

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CC-2022/18v2

**CombICA0 Applet v3 on ID-One Cosmo X (SSCD
Configuration)
(SAAAAR : 203742)**

Paris, le 05 MAI 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-2022/18v2	
Nom du produit	CombiCAO Applet v3 on ID-One Cosmo X (SSCD Configuration)	
Référence/version du produit	SAAAAR : 203742	
Conformité à un profil de protection	Protection profiles for secure signature creation device: <i>Part 2 : Device with key generation, v2.01, 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	IDEMIA 2 place Samuel de Champlain 92400 Courbevoie, France	INFINEON TECHNOLOGIES AG AIM CC SM PS – Am Campeon 1-12, 85579 Neubiberg, 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	 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	6
1.2.4	Identification du produit.....	6
1.2.5	Cycle de vie	6
1.2.6	Configuration évaluée	7
2	L'évaluation.....	7
2.1	Référentiels d'évaluation	8
2.2	Travaux d'évaluation	8
2.3	Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	9
2.4	Analyse du générateur d'aléa.....	9
3	La certification	9
3.1	Conclusion.....	10
3.2	Restrictions d'usage	10
3.3	Reconnaissance du certificat.....	10
3.3.1	Reconnaissance européenne (SOG-IS).....	11
3.3.2	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 « CombiCAO Applet v3 on ID-One Cosmo X (SSCD Configuration), SAAAAR : 203742 » développé par IDEMIA, sur un microcontrôleur développé par INFINEON TECHNOLOGIES AG.

Le produit évalué est de type « carte à puce » pouvant être utilisé en modes avec et sans contact. Il 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 [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

Cette certification correspond à une évaluation avec réduction de portée (voir [NOTE25]). Ici la réduction de portée correspond à la restriction de certaines valeurs de code PIN et au retrait de la fonctionnalité de PIN biométrique du périmètre d'évaluation. Les évolutions concernent ainsi essentiellement les guides du produit (voir [GUIDES]).

1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont décrits dans la cible de sécurité [ST] à la section « *TOE usage and major security features of the TOE* ».

1.2.3 Architecture

Le produit est constitué :

- de la plateforme ouverte JavaCard « ID-One Cosmo X » embarquée sur un microcontrôleur SLC37 ;
- de l'applet « CombiCAO Applet v3 » chargée sur cette plateforme.

1.2.4 Identification du produit

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

La procédure d'identification est décrite au chapitre 4 du guide AGD_PRE (voir [GUIDES]). La version certifiée du produit correspond aux valeurs attendues décrites dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Reference* ».

1.2.5 Cycle de vie

Le cycle de vie du produit est présenté au chapitre 4 de la cible de sécurité. Il présente différentes options selon le moment et le lieu de chargement des composants logiciels du produit.

Le produit a été développé sur les sites suivants (voir [SITES]) :

IDEMIA – Courbevoie [CRB] 2, place Samuel de Champlain 92400 Courbevoie, France	IDEMIA – Pessac [PSC] Bâtiment Elnath, 11 avenue de Canteranne, 33600 Pessac, France
IDEMIA – Vitré [VTR] Avenue d'Helmstedt BP 90308 35503 Vitré Cedex, France	IDEMIA – Shenzhen [SZN] 4F, Great wall technology building No 2, Kefa Rd Science and technology park, Nanshan district, Shenzhen, 518057, PR of China
IDEMIA – Haarlem [HAA] Oudeweg 32, 2031 CC Haarlem, The Netherlands	IDEMIA – Noida [NOI-D] Syscom India Private Limited PLOT-1A, sector 73, Noida Uttar Pradesh 201307, India
IDEMIA – Ostrava [OST] Jelinkova 1174/3A, 721 00 Ostrava-Svinov, Czech Republic	IDEMIA – Noida [NOI-P] Syscom India Private Limited Plot No 60-61, NSEZ, Phase II, Dadri Road, Noida-201305 Uttar Pradesh India
IDEMIA – Jakarta [JKT] AIA Central 38 th Floor, Jl. Jenderal Sudirman Kav. 48A, Jakarta 12910, Indonesia	IDEMIA – Manilla [MNL] 19F BPI – PhilamLife Makati Building, 6811 Ayala Ave., 1209 Makati City, Philippines

Les sites de développement et de production du microcontrôleur et de la plateforme sont couverts par [CER_IC] et [CER-PLF-D].

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 la configuration SSCD du produit, telle que décrite par la cible de sécurité [ST] (voir en particulier les premiers paragraphes du chapitre 3.2) et les [GUIDES].

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] ainsi qu'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 8 mars 2022 sous la référence ANSSI-CC-2022/18, voir [CER]. Elle correspond à une évaluation avec réduction de portée suite à l'identification de vulnérabilité et prend en compte les derniers résultats de la plateforme [CER-PLF-D].

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 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 19 avril 2023 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 9 février 2022, 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

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 des vulnérabilités exploitables 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 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].

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]	Cible de sécurité de référence pour l'évaluation : - <i>Security Target ComblCAO Applet v3 on ID-One Cosmo X (SSCD configuration)</i>, FQR 550 0222 Ed 4, 23 décembre 2022. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - <i>ComblCAO Applet v3 on ID-One Cosmo X (SSCD configuration) Public Security Target</i>, FQR 550 0284 Ed 3, 16 janvier 2023.
[RTE_init]	Rapport technique d'évaluation : - <i>Evaluation Technical Report - HYPERION-N_X</i>, LETI.CESTI.HYPX.FULL.001 – v1.2, 9 février 2022.
[RTE_part]	Rapport technique d'évaluation : - <i>Evaluation Technical Report - HYPERION-N_X</i>, LETI.CESTI.HYPX.FULL.001 — v2.1, 19 avril 2023.
[ANA_CRY]	Cotation des mécanismes cryptographiques HYPERION-N_X, LETI.CESTI.HYPX.RT.001-v1.0, 1 décembre 2021.
[CONF]	<i>ComblCAO Applet V3 Configuration List</i>, FQR 220 1642 Ed 7, 30 mars 2023.
[GUIDES]	- <i>ComblCAO Applet V3 on ID-One Cosmo X – AGD_PRE</i>, FQR 220 1640 Ed 4, 11 janvier 2023 ; - <i>ComblCAO Applet V3 on ID-One Cosmo X – AGD_OPE</i>, FQR 220 1641 Ed 4, 11 janvier 2023 ; - <i>ComblCAO Applet V3, Recommendations for Compatibility with QR</i>, FQR 220 16 46 Ed 1, 1 décembre 2021.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA2020_GEN_v1.0 ; - IDEMIA2021_GEN_v1.0 ; - [CRB] IDEMIA2020_CRB_STAR_V1.1 ; - [JKT] IDEMIA2020_JKT_STAR_V1.0 ; - [MNL] IDEMIA2020_MNL_STAR_V1.0 ; - [HAA] IDEMIA2020_HAARLEM_STAR_v1.0 ; - [NOI-D] IDEMIA2021_NOI-D_STAR_v1.0 ; - [NOI-P] IDEMIA2021_NOI-P_STAR_v1.0 ; - [PSC] IDEMIA2020_PSC_STAR_v1.0 ; - [OST] IDEMIA2021_OST_STAR_v1.0 ; - [SZN] IDEMIA2021_SZN_STAR_v1.0 ; - [VTR] IDEMIA2019_VTR_STAR_v1.1.
[CER]	Rapport de certification ANSSI-CC-2022/18, ComblCAO Applet v3 on ID-One Cosmo X (SSCD Configuration), SAAAAR : 203742, 8 mars 2022.

[CER_IC]	<i>Certification Report BSI-DSZ-CC-1107-V3-2022 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0 & 80.306.16.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 and v2.11.003, optional ACL v3.33.003 and v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and guidance</i> Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) le 16 mai 2022.
[CER-PLF-D]	ID-One Cosmo X (R3 : 093363 ; R4 : 093364 ; R4 patché : 093364 + patch 099441). Certifié par l'ANSSI sous la référence ANSSI-CC-2021/29-S01v2.
[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> - <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.
[IIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[IIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.1, juin 2020.
[COMP] *	<i>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices</i> , version 1.5.1, mai 2018.
[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.
[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.