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-2017/23

annule et remplace le rapport de certification ANSSI-CC-2017/10

Plate-forme STSAFE-J, en configuration fermée, version 1.1.4, sur le composant ST31H320 A03

Paris, le 23 mars 2017

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-2017/23

Nom du produit

Plate-forme STSAFE-J, en configuration fermée, version 1.1.4, sur le composant ST31H320 A03

Référence/version du produit

Version 1.1.4

Conformité à un profil de protection

Java Card Protection profile – Closed Configuration

Version 3.0, ANSSI-CC-PP-2010/07-M01

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

STMicroelectronics S.r.l.

Z.I Marcianise Sud,
81025 Marcianise,
Italie

STMicroelectronics
190 Avenue Celestin COQ
13106 ROUSSET CEDEX, FRANCE

Commanditaire

STMicroelectronics S.r.l.

Z.I Marcianise Sud,
81025 Marcianise,
Italie

Centre d'évaluation

Serma Safety & Security

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit 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

1.1. Présentation du produit

Le produit évalué est la « Plate-forme STSAFE-J, en configuration fermée, version 1.1.4, sur le composant ST31H320 A03 » développée par *ST MICROELECTRONICS S.r.l* sur le microcontrôleur ST31H320 A03 fabriqué par la société *ST MICROELECTRONICS* .

La plateforme est une carte à puce en mode contact. Elle est en configuration fermée, et ne correspond pas à un produit utilisable en tant que tel. Elle est normalement destinée à héberger une ou plusieurs applications, devant être chargées pendant la phase de construction du produit final. De telles applications ne sont toutefois pas couvertes par la présente évaluation.

Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé, etc.) en fonction des logiciels applicatifs qui seront embarqués.

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].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la gestion du cloisonnement entre les différents modules gérés par la plateforme Java Card ;
- la gestion sécurisée des différentes fonctionnalités de la plateforme Java Card, de la mémoire, des opérations sur les clefs, de l'état de fonctionnement de la plateforme ;
- la gestion des opérations sur les clefs : génération, distribution, accès et destruction ;
- les opérations de chiffrement / déchiffrement ainsi que de signature / vérification ;
- la gestion transactionnelle garantissant l'exécution complète de la transaction ;
- les opérations sur le PIN[1] ;
- la gestion de la libération de la mémoire ;
- la gestion des fonctionnalités offertes par le microcontrôleur sous-jacent.

Ils sont détaillés au chapitre 7.7 de [ST].

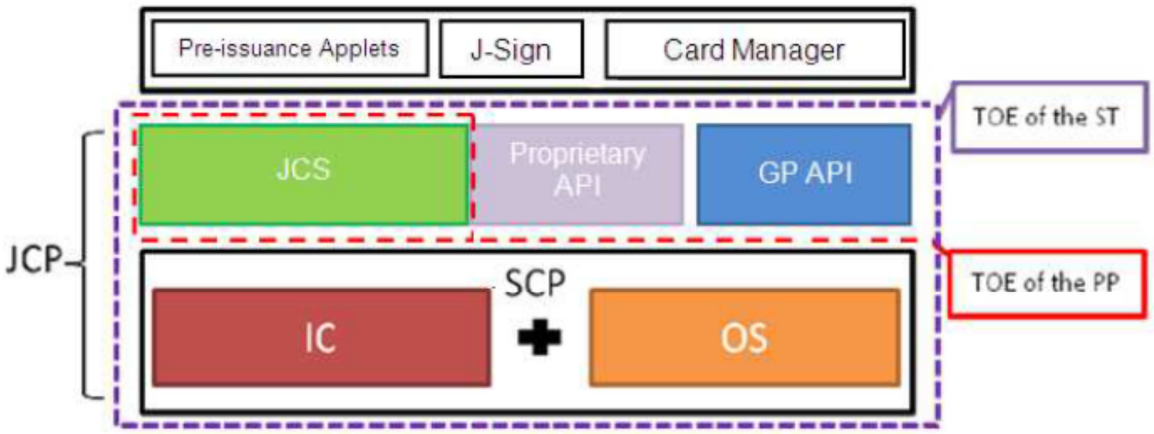
[1] *Personnal Identification Number*.

1.2.3. Architecture

La TOE est constituée des éléments suivants :

- une plate-forme Java Card comprenant une machine virtuelle Java Card, un environnement d'exécution Java Card et des API Java Card standards et propriétaires ;
- une implémentation partielle du standard *Global Platform* restreinte à la gestion du cycle de vie de la carte et des applications, le canal sécurisé, le PIN global et la gestion du contrôle de contenu de la carte (phase de pré-émission uniquement) ;
- un système d'exploitation de bas niveau : gestion mémoire, entrées-sorties, mécanismes transactionnels et accès aux fonctions cryptographiques ;
- le microcontrôleur ST31H320 A03 incluant sa librairie cryptographique NesLib.

Cette architecture est illustrée par le schéma suivant :



1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Le tableau suivant fournit les commandes et réponses permettant d'identifier le produit.

La version certifiée du produit est identifiable par les éléments des *CPLC Data* suivants :

Description	**Réponse en hexadécimale**
Identification du fabricant de microcontroleur	0x4750
Identifiant du microcontrôleur	0x00DE
Identifiant du logiciel STSAFE-J	0x0078
Date d'émission du logiciel STSAFE-J	0x6349
Version du logiciel STSAFE-J	0x0001

Ces valeurs peuvent être vérifiées par une commande GETDATA avec le tag 9F7F comme décrit dans [GUIDES].

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

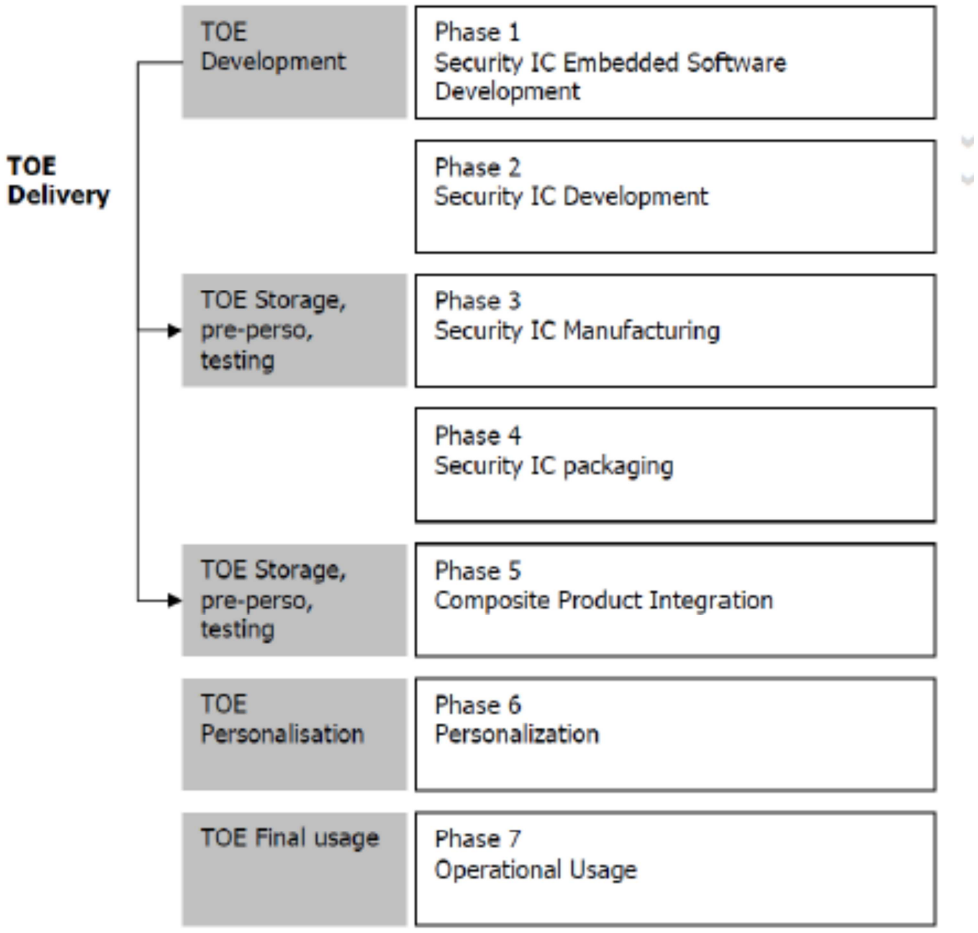


Figure 2 – Cycle de vie

Le périmètre évalué couvre les phases 1 à 3 ou 1 à 5 suivant le modèle de cycle de vie choisi. En effet, la livraison de la TOE peut s'effectuer en fin de phase 3 ou en fin de phase 5.

Le produit a été développé sur les sites suivants :

Site de développement de la plateforme

ST MICROELECTRONICS S.R.L.
Z.I. Marcianise,
81025 Marcianise,
Italie

Sites de développement du microcontrôleur

Voir [CER IC]

1.2.6. Configuration évaluée

Le certificat porte sur la plate-forme *Java* STSAFE-J embarquée en flash sur le composant ST31JH320 A03 en configuration fermée. Aucune application n'est considérée dans le périmètre de cette évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [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 « ST31H320 including optional cryptographic library NESLIB » au niveau EAL5 augmenté des composants ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2 et AVA_VAN.5, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié par l'ANSSI le 25 décembre 2015 sous la référence ANSSI-CC-2015/59 [CER IC] et maintenu le 20 avril 2016 sous la référence ANSSI-CC-2015/59-M01 [M01 IC]. Le niveau de résistance du microcontrôleur a été confirmé le 25 août 2016 dans le cadre du processus de surveillance sous la référence ANSSI-CC-2015/59-S01 [S01 IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 mars 2017, 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 vulnérabilités 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 sous-jacent à la plateforme STSAFE-J (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 le produit « Plate-forme STSAFE-J, en configuration fermée, version 1.1.4, sur le composant ST31H320 A03 » 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.

Ce certificat donne une appréciation de la résistance du produit 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 la plateforme Java Card ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant 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, 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 puces 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] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, la Pologne, 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 Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, 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 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 : - ST SAFE-J on ST31H320 Security Target, version E, référence STSAFE-J_ST31H320_Security Target_E, ST Microelectronics. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST SAFE-J Security Target – Public Version, version A, référence STSAFE-J_ST_Lite_A, janvier 2017, ST Microelectronics.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report, STSAFE-J project, Référence STSAFE_J_ETR_v1.1 Version 1.1, 7 mars 2017, Serma Safety & Security. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation Technical Report, STSAFE-J project, Référence STSAFE_J_ETR_Lite_v1.1 Version 1.1, 7 mars 2017, Serma Safety & Security.
[CONF]	Liste de configuration du produit : - STSAFE-J Configuration List, Référence Kerkey2_JSAFE_Configlist.txt 27/01/2017.
[GUIDES]	Guides de préparation et d'utilisation du produit : - STSAFE-J on ST31H320 – Guidance Document (AGD), version C, référence STSAFE-J_AGD_Rev_C, ST Microelectronics, - Security guidelines for application development on the STSAFE-J100 secure solution, révision 2, référence AN_SECU_STSAFE-J100V2, ST Microelectronics, - User Manual STSAFE-J100, version 1, référence UM_STSAFE-J100_V1, ST Microelectronics.
[PP JCS]	Java Card protection profile – Closed configuration, Version 3.0, décembre 2012. *Certifié sous la reference ANSSI-CC-PP-2010/07 et maintenu sous la référence ANSSI-CC-PP-2010/07-M01.*
[CER IC]	Rapport de certification ANSSI-CC-2015/59, ST31H320 A01 including optional cryptographic library NESLIB, 28 décembre 2015.
[M01 IC]	Rapport de maintenance ANSSI-CC-2015/59-M01, ST31H320 A02 including optional cryptographic library NESLIB, 20 avril 2016.

[S01 IC]	Rapport de surveillance ANSSI-CC-2015/59-S01, du produit ST31H320 A03 including optional cryptographic library NESLIB, 25 août 2016.
[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 de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[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.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, janvier 2012.
[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.