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-PP-2014/01 du profil de protection « Trusted Execution Environment » (référence GPD_SPE_021, version 1.2)

Paris, le 5 janvier 2015

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.
Un profil de protection est un document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

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-CC-PP-2014/01**
Nom du profil de protection **TEE Protection Profile**
Référence/version du profil de protection **GPD_SPE_021, version 1.2**
Conformité à un profil de protection **Néant**
PP-Base certifiée **Trusted Execution Environement**
PP-Modules associés aux PP-Configurations certifiées **PP-module "TEE Time and Rollback"** **PP-module "TEE Debug"** **PP-modules "TEE Time and Rollback" et "TEE Debug"**
Critères d'évaluation et version **Critères Communs version 3.1, révision 4**
Niveau d'évaluation imposé par le PP **EAL 2 augmenté** **AVA_TEE.2**
Rédacteur **Trusted Labs** **5 rue du Baillage** **78000 Versailles, France**
Commanditaire **GlobalPlatform** **544 Hillside Road** **Redwood City, CA 94062, USA**
Centre d'évaluation **THALES (TCS – CNES)** **18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France**
Accords de reconnaissance applicables **CCRA** **SOG-IS**

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 publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Table des matières

1. PRESENTATION DU PROFIL DE PROTECTION 6
1.1. IDENTIFICATION DU PROFIL DE PROTECTION 6
1.2. REDACTEUR 6
1.3. DESCRIPTION DU PROFIL DE PROTECTION 6
1.4. EXIGENCES FONCTIONNELLES 7
1.5. EXIGENCES D'ASSURANCE 8
1.6. CONFIGURATIONS EVALUEES 8
2. L'EVALUATION 9
2.1. REFERENTIELS D'EVALUATION 9
2.2. COMMANDITAIRE 9
2.3. CENTRE D'EVALUATION 9
2.4. TRAVAUX D'EVALUATION 9
3. LA CERTIFICATION 11
3.1. CONCLUSION 11
3.2. RECONNAISSANCE EUROPEENNE (SOG-IS) 11
3.3. RECONNAISSANCE INTERNATIONALE (CC RA) 12
ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 13
ANNEXE 2. REFERENCES 14

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : TEE Protection Profile
Référence : GPD_SPE_021
Version : 1.2
Date : Novembre 2014

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Labs

5 rue du Baillage
78000 Versailles
FRANCE

1.3. Description du profil de protection

Le profil de protection a été rédigé dans le cadre du groupe de travail « Device Committee » de GlobalPlatform.

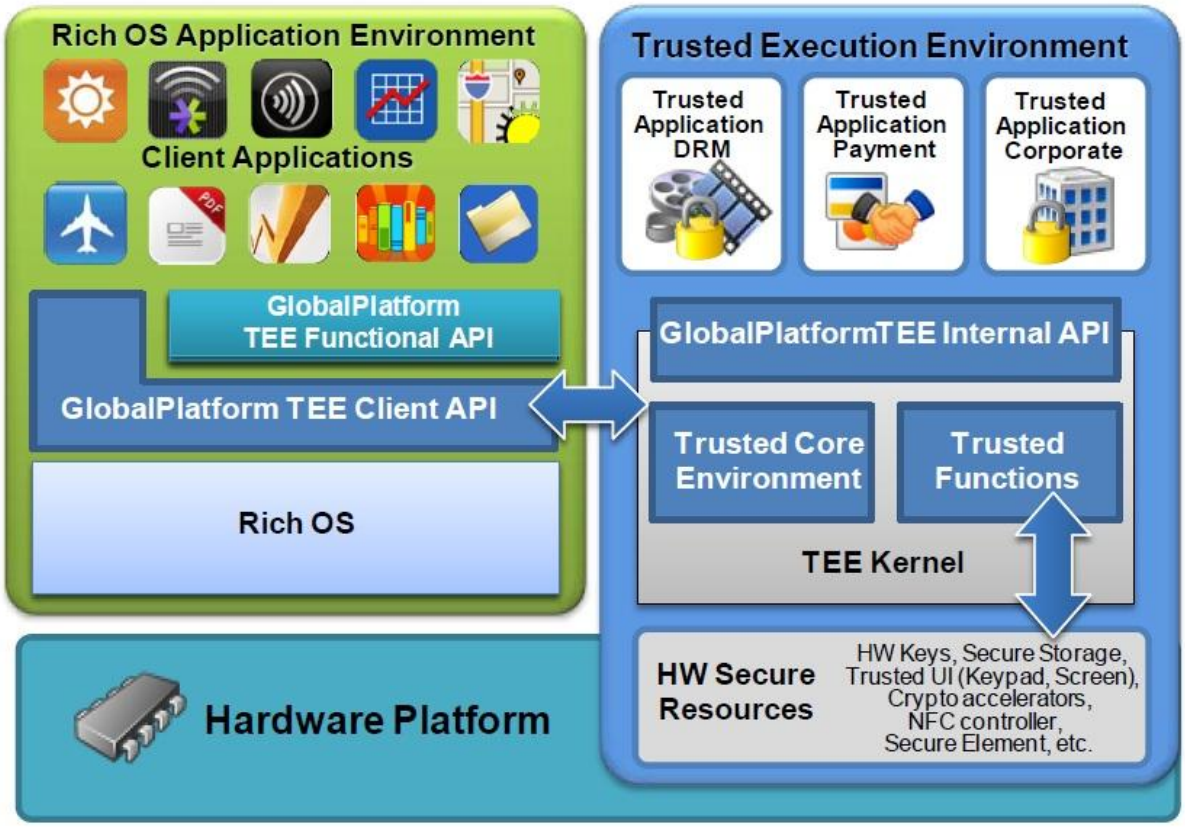
Le TEE, *Trusted Execution Environnement*, ou environnement d'exécution de confiance, est une zone sécurisée, et isolée d'autres environnements d'exécutions, située dans un téléphone portable (ou tout autre équipement mobile). Il est exécuté en parallèle du REE (*Rich Execution Environment*, ou environnement d'exécution du mobile). Le TEE garantit que des données sensibles sont stockées, traitées et protégées dans un environnement de confiance.

Les applications présentes dans le TEE, appelées *Trusted Applications* (TA), ou applications de confiance, bénéficient d'un ensemble de services de sécurité comme l'intégrité de l'exécution du code, les communications sécurisées entre le CA (*Client Applications*) et les TA, le stockage sécurisé des données, la gestion des clefs et d'algorithmes cryptographiques etc.

Le PP TEE comprend un profil de protection de base auquel peuvent s'ajouter deux PP-modules optionnels :

- *TEE Time and Rollback* : implémentation de la protection de *full rollback* et du *persistent monotonic time ;*
- *TEE Debug* : permet l'accès aux fonctions de *debug*.

La figure suivante montre l'architecture du TEE :



Ce profil de protection autorise plusieurs configurations. En effet, il contient une partie « de base » qui consiste à définir des exigences de sécurité minimales pour un TEE, puis deux PP-modules optionnels. Les configurations évaluées sont définies dans le chapitre 1.6.

1.4. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies par le profil de protection[1] sont les suivantes :

- FCS_RNG.1 Random numbers generation
- FPT_INI.1 TSF initialisation

De plus, le profil de protection reprend des exigences fonctionnelles de sécurité définies dans la partie 2 des Critères Communs [CC].

[1] Exigences fonctionnelles étendues non issues de la partie 2 des [CC].

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL2 augmenté du composant AVA_TEE.2**. AVA_TEE.2 correspond à un composant d'assurance étendu[1] 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. Le traitement des deux composants AVA est exigé par le profil de protection.

En dehors du composant d'assurance AVA_TEE.2, toutes les autres exigences d'assurance imposées par le profil de protection sont liées à la partie 3 des Critères Communs [CC].

Ainsi, les reconnaissances SOG-IS et CCRA des produits évalués selon ce profil de protection seront limitées à EAL2.

1.6. Configurations évaluées

Quatre PP-configurations ont été évaluées et sont certifiées :

1. Profil de protection de base ;
2. Profil de protection de base avec le PP-module « *TEE Time and Rollback » ;*
3. Profil de protection de base avec le PP-module « *TEE Debug » ;*
4. Profil de protection de base avec les PP-modules « *TEE Time and Rollback »* et « *TEE Debug »*.

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

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 4** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM] ainsi qu'à l'addendum de ces deux méthodologies [Modular-PP].

2.2. Commanditaire

GlobalPlatform

544 Hillside Road
Redwood City, CA 94062
USA

2.3. Centre d'évaluation

THALES – CEACI (TCS – CNES)

18 avenue Edouard Belin
BPI1414
31401 Toulouse Cedex 9
France

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 1er décembre 2014, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives aux composants d'assurance ci-dessous sont à « **réussite** ».

Pour la configuration 1 (Profil de protection de base, voir le chapitre 1.6), les composants évalués (définis dans [CC]) sont les suivants :

Composants	Descriptions
APE_CCL.1	Conformance claims
APE_ECD.1	Extended components definition
APE_INT.1	Protection profile introduction
APE_OBJ.2	Security objectives
APE_REQ.2	Derived security requirements
APE_SPD.1	Security problem definition

Tableau 1 - Evaluation du PP pour la configuration 1

Pour les configurations 2, 3 et 4 (Profil de protection de base et les différents PP-modules) les composants évalués (définis dans [Modular-PP]) sont les suivants :

Composants	Descriptions
ACE_CCL.1	Conformance claims
ACE_ECD.1	Extended components definition
ACE_INT.1	Protection profile introduction
ACE_OBJ.2	Security objectives
ACE_REQ.2	Derived security requirements
ACE_SPD.1	Security problem definition
ACE_MCO.1	PP-module consistency
ACE_CCO.1	PP-configuration consistency

Tableau 2 - Evaluation du PP pour les configurations 2, 3 et 4

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.

3.2. Reconnaissance européenne (SOG-IS)

Ce rapport de certification 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 les classes d'assurance APE et ACE. 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.

3.3. Reconnaissance internationale (CC RA)

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs. La reconnaissance s'applique pour les classes d'assurance APE et ACE. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] 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, 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**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**2**	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**	Architectural design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**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**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**2**	Implementation representation CM coverage
	ADO_DEL		**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**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**1**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**		
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**2**	Vulnerability analysis
	AVA_TEE		**2**						**2**	TEE vulnerability analysis

Annexe 2. Références

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.	
[CPP-P-01]	Procédure ANSSI-CC-CPP-P-01 Certification de profils de protection, version 2 du 30 mai 2011. ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.
[Modular-PP]	CC and CEM addenda - Modular PP, March 2014, version 1.0, ref CCDB-2014-03-001.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[PP]	TEE Protection Profile, version 1.2, reference GPD_SPE_021.
[RTE]	Evaluation Technical Report - project: TEE Protection Profile, version 5.0, référence TEE_ETR, 1er décembre 2014.