PREMIER 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-2018/57v2

Annule et remplace le rapport de certification ANSSI-CC-2018/57 pour en réduire la portée

eTravel v2.3 on MultiApp v4.1 platform, PACE, EAC and AA activated

Paris, le 17 décembre 2021

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 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-2018/57v2

Nom du produit

eTravel v2.3 on MultiApp v4.1 platform, PACE, EAC and AA activated

Référence/version du produit

Version de l'application eTravel : 2.3
Version de la plateforme Java Card MultiApp : 4.1

Conformité à un profil de protection

Machine Readable Travel Document with « ICAO Application », Extended Access Control with PACE, version 1.3.2
Certifié BSI-CC-PP-0056-V2-2012-MA-02

Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.0.1
Certifié BSI-CC-PP-0068-V2-2011-MA-01

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5

Développeurs

THALES DIS FRANCE SAS
6, rue de la Verrerie
92190 Meudon, France

SAMSUNG ELECTRONICS CO. LTD
17 Floor, B-Tower, DSR building,
Samsungjeonja-ro 1-1, Hwaseong-si, Gyenonggi-do, 445-330 South Korea

Commanditaire

THALES DIS FRANCE SAS
6 rue de la Verrerie
92190 Meudon, France

Centre d'évaluation

SERMA SAFETY & SECURITY
14 rue Galilée, CS 10071,
33608 Pessac Cedex, 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

1.1 Présentation du produit

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

Le produit 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. Il est disponible en mode contact ou sans contact.

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 strictement conforme aux profils de protection [PP EACv2] et [PP PACE].

Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée (voir [NOTE25]), la cible de sécurité [ST] identifie clairement les évolutions du périmètre d'évaluation par rapport à celui de la certification initiale (voir [CER]). Ici, la réduction de portée correspond au retrait de la fonctionnalité PACE-CAM du périmètre d'évaluation.

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 chaine 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] 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 : '0B0 58 20' (eTravel 2.3 on MultiApp 4.1) Configuration : '01', version : '0000' (Release 1.0) Tag de compilation : MultiAppV41_EIR17_LBL01	
Identification de la plateforme	Référence : '19 81' (pour MultiApp) Date de *release* : '80 02' (pour le 2 janvier 2018) Version : '04 01' (pour 4.1)	
Identification du circuit intégré	Fabriquant: '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 :
  - 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 ;
  - 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 produit a été développé sur les sites suivants :

Gemalto Meudon 6 Rue de la Verrerie 92190 Meudon, France	*Gemalto* Singapore 12 Ayer Rajah Crescent Singapor 139941, Singapour
Gemalto Gémenos Avenue du Pic de Bertagne 13881 Gémenos, France	*Gemalto* La Ciotat Avenue du Jujubier, ZI Athelia IV 13705 La Ciotat, France
ATOS Paris (Aubervilliers / Croissy) 4 rue des Vieilles Vignes 77 183 Croissy-Beaubourg, France	*ATOS* Bydgoszcz – (*ATOS* Poland) Biznes Park, ul. Kraszewskiego 1 85-240 Bydgoszcz, Pologne
Gemalto Barcelona Poligono Industrial Llevant CL Llevant 12, 08150 Parets del Valles,Barcelona, Espagne	*Gemalto* Montgomeryville 101 & 106 Park Drive Montgomeryville, PA 18 936 Etats Unis d'Amérique
Gemalto Curitiba Rodovia Dep. Leopoldo Jacomel, 13102 83323-410 Pinhais, PR Brésil	*Gemalto* Vantaa Myllynkivenkuja 4, Vantaa, Finlande, FI-01620
Gemalto Tczew Ul. Skarszewska 2 33-110 Tczew, Pologne	*Gemalto* Pont Audemer Z.I. Saint Ulfrant rue de Saint Ulkfrant 27500 Pont Audemer, France

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

NB : Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée, la validité des audits n'a pas été vérifiée.

1.2.6 *Configuration évaluée*

Le certificat porte sur l'application « eTravel v2.3 » avec les fonctionnalités PACE, 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], à la méthodologie d'évaluation définie dans le manuel [CEM] et aux dispositions de [NOTE25].

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 s'appuie sur les résultats d'évaluation de ce même produit certifié le 12 décembre 2018 sous la référence ANSSI-CC-2018/57, voir [CER]. Elle correspond à une évaluation avec réduction de portée suite à l'identification de vulnérabilité.

L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat [CER] n'a pas été conduite dans le cadre de cette réévaluation partielle. Le niveau de résistance d'un produit certifié se dégrade au cours du temps. Seule une réévaluation ou une surveillance de cette version du produit permettrait de maintenir le niveau de confiance dans le temps.

Le CESTI en charge de l'évaluation initiale a émis un rapport d'analyse de réduction de portée (référence [RTE_part]) pour réévaluer les composants d'assurance impactés par l'évolution de la cible de sécurité du produit.

Le rapport technique d'analyse de réduction de portée [RTE_part], remis à l'ANSSI le 8 octobre 2021, pour réévaluer les composants d'assurance ASE, ADV, ALC (hors audits), et ATE impactés par l'évolution de la cible de sécurité [ST] détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

Le rapport technique [RTE_init], remis à l'ANSSI le 6 décembre 2018 détaille les travaux initialement réalisés menés par le centre d'évaluation et atteste que la résistance du produit atteignait VAN.5 lors de son édition.

2.3 Analyse 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 vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé à la date de certification initiale (voir [CER]).

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 [REF], 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 à la date de certification initiale (voir [CER]).

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 conformément à [NOTE25], répond aux caractéristiques de sécurité spécifiées dans la cible de sécurité [ST] pour le niveau d'évaluation visé à la date de certification initiale (voir [CER]). Pour rappel, les travaux d'analyse de la réduction de portée sont centrés sur l'impact de cette réduction de portée sur les tâches de conformité de l'évaluation initiale. La résistance globale du produit aux attaques de l'état de l'art n'a pas été mise à jour depuis la certification initiale.

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[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

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

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

[2] 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 : - *MutliApp V4.1 : eTravel 2.3 EAC on SAC Security Target*, référence D1417547, version 1.8, 9 septembre 2021. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *eTravel v2.3 on MultiApp v4.1 platform PACE, EAC and AA activated - Security Target Lite*, référence D1417547, version 1.8p, 21 septembre 2021.
[RTE]	Rapport technique d'évaluation : - [RTE_init] *Evaluation Technical Report SUNDANCE-E2 Project*, référence SUNDANCE-E2_ETR_v1.1, version 1.1, 6 décembre 2018 ; - [RTE_part] *ETR for Partial Re-Evaluation SUNDANCE-E-PC Project*, référence SUNDANCE-E_ETR-PR_v1.0, version 1.0, 8 octobre 2021.
[CONF]	Liste de configuration du produit : - *MultiApp V4.1 : ALC LIS document – eTravel v2.3*, référence D1466245, version 1.3, 21 septembre 2021.
[GUIDES]	Guide d'installation, et d'utilisation du produit : [APP_AGD] : - *MultiApp V4.1: AGD PRE document – eTravel v2.3*, référence D1425962, version 1.2, 9 septembre 2021 ; - *MultiApp V4.1 : AGD OPE document – eTravel v2.3*, référence D1425961, version 1.3, 9 septembre 2021 ; - *eTravel v2.2 and 2.3 Reference Manual*, référence D1392378, version C.9, 29 juillet 2021 ; - *Global Dispatcher Personalization Applet - User Guide*, référence D1390286Q, 3 mai 2021. Guides d'installation et d'administration de la plateforme [PTF_AGD]: - *MultiApp V4.1 AGD_PRE document - Javacard Platform*, référence D1431307, version 1.2, 25 mai 2021 ; - *MultiApp V4.1 : AGD_OPE document – Javacard Platform*, référence D1424308, version 1.7, 25 mai 2021. Guide de développement d'applications basiques [PTF_AGD-Dev_Basic] : - *Rules for applications on Multiapp certified product,* référence D1390963, version 1.2, novembre 2017. Guide de développement d'applications sécurisées [PTF_AGD-Dev_Sec] : - *Guidance for secure application development on Multiapp platforms,* référence D1390326, version A01, mars 2018. Guides pour l'autorité de vérification [AGD_OPE_VA] : - *Verification process of Gemalto non sensitive applet,* référence D1390670, version A01, février 2016 *;* - *Verification process of Third Party non sensitive applet,* référence D1390671, version A01, février 2016.

[CER]	Rapport de certification ANSSI-CC-2018/57, eTravel v2.3 on MultiApp v4.1 platform, PACE, EAC and AA activated. Certifié par l'ANSSI le 12 décembre 2018 sous la référence ANSSI-CC-2018/57.
[CER-IC]	Rapport de certification ANSSI-CC-2017/24, S3FT9MH / S3FT9MV / S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software. Certifié par l'ANSSI le 11 mai 2017 sous la référence ANSSI-CC-2017/24.
[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.
[PP EACv2]	*Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control*, version 1.3.2, 5 décembre 2012. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0056-V2-2012-MA02.
[PP PACE]	*Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE*, version 1.0.1, 22 juillet 2014. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0068-V2-2011-MA-01.
[CER-PTF]	Rapport de certification ANSSI-CC-2018/32v2, Plateforme ouverte Java Card MultiApp V4.1 en configuration ouverte masquée sur le composant S3FT9MH. Certifié par l'ANSSI le 8 octobre 2021 sous la référence ANSSI-CC-2018/32v2.

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 4.0.
[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 3.1, juin 2020.
[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*.
[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.
[NOTE25]	Note d'application: Réduction de portée d'un certificat CC, référence ANSSI-CC-NOTE-25_v1.0, version 1.0, 23 septembre 2021.

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