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-2020/53-R01

IAS ECC v2, version 1.3, in configuration #4 on ID-One Cosmo v8.2 open platform on NXP P6022M VB (Identification de l'application : F0 02 02 13)

Paris, le 10 Novembre 2023

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

Référence du rapport de certification

ANSSI-CC-2020/53-R01

Nom du produit

IAS ECC v2, version 1.3, in configuration #4 on ID-One Cosmo v8.2 open platform on NXP P6022M VB

Référence/version du produit

Identification de l'application : F0 02 02 13

Conformité à un profil de protection

Protection profiles for secure signature creation device:

Part 2 : Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-01 *;*
Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012 *;*
Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012.

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL5 augmenté
ALC_DVS.2, AVA_VAN.5

Développeurs

IDEMIA
2 Place Samuel de Champlain,
92400 Courbevoie, France

NXP SEMICONDUCTORS GMBH
Beiersdorfstraße 12,
22529 Hamburg, Allemagne

Commanditaire

IDEMIA
2 Place Samuel de Champlain,
92400 Courbevoie, France

Centre d'évaluation

CEA - LETI
17 avenue des martyrs,
38054 Grenoble Cedex 9, 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 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 7
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
3.4 Reconnaissance du certificat 11
3.4.1 Reconnaissance européenne (SOG-IS) 11
3.4.2 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 « *IAS ECC v2, version 1.3, in configuration #4 on ID-One Cosmo v8.2 open platform on NXP P6022M VB*, Identification de l'application : F0 02 02 13 » développé par IDEMIA et masquée sur le composant NXP P6022M VB développé par NXP SEMICONDUCTORS GMBH.

Ce produit est une carte à puce constituée d'un logiciel conforme au standard IAS ECC v2 et d'un microcontrôleur sécurisé. Il est destiné à être utilisé comme dispositif sécurisé de création de signature ou de sceau électronique (SSCD[1]). Il peut être utilisé dans différents types de documents (carte d'identité, permis de conduire, carte d'entreprise, passeport, etc.) disposant d'interfaces avec et/ou sans contact.

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-SSCD-Part2], [PP-SSCD-Part3] et [PP-SSCD-Part4].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont détaillés dans la cible de sécurité [ST] aux chapitres 3.3.5 « *Usage and Major Security features* ». Ils sont résumés ci-après :

- la création de signature ou de sceau électronique ;
- la génération des clés de signature (c'est-à-dire la génération de la donnée de création de signature (SCD[2]) et de la donnée de vérification de signature (SVD[3]) associée) ;
- l'import des clés de signature (c'est-à-dire de la SCD et, optionnellement, de la SVD associée) ;
- l'export de clé publique (c'est-à-dire la SVD) ;
- l'établissement d'un canal de confiance pouvant permettre la création de signature électronique, l'import de la SCD ou l'export de la SVD dans un environnement non protégé ;
- l'authentification du porteur de carte basée sur la vérification d'un code PIN ou de données biométriques, appelés indistinctement donnée d'authentification de référence (RAD[4]) ;
- le déblocage de la RAD.

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

[1] *Secure Signature Creation Device*

[2] *Signature Creation Data*

[3] *Signature Verification Data*

[4] *Reference Authentication Data*

1.2.3 *Architecture*

Le produit est constitué :

- du microcontrôleur « NXP P6022M VB » certifié sous la référence [CER-IC] ;
- de la plateforme *JavaCard* ouverte « ID-One Cosmo V8.2 » certifiée sous la référence [CER-PTF] ;
- de l'application « IAS ECC v2 version 1.3 » en configuration #4.

Des applications peuvent être chargées sur la plateforme *JavaCard* ouverte, à côté de l'application « IAS ECC v2, version 1.3 ». Il s'agit soit des applications identifiées dans le certificat de la plateforme [CER-PTF], soit d'applications inconnues à condition que leur chargement respecte les [GUIDES]. La conformité aux prescriptions du document [OPEN] pour le chargement d'applications a été prise en compte lors de l'évaluation de la plateforme [CER-PTF].

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 détaillés dans la cible de sécurité [ST] au chapitre 3.2 « *TOE Reference* » et dans les [GUIDES].

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au paragraphe 3.5 de [ST] ; il est conforme à celui décrit dans [PP0084]. Il est composé des phases listées dans le tableau suivant, pouvant être regroupées en trois étapes :

- le développement (phases 1 à 3) ;
- la production (phases 4 et 5) ;
- l'état opérationnel (phases 6 et 7).

Le point de livraison de la TOE est en sortie de la phase 3. Après cette phase la TOE est considérée comme auto-protégée.

Phases	Tâches	Classes d'assurance	Acteurs ou Sites
1	Développement des parties logicielles	ALC	IDEMIA (Courbevoie et Pessac) Sites de [CER-PTF]
2	Développement du microcontrôleur	ALC	Sites de [CER-IC]
3	Fabrication	ALC	Sites de [CER-PTF] et [CER-IC]
Point de livraison de la TOE			
4	*Packaging* et initialisation	AGD_PRE	Agent de fabrication
5	Pré-personnalisation	AGD_PRE	Agent de fabrication
6	Personnalisation	AGD_PRE	Agent personnalisateur
7	Utilisation	AGD_OPE	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].

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

1.2.6 *Configuration évaluée*

Le certificat porte sur le produit identifié au paragraphe 1.2.4 et configuré comme suit :

- l'application « IAS ECC v2 » est instanciée sur la plateforme *JavaCard* ouverte couverte par le certificat [CER-PTF] ;
- les recommandations des [GUIDES] sont strictement appliquées pendant les phases de « Pré-personnalisation » et « Personnalisation » afin de personnaliser l'application en configuration #4.

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 dans [CER-PTF] 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 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 [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.

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 en ce qui concerne la vérification et le chargement d'applications, qui doivent être effectués conformément aux résultats de l'évaluation de la plateforme (voir [CER-PTF]).

3.4 Reconnaissance du certificat

3.4.1 *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[5], 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 :

3.4.2 *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[6] , 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 :

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

[6] 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 : - *Clytemnestre-R in Configuration #4 IAS ECC V2 Security Target*, FQR 110 8967, version 7, 22 septembre 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *IAS ECC v2, version 1.3, in configuration #4 on ID-One Cosmo v8.2 open platform on NXP P6022M VB - Public Security Target*, référence FQR 110 9187, version 5, 22 septembre 2023.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report CLYTEMNESTRE-R2*, référence LETI.CESTI.CLR2.FULL.001, version 4.3, 26 octobre 2023.
[ANA_CRY]	Cotation des mécanismes cryptographiques CLYTEMNESTRE-R2, référence LETI.CESTI.CLR2.RT.002 - V1.2, 19 octobre 2023.
[CONF]	Liste de configuration du produit : - *CLYTEMNESTRE_R CONFIGURATION LIST*, référence 110 9083, version 6, 25 septembre 2023.
[GUIDES]	Guide d'installation du produit : - [AGD_PRE] CLYTEMNESTRE-R ADV_PRE, référence FQR 110 8968, version 2, 11 avril 2019. Guide d'administration du produit : - [AGD_OPE] CLYTEMNESTRE-R ADV_OPE, référence FQR 110 8969, version 3, 5 août 2019. Guide d'utilisation du produit : - [AGD_QUA] CLYTEMNESTRE Recommandations pour la compatibilité avec le référentiel de qualification renforcée, référence 110 9078, version 3, 26 juin 2023.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA2022_GEN_v1.0 ; - [CRB] IDEMIA2022_CRB_STAR_v1.1 ; - [PSC] IDEMIA2022_Pessac_STAR_v1.0.
[CER-IC]	*Certification Report BSI-DSZ-CC-1059-V5-2022 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH* Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-DSZ-CC-1059-V5-2022.
[CER-PTF]	Rapport de certification Plateforme *ID-One Cosmo v8.2* masquée sur le composant NXP P60D145. Certifiée par l'ANSSI sous la référence ANSSI-CC-2020/26-R01.

[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 23 janvier 2012. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.
[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 24 juillet 2012. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.
[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 14 novembre 2012. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.
[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.

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]	*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 3.2, novembre 2022.
[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.