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-2016/05 du profil de protection « Protection profiles for TSP Cryptographic modules - Part 5- Cryptographic Module for Trust Services » (prEN 419 221-5, version 0.15)

*Paris, le 16 décembre 2016*

*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@ssi.gouv.fr

| |
|---|
| *Référence du rapport de certification*<br>**ANSSI-CC-PP-2016/05** |
| *Nom du profil de protection*<br>**Protection profiles for TSP Cryptographic modules - Part 5- Cryptographic Module for Trust Services** |
| *Référence/version du profil de protection*<br>**prEN 419 221-5, version 0.15** |
| *Conformité à un profil de protection*<br>**Néant** |
| *PP-Base certifiée*<br>**Néant** |
| *PP-Modules associés aux PP-Configurations certifiées*<br>**Néant** |
| *Critères d'évaluation et version*<br>**Critères Communs version 3.1, révision 4** |
| *Niveau d'évaluation imposé par le PP*<br>**EAL 4 augmenté**<br>**AVA_VAN.5** |
| *Rédacteur*<br>**CEN/ISSS Secretariat**<br>**17 avenue Marnix, 1000 Bruxelles, Belgique** |
| *Commanditaire*<br>**ANSSI**<br>**51 boulevard de la Tour Maubourg, 75700 Paris cedex 07 SP, France** |
| *Centre d'évaluation*<br>**Oppida**<br>**4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France** |
| *Accords de reconnaissance applicables*<br>**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. Présentation du profil de protection

## 1.1. Identification du profil de protection

Titre : « Protection profiles for TSP Cryptographic modules - Part 5- Cryptographic Module for Trust Services »
Référence, version : prEN 419 221-5, version 0.15
Date : 29/11/2016

## 1.2. Rédacteur

Ce profil de protection a été rédigé par :

**CEN/ISSS Secretariat**
17 avenue Marnix
1000 Bruxelles
Belgique

## 1.3. Description du profil de protection

Le profil de protection [PP] a été rédigé par le CEN, le comité de standardisation européen, dans le cadre de travaux liés au règlement eIDAS [eIDAS].

Le profil de protection [PP] définit les exigences de sécurité des modules cryptographiques mis en œuvre par les prestataires de services de confiance (*Trusted Services Providers*, TSP).
La cible d'évaluation (*Target Of Evaluation*, TOE) définie dans le profil de protection [PP] est un ensemble de composants logiciels et matériels qui offre les fonctionnalités suivantes :

- la génération et la vérification de signatures électroniques ;
- le calcul de condensats (*hash*) de messages ;
- la génération et la vérification de messages d'authentification ;
- le chiffrement symétrique et asymétrique et le déchiffrement de données ;
- la génération de clés cryptographiques ;
- la dérivation de clés ;
- la génération de secrets partagés ;
- la négociation et la distribution de clés ;
- le support cryptographique pour l'utilisation de mots de passe à usage unique et d'autres mécanismes d'authentification ne s'appuyant pas sur une infrastructure de gestion de clés ;
- la génération de nombres aléatoires.

Le profil de protection est relatif à des services cryptographiques génériques. Pour obtenir un service de confiance spécifique (signature électronique qualifiée, horodatage, …), il est nécessaire de compléter ce profil de protection avec des exigences de sécurité ou d'autres profils de protection adaptées à ce service spécifique.

## 1.4. Exigences fonctionnelles

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

- generation of random numbers (FCS_RNG.1) ;
- basic TSF Self Testing (FPT_TST_EXT.1).

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

- Audit data generation (FAU_GEN.1) ;
- User identity association (FAU_GEN.2) ;
- Guarantees of audit data availability (FAU_STG.2) ;
- Cryptographic key generation (FCS_CKM.1) ;
- Cryptographic key destruction (FCS_CKM.4) ;
- Cryptographic operation (FCS_COP.1) ;
- Subset access control (FDP_ACC.1) ;
- Security attribute based access control (FDP_ACF.1) ;
- Subset information flow control (FDP_IFC.1) ;
- Simple security attributes (FDP_IFF.1) ;
- Subset residual information protection (FDP_RIP.1) ;
- Stored data integrity monitoring and action (FDP_SDI.2) ;
- Authentication failure handling (FIA_AFL.1) ;
- Timing of authentication (FIA_UAU.1) ;
- Re-authenticating (FIA_UAU.6) ;
- Timing of identification (FIA_UID.1) ;
- Management of security attributes (FMT_MSA.1) ;
- Static attribute initialisation (FMT_MSA.3) ;
- Management of TSF data (FMT_MTD.1) ;
- Specification of Management Funct (FMT_SMF.1) ;
- Security roles (FMT_SMR.1) ;
- Failure with preservation of secure state (FPT_FLS.1) ;
- Reliable time stamps (FPT_STM.1) ;
- Passive detection of physical attack (FPT_PHP.1) ;
- Resistance to physical attack (FPT_PHP.3) ;
- Trusted Path (FTP_TRP.1).

[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 **EAL4 augmenté du composant d'assurance AVA_VAN.5**.

Toutes les exigences d’assurance imposées par le profil de protection sont extraites de la partie 3 des Critères Communs [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].

## 2.2. Commanditaire

**ANSSI**
51 boulevard de la Tour Maubourg
75700 Paris cedex 07 SP
France

## 2.3. Centre d'évaluation

**OPPIDA**
4-6 avenue du vieil étang
Bâtiment B
78180 Montigny le Bretonneux
France

## 2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 novembre 2016, 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** ».

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**

# 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 classes d'assurance APE. 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. 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, 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 4+ | 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 | **4** | Complete functional specification |
| | ADV_IMP | | | | **1** | 1 | 2 | 2 | **1** | Implementation representation of TSF |
| | ADV_INT | | | | | 2 | 3 | **3** | | |
| | ADV_SPM | | | | | | 1 | 1 | | |
| | ADV_TDS | | 1 | 2 | **3** | 4 | 5 | 6 | **3** | Basic modular 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 | **4** | Production support, acceptance procedures and automation |
| | ALC_CMS | 1 | 2 | 3 | **4** | 5 | 5 | 5 | **4** | Problem tracking CM coverage |
| | ALC_DEL | | 1 | 1 | **1** | 1 | 1 | 1 | **1** | Delivery procedures |
| | ALC_DVS | | | **1** | 1 | 1 | **2** | 2 | **1** | Identification of security measures |
| | ALC_FLR | | | | | | | | | |
| | ALC_LCD | | | 1 | **1** | 1 | 1 | 2 | **1** | Developer defined life-cycle model |
| | ALC_TAT | | | | **1** | 2 | 3 | 3 | **1** | Well-defined development tools |
| **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 | **2** | Analysis of coverage |
| | ATE_DPT | | | 1 | **1** | 3 | 3 | 4 | **1** | Testing: basic design |
| | 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 | **5** | Advanced methodical 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.<br>ANSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation :<br>Part 1: Introduction and general model,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-001;<br>Part 2: Security functional components,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-002;<br>Part 3: Security assurance components,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology,<br>September 2012, version 3.1, révision 4, ref CCMB-2012-09-004. |
| [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. |
| [eIDAS] | Règlement (UE) n°910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la direction 1999/93/CE. |
| [PP] | Protection profiles for TSP Cryptographic modules - Part 5- Cryptographic Module for Trust Services, référence prEN 419 221-5, version 0.15. |
| [RTE] | Evaluation Technical report – PP CMTS, référence : OPPIDA/CESTI/PP_CMTS/RTE/2.0. |