées pendant cette évaluation conformément à [OPEN] au titre des tâches ALC ;
- les chargements en phase 5 (pré-émission), 6 et 7 (post-émission) doivent être protégés conformément à [AGD_ALP].

Le guide [AGD_ALP] identifie également des recommandations relatives à la livraison des futures applications à charger sur la plateforme. Le guide [AGD_OPE] présente une aide pour le développement pour toutes les applications. Le guide [AGD-Dev_Sec] présente les recommandations obligatoires pour le développement des applications sensibles.

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le « prépersonnalisateur », le « personnalisateur » et le *Card Manager*, et comme utilisateur du produit les développeurs des applications à charger sur la plateforme.

1.2.6 *Configuration évaluée*

Le certificat porte sur la configuration de la plateforme telle qu'elle est identifiée au paragraphe 1.2.4.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

Toutes les applications identifiées dans la cible de sécurité ont été vérifiées conformément aux exigences définies dans le chapitre 2.4.4 de [ST].

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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 dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « *NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software* », voir [CER_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 d'attaquant visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

2.4 Analyse du générateur d'aléa

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 [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant 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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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 :

- toutes les futures applications chargées sur ce produit (chargement post--émission) doivent respecter les contraintes listées dans [AGD-Dev_Sec] ;
- les autorités de vérification doivent appliquer les exigences définies au chapitre 3.6 « *TOE Guidances* » de la cible de sécurité [ST] sur toutes les applications chargées sur ce produit ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement pré-émission et post-émission) doit être activée conformément aux indications décrites dans le guide [AGD_ALP].

3.4 Reconnaissance du certificat

3.4.1 *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[10], 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 :

3.4.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[11] , 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 :

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

[11] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security Target ERATO R2 ID-One COSMO V8.2*, FQR 110 A223, version 5, 21 septembre 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *ID-ONE COSMO V8.2 Public Security Target*, FQR 110 A220, version 5, 21 septembre 2023.
[RTE]	Rapport technique d'évaluation : *Evaluation Technical Report – ERATO-R2*, référence LETI.CESTI.ERR.FULL.001, version 4.3, 22 septembre 2023.
[ANA_CRY]	Cotation des mécanismes cryptographiques ERATO-R2, référence LETI.CESTI.ER2.RT.001 – V1.1, 22 septembre 2023.
[CONF]	Liste de configuration du produit : - *ID-One Cosmo V8.2 Configuration List*, référence FQR 110 9114, version 16, 22 septembre 2023.
[GUIDES]	Guide d'installation du produit : - [AGD_PRE] *ID-One Cosmo V8.2 Pre-Perso Guide*, FQR 110 8875, version 10, 18 juin 2020. Guide d'administration du produit : - [AGD_OPE] *ID-One Cosmo V8.2 Reference Guide*, FQR 110 8885, version 11, 20 septembre 2023. Guide de développement d'applications sécurisées : - [AGD-Dev_Sec] *ID-One Cosmo V8.2 on P60D145 - Applet Security Recommandations*, FQR 110 8963, version 5, 7 juillet 2023 ; - [AGD_ALP] *ID-One Cosmo V8.1-n Application Loading Protection Guidance*, FQR 110 8001, version 1, 11 octobre 2016. Guide cryptographique : - *ID-One Cosmo V8.2 on P60D145 French Conformance Guidance*, FQR 110 A23F, version 2, 3 juillet 2023.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA2022_GEN_v1.0 ; - [CRB] IDEMIA2022_CRB_STAR_v1.1 ; - [PSC] IDEMIA2022_Pessac_STAR_v1.0.
[CER_IC]	*Certification Report BSI-DSZ-CC-1059-V5-2022 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH*. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-DSZ-CC-1059-V5-2022.
[PP JCS-O]	*Java Card System Protection Profile - Open Configuration*, version 3.0 Maintenu par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01.

ANNEXE B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[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 and similar devices*, version 3.2, novembre 2022.
[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.
[CCRA]	*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.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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