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-CSPN-2012/07

Trusted Foundations
Version SMCAG01.06.36315

Paris, le 7 janvier 2013

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

Patrick Pailloux
[ORIGNAL SIGNE]

SÉCURITÉ CERTIFICATION

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.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2012/07**
Nom du produit **Trusted Foundations**
Référence/version du produit **SMCAG01.06.36315**
Catégorie de produit **Environnement d'exécution sécurisé**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **Trusted Logic Mobility S.A.S.** **6, rue de la verrerie** **92197 Meudon Cedex** **France**
Commanditaire **Trusted Logic Mobility S.A.S.** **6, rue de la verrerie** **92197 Meudon Cedex** **France**
Centre d'évaluation **Amossys** **4 bis, allée du Batiment** **35000 Rennes** **France**

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

1.1. Présentation du produit

Le produit évalué est **« Trusted Foundations pour environnement OMPA4, version SMCAG01.06.36315 »** développé par Trusted Logic Mobility S.A.S.

Le produit **Trusted Foundations** (*TF*) est un système d'exploitation (OS) sécurisé destiné à s'exécuter sur un dispositif portable tel qu'un téléphone mobile ou une tablette tactile. TF apporte des services dédiés permettant de sécuriser le dispositif portable sans en perturber son fonctionnement.

TF partage son environnent d'exécution avec d'autres applications non-sécurisées en tirant avantage des fonctions d'isolation entre deux mondes d'exécution mises à disposition par le processeur sur lequel il s'exécute[1] :

- le monde normal (*Rich Execution Environment* ou REE) dans lequel s'exécute un système d'exploitation classique, comme Android, Linux, Windows Mobile, Symbian OS, ou tout autre OS ;
- le monde sécurisé (*Trusted Execution Environment* ou TEE) dans lequel s'exécute le système d'exploitation sécurisé TF qui permet l'exécution de fonctions sensibles avec un niveau de sécurité et d'intégrité supérieur à celui du monde normal.

Communication entre le monde sécurisé et le monde normal :
Un moyen unique appelé « SChannel » est dédié aux échanges entre le monde normal et le monde sécurisé. Il s'agit d'un protocole de communication dédié qui sait gérer plusieurs requêtes concurrentes issues d'applications différentes et/ou multi-instanciées (*multithread*).

Le Trusted Foundations Secure World (*TFSW*) est la partie logicielle qui s'exécute dans le monde sécurisé. Elle s'accompagne d'une bibliothèque de fonctions qui s'intègre au système d'exploitation dans le monde « normal » et qui propose des interfaces (*API*) pour invoquer les services disponibles dans le TFSW grâce à SChannel.

Ce produit est intégré par les fabricants de plateformes mobiles et destiné à être utilisé par des développeurs d'applications sensibles souhaitant profiter des fonctions offertes par le monde sécurisé. Les appels aux fonctionnalités de TF sont donc transparents pour l'utilisateur final de la plateforme.

[1] Trusted Foundations nécessite pour cela d'être intégré sur une plateforme possédant un processeur ARM avec l'extension de sécurité TrustZone.

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☐ 3 – firewall
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☐ 6 - identification, authentification et contrôle d'accès
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 - matériel et logiciel embarqué
☒ **99- Autres : environnement d'exécution sécurisé**

1.2.2. Identification du produit

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

Le numéro de version est obtenu depuis le fichier « index.html » fourni dans l'archive du produit. L'entête de ce fichier mentionne le champ suivant :

SMC OMAP4 Android / Version AG01.06p5.36315 - Release

Il est également possible d'obtenir les mêmes informations depuis l'environnement Android, en utilisant la commande suivante :

```
$ tfctrl list
```

1.2.3. Services de sécurité

TF propose un ensemble de services aux applications du monde normal. Il n'intervient que sur demande et se comporte en mode client / serveur. Il peut traiter en parallèle plusieurs requêtes provenant potentiellement de clients différents.

Les principaux services de sécurité fournis par le produit sont :

- cloisonnement mémoire entre les deux mondes ;
- communication sécurisée entre les deux mondes (protocole SChannel) ;
- mutisme[1] ;
- stockage sécurisé des données clients ;
- fourniture de services cryptographiques ;
- authentification et gestion des autorisations.

1.2.4. Configuration évaluée

La configuration évaluée est celle mettant en œuvre l'ensemble des services offerts par Trusted Foundation.

[1] Comme indiqué dans la cible de sécurité [CDS] la fonctionnalité de mutisme consiste à rendre le monde sécurisé inopérant lorsque le produit se retrouve dans un état instable.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 2 « Argumentaire du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 « Description des biens sensibles que le produit doit protéger »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 5 « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2.6 « Description des utilisateurs typiques »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Comme illustré ci-dessous, la plate-forme de test est composée d'une tablette tactile (**Produit**) et de deux PC de test (**PC-1** et **PC-2**).

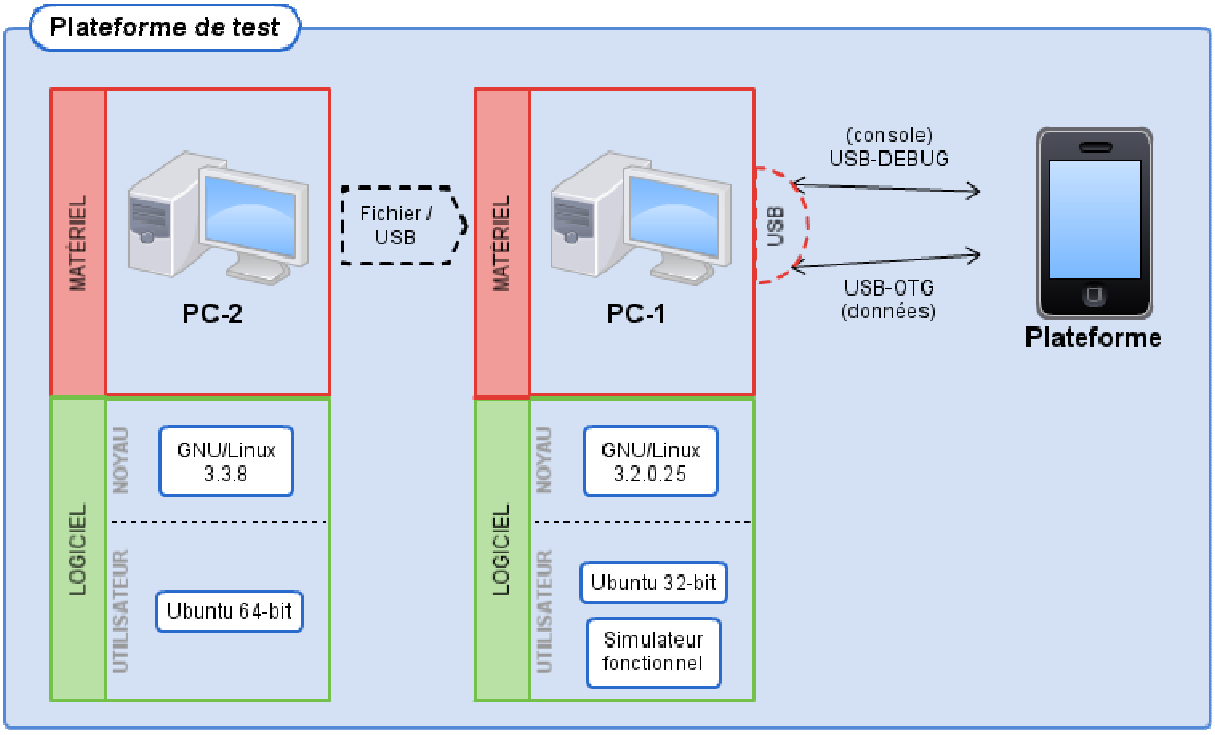

Figure 1 : Plateforme de test

Le PC-1 est utilisé pour interagir avec la cible d'évaluation. Le PC-2 est utilisé pour développer et simuler un environnement parallèle intégré à la plateforme pour certains travaux d'évaluation. Le développement réalisé sur le PC-2 nécessite la suite de compilation ARM fonctionnant uniquement sur un processeur 64 bits.

La configuration des éléments de la plateforme est la suivante :

Plateforme mobile	
Type :	Tablette tactile Texas Instrument
Noyau :	GNU/Linux 64bit 3.0.8-00215-g05eb78
OS du monde normal :	Android 4.0.3
OS du monde sécurisé :	TFSW
Carte mère	OMAP4 4430
Processeur :	2 x ARM-Cortex-A9 Processor rev 2 (v7l)
RAM :	3GB
Stockage :	504MB FLASH

2.3.2.2. Particularités de paramétrage de l'environnement

L'évaluation nécessitant des droits supplémentaires sur le produit, la plateforme fournie pour l'évaluation avait été préalablement configurée afin d'obtenir les privilèges administrateur.

2.3.2.3. Options d'installation retenues pour le produit

Sans objet.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

L'évaluateur a eu accès à la documentation technique du produit. La documentation est claire et détaillée, aucune non-conformité n'a été relevée.

2.3.2.5. Durée de l'installation

L'installation du produit s'est déroulée en quelques heures. L'installation des dépendances liées à l'évaluation a duré 4 jours.

2.3.2.6. Notes et remarques diverses

L'étape de configuration préliminaire à l'intégration est documentée et peut être effectuée seule.

L'intégration nécessite par contre un niveau d'expertise plus important ainsi qu'un accompagnement de la part du développeur pour préparer et déployer le produit.

L'installation est totalement transparente et ne requière aucune action de la part de l'utilisateur.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée.

2.3.4. Revue du code source (facultative)

L'évaluateur a eu accès au code source. Le code est correctement documenté, lisible et jugé simple à maintenir.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Cloisonnement mémoire entre les deux mondes	**Réussite**
Communication entre les deux mondes	**Réussite**
Mutisme	**Non validée**
Stockage sécurisé des données clients	**Réussite**
Services cryptographiques	**Réussite**
Authentification et gestion des autorisations	**Réussite**

L'évaluateur n'est pas parvenu à mettre le produit dans un état instable et n'a donc pas pu observer la fonctionnalité de mutisme offerte par le produit.

2.3.6. Fonctionnalités non testées

L'évaluateur n'ayant pas eu la possibilité de charger des applications dans le monde sécurisé, le cloisonnement mémoire entre applications au sein du TEE n'a pas pu être testé.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

Sans objet.

2.3.8. Avis d'expert sur le produit

L'analyse réalisée a montré que la solution Trusted Foundations est en mesure d'offrir un environnement d'exécution isolé avec lequel l'utilisateur final ne dispose d'aucune possibilité d'interaction directe.

L'installation de l'application, même dans un contexte nominal, souffre d'une documentation constructeur trop succinte. L'utilisation d'outils tiers est indispensable et ceux-ci peuvent être soumis à des restrictions d'utilisation. L'intégrateur doit pour l'instant se référer à la documentation communautaire de l'éditeur OMAP.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Cloisonnement de la mémoire entre le monde sécurisé et le monde normal
Robustesse du protocole SChannel
Services cryptographiques

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Pour l'ensemble des mécanismes et fonctions précités, le produit met en œuvre une bonne protection des données à la fois en termes d'isolation et de chiffrement.

En particulier, la résistance du protocole SChannel a été jugée suffisante. Les services exposés par le protocole prennent en compte les protections nécessaires (vérification du format des données, de leur taille, etc.). L'envoi frauduleux de données via ce protocole de communication est rendu difficile par la nécessité d'obtenir les droits administrateur sur la plateforme.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier.

2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Aucune vulnérabilité n'a été identifiée pendant l'évaluation du produit.

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

L'ensemble de la sécurité du produit reposant sur la validation successive des clés de signature des différents chargeurs, puis du produit Trusted Foundation, la compromission d'une de ces clés, quelle qu'elle soit, remet en cause l'intégrité du produit entier. La chaîne de confiance établie entre le constructeur de la plateforme et l'éditeur du produit est donc primordiale pour la sécurité du produit.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Recommandations à usage du développeur d'application

De nombreux mécanismes cryptographiques fournis par le produit n'offrent pas un niveau de résistance suffisant. Le développeur doit donc veiller à n'utiliser que des mécanismes conformes au référentiel de l'ANSSI [REF-CRY].

Recommandations à usage de l'intégrateur

Afin de protéger la plateforme d'une interception des données stockées dans le monde sécurisé, il est recommandé de charger le produit sur un appareil ne disposant pas des privilèges d'administration.

Il est également recommander de restreindre l'accès physique au port JTAG qui permet d'interagir directement avec les différents modules de la chaîne de démarrage.

2.3.12.3. Avis d'expert sur la facilité d'emploi

Pour l'utilisateur final, l'utilisation de Trusted Foundation est totalement transparente.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

La liste des mécanismes cryptographiques est fournie par la cible de sécurité [CDS] et les spécifications cryptographiques [SPEC_CRY].

La résistance des mécanismes a été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et concluent que de nombreux mécanismes cryptographiques ne sont pas conformes au référentiel de l'ANSSI [REF-CRY]. Cependant, le produit offre également des mécanismes conformes à ce référentiel qui peuvent être choisis par le développeur d'applications (cf. §2.3.12.2).

2.5. Analyse du générateur d'aléas

Le générateur d'aléas étant dépendant de la plateforme sur laquelle le produit s'exécute, il n'a pas été analysé durant cette évaluation.

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.

Ce certificat atteste que le produit « Trusted Foundations**,** SMCAG01.06.36315 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

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 spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport et dans l'ensemble des guides [GUIDES].

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN - Logiciel Trusted Foundations pour environnement OMAP4* ; Version : *1.0.1* ; Date : 29/06/2012.
[RTE]	*RTE CSPN PARASOL* ; Référence : *TLB002-RTE-CSPN-PARASOL* ; Version : *1.02* ; Date : 16/10/2012.
[SPEC-CRY]	*Spécifications des mécanismes cryptographiques ; R*éférence : *CP-2011-RT-692* ; Version : *1.0.2* ; Date : 29/06/2012.
[ANA-CRY]	*Analyse des mécanismes cryptographiques* ; Référence : *TLB002-CRYPTO-PARASOL* ; Version : *1.01* ; Date : 16/10/2012.
[GUIDES]	Guide d'intégration : *SMC OMAP4 Integration Guide ;* Référence : *CP-2010-RT-502*; Date : *16/12/2011.* Guide de développement : *Developer Reference Manual (APIs V3.0)* Référence : *CP-2010-RT-533-V1.0.1* ; Date : *11/02/2011.*

Annexe 2. Références 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.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr