



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-2019/08**

### **Xaica-AlphaPLUS**

### **Version 0118 / 0100 (SPI-001-05)**

*Paris, le 13 février 2019*

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

Guillaume POUPARD  
[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 présumées 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](mailto:certification@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.



<i>Référence du rapport de certification</i>	
<b>ANSSI-CC-2019/08</b>	
<i>Nom du produit</i>	
<b>Xaica-AlphaPLUS</b>	
<i>Référence/version du produit</i>	
<b>Version 0118 / 0100 (SPI-001-05)</b>	
<i>Conformité à un profil de protection</i>	
<b>[PP-PNC], version 1</b> <b>Personal Number Cards Protection Profile</b>	
<i>Critères d'évaluation et version</i>	
<b>Critères Communs version 3.1 révision 5</b>	
<i>Niveau d'évaluation</i>	
<b>EAL 4 augmenté</b> <b>ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2,</b> <b>AVA_VAN.5</b>	
<i>Développeurs</i>	
<b>NTT DATA Corporation</b> Toyosu Center Bldg. Annex, 3-9 Toyosu 3-chome, Koto-ku, Tokyo 135-8671, Japon	<b>Toppan Printing Co. LTD</b> 1-3-3, Suido, Bunkyo-ku Tokyo 112-8531, Japon
<b>STMicroelectronics</b> 190 Avenue Célestin Coq, ZI de Rousset, 13106 Rousset Cedex, France	
<i>Commanditaire</i>	
<b>Toppan Printing Co. LTD</b> 1-3-3, Suido, Bunkyo-ku Tokyo 112-8531	
<i>Centre d'évaluation</i>	
<b>Serma Safety &amp; Security</b> 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France	
<i>Accords de reconnaissance applicables</i>	
	
<b>Ce certificat est reconnu au niveau EAL2</b>	

# 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](http://www.ssi.gouv.fr).



# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Introduction</i> .....	6
1.2.2. <i>Services de sécurité</i> .....	6
1.2.3. <i>Architecture</i> .....	7
1.2.4. <i>Identification du produit</i> .....	7
1.2.5. <i>Cycle de vie</i> .....	8
1.2.6. <i>Configuration évaluée</i> .....	8
<b>2. L’EVALUATION .....</b>	<b>9</b>
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
<b>3. LA CERTIFICATION .....</b>	<b>10</b>
3.1. CONCLUSION .....	10
3.2. RESTRICTIONS D’USAGE .....	10
3.3. RECONNAISSANCE DU CERTIFICAT .....	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	11
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT .....</b>	<b>12</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>13</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>15</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est « Xaica-AlphaPLUS, Version 0118 / 0100 (SPI-001-05) » développé par *NTT DATA CORPORATION*, *TOPPAN PRINTING Co. LTD* et *STMICROELECTRONICS*.

Le produit évalué est de type carte à puce avec et sans contact. Il implémente une carte d'identité et des applications gouvernementales japonaises.

## 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-PNC]. La conformité est démontrable.

### 1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection de l'intégrité des données du porteur stockées dans la carte : pays ou organisation de délivrance, numéro du document, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait du porteur, autres données optionnelles ;
- la protection de l'intégrité et de la confidentialité des données lues à l'aide du mécanisme *secure messaging* ;
- l'authentification du microcontrôleur pour l'exécution des applications BANGO-AP, JUKI-AP, JPKE-AP et KENMEN-AP (voir [ST] pour la description des applications).

### 1.2.3. Architecture

L'architecture du produit est résumée par la figure 1 :

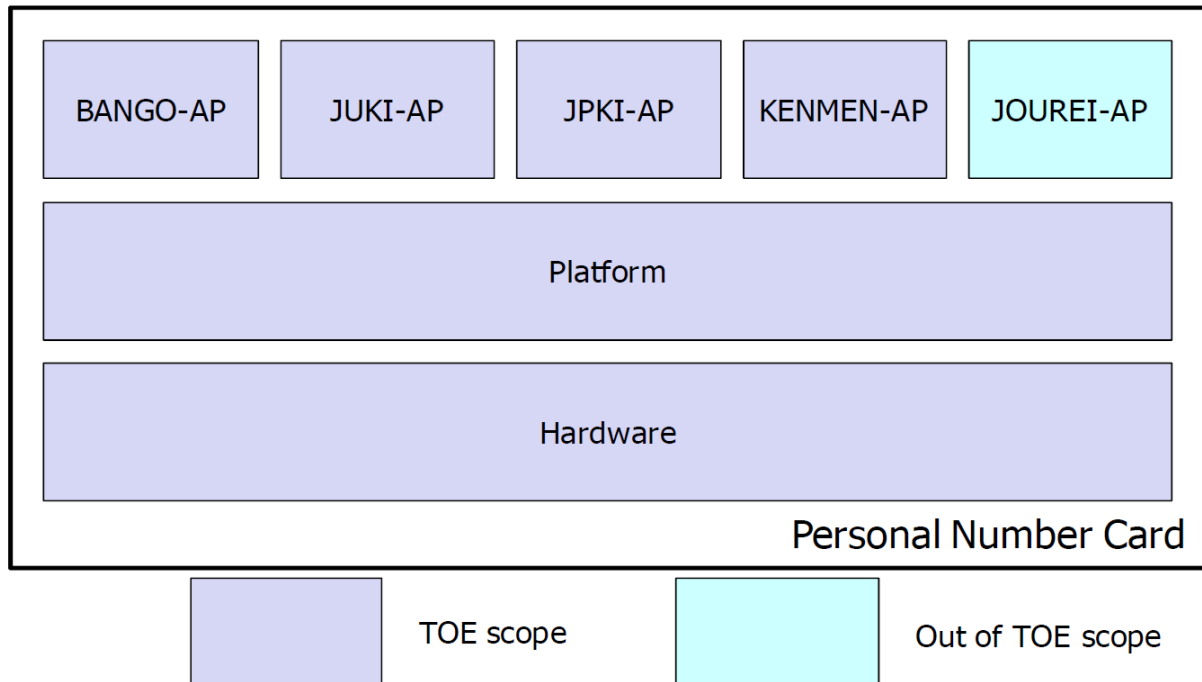


Figure 1 – Architecture du produit

Le produit est une carte à puce constituée :

- du microcontrôleur ST31G480 en révision interne C01 avec la librairie cryptographique NesLib v5.2, développé et fabriqué par *STMICROELECTRONICS* ;
- d'un système d'exploitation et d'applications natives développés par *TOPPAN PRINTING Co. LTD* et *NTT DATA CORPORATION* ;
- de l'application IAP (application d'initialisation) permettant de personnaliser les cartes vierges ;
- des applications requises par le profil de protection [PP-PNC], identifiées dans [ST] et dans [GUIDES] : BANGO-AP, JUKI-AP, JPKI-AP et KENMEN-AP ;
- d'un *Card Manager* se comportant comme une application *Global Platform*. Il permet notamment de créer les fichiers requis par les applications susmentionnées.

Note : le profil de protection [PP-PNC] mentionne que d'autres applications gouvernementales peuvent être installées sur la plateforme (application JOUREI-AP en dehors du périmètre de la TOE décrit ci-dessus figure 1).

### 1.2.4. Identification du produit

La version certifiée du produit est identifiable par les éléments du tableau ci-après, qui sont renvoyés par le produit suite à la commande GET DATA avec le tag '46h' (voir [GUIDES]) :

Champ	Valeur	Signification
<i>IC Manufacturer</i>	'0000000002'	<i>STMICROELECTRONICS</i>
<i>Card Manufacturer</i>	'4A50303342'	Outsource
<i>Issue identification</i>	'16141B01'	BANGO card

<i>TOE Version</i>	'0118'	BANGO card sur microcontrôleur ST31G480 en révision interne C01, incluant NesLib V5.2
<i>Softmask revision</i>	'0100'	SPI-001-05

### 1.2.5. Cycle de vie

Le cycle de vie du produit est basé sur celui du profil de protection [PP-PNC] :

- phase 1 : développement du composant et du logiciel ;
- phase 2 : développement du logiciel (développement de la plateforme, des applications susmentionnées et du script de pré-personnalisation appelé *OUT SOURCE*) ;
- phase 3 : fabrication ;
- phase 4 : personnalisation ;
- phase 5 : installation des applications additionnelles ;
- phase 6 : utilisation de la carte.

Le produit a été développé et fabriqué sur les sites suivants :

- sites de développement du logiciel :
  - **NTT DATA CORPORATION, Toyosu Center Building**  
3-9, Toyosu 3-chome  
Koto-ku; Tokyo 135-8671  
Japan
  - **TOPPAN PRINTING CORPORATION, Koishikawa Building**  
1-3-3, Suido  
Bunkyo-ku Tokyo 112-8531  
Japan

Les composants sont développés et fabriqués par *STMICROELECTRONICS*. Les sites de développement et de fabrication des puces *STMICROELECTRONICS* sont détaillés dans le rapport de certification [CER-IC].

### 1.2.6. Configuration évaluée

Le certificat porte sur la configuration de la TOE décrite au paragraphe 1.2.3 et configuré conformément aux [GUIDES]. La TOE est considérée comme étant une plateforme fermée sans l'application JOUREI-AP (les interfaces de la TOE avec cette application ne sont pas évaluées).



## 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 dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « *ST31G480 C01* » au niveau EAL4 augmenté des composants ADV\_IMP.2, ADV\_INT.3, ADV\_TDS.5, ALC\_CMC.5, ACL\_DVS.2, ALC\_FLR.1, ALC\_TAT.3, ATE\_COV.3, ATE\_FUN.2, AVA\_VAN.5, ASE\_TSS.2 conforme au profil de protection [PP-0035]. Ce microcontrôleur a été certifié le 5 octobre 2017 sous la référence [CER-IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 octobre 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-CRY] 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 d'aléas du produit était en dehors du périmètre de l'évaluation et n'a pas été analysé.

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a cependant été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).

## 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 « Xaica-AlphaPLUS, Version 0118 / 0100 (SPI-001-05) » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ADV\_FSP.5, ADV\_INT.2, ADV\_TDS.4, ALC\_CMS.5, ALC\_DVS.2, ALC\_TAT.2, 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].

### 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<sup>1</sup>, 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<sup>2</sup>, 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 :



---

<sup>1</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.org](http://www.sogis.org).

<sup>2</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://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 4+	Intitulé du composant	
<b>ADV</b> <b>Développement</b>	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
<b>AGD</b> <b>Guides d'utilisation</b>	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
<b>ALC</b> <b>Support au cycle de vie</b>	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
<b>ASE</b> <b>Evaluation de la cible de sécurité</b>	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
<b>ATE</b> <b>Tests</b>	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
<b>AVA</b> <b>Estimation des vulnérabilités</b>	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

## Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- Xaica-alphaPLUS Security Target, 24 janvier 2019, référence Xaica-alphaPLUS-SPC_ST, version 3.9.</li> </ul> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> <li>- Xaica-alphaPLUS Security Target Lite, 24 janvier 2019, référence Xaica-alphaPLUS-SPC_ST_lite, version 3.2.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report – ALPHA PLUS 2 Project, 31 janvier 2019, référence ALPHA_PLUS_2_ETR_v1.1, version 1.1</li> </ul>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>- Xaica-alphaPLUS-TCL-TOE Configuration List, version 3.50, 16 octobre 2018, NTT DATA Corporation.</li> </ul>
[GUIDES]	<p>Guide de préparation du produit :</p> <ul style="list-style-type: none"> <li>- Delivery Procedure ICard, référence Xaica-alphaPLUSDPSversion 3.10, 25 juillet 2018, NTT DATA Corporation ;</li> <li>- Manual for BANGO-AP administrator, reference Xaica-alphaPLUSMBA, 20 September 2018, version 3.30, NTT DATA Corporation ;</li> <li>- Manual for JPKE-AP administrator, reference Xaica-alphaPLUSMJP, 20 September 2018, version 3.30, NTT DATA Corporation ;</li> <li>- Manual for JUKI-AP administrator, reference Xaica-alphaPLUSMJU, 20 September 2018, version 3.30, NTT DATA Corporation ;</li> <li>- Manual for KENMEN-AP, administrator, reference Xaica-alphaPLUSMKE, 20 September 2018, version 3.30, NTT DATA Corporation ;</li> <li>- Manual for Platform administrator, reference Xaica-alphaPLUSMPF, 20 September 2018, version 3.30, NTT DATA Corporation ;</li> <li>- Manual for PrePerso and OUTSOURCE Specifications, reference, 20 September 2018, version 3.20, NTT DATA Corporation;</li> <li>- Manual for Cardholder, reference Xaica-alphaPLUSMCH, 25 juillet 2018, version 3.10, NTT DATA Corporation.</li> </ul>
[CER-IC]	<p>Rapport de certification ANSSI-CC-2017/61 – ST31G480 C01 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X. <i>Certifié par l'ANSSI le 5 octobre 2017 sous la référence ANSSI-CC-2017/61.</i></p>

[PP-PNC]	Protection Profile, Personal Number Cards Protection Profile, version 1.0, mai 2015. <i>Certifié par le JISEC (Japan IT Security Evaluation and Certification Scheme) sous la référence CRP-C0431-01.</i>
[PP0035]	Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i>

### 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 : <ul style="list-style-type: none"> <li>- Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;</li> <li>- Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;</li> <li>- Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.</li> </ul>
[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.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5.1, mai 2018.
[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-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.11 du 24 octobre 2008, voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .

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