



**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-2023/55**

**eTravel v2.3 on MultiApp v4.1 platform, PACE, EAC and  
AA activated  
(version 2.3.0.1)**

Paris, le 14 Décembre 2023

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

Emmanuel NAEGELEN

[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.

Référence du rapport de certification	<b>ANSSI-CC-2023/55</b>	
Nom du produit	<b>eTravel v2.3 on MultiApp v4.1 platform, PACE, EAC and AA activated</b>	
Référence/version du produit	<b>version 2.3.0.1</b>	
Conformité à un profil de protection	<b>Machine Readable Travel Document with « ICAO Application », Extended Access Control with PACE, version 1.3.2</b> Certifié BSI-CC-PP-0056-V2-2012-MA-02  <b>Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.0.1</b> Certifié BSI-CC-PP-0068-V2-2011-MA-01	
Critère d'évaluation et version	<b>Critères Communs version 3.1 révision 5</b>	
Niveau d'évaluation	<b>EAL5 augmenté</b> <b>ALC_DVS.2, AVA_VAN.5</b>	
Développeurs	<b>THALES DIS France</b> 6, rue de la Verrerie 92190 Meudon, France	<b>SAMSUNG ELECTRONICS CO. LTD</b> 17 Floor, B-Tower, DSR building, Samsungjeonja-ro 1-1, Hwaseong-si, Gyeonggi-do, 445-330 South Korea
Commanditaire	<b>THALES DIS FRANCE SAS</b> 6 rue de la Verrerie 92190 Meudon, France	
Centre d'évaluation	<b>SERMA SAFETY &amp; SECURITY</b> 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France	
Accords de reconnaissance applicables	 <b>CCRA</b>	 <b>SOG-IS</b>
Ce certificat est reconnu au niveau EAL2.		

## 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.cyber.gouv.fr](http://www.cyber.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.....	7
1.2.5	Cycle de vie .....	8
1.2.6	Configuration évaluée .....	8
2	L'évaluation.....	9
2.1	Référentiels d'évaluation .....	9
2.2	Travaux d'évaluation .....	9
2.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	9
2.4	Analyse du générateur d'aléa.....	9
3	La certification .....	10
3.1	Conclusion.....	10
3.2	Restrictions d'usage .....	10
3.3	Reconnaissance du certificat.....	11
3.3.1	Reconnaissance européenne (SOG-IS).....	11
3.3.2	Reconnaissance internationale critères communs (CCRA).....	11
ANNEXE A.	Références documentaires du produit évalué .....	12
ANNEXE B.	Références liées à la certification .....	14

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est l'application « eTravel v2.3 on MultiApp v4.1 platform, PACE, EAC and AA activated, version 2.3.0.1 » développé par THALES DIS France et embarquée sur le microcontrôleur S3FT9MH fabriqué par la société SAMSUNG ELECTRONICS CO. LTD.

Le produit est de type « carte à puce » pouvant être utilisé en modes avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit permet la vérification de l'authenticité du document de voyage et l'identification de son porteur notamment lors du contrôle aux frontières, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports ou dans une carte plastique. Ils peuvent être intégrés sous forme de module ou d'*inlay*.

## 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 aux profils de protection [PP EACv2] et [PP PACE].

### 1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité des données du porteur stockées dans la carte ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- l'authentification du microcontrôleur par le mécanisme « *Active Authentication* » (AA) ;
- l'authentification entre document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme « *Supplemental Access Control* » (PACE) ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de « *Secure Messaging* », des données lues ;
- l'authentification forte (avec validation de la chaîne de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme « *Extended Access Control* » (EAC) préalablement à tout accès aux données biométriques.

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

### 1.2.3 Architecture

Le produit est constitué :

- du microcontrôleur « S3FT9MH » certifié sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte « MultiApp V4.1 » certifiée sous la référence [CER-PTF] ;
- de l'application « eTravel v2.3 » implémentant les spécifications « *Machine Readable Travel Document* » (MRTD), avec les fonctionnalités PACE, EAC et AA activées.

Des applications peuvent être chargées sur la plateforme *Java Card* aux côtés de l'application « eTravel v2.3 ». La conformité aux prescriptions du document [OPEN] pour le chargement d'applications a été prise en compte pour les seules applications identifiées dans le certificat de la plateforme [CER-PTF].

Les guides [PTF\_AGD] identifient les recommandations relatives à la livraison des applications à charger sur cette carte. Par ailleurs, les guides [PTF\_AGD-Dev\_Basic] et [PTF\_AGD-Dev\_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; les guides [AGD\_OPE\_VA] décrivent les règles de vérification qui doivent être appliquées par l'autorité de vérification.

### 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] au chapitre 1.2 « *TOE Reference* » et dans les [GUIDES].

Eléments de configuration		Origine
Nom de la TOE	eTravel 2.3 EAC/SAC on MultiApp V4.1	THALES DIS FRANCE SAS
Référence de la TOE	eTravel 2.3 EAC/SAC Release 1.0	
Identification du produit	Référence : 'B0 58 20' (eTravel 2.3 on MultiApp 4.1) Configuration : '01', version : '0000' (Release 1.0)	
Identification de la plateforme	Référence : '19 81' (pour MultiApp) Date de release : '8271' (pour le 28 septembre 2018 – configuration 2) Version : '04 01' (pour 4.1)	
Identification du circuit intégré	Fabricant : '42 50' (pour Samsung) Référence : '16 11' (pour S3FT9MH)	SAMSUNG ELECTRONICS CO. LTD

Ces éléments peuvent être vérifiés en utilisant la commande GET DATA sur le CPLC (voir [GUIDES]).

La configuration des fonctionnalités supportées par le produit, telles que PACE, EAC et AA s'effectue lors de la phase de personnalisation, comme décrit dans les guides de la plateforme (voir [PTF\_AGD]).

### 1.2.5 Cycle de vie

Le cycle de vie est décrit au chapitre 2.4.2 de la cible de sécurité [ST]. Il est décomposé en quatre étapes :

- le développement (phases 1 à 2) ;
- la fabrication (phases 3 à 5) ;
- la personnalisation (phase 6) ;
- l'utilisation opérationnelle (phase 7).

Le périmètre de l'évaluation se limite aux deux premières étapes, correspondant aux phases 1 à 5 décrites dans le profil de protection [PP0084] :

- les phases 1 et 2 correspondent au développement du produit, plus précisément :
  - o au développement du logiciel embarqué : le *firmware* dédié au microcontrôleur, le système d'exploitation, le système *Java Card*, la documentation, des *applets* et d'autres parties logicielles de la plateforme ;
  - o au développement du microcontrôleur,
- les phases 3 et 4 correspondent à la fabrication et au conditionnement (*packaging*) du microcontrôleur ;
- la phase 5 correspond au chargement du logiciel embarqué (hormis le *firmware* qui est déjà masqué durant l'étape 3) dans le microcontrôleur. Il est à noter que le point de livraison, ou d'émission de la carte, est en sortie de phase 5.

Le cycle de vie est conforme à celui décrit dans [PP0084]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

### 1.2.6 Configuration évaluée

Le certificat porte sur l'application « eTravel v2.3 » avec les fonctionnalités EAC et AA activées, en composition sur la plateforme *Java Card* « MultiApp V4.1 » en configuration ouverte, masquée sur le microcontrôleur S3FT9MH, telles que présentées au chapitre « 1.2.3 Architecture ».

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte « cloisonnante ». Tout chargement de nouvelles applications doit être effectué conformément aux processus audités et doit répondre aux contraintes exposées au chapitre 3.2 du présent rapport de certification.



## 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 sur la plateforme déjà certifiée par ailleurs (voir [CER-PTF]).

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 [RTE].

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 applications chargées en post-émission sur ce produit doivent respecter les contraintes de développement de la plateforme ([PTF\_AGD-Dev\_Basic] et [PTF\_AGD-Dev\_Sec]) ;
- les autorités de vérification doivent appliquer les guides [AGD\_OPE\_VA] ;
- la protection du chargement de toutes les applications sur ce produit doit être activée conformément aux indications des guides [PTF\_AGD] ;
- l'utilisation du protocole SCP03 est à privilégier plutôt que les protocoles SCP01 et SCP02 qui sont déconseillés. Toutefois, si l'usage de l'un de ces deux derniers était rendu nécessaire, il est recommandé de le faire dans un environnement physiquement sécurisé et de chiffrer les données échangées (voir [APP\_AGD]).

### 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 [CCRA].

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.eu](http://www.sogis.eu).

<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 A. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- <i>MutliApp V4.1 : eTravel 2.3 EAC on SAC Security Target</i>, référence D1417547, version 1.13, 25 septembre 2023.</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>- <i>eTravel v2.3 on MultiApp v4.1 platform PACE, EAC and AA activated</i>, référence D1417547, version 1.13p, 25 septembre 2023.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- <i>Evaluation Technical Report SUNDANCE-E-NS Project</i>, référence SUNDANCE-E-NS_ETR_v1.2, version 1.2, 9 novembre 2023.</li> </ul>
[CONF]	<p>Liste de configuration du produit :</p> <p><i>MultiApp V4.1 : ALC LIS document – eTravel v2.3</i>, référence D1466245, version 1.7, 28 septembre 2023.</p>
[GUIDES]	<p>Guide d'installation, et d'utilisation du produit :</p> <p>[APP_AGD] :</p> <ul style="list-style-type: none"> <li>- <i>MultiApp V4.1 : AGD PRE document – eTravel v2.3</i>, référence D1425962, version 1.3, 30 mai 2023 ;</li> <li>- <i>MultiApp V4.1 : AGD OPE document – eTravel v2.3</i>, référence D1425961, version 1.4, 30 mai 2023 ;</li> <li>- <i>eTravel v2.2 and 2.3 Reference Manual</i>, référence D1392378, version C.9, 29 juillet 2021;</li> <li>- <i>Global Dispatcher Personalization Applet - User Guide</i>, référence D1390286Q, 3 mai 2021.</li> </ul> <p>Guides d'installation et d'administration de la plateforme [PTF_AGD]:</p> <ul style="list-style-type: none"> <li>- <i>MultiApp V4.1 AGD_PRE document - JavaCard Platform</i>, référence D1431307, version 1.2, 25 mai 2021 ;</li> <li>- <i>MultiApp V4.1 : AGD_OPE document – JavaCard Platform</i>, référence D1424308, version 2.1, 7 juillet 2023.</li> </ul> <p>Guide de développement d'applications basiques [PTF_AGD-Dev_Basic] :</p> <ul style="list-style-type: none"> <li>- <i>Rules for applications on Multiapp certified product</i>, référence D1390963, version 1.2, novembre 2017.</li> </ul> <p>Guide de développement d'applications sécurisées [PTF_AGD-Dev_Sec] :</p> <ul style="list-style-type: none"> <li>- <i>Guidance for secure application development on Multiapp platforms</i>, référence D1390326, version A02, janvier 2023.</li> </ul> <p>Guides pour l'autorité de vérification [AGD_OPE_VA] :</p> <ul style="list-style-type: none"> <li>- <i>Verification process of Gemalto non sensitive applet</i>, référence D1390670, version A01, février 2016 ;</li> <li>- <i>Verification process of Third Party non sensitive applet</i>, référence D1390671, version A01, février 2016.</li> </ul>
[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p>

	<ul style="list-style-type: none"> <li>- DISGEN21_ALC_GEN_v1.0 ;</li> <li>- DISGEN22_ALC_GEN_v1.0 ;</li> <li>- DISGEN23_ALC_GEN_v1.0 ;</li> <li>- [CBA] DISGEN23_CUR_STAR_v1.0 ;</li> <li>- [MDN] DISGEN21_MDN_STAR_v1.1 ;</li> <li>- [SGP] DISGEN22_SGP_STAR_v1.0 ;</li> <li>- [GEM] DISGEN22_GEM_STAR_v1.0 ;</li> <li>- [VAN] DISGEN23_VAN_STAR_v1.0 ;</li> <li>- [LVG] DISGEN22_LVG_STAR_v1.0 ;</li> <li>- [TCZ] DISGEN23_TCZ_STAR_v1.0 ;</li> <li>- [CAL] DISGEN23_VFO-CAL_STAR_v1.0 ;</li> <li>- [LCY] DISGEN22_LCY_STAR_v1.0 ;</li> <li>- [MAR] DISGEN21_MAR_STAR_v1.1 ;</li> <li>- [MGY] DISGEN23_MGY_STAR_v1.0 ;</li> <li>- [PUN] DISGEN23_PUN_STAR_v1.0 ;</li> <li>- [PAU] DISGEN22_PAU_STAR_v1.0.</li> </ul>
[CER-IC]	<p>Rapport de certification <i>S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional CE1 Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software (S3FT9MH_20220713)</i>. Certifié par l'ANSSI sous la référence ANSSI-CC-2023/20.</p>
[CER-PTF]	<p>Rapport de certification Plateforme ouverte <i>Java Card MultiApp V4.1</i> en configuration ouverte masquée sur le composant S3FT9MH (Version 4.1.0.2). Certifiée par l'ANSSI sous la référence ANSSI-CC-2023/30.</p>
[PP0084]	<p><i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages</i>, version 1.0, 13 janvier 2014. Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-PP-0084-2014.</p>
[PP EACv2]	<p><i>Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control</i>, version 1.3.2, 5 décembre 2012. Maintenu par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-CC-PP-0056-V2-2012-MA02.</p>
[PP PACE]	<p><i>Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE</i>, version 1.0.1, 22 juillet 2014. Maintenu par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-CC-PP-0068-V2-2011-MA-01.</p>

## 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]	<i>Common Criteria for Information Technology Security Evaluation:</i> <ul style="list-style-type: none"> <li>- <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;</li> <li>- <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;</li> <li>- <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.</li> </ul>
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[JIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.2, novembre 2022.
[COMP] *	<i>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices</i> , version 1.5.1, mai 2018.
[OPEN]	<i>Certification of « Open » smart card products</i> , version 1.1 (for trial use), 4 février 2013.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , 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.