



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2017/03

Kinibi v311A on Exynos 7870
Référence t-base-EXYNOS64-Android-311A-V004-
20160527_225213_11082_38854

Paris, le 17 février 2017

*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-2017/03
Nom du produit	Kinibi v311A on Exynos 7870
Référence/version du produit	Référence t-base-EXYNOS64-Android-311A-V004-20160527_225213_11082_38854, Version 311A
Conformité à un profil de protection	Néant
Critères d'évaluation et version	Critères Communs version 3.1 révision 4
Niveau d'évaluation	EAL 2 augmenté AVA_TEE.2
Développeur(s)	Trustonic 20 Station Road Cambridge BD1 2ID United Kingdom
Commanditaire	Trustonic 20 Station Road Cambridge BD1 2ID United Kingdom
Centre d'évaluation	THALES (TCS – CNES) 18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9 France
Accords de reconnaissance applicables	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>CCRA</p>  </div> <div style="text-align: center;"> <p>SOG-IS</p>  </div> </div> <p>Le produit est reconnu au niveau EAL2. Le produit est reconnu au niveau EAL2.</p>

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>	9
1.2.5. <i>Cycle de vie</i>	9
1.2.6. <i>Configuration évaluée</i>	10
2. L’EVALUATION	11
2.1. REFERENTIELS D’EVALUATION	11
2.2. TRAVAUX D’EVALUATION	11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	11
2.4. ANALYSE DU GENERATEUR D’ALEAS	11
3. LA CERTIFICATION	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS D’USAGE	12
3.3. RECONNAISSANCE DU CERTIFICAT	15
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	15
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	18

1. Le produit

1.1. Présentation du produit

Le produit évalué est le système d'exploitation « Kinibi v311A on Exynos 7870, référence t-base-EXYNOS64-Android-311A-V004-20160527_225213_11082_38854, version 311A » développé par *TRUSTONIC*.

Le produit Kinibi est l'implémentation par *TRUSTONIC* d'un système d'exploitation (*Trusted OS*), conçu pour être exécuté par un environnement d'exécution de confiance (TEE - *Trusted Execution Environment*).

Le but du TEE est de créer deux environnements cloisonnés : un « *Normal World* » et le « *Secure World* ». Le « *Normal World* », aussi appelé REE (*Rich Execution Environment*, ou environnement d'exécution riche) est le système d'exploitation principal (Android, iOS par exemple), tandis que le « *Secure World* » est le TEE. Les deux sont exécutés en parallèle et le TEE garantit que des données sensibles sont stockées, traitées et protégées dans un environnement de confiance.

Comme un système d'exploitation traditionnel, le TEE est capable d'exécuter des applications, appelées *Trusted Applications* (TA), ou applications de confiance, qui bénéficient d'un ensemble de services de sécurité comme l'intégrité de l'exécution du code, les communications sécurisées entre les *Client Applications* (CA)¹ et les TA, le stockage sécurisé des données, la gestion de clés et d'algorithmes cryptographiques, etc.

Le *Trusted OS* est destiné à être utilisé dans des équipements mobiles pour offrir des services de sécurité mobiles tels que la gestion des droits numériques, le paiement mobile, ou encore de l'authentification.

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 n'est pas conforme au profil de protection [PP-TEE], car la TOE se limite à la partie *software* (*Trusted OS*) contrairement au profil de protection [PP-TEE] qui inclut également les parties *hardware* et *firmware*.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'initialisation sécurisée du TEE : garantit que l'environnement d'exécution lui-même peut-être de confiance, c'est-à-dire que l'authenticité et l'intégrité de son code sont vérifiées ;

¹ Applications exécutées dans le REE.

- les fonctionnalités de sécurité générales du produit Kinibi :
 - o la gestion de la mémoire : aucune information résiduelle n'est présente en mémoire après exécution. De plus, les espaces mémoires sont séparés et dédiés soit au « *Normal World* », soit au « *Secure World* » ;
 - o l'atomicité des opérations : une opération est complètement effectuée ou non effectuée, sans effet dans le cas d'interruption ;
 - o le mécanisme d'isolation : isolation des services du TEE, de ses ressources ainsi que des applications de confiance vis-à-vis du REE au niveau de l'exécution ;
 - o le stockage de confiance : les données des applications de confiance, les données du TEE ainsi que les clés secrètes sont stockées de manière sûre et manipulées de manière à garantir leur protection en authenticité, confidentialité et intégrité ;
 - o l'identification de l'équipement : le produit offre un service de stockage et de récupération de l'identifiant unique de périphérique ;
 - o la gestion des paramètres : les paramètres sensibles de gestion de la TOE sont stockés dans des fichiers spécifiques en accès restreint, accessibles uniquement par les administrateurs,
- les fonctionnalités de gestion des applications TEE :
 - o l'installation et le chargement sécurisé des TA : les applications sont chargées à l'exécution, de façon sécurisée en vérifiant l'authenticité et en réalisant l'initialisation. Ceci permet donc la protection du chargement d'applications *post-issuance* ;
 - o l'identification des applications TEE : l'identité d'une application est garantie et ne peut être usurpée ;
 - o un mécanisme permettant la création d'un *container* (appelé « *security objects* » - objets de sécurité) dans lequel les données de l'application sont protégées en confidentialité et intégrité, à l'extérieur du TEE,
- des opérations cryptographiques et la gestion des clés : fournit un contexte d'exécution sécurisé pour :
 - o la génération de nombres aléatoires ;
 - o la génération et vérification de signature numérique ;
 - o le chiffrement et déchiffrement de données ;
 - o le calcul de hash ;
 - o la génération et vérification de MAC ;
 - o la génération, destruction, remplacement et stockage de clés ;
 - o l'utilisation des primitives cryptographiques DES, AES, RSA, DSA et ECC,
- des API fournissant des services de sécurité pour les applications de confiance (appelées « *services to TEE applications* ») ;
- un compteur monotone qui peut être utilisé par les applications de confiance (appelé « *secure time* »).

1.2.3. Architecture

Le périmètre de l'évaluation se limite à la partie logicielle du TEE, ce qui inclut le noyau, les drivers de confiance (TD - *Trusted Drivers*), la couche d'exécution (*Runtime Management*) et des applications de confiance comprises dans l'image logicielle de Kinibi.

La figure 1 décrit l'architecture du produit.

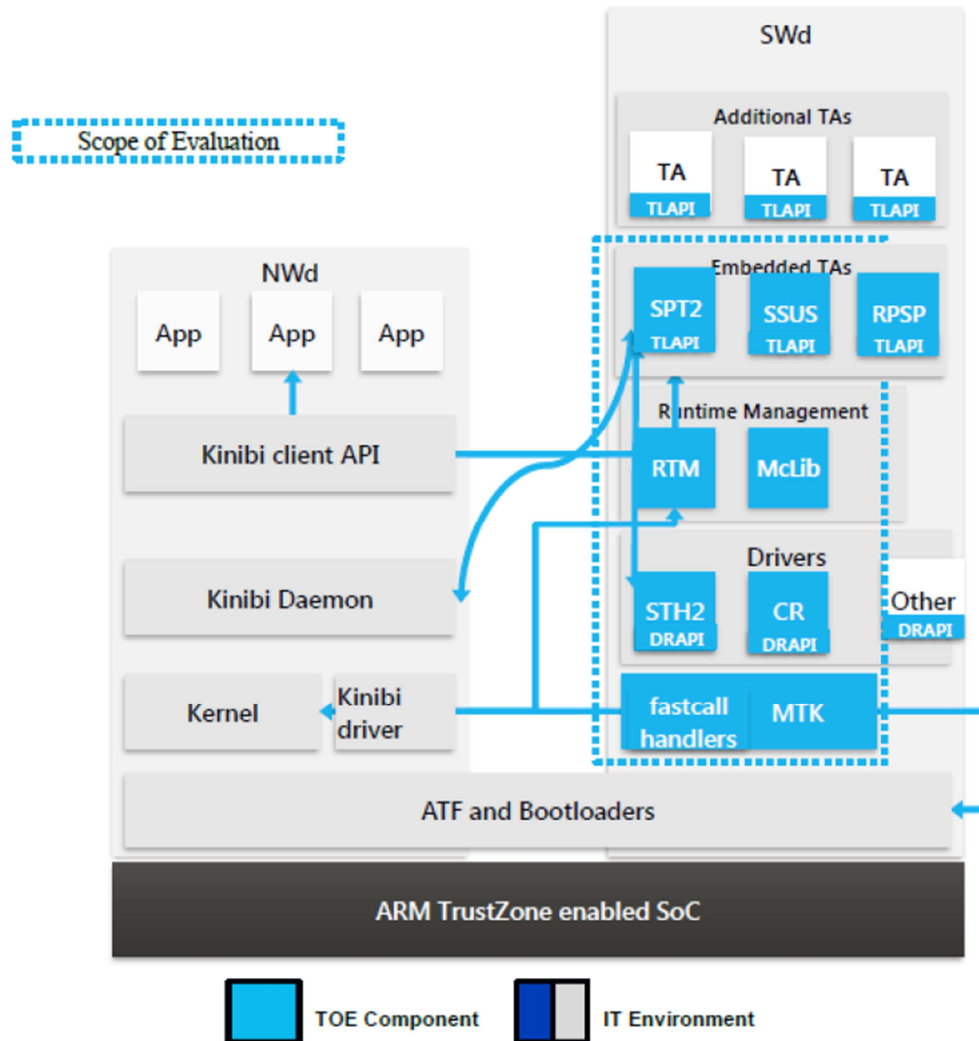


Figure 1 : Architecture du produit

Plus précisément, le produit est constitué des éléments suivants :

- *Kinibi Kernel* (MTK) : composant assurant l'isolation entre les tâches, les communications interprocessus et l'ordonnancement préemptif ;
- *Storage driver* (STH2) : composant donnant accès au stockage sécurisé aux applications et drivers de confiance ;
- *Cryptographic Driver* (CR) : composant donnant accès aux services cryptographiques aux applications et drivers de confiance ;
- *Runtime Manager* (RTM) : composant gérant le chargement des tâches, la mémoire, les sessions, les échanges de messages et les exceptions ;
- *Application library* (McLib) : composant exposant aux TA les API Legacy (tlAPI), GlobalPlatform (GPAPI) et *Secure Drivers* (DrAPI) ;
- les applications déjà chargées dans le produit sont les applications de confiance SSUS, SPT2 et RPSP. Ces composants sont embarqués dans l'image logicielle de Kinibi. Elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [Open_Certif]. En effet, ces applications ont été vérifiées conformément aux contraintes de développements d'applications décrites dans [GUIDES].

Les éléments ci-dessous ne sont pas dans le périmètre de l'évaluation :

- *Trusted User Interface Driver (TUI)* : composant chargé en tant que driver de confiance pendant la phase « Manufacturing », après l'intégration de l'image logicielle de Kinibi ;
- applications de confiance CMTA et LTA: applications de confiance chargées pendant la phase « Manufacturing », après l'intégration de l'image logicielle de Kinibi ;
- applications de confiance ou drivers de confiance développés par les SiP¹ ou OEM² et chargés en tant que applications de confiance du système ;
- *Client Applications*.

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 suivants :

Composant	Version
Identifiant de MobiCore	t-base-EXYNOS64-Android-311A-V004-20160527_225213_11082_38854
MobiCore Control Interface (versionMci)	0x00010004
Secure Objects (versionSo)	0x00020002
MobiCore Load Format (versionMclf)	0x00020005
MobiCore Container Format (versionContainer)	0x00020001
MobiCore Configuration Block Format (versionMcConfig)	0x00000003
MobiCore TA API Implementation (versionTlApi)	0x00010013
MobiCore Driver API Implementation (versionDrApi)	0x00010004
ContentManagement Protocol (versionCmp)	0x00040000

La version des composants peut être récupérée pendant l'exécution de deux façons différentes :

- depuis le « *Secure World* », une TA peut utiliser l'API `tlApiGetMobiCoreVersion` ;
- depuis le « *Normal World* », une CA peut utiliser l'API `mcGetMobiCoreVersion`.

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

- Phase 0 : la conception et le développement de l'environnement (*hardware, firmware* et REE) ;
- Phase 1 : la conception et développement du produit ;
- Phase 2 : le portage du produit sur un *System on Chip* (SoC) spécifique ;
- Phase 3 : la TOE est livrée aux SiP et à l'OEM qui ensuite développent et valident la version du produit qui va être installée (TEE, TA préinstallées, TD ainsi que le REE) ;
- Phase 4 : l'image du produit est flashée par l'OEM sur son équipement. A cette étape est également injectée la racine de confiance (*root of trust*) ;

¹*Silicon Provider* – Fondateur de la puce.

²*Original Equipment Manufacturer*-fabricant d'équipement initial.

- Phase 5 : la phase utilisateur où des applications peuvent être chargées. Ces chargements doivent être protégés conformément à [TECH-LOAD].

Le produit a été développé sur le site suivant :

Trustonic Sophia Antipolis
535 Route des Lucioles
06560 Valbonne

Le guide [AGD-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur le produit.

Par ailleurs, le guide [TECH_LOAD] décrit les règles de développement des applications destinées à être chargées sur ce produit.

Pour l'évaluation, l'évaluateur a considéré utilisateur du produit le développeur de TA et de TD.

1.2.6. Configuration évaluée

Le certificat porte sur le produit tel que décrit au paragraphe « 1.2.4 Identification du produit », configuré conformément au guide de personnalisation (cf. [GUIDES]) et exécuté sur le processeur Exynos7870 EVT0_REV0.0 (« Joshua » Generic ARMv8) fabriqué par *SAMSUNG LSI*.

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 et réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4 [CC]** et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour répondre aux spécificités des TEE, l'annexe A du [PP_TEE] a été appliquée. Ainsi, le niveau AVA_TEE a été déterminé en suivant l'échelle de cotation de cette annexe. 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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 16 janvier 2017, 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 vulnérabilités de conception et de construction pour le niveau AVA_TEE.2 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final n'a pas été évalué. Par ailleurs, la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique. La sortie du générateur a fait l'objet d'une analyse se basant sur le référentiel [NIST SP 800-90A], conformément à la cible de sécurité. 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_TEE.2 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 « Kinibi v311A on Exynos 7870, référence t-base-EXYNOS64-Android-311A-V004-20160527_225213_11082_38854, version 311A » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 2 augmenté du composant AVA_TEE.2. Pour mémoire, le composant AVA_TEE.2 correspond à un composant d'assurance étendu¹ qui s'ajoute au composant d'assurance AVA_VAN.2. Il traite de l'analyse de vulnérabilité en utilisant la table de cotation spécifique définie dans le profil de protection [PP TEE].

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], à savoir :

- OE.INTEGRATION_CONFIGURATION : l'intégration et la configuration de la TOE par le fabricant de l'appareil doivent s'appuyer sur les directives définies par le fournisseur de la TOE ;
- OE.PROTECTION_AFTER_DELIVERY : la TOE doit être protégée par l'environnement après la livraison et avant d'entrer dans la phase finale d'utilisation. Les personnes manipulant la TOE dans l'environnement opérationnel doivent appliquer les guides de la TOE [GUIDES]. Les responsables de l'application des procédures contenues dans les guides et les personnes impliquées dans la livraison et la protection du produit ont les compétences requises et sont conscients des problèmes de sécurité ;
- OE.ROLLBACK : le développeur de TA doit tenir compte du fait que le TEE n'offre pas une protection complète contre l'annulation des données TEE persistantes, des données et des clés de la TA et du code de la TA ;
- OE.SECRETS : la gestion des données secrètes (par exemple la génération, le stockage, la distribution, la destruction, le chargement dans le produit de clés cryptographiques privées, symétriques, de données d'authentification utilisateur) effectuées en dehors du TEE doit assurer l'intégrité et la confidentialité de ces données ;

¹ Composant d'assurance non issu de la partie 3 des [CC].

- OE.TA_DEVELOPMENT : les développeurs de TA doivent se conformer aux guides de développement des TA établies par le fournisseur de TEE. En particulier, les développeurs de TA doivent appliquer les recommandations de sécurité suivantes au cours du développement des TA :
 - o les identifiants de la CA sont générés et gérés par le REE, en dehors du champ d'application du TEE ; les TA ne doivent pas présumer pas que les identifiants de la CA sont authentiques ;
 - o les TA ne doivent pas divulguer de données sensibles au REE par l'intermédiaire de la CA (l'interaction avec la CA peut exiger des moyens d'authentification) ;
 - o l'intégrité des données qu'une TA écrit dans un buffer partagé ne peut être assurée ; les TA doivent toujours lire les données une seule fois à partir du buffer partagé, puis les valider ;
 - o les TA doivent copier le contenu des buffers partagés dans la mémoire appartenant à l'instance TA chaque fois que ces contenus doivent être constants,

- OE.UNIQUE_TEE_ID : la génération de l'identifiant TEE, à l'extérieur ou à l'intérieur du TEE, doit faire respecter le caractère unique de ces données ;

- OE.CONFIGURATION : la TOE doit être installée et configurée correctement afin de démarrer dans un état sécurisé. Le matériel / *firmware* et les composants de l'environnement logiciel doivent être installés et configurés de manière sécurisée en tirant parti des mécanismes de sécurité fournis par la TOE ;

- OE.TRUSTED_HARDWARE : le matériel / *firmware* met en œuvre les protocoles et les mécanismes requis par les fonctions de sécurité de la TOE pour appliquer la politique de sécurité. Ces systèmes fournissent les fonctions requises par la TOE (par exemple, la clé maître symétrique, individuelle du dispositif) et sont suffisamment protégés contre toute attaque qui peut amener ces fonctions à fournir de faux résultats. Les matériels / *firmware* sont dans le même domaine de gestion que la TOE et sont gérés sur la base des mêmes règles et politiques applicables à la TOE ;

- OE.TRUSTED_FIRMWARE : les développeurs du *firmware* et des drivers sont supposés compétents et dignes de confiance. Ils sont capables et disposés à veiller à ce que le *TA management software* soit la seule entité capable de déployer une TA privilégiée et que seul le propriétaire de l'identité de la TA peut déployer une TA contenant cette identité. Ils sont capables et disposés à veiller à ce que tout logiciel additionnel ne remet pas en cause la sécurité apportée par la TOE. Les développeurs de *TA management software* doivent se conformer aux guides de développement ;

- OE.TA_MANAGEMENT : les développeurs de logiciels de gestion des TA sont supposés compétents et dignes de confiance. Ils sont capables et disposés à veiller à ce que le logiciel de gestion de TA s'assure que seules les entités de confiance peuvent déployer des applications approuvées privilégiées et que seul le propriétaire d'une identité d'assistance technique peut déployer une TA portant cette identité. Ils sont capables et disposés à veiller à ce que le logiciel supplémentaire ne rompt pas toute garantie de sécurité de la TOE. Les développeurs de logiciels de gestion des TA doivent appliquer les guides de développement des TA ;

- OE.RNG : le SoC doit fournir un générateur de nombre aléatoires approprié comme source d'entropie, tel que spécifié dans le [NIST SP 800-90A]. Les nombres aléatoires générés par ce générateur ne doivent pas être prévisibles et doivent avoir une entropie suffisante. Le SoC doit s'assurer qu'aucune information sur les nombres aléatoires produits n'est disponible pour un attaquant puisqu'ils peuvent être utilisés pour générer des clés cryptographiques ;
 - OE.INITIALIZATION : le TEE doit être lancé par un processus d'initialisation sécurisé qui assure :
 - o l'intégrité du code d'initialisation du TEE et les données utilisées pour charger le *firmware* du TEE ;
 - o l'authenticité du *firmware* du TEE ;
 - o et que le TEE est lié au SoC de l'équipement. En particulier, le TEE doit protéger le *firmware* du TEE contre les attaques de type *downgrade attack*.
- Note d'application : Le fait que le processus est lié au SoC signifie que la racine de confiance pour les données TEE ne peut pas être modifiée ou altérée.

De plus, l'utilisateur du produit certifié devra suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doivent respecter les contraintes de développement de la plateforme cf. [GUIDES] selon la sensibilité de l'application considérées ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doit être activée conformément aux indications de [TECH_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 jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 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 [CC RA].

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 Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

² Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

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 2+	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	2	2	Security-enforcing functional specification
	ADV_IMP				1	1	2	2			
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	1	1	Basic 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	2	2	Use of a CM system
	ALC_CMS	1	2	3	4	5	5	5	2	2	Parts of the TOE CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2			
	ALC_FLR										
	ALC_LCD			1	1	1	1	2			
	ALC_TAT				1	2	3	3			
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	1	1	Evidence of coverage
	ATE_DPT			1	2	3	3	4			
	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	2	2	Vulnerability analysis
	AVA_TEE		2						2	2	TEE 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"> - Kinibi v311A Security Target, référence TT-CC-2016-ST, version 1.8, 10/01/2017. <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"> - Kinibi v311A Security Target, référence TT-CC-2016-ST, version 1.8, 10/01/2017.
[RTE]	Rapport technique d'évaluation : Evaluation Technical Report Project Kinibi, référence Kinibi_ETR, version 3.1, 16/01/2017.
[CONF]	Liste de configuration du produit : ALC_CMC ALC_CMS Kinibi configuration Management, référence Trustonic-Kinibi-ALC_CMC_CMS, version 1.2, chapitre 4, 24/11/2016.
[GUIDES]	<p>[ISO_VERIF]</p> <ul style="list-style-type: none"> - Kinibi Integration Guide, 23/11/2016; - Kinibi Developer's Guide ; - Kinibi Driver Developer's Guide. <p>[ORG_LOAD]</p> <ul style="list-style-type: none"> - [AGD_OPE]: Kinibi v311A - Operational User Guidance, version 1.3, 29/08/2016 ; - [AGD_PRE]: Kinibi v311A - Preparative Procedures Guidance, version 1.3, 30/08/2016. <p>[TECH_LOAD]</p> <ul style="list-style-type: none"> - Kinibi Integration Guide, 23/11/2016 ; - Kinibi Developer's Guide.
[PP TEE]	Protection Profile, Trusted Execution Environment, référence GPD_SPE_021, version 1.2, 5 janvier 2015. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2014/01.</i>
	Protection Profile, Trusted Execution Environment, référence GPD_SPE_021, version 1.2.1, 13 décembre 2016. <i>Maintenu par l'ANSSI sous la référence ANSSI-CC-PP-2014/01-M01.</i>

Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.</p>
[CC]	<p>Common Criteria for Information Technology Security Evaluation :</p> <ul style="list-style-type: none"> - Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001 ; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002 ; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.</p>
[OPEN]	<p>Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.</p>
[SOG-IS]	<p>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.</p>
[NIST SP 800-90A]	<p>Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST SP 800-90A, janvier 2012.</p>
[REF]	<p>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.</p>