



**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-2025/05

PPCA application on MultiApp V5.1 Platform (version 1.0.1.A)

Paris, le 02 Mars 2025

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

Vincent STRUBEL

[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

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

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 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.

TABLE DES MATIERES

1	Résumé	5
2	Le produit.....	7
2.1	Présentation du produit.....	7
2.2	Description du produit.....	7
2.2.1	Introduction	7
2.2.2	Services de sécurité.....	7
2.2.3	Architecture	7
2.2.4	Identification du produit.....	7
2.2.5	Cycle de vie	8
2.2.6	Configuration évaluée	8
3	L'évaluation.....	9
3.1	Référentiels d'évaluation	9
3.2	Travaux d'évaluation	9
3.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	10
3.4	Analyse du générateur d'aléa.....	10
4	La certification	11
4.1	Conclusion.....	11
4.2	Restrictions d'usage	11
4.3	Reconnaissance du certificat.....	12
4.3.1	Reconnaissance européenne (SOG-IS).....	12
4.3.2	Reconnaissance internationale critères communs (CCRA).....	12
ANNEXE A.	Références documentaires du produit évalué	13
ANNEXE B.	Références liées à la certification	15

1 Résumé

Référence du rapport de certification	ANSSI-CC-2025/05
Nom du produit	PPCA application on MultiApp V5.1 Platform
Référence/version du produit	version 1.0.1.A
Type de produit	Cartes à puce et dispositifs similaires
Conformité à un profil de protection	Néant
Critère d'évaluation et version	Critères Communs version 3.1 révision 5
Niveau d'évaluation	EAL4 augmenté ALC_DVS.2, ATE_DPT.2, AVA_VAN.5
Référence du rapport d'évaluation	<i>Evaluation Technical Report, NOUMEA Project</i> référence NOUMEA_ETR_v1.0 version 1.0 26 novembre 2024
Fonctionnalité de sécurité du produit	Cf. 2.2.2 Services de sécurité
Exigences de configuration du produit	Hypothèses liées à l'environnement d'exploitation Cf. 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation	Cf. 4.2 Restrictions d'usage
Développeur	THALES DIS FRANCE SAS La Vigie – Avenue du jujubier – ZI Athelia IV 13705 La Ciotat Cedex
Commanditaire	THALES DIS FRANCE SAS La Vigie – Avenue du jujubier – ZI Athelia IV 13705 La Ciotat Cedex
Centre d'évaluation	SERMA SAFETY & SECURITY 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France
Accords de reconnaissance applicables	



Ce certificat est reconnu au niveau EAL2

SOG-IS



2 Le produit

2.1 Présentation du produit

Le produit évalué est « PPCA application on MultiApp V5.1 Platform, version 1.0.1.A » développé par THALES DIS FRANCE SAS.

Le contexte dans lequel ce produit est destiné à être utilisé est décrit à la section 3 « *TOE Overview* » de la cible de sécurité [ST].

2.2 Description du produit

2.2.1 Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité s'inspire du profil de protection [PP].

2.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont décrits au chapitre 3.2 « *TOE Description* » de la cible de sécurité [ST].

2.2.3 Architecture

L'architecture du produit est décrite au chapitre 3.1 « *Product Architecture* » de la cible de sécurité [ST].

2.2.4 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 suivants :

- Name (C0 Tag) : PPCA ;
- Version (C1 Tag) : 1.0.1.A.

2.2.5 Cycle de vie

Le cycle de vie du produit est décrit au chapitre 3.4 « *TOE Life-cycle* » de la cible de sécurité [ST]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

2.2.6 Configuration évaluée

Le certificat porte sur le produit identifié dans la cible de sécurité [ST] au chapitre 2.2 « *TOE identification* ».

La configuration ouverte du produit a été évaluée conformément à [OPEN] dans cadre de l'évaluation de la plateforme voir [CER] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 4.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

3 L'évaluation

3.1 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).

3.2 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 de l'application sur la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du produit « MultiApp V5.1, version 5.1 », voir [CER].

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

3.3 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.

3.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [ANSSI Crypto], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléa n'a pas révélé de faiblesse.

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.

4 La certification

4.1 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 (Cf § 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2025/05, a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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].

4.3 Reconnaissance du certificat

4.3.1 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'accord¹, 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 :



4.3.2 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 signataires², 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]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - <i>PPCA application on MultiApp V5.1 Platform Security Target</i>, référence D1606584, version 1.2, 23 avril 2024. <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"> - <i>PPCA application on MultiApp V5.1 Platform Security Target public version</i>, référence D1606584, version 1.2p.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - <i>Evaluation Technical Report, NOUMEA Project</i>, référence NOUMEA_ETR_v1.0, version 1.0, 26 novembre 2024.
[CONF]	<p>Listes de configuration du produit :</p> <ul style="list-style-type: none"> - <i>PPCA Code Configuration List</i>, référence ppca.mav51-1.0.1.A_filelist ; - <i>PPCA 1.0 application on MultiApp V5.1 Platform - Documentation list</i>, référence D161228, 14 mai 2024.
[GUIDES]	<ul style="list-style-type: none"> - <i>PPCA 1.0 application on MultiApp V5.1 Platform – AGD top level PPCA V1.0</i>, référence D1610581, version 1.0, 19 janvier 2024 ; - <i>Global Dispatcher Personalization AppletPPCA</i>, référence D1390286R, 4 novembre 2024 ; - <i>MultiApp ID Operating System - Reference Manual</i>, référence D1525385C, 7 décembre 2022 ; - <i>Polymorphic Pseudonym Card Application V1.0 Reference Manual</i>, référence D1430671F, 17 janvier 2024.
[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> - DISGEN24_ALC_GEN_v1.1 ; - DISGEN22_CHA_STAR_v1.0 ; - DISGEN23_CUR_STAR_v1.0 ; - DISGEN24_GEM_STAR_v1.0 ; - DISGEN24_LVG_STAR_v1.0 ; - DISGEN23_MDN_STAR_v1.0 ; - DISGEN22_PAU_STAR_v1.0 ; - DISGEN24_SGP_STAR_v1.0 ; - DISGEN23_SSN_SSC_STAR_v1.0 ; - DISGEN23-TCZ_STAR_v1.0 ; - DISGEN23_TLH_STAR_v1.0 ; - DISGEN23_VAN_STAR_v1.0 ; - DISGEN23_VFO-CAL_STAR_v1.0.
[CER]	<p>MultiApp V5.1 (version 5.1) Certifié par l'ANSSI le 28 août 2023 sous la référence ANSSI-CC-2023/31.</p>

[PP]	<p><i>Electronic Document implementing Extended Access Control version 2 defined in BSI TR-03110 (EAC2-PP), version 1.01, 13 juillet 2025.</i></p> <p>Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-CC-PP-0086-2015.</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, 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"> - <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[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 3.2.1, février 2024.
[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), version 2.0, mai 2024.
[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.