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-2025/40

IAS Classic v5.2.3 with MOC Server v3.1.1 on MultiApp V5.2 (Versions 5.2.3.A.C et 5.2.3.A.O)

Paris, le 15/12/2025 | 13:41 CET

Vincent Strubel

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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

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

Référence du rapport de certification **ANSSI-CC-2025/40**
Nom du produit **IAS Classic v5.2.3 with MOC Server v3.1.1 on MultiApp V5.2**
Référence/version du produit **Versions 5.2.3.A.C et 5.2.3.A.O**
Type de produit **Cartes à puce et dispositifs similaires**
Conformité à un profil de protection ***Protection profiles for secure signature creation device:*** *Part 2 : Device with key generation, v2.01, BSI-CC-PP-0059-2009-MA-02 ;* *Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012-MA-01 ;* *Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012-MA-01 ;* *Part 5 : Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012-MA-01 ;* *Part 6 : Extension for device with key import and trusted communication with signature creation application, v1.0.4, BSI-CC-PP-0076-2013-MA-01.*
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL5 augmenté** ALC_DVS.2, AVA_VAN.5
Référence du rapport d'évaluation *Evaluation Technical Report* – HOOKIPA-C référence LETI.CESTI.HOC.FULL.001 version 1.6 11 décembre 2025.
Fonctionnalité de sécurité du produit voir 2.2.2 Services de sécurité
Exigences de configuration du produit voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation voir 4.2 Restrictions d'usage
Développeur **THALES DIS FRANCE** 6, rue de la Verrerie 92190 Meudon, France

Commanditaire

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

Centre d'évaluation

CEA - LETI
17 avenue des martyrs,
38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

2 Le produit

2.1 Présentation du produit

Le produit évalué est « IAS Classic v5.2.3 with MOC Server v3.1.1 on MultiApp V5.2, Versions 5.2.3.A.C et 5.2.3.A.O » développé par THALES DIS FRANCE.

Ce produit est destiné à être utilisé comme dispositif sécurisé de création de signature (SSCD).

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.

Cette cible de sécurité est conforme aux profils de protection *Protection profiles for secure signature creation device* [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont détaillés dans la cible de sécurité [ST] au chapitre 2.1. « *TOE Description* ».

2.2.3 *Architecture*

Le produit est décrit au chapitre 2.2. « *TOE Boundaries* ».

Le produit s'appuie sur la librairie cryptographique développée par THALES DIS FRANCE SAS.

Des applications peuvent être chargées sur la plateforme *JavaCard* ouverte, au côté des applications *« IAS Classic V5.2.3 » et « MOC Server Application V3.1.1 »*. 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_PF].

Bien que ces applications ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, ces applications ont été vérifiées conformément aux contraintes de développements d'applications décrites dans le rapport de certification [CER_PF].

2.2.4 *Identification du produit*

La version certifiée du produit est identifiable par les éléments détaillés dans la cible de sécurité [ST] au chapitre 1.3 « *TOE Identification* ».

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans le guide [AGD_PRE_OPE] aux chapitres 3.1.1 et 3.1.2 (voir [GUIDES]).

Deux configurations existent pour cette application, *Full configuration* et *Compact configuration*.

2.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 2.3 « *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].

Pour l'évaluation, l'évaluateur a considéré comme :

- administrateur du produit : les agents qui agissent au nom de l'Etat ou de l'organisation émettrice et qui personnalisent le produit avec des données correspondant à l'identité de l'utilisateur ;
- utilisateur du produit : le titulaire légitime du produit.

2.2.6 *Configuration évaluée*

Le certificat porte sur l'application « *IAS Classic V5.2.3* » intégrant l'application « *MOC Server 3.1.1*» sur la plateforme ouverte *JavaCard « MultiApp 5.2 Premium PQC* » en configuration ouverte, telle que présentée plus haut au chapitre « 2.2.3 Architecture ».

La configuration ouverte du produit a été évaluée conformément à [OPEN] : 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 du logiciel dans la plateforme déjà certifiée dans le cadre d'un schéma national reconnu au titre de l'accord du SOG-IS.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « MultiApp 5.2 Premium PQC », voir [CER_PF].

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** ».

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 [ANA_CRY].

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.

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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2025/40 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]. Notamment :

- toutes les futures applications chargées sur ce produit (chargement après émission) doivent respecter les contraintes de développement de la plateforme (guides [AGD_PRE_OPE]) selon la sensibilité de l'application considérées ;
- les autorités de vérification doivent appliquer le guide [AGD_PRE_OPE] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement après émission) doit être activée conformément aux indications de [AGD_PRE_OPE].

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'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 :

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 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 : - *IAS Classic V5.2.3 with MOC Server v3.1.1 on MultiApp V5.2: Security Target*, référence D1598431, version 1.6, 6 octobre 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *IAS Classic V5.2.3 with MOC Server v3.1.1 on MultiApp V5.2: Security Target - Public Version*, référence D1598431, version 1.6p, 6 octobre 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report - HOOKIPA-C*, référence LETI.CESTI.HOC.FULL.001 - V1.6, version 1.6, 11 décembre 2025.
[ANA_CRY]	Cotation des mécanismes cryptographiques HOOKIPA-C, référence LETI.CESTI.HOC.RT.009-V1.2, version 1.2, 5 décembre 2025.
[GUIDES]	Guide d'installation et d'administration du produit : - [AGD_PRE_OPE] *MultiApp V5.2: AGD OPE and PRE - IAS Classic v5.2.3*, référence D1617386, version 1.6, 25 septembre 2025 ; - *IAS Classic Applet v5.2 Personalization Guide*, référence D1546633, version B, 20 septembre 2022. Guide d'utilisation du produit : - *IAS Classic Applet V5.2 Reference Manual*, référence D1542053, version E, 25 novembre 2024 ; - *BioPIN Manager V3.1 Reference Manuel*, référence D1596852, version A, 19 juin 2023. Guides de développement et de protection des applications : - [PTF_AGD] *MultiApp Guidance Document - Guidance for secure development on Multiapp products*, référence D1539156, version 1.3A.1, 1er septembre 2025.
[SITES]	Rapports d'audit de site pour la réutilisation : - DISGEN23_ALC_GEN_v1.1 ; - DISGEN24_ALC_GEN_v1.1 ; - DISGEN25_ALC_GEN_v1.1 ; - DISGEN24_LVG_STAR_v1.1 ; - DISGEN23_MDN_STAR_v1.0 ; - DISGEN25_VAN_STAR_v1.0 ; - DISGEN24_GEM_STAR_v1.0 ; - DISGEN24_SGP_STAR_v1.0 ; - DISGEN25_TCZ_STAR_v1.0 ;

	- DISGEN24_CHA_STAR_v1.0 ; - DISGEN25_CUR_STAR_v1.0 ; - DISGEN24_PAU_STAR_v1.0 ; - DISGEN23_SSN_SSC_STAR_v1.0 ; - DISGEN24_ELC_STAR_v1.1 ; - DISGEN25_MGY_STAR_v1.0 ; - DISGEN25_VFO-CAL_STAR_v1.0 ; - DISGEN23_TLH_STAR_v1.0.
[CER_IC]	*IFX_CCI_00003Bh, 000043h, 00005Dh, 00005Eh, 00005Fh, 000060h, 000061h, 000062h, 000063h, 000064h, design step S11 with firmware 80.309.05.0, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000, optional ACL v3.33.003 and v3.34.000 and v3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance.* Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 13 septembre 2024 sous la référence BSI-DSZ-CC-1169-V4-2024.
[CER_PF]	Plateforme *JavaCard* MultiApp 5.2 Premium PQC, (version 5.2). Certifiée par l'ANSSI sous la référence [ANSSI-CC-2025/32].
[PP-SSCD-Part2]	*Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 419211-2:2013, version 2.0.1 datée du 18 mai 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0059-2009-MA-02.
[PP-SSCD-Part3]	*Protection profiles for secure signature creation device – Part 3: Device with key import*, référence : prEN 419211-3:2013, version 1.0.2 datée du 14 septembre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0075-2012-MA-01.
[PP-SSCD-Part4]	*Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application*, référence : prEN 419211-4:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0071-2012-MA-01.
[PP-SSCD-Part5]	*Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application*, référence : prEN 419211-5:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0072-2012-MA-01.

[PP-SSCD-Part6]	*Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application*, référence : prEN 419211-6:2014, version 1.0.4 datée du 25 juillet 2014. Maintenu par le BSI le 30 juin 2016 sous la référence BSI-CC-PP-0076-2013-MA-01.

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 5.4.
[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]	*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,* version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG AP] *	*Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.2.1, février 2024.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[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.
[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.