PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2021/48

iTrustee (Version 5.0)

Paris, le 11 novembre 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2021/48

Nom du produit

iTrustee

Référence/version du produit

Version 5.0

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté

ADV_FLR.1

Développeurs

HUAWEI TECHNOLOGIES FRANCE
18 quai du Point du Jour
92659 Boulogne Billancourt Cedex

HUAWEI CENTRAL SOFTWARE
Building Q27, No. 156 Beiqing Rd, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan, Hai-Dian District
Beijing 100095 P.R., China

Commanditaire

HUAWEI TECHNOLOGIES FRANCE
18 quai du Point du Jour
92659 Boulogne Billancourt Cedex

Centre d'évaluation

THALES / CNES
290 allée du Lac,
31670 Labège, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.

SOG-IS

.

PREFACE

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit 6
1.1 Présentation du produit 6
1.2 Description du produit 6
1.2.1 Introduction 6
1.2.2 Services de sécurité 6
1.2.3 Architecture 6
1.2.4 Identification du produit 7
1.2.5 Cycle de vie 8
1.2.6 Configuration évaluée 8
2 L'évaluation 9
2.1 Référentiels d'évaluation 9
2.2 Travaux d'évaluation 9
2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI 9
2.4 Analyse du générateur d'aléa 9
3 La certification 10
3.1 Conclusion 10
3.2 Restrictions d'usage 10
3.3 Reconnaissance du certificat 10
3.3.1 Reconnaissance européenne (SOG-IS) 10
3.3.2 Reconnaissance internationale critères communs (CCRA) 10
ANNEXE A. Références documentaires du produit évalué 12
ANNEXE B. Références liées à la certification 13

1 Le produit

1.1 Présentation du produit

Le produit évalué est « iTrustee, Version 5.0 » développé par HUAWEI TECHNOLOGIES FRANCE.

Ce produit est un environnement d'exécution de confiance *(Trusted Execution Environment* – TEE) pour des mobiles. Il s'agit d'un environnement d'exécution isolé de tout autre environnement d'exécution, y compris l'environnement d'exécution du mobile (*Rich Execution Environment* – REE) et leurs applications qui sont exécutées dans ce REE.

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 tels que les communications sécurisées entre les *Client Applications* (CA) et les TA, le stockage sécurisé des données, la gestion de clés, des algorithmes cryptographiques, etc.

Le produit est destiné à être utilisé dans des téléphone portables HUAWEI de la gamme MATE et P pour offrir des services de sécurité mobiles tels que la gestion des droits numériques, le paiement mobile, ou encore 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 s'inspire du profil de protection [GP_TEECore].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la protection de la TOE qui inclut l'initialisation sécurisée du TEE pour garantir l'authenticité et l'intégrité de la TOE ;
- le stockage de confiance qui fournit la protection en confidentialité et intégrité de données des TA ;
- l'horodatage fiable qui peut être utilisé par les applications de confiance ;
- l'identification des utilisateurs et le contrôle d'accès pour restreindre l'accès des TA à certaines ressources ;
- l'audit de sécurité pour détecter les potentielles violations de sécurité ;
- la protection de la TA pendant tout le cycle de vie ;
- l'instanciation de sécurité du TEE grâce à un processus d'initialisation sécurisé ;
- le support cryptographique pour les TA selon les spécifications de *GlobalPlatform Internal API* [GP_TEECore].

1.2.3 *Architecture*

Le périmètre d'évaluation contient :

- le système d'exploitation iTrustee ;
- les firmwares pour le démarrage sécurisé (Security Boot) et ARM Trusted Firmware (ATF) ;

- les composants matériels suivants : RAM, les accélérateurs cryptographiques, le CPU, le ROM et l'OTP.

La figure 1 décrit l'architecture logicielle et le firmware du produit.

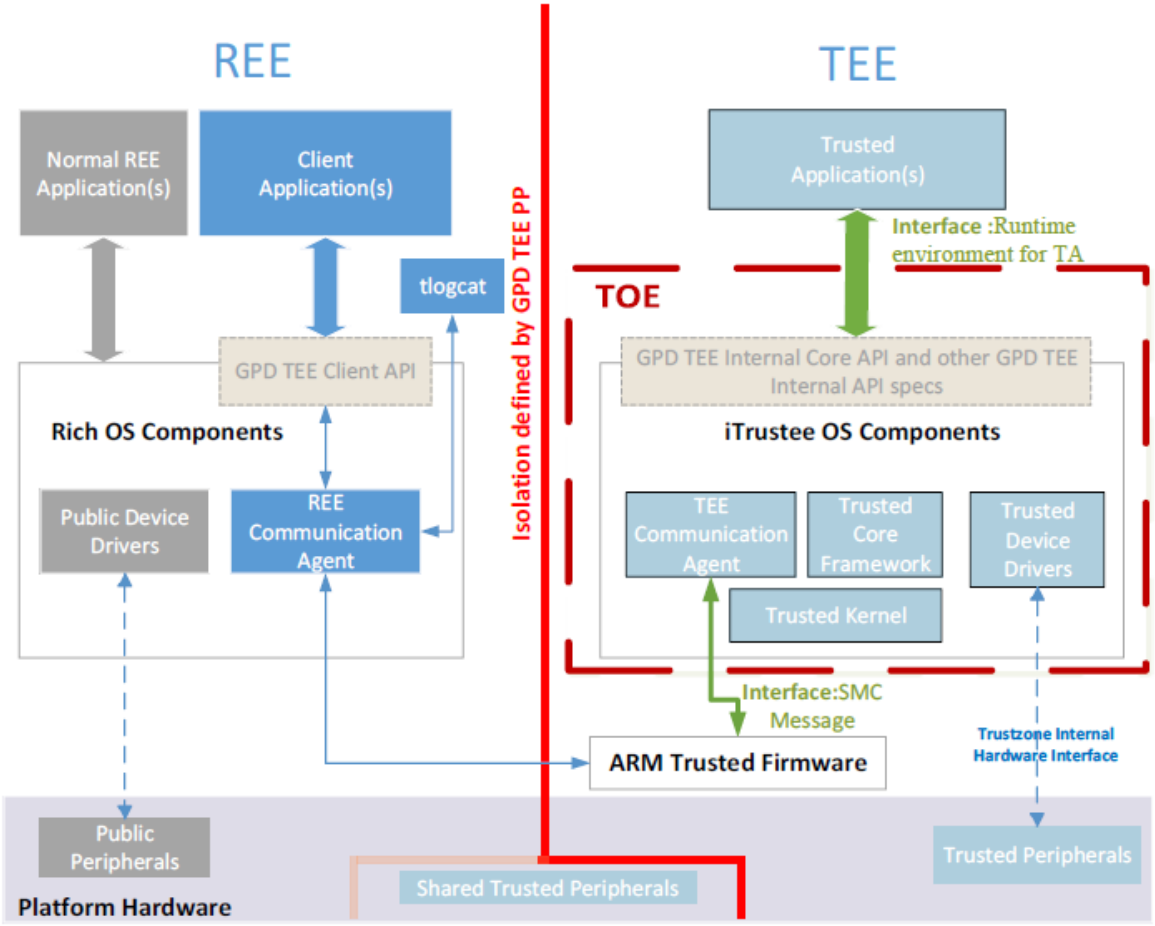

Figure 1 : Architecture logicielle et firmware du produit

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 la cible de sécurité [ST] au chapitre 1.2 « *TOE Identification* ».

Eléments de configuration		Origine
HUAWEI iTrustee	Version 5.0	*HUAWEI TECHNOLOGIES CO., LTD*
Software binary image	6.1.2	

La version de ces éléments peut être vérifiée de la façon suivante :

```
root@Intruder318:~# adb shell
HWTAS:/ # tlogcat -t
tlogcat start ++
---------------------------
iTrustee 5.0(HM)                Release iTRUSTEE_MAIN_6.1.2, Sep 17 2020.10:49:52
Commit ID: ca38083,cc3534f
```

1.2.5 *Cycle de vie*

Le cycle de vie du produit est le suivant :

- Phase 1 : Conception du logiciel, *firmware* et matériel ;
- Phase 2 : Conception de la plateforme matérielle du TEE ;
- Phase 3 : Fabrication des composants matériels ;
- Phase 4 : Intégration des logiciels ;
- Phase 5 : Assemblage de l'appareil ;
- Phase 6 : Utilisation finale.

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

Huawei Beijing Research Institute Beijing China	**Huawei Mobile Dept** Shanghai China
Huawei Machine Co., Ltd Dongguan China	**Shenzhen FuThaiHong Precision Industry Co., Ltd** Shenzhen China

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit les développeurs de TA et CA.

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]).

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].

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 2 août 2021, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY/P/01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le potentiel d'attaque visé.

2.4 Analyse du générateur d'aléa

Le produit ne comporte pas de générateur d'aléa entrant dans le périmètre d'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. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

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'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour certains équipements matériels avec boîtiers sécurisés, 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 signataires[2] , des certificats Critères Communs.

[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.

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 :

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Huawei iTrustee Software V5.0 Security Target*, version 1.6, 26/07/2021. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *CC Huawei iTrustee Software V5.0 Security Target*, version 1.6, 26/07/2021.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report Project : JASMIN*, référence JASMIN_RTE, version 2.2, 02/08/2021.
[CONF]	Liste de configuration du produit : - Huawei iTrustee Software V5.0 CM Scope, version 1.1, 28/07/2021.
[ANA_CRY]	*Analysis of Cryptographic Mechanisms Project: JASMIN, reference JASMIN_CRY*, version 1.1, 03/06/2021.
[GUIDES]	Guide d'installation du produit : - [AGD_PRE] *Huawei iTrustee Software v5.0 Preparative Procedures for User*, version 1.1, 12/08/2020. Guide d'utilisation du produit : - [AGD_OPE] *Huawei iTrustee Software v5.0 Operational User Guidance*, version 1.2, 26/07/2021.
[GP_TEECore]	*GlobaPlatform Technology TEE Internal Core API Specification, reference GPD_SPE_010*, version 1.2, 05/2019.

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]	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.
[CRY-P-01]	Procédure ANSSI-CC-CRY-P01 Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, ANSSI.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.