



PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2019/28

Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145 Identification du matériel 091121

Paris, le 19 juillet 2019

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

Guillaume POUPARD
[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-2019/28

Nom du produit

**Plateforme ID-One Cosmo v8.2 masquée sur le composant
NXP P60D145**

Référence/version du produit

Identification du matériel : 091121

Conformité à un profil de protection

**[PP JCS-O] Java Card Protection Profile Open
Configuration, version 3.0**

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

**EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5**

Développeurs

Idemia
2 place Samuel de Champlain
92400 Courbevoie, France

NXP Semiconductors GmbH
Troplowitzstasse 20
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



SOG-IS



Ce certificat est reconnu au niveau EAL2.

Préface

La certification

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 Premier ministre 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 matières

| | |
|---|-----------|
| 1. LE PRODUIT | 6 |
| 1.1. PRESENTATION DU PRODUIT | 6 |
| 1.2. DESCRIPTION DU PRODUIT | 6 |
| 1.2.1. <i>Introduction</i> | 6 |
| 1.2.2. <i>Services de sécurité</i> | 6 |
| 1.2.3. <i>Architecture</i> | 7 |
| 1.2.4. <i>Identification du produit</i> | 8 |
| 1.2.5. <i>Cycle de vie</i> | 9 |
| 1.2.6. <i>Configuration évaluée</i> | 11 |
| 2. L’EVALUATION | 12 |
| 2.1. REFERENTIELS D’EVALUATION | 12 |
| 2.2. TRAVAUX D’EVALUATION | 12 |
| 2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI | 12 |
| 2.4. ANALYSE DU GENERATEUR D’ALEAS | 12 |
| 3. LA CERTIFICATION | 14 |
| 3.1. CONCLUSION | 14 |
| 3.2. RESTRICTIONS D’USAGE | 14 |
| 3.3. RECONNAISSANCE DU CERTIFICAT | 14 |
| 3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> | 14 |
| 3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> | 15 |
| ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT | 16 |
| ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE | 17 |
| ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION | 19 |

1. Le produit

1.1. Présentation du produit

Le produit évalué est la « Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145, identification du matériel 091121 ». Elle est développée par *IDEMIA* et embarquée sur le microcontrôleur NXP P60D145 développé et fabriqué par *NXP SEMICONDUCTORS GMBH*.

Le produit dispose d'interfaces avec et sans contact. Il est destiné à héberger et exécuter une ou plusieurs applications, dites *applets* dans la terminologie Java Card. Ces *applets* peuvent revêtir un caractère sécuritaire différent (selon qu'elles soient « sensibles » ou « basiques ») et peuvent être chargées et instanciées avant ou après émission du produit. Les logiciels applicatifs ne sont pas inclus dans le périmètre de l'évaluation, mais ont été pris en compte au titre de [OPEN].

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.

La cible de sécurité est conforme au profil de protection [PP JCS-O]. La conformité est démontrable.

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 3.2 « *Major Security feature of the TOE* » et 10 « *TOE Summary Specification* ». Ils sont résumés ci-après :

- le chargement (avec vérification de signature DAP¹), l'installation, « l'extradition² » et la suppression d'occurrences d'*applets* ou de *packages* par le *Card Manager* ;
- l'identification et l'authentification de l'utilisateur du produit ;
- la protection en confidentialité et en intégrité des données sensibles ;
- l'effacement sécurisé des données sensibles ;
- la mise à jour des données en mémoire persistante à travers un mécanisme de transactions atomiques ;
- des mécanismes de chiffrement, déchiffrement, signature et génération de nombres aléatoires ;
- la gestion des clés ;
- un mécanisme de pare-feu ;

¹ *Data Authentication Pattern*.

² « L'extradition » permet à plusieurs applications de partager un domaine de sécurité dédié.

- la gestion des exceptions ;
- la protection du chargement d'applications post-émission ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

1.2.3. Architecture

L'architecture du produit est décrite par la figure ci-après.

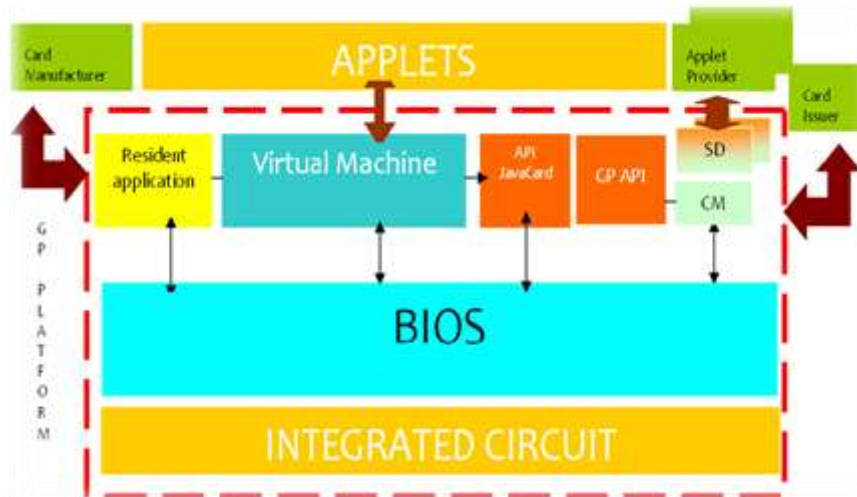


Figure 1 : Architecture du produit

Le périmètre d'évaluation (TOE¹) est délimité par les tirets rouges, il est constitué :

- du microcontrôleur NXP P60D145 (P6022y VB), développé par NXP SEMICONDUCTORS GMBH et certifié sous la référence [CER_IC] ;
- des parties logicielles suivantes, développées par IDEMIA et masquées en ROM :
 - o un système d'exploitation composé :
 - d'une interface entre les composants matériels et les composants natifs, nommée BIOS² ;
 - de fonctionnalités cryptographiques ;
 - d'une machine virtuelle Java (JVM³) ;
 - d'un environnement d'exécution Java Card (JCRE⁴) ;
 - des interfaces de programmation d'application (API⁵) : Java Card et Global Platform ;
 - o un dispatcher nommé Resident Application et chargé de répartir les commandes envoyées à la carte vers les applications et modules correspondants ;
 - o un gestionnaire d'applications (Card Manager) dont les fonctionnalités sont implémentées dans une applet dédiée du même nom ;

¹ Target Of Evaluation.

² Basic Input/Output System.

³ Java Virtual Machine.

⁴ Java Card Runtime Environnement.

⁵ Application Programming Interface.

- d'un algorithme de biométrie *Match-On-Card* (MOC) développé par la société *ID3* et masqué en ROM ;
- d'un mécanisme de chargement de *patch*. Les *patches* sont développés par *IDEMIA* et chargés en EEPROM.

Le produit est aussi composé des éléments hors TOE suivants, développés par *IDEMIA*:

- d'un *patch* optionnel pouvant être utilisé par les applications en composition ;
- de potentiels *patches* logiciels chargés en EEPROM représentant des mises à jour des *applets* ;
- des applications masquées en ROM : SAC Server v1.1, CHV2.2 v2.2, IAS ECC V2 v2.0, LDS V10 v10.1, PIV v2.4.1 et CPS2ter v2.

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, elles ont été vérifiées conformément aux contraintes listées dans la cible de sécurité [ST] au chapitre 3.5.1.

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 du tableau ci-après, détaillés dans [ST] aux chapitres 2.3 « *TOE Reference* » et 2.4 « *TOE Identification* ».

| Eléments de configuration | | Origine |
|--------------------------------------|--|-------------------------|
| Nom du produit | ID-One Cosmo v8.2 on P60D145 | Idemia |
| Identification matérielle du produit | 09 11 21 (produit) 08 02 00 00 00 (version) | |
| Nom de la TOE | ID-One Cosmo v8.2 Platform | Idemia |
| Identification de la plateforme | 6F 01 (pour Large Platform Mask version 1) | |
| Identification du composant | 30 (pour NXP P60D145) | NXP Semiconductors GmbH |

Tableau 1 - Identification du produit et de la TOE

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET DATA ou à la lecture de l'ATR. La procédure d'identification du produit est décrite dans le guide [AGD_OPE].

Par exemple :

- l'identification du produit « 09 11 21 » peut être lue dans la réponse ATR « 3B DB 96 00 80 B1 FE 45 1F 87 00 31 C1 64 **09 11 21** 30 00 90 00 » ;
- les données d'identification du composant « 30 » et de la plateforme « 6F 01 » peuvent être lues dans la réponse à la commande GET DATA avec le tag « DF 52 » (*subTag* « 01 » pour le composant et « 03 » pour la plateforme).

La principale différence entre le produit et la TOE correspond aux applications chargées en pré-émission et au *patch* optionnel pouvant être installé en pré-personnalisation.

La conception et l'intégration de ces applications en ROM sont réalisées en même temps que pour la plateforme. Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après et dans la cible de sécurité [ST]. Ce tableau liste les applications et les paquetages (*packages*) inclus dans le produit, associés à leur nom et leur AID¹. La commande GET STATUS permet à l'utilisateur du produit de vérifier quelles applications et quels *packages* sont installés dans le produit à sa disposition.

| Nom de l'applet | AID (valeur en hexadécimal) | Nom du package |
|---------------------------|----------------------------------|-----------------------|
| CHV2.2 version 2.2 | A0000000770108080720000000000003 | Chv |
| | A0000000770108080720000000000002 | Cvm |
| | A0000000770108080720000000000001 | id3 |
| | A0000000770108080720000000000006 | Pw |
| | A0000000770108080720000000000005 | pw_fp |
| SAC Server version 1.1 | A0000000770108000710000000000015 | SAC Applet Manager |
| | A0000000770108000710000000000018 | SAC Java Applet |
| IAS ECC V2 version 2.0 | A000000077010800071000000000000B | Server Applet Manager |
| | A000000077010800071000000000000D | IAS ECC API |
| | A0000000770108000710000000000013 | IAS lihgt Add-On |
| LDS V10 version 10.1 | A000000077010000071000000000000E | Ldslib |
| | A0000000770100000710000000000005 | Ldseac |
| PIV 2.4 version 2.4.1 | A0000000770100000610000000000024 | PIV |
| CPS2ter version 2 | A000000077010800071000000000000C | CPS2ter |

Tableau 2 - Applications du produit

Le *patch* optionnel peut être installé en phase de pré-personnalisation. La procédure d'identification de ce patch est décrite dans le guide [AGD_OPT] ; les données d'identification peuvent être obtenues par l'intermédiaire de la commande GET DATA « 80 CA DF 52 8A ». La carte renvoie les valeurs d'identification correspondantes au subtag 04 : « 09 30 82 00 A5 42 56 F2 84 5C BC DE 33 3E FE 7B 88 45 E0 30 1A 7F A6 EC 01 1F 5B 7B 49 D9 A9 C5 49 FF 32 15 » lorsque le patch optionnel est présent, « 00 » sinon.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit par la figure 2 ci-après, voir aussi [ST].

La phase 1 correspond à la conception et au développement de la plateforme, plus précisément :

- à la définition et écriture des données de l'utilisateur ;
- au développement du socle logiciel incluant l'algorithme de biométrie MOC ;
- au développement de *patches*.

Les phases 2 et 3 correspondent respectivement au développement et à la fabrication du microcontrôleur et sont effectuées chez *NXP SEMICONDUCTORS GMBH*. La phase 3 inclut l'écriture en ROM du logiciel embarqué et en EEPROM de données de l'utilisateur et de

¹ Application Identifier.

patches tels que les *patches* générique et additionnel identifiés dans la cible de sécurité [ST]. Ces phases sont couvertes par l'évaluation du microcontrôleur [CER-IC].

La livraison de la TOE s'opère à la fin de la phase 3. Après cette phase, la TOE est considérée comme auto-protégée.

La phase 4 correspond au conditionnement (*packaging*) du produit, c'est-à-dire à l'intégration de la TOE au format final (par exemple, au format carte). Le produit est activé à partir de la phase 5. Cette phase supporte notamment :

- la configuration du logiciel embarqué de la plateforme (chargement de données de l'utilisateur et du code optionnel non chargé en phase 3) ;
- le *Card Content Management*¹ géré par le *dispatcher* et le *Card Manager* (chargement, installation, et suppression des fichiers de chargement, *Load Files*, et des instances d'application) ;
- après cette phase, aucun *patch* ne peut être chargé, le mécanisme de chargement de *patch* est désactivé. Ces deux phases sont couvertes par le guide d'administration du produit [AGD_PRE].

La phase 6 correspond à la personnalisation du produit et la phase 7 correspond à la phase opérationnelle du produit. Ces phases sont couvertes par le guide d'utilisation du produit [AGD_OPE].

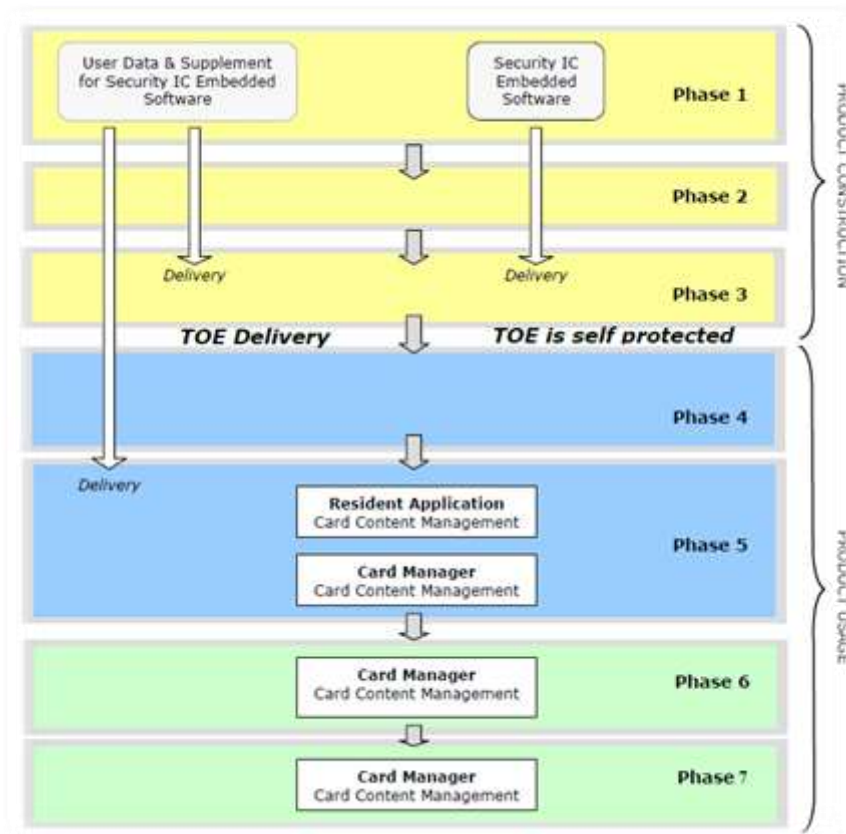


Figure 2 : Cycle de vie du produit

¹ Gestion du contenu de la carte (terme Global Platform).



Le produit a été développé par *IDEMIA* sur les sites suivants (voir [SITES]), à l'exception du MOC qui a été développé par *ID3* (voir [CER-PTF-C9] qui identifie notamment les sites de développements) :

| | |
|--|---|
| <i>IDEMIA – Courbevoie</i> [CRB] 2, place Samuel de Champlain 92400 Courbevoie, France | <i>IDEMIA – Pessac</i> [PSC] Bâtiment Elnath, 11 avenue de Canteranne, 33600 Pessac, France |
|--|---|

Le microcontrôleur est développé et fabriqué par *NXP SEMICONDUCTORS GMBH*. Les sites de développement et de fabrication de ce microcontrôleur sont détaillés dans le rapport de certification [CER-IC].

Le produit permet le chargement d'applications en phase 3 (avant le point de livraison), en phase 5 (pré-émission) ou en phase 6 et 7 (post-émission) :

- le développement des applications masquées en ROM en phase 3 et identifiées dans la cible de sécurité [ST] a été réalisé sur les sites de Courbevoie et Pessac. Leur livraison et leur vérification ont été analysées pendant cette évaluation conformément à [OPEN] au titre des tâches ALC ;
- les chargements en phase 5 (pré-émission), 6 et 7 (post-émission) doivent être protégés conformément à [AGD_ALP].

Le guide [AGD_ALP] identifie également des recommandations relatives à la livraison des futures applications à charger sur la plateforme. Le guide [AGD_OPE] présente une aide pour le développement pour toutes les applications. Le guide [AGD-Dev_Sec] présente les recommandations obligatoires pour le développement des applications sensibles.

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le « pré-personnalisateur », le « personnalisateur » et le *Card Manager*, et comme utilisateur du produit les développeurs des applications à charger sur la plateforme.

1.2.6. Configuration évaluée

Le certificat porte sur la configuration de la plateforme telle qu'elle est identifiée au paragraphe 1.2.4.

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 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. Toutes les applications identifiées dans la cible de sécurité ont été vérifiées conformément aux exigences définies dans le chapitre 2.4.4 de [ST].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [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 « NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software » au niveau EAL6 augmenté des composants ALC_FLR.1 et ASE_TSS.2, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 18 mai 2018 sous la référence BSI-DSZ-CC-1059-2018 [CER-IC].

L'évaluation s'appuie sur les résultats d'évaluation de la « Plateforme ID-One Cosmo v8.1-N - Large, masquée sur le composant NXP P6022M VB, identification du matériel 084021 », certifiée le 5 septembre 2017 sous la référence ANSSI-CC-2017/49, voir [CER-PTF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 2 juillet 2019, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur [CER-IC]. Par ailleurs, comme requis



dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

Les résultats ont été pris 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 AVA_VAN.5 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 « Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145, identification du matériel 091121 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 0 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 :

- le développement des applications sensibles doit respecter les contraintes listées dans [AGD-Dev_Sec] ;
- les autorités de vérification doivent appliquer les exigences définies dans la cible de sécurité [ST] chapitre 3.5.1 sur toutes les applications chargées sur ce produit ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement pré-émission et post-émission) doit être activée conformément aux indications décrites dans le guide [AGD_ALP].

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 :

¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.



3.3.2. *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires¹, 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 CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Annexe 1. Niveau d'évaluation du produit

| Classe | Famille | Composants par niveau d'assurance | | | | | | | Niveau d'assurance retenu pour le produit | | |
|---|---------|-----------------------------------|-------|-------|-------|-------|-------|-------|---|--|---|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 5+ | Intitulé du composant | |
| ADV Développement | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security architecture description |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 | 5 | 5 | Complete semi-formal functional specification with additional error information |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 | 1 | 1 | Implementation representation of the TSF |
| | ADV_INT | | | | | 2 | 3 | 3 | 2 | 2 | Well-structured internals |
| | ADV_SPM | | | | | | 1 | 1 | | | |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 | 4 | 4 | Semiformal modular design |
| AGD Guides d'utilisation | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Operational user guidance |
| | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Preparative procedures |
| ALC Support au cycle de vie | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 | 4 | 4 | Production support, acceptance procedures and automation |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 | 5 | 5 | Development tools CM coverage |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Delivery procedures |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 | 2 | 2 | Sufficiency of security measures |
| | ALC_FLR | | | | | | | | | | |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 | 1 | 1 | Developer defined life-cycle model |
| ALC_TAT | | | | 1 | 2 | 3 | 3 | 2 | 2 | Compliance with implementation standards | |
| ASE Evaluation de la cible de sécurité | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Conformance claims |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Extended components definition |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | ST introduction |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Security objectives |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Derived security requirements |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security problem definition |
| ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | TOE summary specification | |
| ATE Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | Analysis of coverage |
| | ATE_DPT | | | 1 | 1 | 3 | 3 | 4 | 3 | 3 | Testing: modular design |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | Functional testing |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | Independent testing: sample |
| AVA Estimation des vulnérabilités | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 | 5 | 5 | Advanced methodical vulnerability analysis |

Annexe 2. Références documentaires du produit évalué

| | |
|----------|--|
| [ST] | <p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none">- Security Target Erato R ID-One COSMO V8.2, référence FQR 110 8960, version 4.0, 02/07/2019, <i>IDEMIA</i>. <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">- ID-ONE COSMO V8.2 Public Security Target, référence FQR 110 9067, version 4, juillet 2019, <i>IDEMIA</i>. |
| [RTE] | <p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none">- Evaluation Technical Report – ERATO-R, référence LETI.CESTI.ERR.FULL.001, version 1.3, 02/07/2019, <i>CEA-LETI</i> |
| [CONF] | <p>Liste de configuration du produit :</p> <ul style="list-style-type: none">- ID-One Cosmo V8.2 Configuration List, référence FQR 110 9114, version 4, 02/07/2019, <i>IDEMIA</i>. |
| [GUIDES] | <p>Guide d'installation du produit :</p> <ul style="list-style-type: none">- [AGD_PRE] ID-One Cosmo V8.2 Pre-Perso Guide, référence FQR 110 8875 version 3, 13/03/2019, <i>IDEMIA</i>. <p>Guide d'administration du produit :</p> <ul style="list-style-type: none">- [AGD_OPE] ID-One Cosmo V8.2 Reference Guide, référence FQR 110 8885, version 3, 06/03/2019, <i>IDEMIA</i>.- [AGD_OPT] Optional code R1.0 Appli deselection before Desfire, référence FQR 110 9106, version 2, 02/04/2019, <i>IDEMIA</i>. <p>Guide de développement d'applications sécurisées :</p> <ul style="list-style-type: none">- [AGD-Dev_Sec] ID-One Cosmo V8.2 on P60D145 - Applet Security Recommendations, référence FQR 110 8963, version 4, 18/03/2019, <i>IDEMIA</i>;- [AGD_ALP] ID-One Cosmo V8.1-n Application Loading Protection Guidance, référence FQR 110 8001, version 1, 11/10/2016, <i>IDEMIA</i>. |

| | |
|--------------|--|
| [SITES] | <p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> - [CRB] <ul style="list-style-type: none"> ○ IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities, reference IDEMIA R&D site 2018_GEN_v1.1, 19 juin 2019, <i>SERMA SAFETY & SECURITY</i>). ○ Site Technical Audit Report CRB, référence IDEMIA R&D site 2018_CRB_STAR_v1.3, 26/06/2019, <i>SERMA SAFETY & SECURITY</i>. - [PSC] <ul style="list-style-type: none"> ○ IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities, reference IDEMIA R&D site 2018_GEN_v1.0, 29 novembre 2018, <i>SERMA SAFETY & SECURITY</i>). ○ Site Technical Audit Report PSC, reference IDEMIA R&D site 2018_PSC_STAR_v1.1, 22/05/2019, <i>SERMA SAFETY & SECURITY</i>. |
| [CER-IC] | <p>Certification Report BSI-DSZ-CC-1059-2018 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 18 mai 2018, sous la référence BSI-DSZ-CC-1059-2018.</i></p> |
| [CER-PTF] | <p>Rapport de certification ANSSI-CC-2017/49, Plateforme ID-One Cosmo v8.1-N – Large, masquée sur le composant NXP P6022M VB, identification du matériel 084021. <i>Certifié par l'ANSSI le 5 septembre 2017 sous la référence ANSSI-CC-2017/49.</i></p> |
| [CER-PTF-C9] | <p>Certification Report ID-ONE Cosmo V9 Essential version 3 (Cosmo V9). <i>Certifié par NSCIB le 11 décembre 2018 sous la référence NSCIB-CC-18-200833.</i></p> |
| [PP JCS-O] | <p>SUN Java Card System Protection Profile - Open Configuration, version 3.0. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01.</i></p> |
| [PP0084] | <p>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.</i></p> |

Annexe 3. 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] | Procédure ANSSI-CC-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, ANSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation : <ul style="list-style-type: none"> - 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, version 2.9, janvier 2013. |
| [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. |
| [CC RA] | 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. |
| [REF] | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr . |

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.