



**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-2023/42

**IAS Classic v5.2.1 with MOC Server v3.1 on MultiApp
V5.1
(Versions 5.2.1.A.C et 5.2.1.A.O)**

Paris, le 22 Septembre 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

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

Référence du rapport de certification	ANSSI-CC-2023/42	
Nom du produit	IAS Classic v5.2.1 with MOC Server v3.1 on MultiApp V5.1	
Référence/version du produit	Versions 5.2.1.A.C et 5.2.1.A.O	
Conformité à un profil de protection	Protection profiles for secure signature creation device: <i>Part 2 : Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-02 ;</i> <i>Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012-MA-01 ;</i> <i>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 ;</i> <i>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 ;</i> <i>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.</i>	
Critère d'évaluation et version	Critères Communs version 3.1 révision 5	
Niveau d'évaluation	EAL5 augmenté ALC_DVS.2, AVA_VAN.5	
Développeurs	THALES DIS FRANCE SAS 6 rue de la Verrerie 92190 Meudon, France	THALES DIS DESIGN SERVICES Arteparc, Bât D, Route de la côte d'Azur 13590 Meyreuil, France
Commanditaire	THALES DIS FRANCE SAS 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	  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.ssi.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.....	8
1.2.5	Cycle de vie	9
1.2.6	Configuration évaluée	10
2	L'évaluation.....	11
2.1	Référentiels d'évaluation	11
2.2	Travaux d'évaluation	11
2.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	11
2.4	Analyse du générateur d'aléa.....	11
	La certification	12
2.5	Conclusion.....	12
2.6	Restrictions d'usage	12
2.7	Reconnaissance du certificat.....	13
2.7.1	Reconnaissance européenne (SOG-IS).....	13
2.7.2	Reconnaissance internationale critères communs (CCRA).....	13
ANNEXE A.	Références documentaires du produit évalué	14
ANNEXE B.	Références liées à la certification	16

1 Le produit

1.1 Présentation du produit

Le produit évalué est l'application « IAS Classic v5.2.1 with MOC Server v3.1 on MultiApp V5.1, Versions 5.2.1.A.C et 5.2.1.A.O » développée par THALES DIS FRANCE SAS et embarquée sur le microcontrôleur AQUARIUS_BA_09 fabriqué par THALES DIS.

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

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 *Protection profiles for secure signature creation device* [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- ceux de la plateforme *JavaCard* en configuration ouverte MultiApp V5.1, certifiée sous la référence [ANSSI-CC-2023/31] ;
- la génération de la donnée de création de signature (*Signature Creation Data* ou SCD) et de la donnée de vérification de signature (*Signature Verification Data* ou SVD) associée ;
- l'export de la donnée de vérification de signature (SVD) pour une création de certificat électronique ;
- l'import de la donnée de création de signature (SCD) et de la donnée de vérification de signature (SVD) associée ;
- la réception et le stockage du certificat électronique ;
- le passage de l'état non-opérationnel à l'état opérationnel ;
- la création de signature électronique via un canal de confiance ;
- l'authentification de l'administrateur ;
- l'authentification du signataire par un code PIN ou des données biométriques d'empreintes digitales.

1.2.3 Architecture

Le produit est constitué :

- de l'application *IAS Classic V5.2.1* ;
- de la plateforme *JavaCard MultiApp V5.1* ;
- de l'application de PIN biométrique *MOC Server Application V3.1.1* ;
- du composant *AQUARIUS_BA_09* ;
- d'autres applications extérieures à la Cible d'Évaluation.

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 V5.2.1* » et « *MOC Server Appliation 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].

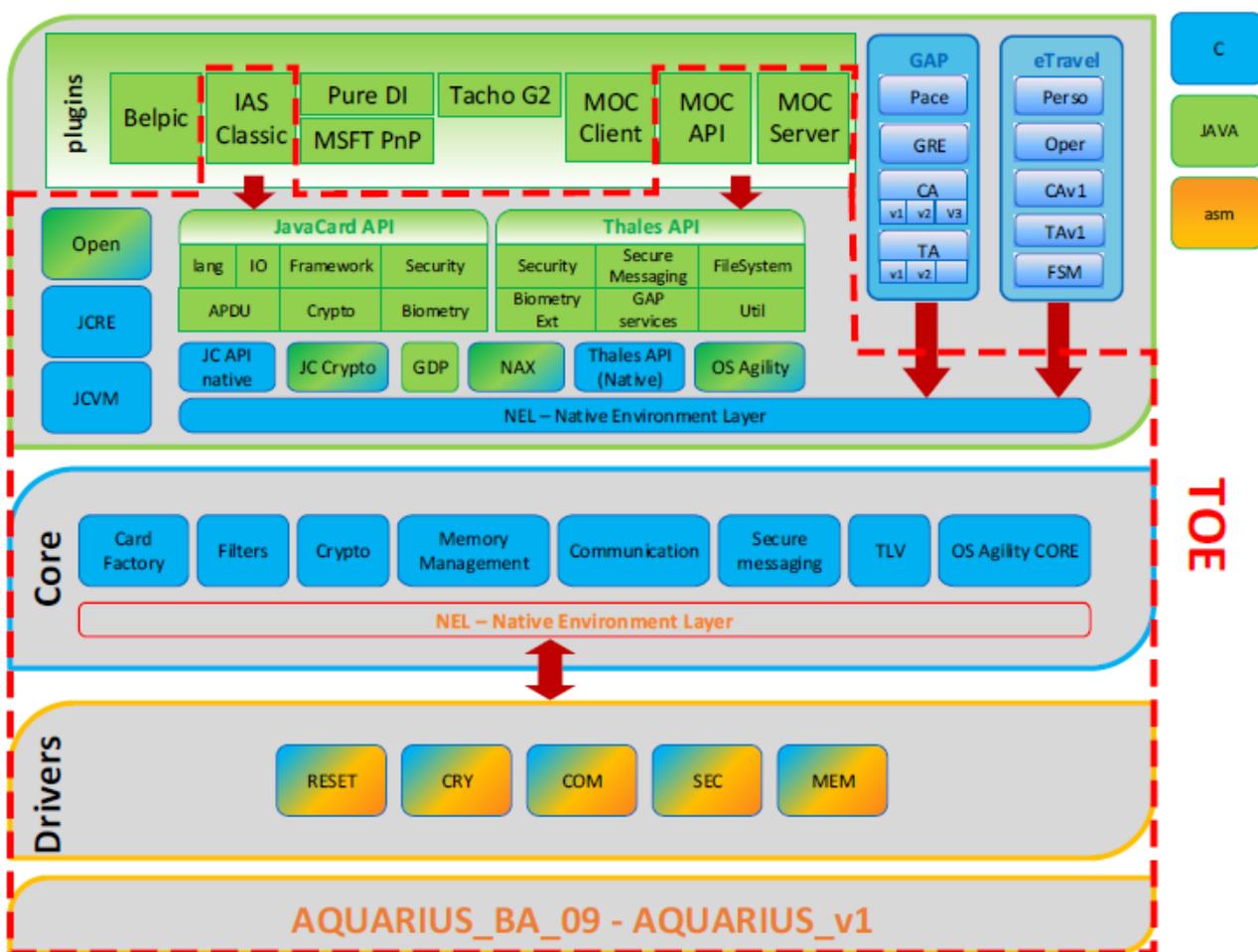


Figure 1 Limites de la TOE

1.2.4 Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

1.2.4.1 Identification de l'application IAS Classic

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

Tag	Donnée
9F7Fh	<i>CPLC data</i>
7F30h	<i>Software version</i>
DF30h	<i>Applet version</i>

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET DATA. La procédure d'identification est décrite dans le guide [AGD_OPE] (voir [GUIDES]).

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

CPLC

La valeur des *CPLC* est identique pour les deux configurations. Les valeurs ci-dessous participent à l'identification du produit.

Donnée	Valeur
<i>IC fabricant</i>	1290h
<i>IC type</i>	0013h
<i>Operating system identifier</i>	1981h
<i>Operating system release date</i>	3055h
<i>Operating system release level</i>	0510h

Software version

Cette donnée contient deux données, *Applet label* et *Applet version*, identifiées par les tags C0 et C1.

Application en *Full configuration* :

Tag	Donnée	Valeur
C0	<i>Applet label</i>	ASCII : « IAS Classic v5 » hexadécimal : 49415320436C6173736963207635h
C1	<i>Applet version</i>	ASCII : « 5.2.1.A.C » hexadécimal : 352E322E312E412E43h

Application en *Compact configuration* :

Tag	Donnée	Valeur
C0	<i>Applet label</i>	ASCII : « IAS Classic v5 » hexadécimal : 49415320436C6173736963207635h
C1	<i>Applet version</i>	ASCII : « 5.2.1.A.O » hexadécimal : 352E322E312E412E4Fh

Applet version

La valeur de cette donnée est identique à celle du tag C1 de *Software version*.

1.2.4.2 Identification de l'application MOC Server

L'application *MOC Server* est identifiable par la commande GET VERSION, décrite au chapitre 1.3.4 de [ST].

Tag	Donnée	Valeur
A0	<i>Applet label</i>	ASCII : "MOCA SERVER 3.1" Hexadécimal : 4D4F43412053455256455220332E31h
A1	<i>Applet version</i>	ASCII : "3.1.1.A" Hexadécimal : 332E312E312E41h
A2	<i>Fingerprint Algo version</i>	00CEh
A3	<i>Face Algo version</i>	0502h
A4	<i>Iris Algo version</i>	0300h

1.2.5 Cycle de vie

Le cycle de vie du produit est décrit dans [ST] au chapitre 2.3.2, *Four phases* et se découpe en quatre phases.

- La phase de développement correspond aux étapes de conception du produit, comprenant :
 - o La conception du composant ;
 - o La conception du logiciel embarqué ;
 - o la rédaction des documents de référence ;
- La phase de fabrication correspond aux étapes de fabrication, assemblage et conditionnement du produit ;
- La phase de personnalisation correspond à l'étape où les données de l'utilisateur final sont inscrites dans le produit ;
- La phase opérationnelle correspond à l'utilisation du produit par son utilisateur final.

Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES]. Le guide [AGD-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs, le guide [PTF_AGD-Dev] décrit les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD-OPE_VA] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

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.

1.2.6 Configuration évaluée

Le certificat porte sur l'application « *IAS Classic V5.2.1* » intégrant l'application « *MOC Server 3.1.1* » sur la plateforme ouverte *JavaCard* « *MultiApp V5.1* » en configuration ouverte, masquée sur le composant « *AQUARIUS_BA_09* », telle que présentée plus haut au chapitre « 1.2.3 Architecture » et personnalisée conformément à [AGD_PRE].

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 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

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 dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « AQUARIUS_BA_09 », certifié le 11 janvier 2023 sous la référence [ANSSI-CC-2023/01] (voir [CER_IC]).

L'évaluation s'appuie sur les résultats d'évaluation de la plateforme *JavaCard* « MultiApp 5.1 » certifiée sous la référence [ANSSI-CC-2023/31], 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** ».

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 [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 potentiel d'attaque 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 traitement 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 potentiel d'attaque 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 futures applications chargées sur ce produit (chargement post-émission) doivent respecter les contraintes de développement de la plateforme (guide [AGD-Dev]) selon la sensibilité de l'application considérée ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications de [TECH_LOAD] ;
- le chargement des applications pré- émission doit être protégé conformément au guide [ORG_LOAD] ;

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'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 :



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 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>IAS Classic v5.2.1 with MOC Server v3.1.1 on MultiApp v5.1 Security Target</i>, référence D1569576, version 1.0, 02 mai 2023. <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>IAS Classic v5.2.1 with MOC Server v3.1.1 on MultiApp v5.1 Security Target Lite</i>, référence D1569576, version 1.0p, 04 mai 2023.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - <i>Evaluation Technical Report – NIGELLE C</i>, référence LETI.CESTI.NIC.FULL.001 – V1.2, version 1.2, 11 août 2023.
[ANA_CRY]	<p>Cotation des mécanismes cryptographiques NIGELLE-C, référence LETI.CESTI.NIC.RT.009- V1.0, version 1.0, 05 mai 2023.</p>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - <i>IAS Classic 5.2.1 on MultiApp V5.1: ALC LIS CC document</i>, référence D1580146, version 1.14, 04 mai 2023 ; - <i>ALC LIS Common Criteria IAS Classic v5.2.1 – MAV 5.1</i>, référence D1593250, version v1.1, 20 avril 2023 ; - <i>ALC LIS Common Criteria MOC Server – MAV5.1</i>, référence D1593251, version v1.1, 20 avril 2023.
[GUIDES]	<p>Guide d'installation et d'administration du produit :</p> <ul style="list-style-type: none"> - <i>IAS Classic Applet v5.2 Personalization Guide</i>, référence D1546633, version B, 20 septembre 2022 ; - <i>MultiApp V5.1 AGD OPE and PRE document IAS Classic v5.2.1</i>, référence D1588538, version 1.4, 03 mai 2023. <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - <i>IAS Classic Applet V5.2 Reference Manual</i>, référence D1542053, version C, 26 octobre 2022 ; - <i>BioPIN Manager V3 Reference Manuel</i>, référence D1481720, version E, 25 juin 2021. <p>Guides de développement et de protection des applications :</p> <ul style="list-style-type: none"> - [PTF_AGD] <i>MultiApp Guidance for secure application development on Multiapp platforms</i>, référence D1539156, version 1.2, 24 mars 2023. <p>Guides pour l'autorité de vérification [AGD-OPE_VA] :</p> <ul style="list-style-type: none"> - <i>Verification process of Gemalto non sensitive applet</i>, référence D1484874, version 1.2, février 2021 ; - [ORG_LOAD] <i>Verification process of Third Party non sensitive applet</i>, référence D1484875, version 1.21, février 2021.
[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> - DISGEN20_ALC_GEN_v1.1 ; - DISGEN21_ALC_GEN_v1.1 ; - DISGEN22_ALC_GEN_v1.1 ;

	<ul style="list-style-type: none"> - [CBA] DISGEN21_CTB_STAR_v1.1 ; - [MDN] DISGEN21_MDN_STAR_v1.1 ; - [SGP] DISGEN22_SGP_STAR_v1.0 ; - [GEM] DISGEN22_GEM_STAR_v1.0 ; - [VAN] DISGEN21_VAN_STAR_v1.0 ; - [VIG] DISGEN20_VIG_STAR_v1.1 ; - [TCZ] DISGEN20_TCZ_STAR_v1.0 ; - [CAL] DISGEN21_VFO-CAL_STAR_v1.0 ; - [LCY] DISGEN22_LCY_STAR_v1.0 ; - [MAR] DISGEN21_MAR_STAR_v1.1 ; - [CHA] DISGEN21_CHA_STAR_v1.0 ; - [PUN] DISGEN21_PUN_STAR_v1.0 ; - [PAU] DISGEN22_PAU_STAR_v1.0.
[CER_PF]	Plateforme <i>JavaCard</i> « MultiApp 5.1 ». Certifiée par l'ANSSI sous la référence [ANSSI-CC-2023/31].
[CER_IC]	Rapport de certification ANSSI/01.AQUARIUS_BA_09, AQUARIUS_v1 Certifié par l'ANSSI sous la référence [ANSSI-CC-2023/01].
[PP-SSCD-Part2]	<i>Protection profiles for secure signature creation device – Part 2: Device with key generation</i> , référence : prEN 419211-2:2013, version 2.0.1 datée du 18 mai 2013. Maintenu par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) le 30 juin 2016 sous la référence BSI-CC-PP-0059-2009-MA-02.
[PP-SSCD-Part3]	<i>Protection profiles for secure signature creation device – Part 3: Device with key import</i> , référence : prEN 419211-3:2013, version 1.0.2 datée du 14 septembre 2013. Maintenu par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) le 30 juin 2016 sous la référence BSI-CC-PP-0075-2012-MA-01.
[PP-SSCD-Part4]	<i>Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application</i> , référence : prEN 419211-4:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) le 30 juin 2016 sous la référence BSI-CC-PP-0071-2012-MA-01.
[PP-SSCD-Part5]	<i>Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application</i> , référence : prEN 419211-5:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) le 30 juin 2016 sous la référence BSI-CC-PP-0072-2012-MA-01.
[PP-SSCD-Part6]	<i>Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application</i> , 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, 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"> - <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, 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.