Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification PP 2006/03

Profil de Protection Pare-feu Personnel (PP-PFP)

Paris, le 11 juillet 2006.

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ Ti 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. Les produits ainsi définis satisfont les besoins de sécurité communs à un groupe d'utilisateurs.
La certification d'un profil de protection ne constitue pas en soi une recommandation de ce profil de protection par le centre de certification.

Table des matières

1. PRESENTATION DU PROFIL DE PROTECTION 5

1.1. IDENTIFICATION DU PROFIL DE PROTECTION 5
1.2. REDACTEUR 5
1.3. DESCRIPTION DU PROFIL DE PROTECTION 5
1.3.1. Généralités 5
1.3.2. Périmètre de la cible d'évaluation 5
1.4. EXIGENCES FONCTIONNELLES 5
1.5. EXIGENCES D'ASSURANCE 6
1.6. OBJECTIFS DE SECURITE SUR L'ENVIRONNEMENT 7

2. L'EVALUATION 8

2.1. CENTRE D'EVALUATION 8
2.2. COMMANDITAIRE 8
2.3. REFERENTIELS D'EVALUATION 8
2.4. EVALUATION DU PROFIL DE PROTECTION 8

3. CONCLUSIONS DE L'EVALUATION 9

3.1. RAPPORT TECHNIQUE D'EVALUATION 9
3.2. NIVEAU D'EVALUATION 9
3.3. RECOMMANDATIONS ET LIMITATIONS D'USAGE 9
3.4. SYNTHESE DES RESULTATS 9
3.5. RECONNAISSANCE EUROPEENNE (SOG-IS) 9
3.6. RECONNAISSANCE INTERNATIONALE (CC RA) 9

ANNEXE 1. NIVEAUX D'ASSURANCE PREDEFINIS 10

ANNEXE 2. REFERENCES 11

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)

Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

[2] En juin 2006, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande, le Japon, la Norvège, les Pays-Bas et la Corée du Sud ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Suède, la Turquie, la République Tchèque, Singapour, l'Inde et le Danemark.

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Profil de Protection Pare-feu Personnel
Référence : PP-PFP
Version : 1.4
Date : 2 mai 2006

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Fidens

8-10, rue Emile Sehet
95257 Taverny cedex.

1.3. Description du profil de protection

1.3.1. Généralités

Ce profil de protection est conforme aux préconisations de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) pour la qualification de produits de sécurité au niveau standard [QUA-STD]. En mettant ce profil de protection à la disposition des fournisseurs de produits, la DCSSI souhaite encourager la qualification d'applications de signature sur la base du présent profil.

1.3.2. Périmètre de la cible d'évaluation

La cible d'évaluation définie dans le profil de protection [PP] est un composant logiciel installé sur un poste de travail et destiné à assurer le filtrage des flux réseau entrant et sortant de ce poste de travail.

1.4. Exigences fonctionnelles

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

- FAU_ARP.1 security audit automatic response
- FAU_GEN.2 audit data generation with time
- FAU_SAA.3 simple attack heuristics
- FCO_CED.1 confidentiality of exported data
- FCO_CID.1 confidentiality of imported data
- FCO_ETC.1 export of data and/or security attributes
- FCO_IED.1 integrity of exported data without recovery

- FCO_IID.1 integrity of imported data without recovery
- FCO_ITC.1 import without security attributes
- FDP_ACC.1access control
- FDP_ISA.1 security attribute initialisation
- FDP_MSA.1 management of security attributes
- FIA_AFL.1 authentication failure handling
- FIA_QAD.1 verification of quality of authentication data
- FIA_QAD.2 TSF generation of authentication data
- FIA_SUA.1 TSF authentication
- FIA_TBR.1 TSF binding rules
- FIA_TOB.1 TSF-initiated termination of binding
- FIA_TOB.2 user-initiated termination of binding
- FIA_UAU.1 user authentication by TSF
- FIA_UAU.6 limited authentication feedback
- FIA_UID.1 anonymous users
- FIA_UID.2 user identification
- FIA_URE.2 user registration with storage of authentication data
- FIA_USB.1 user-subject binding
- FMI_CHO.1 choice
- FPT_RIP.2 removal after use
- FPT_RSA.1 maximum quotas for subjects and objects
- FPT_TST.1 TSF self-testing
- FPT_TST.2 integrity testing

Toutes les exigences fonctionnelles du profil de protection sont extraites de la partie 2 des Critères Communs [CC].

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau d'assurance de la qualification standard [QS-QR], **EAL2[1] augmenté des composants d'assurance suivants** :

[1] Annexe 1 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

Composants	Descriptions
ADV_TDS.3**	Basic modular design
ALC_DVS.1	Identification of security measures
ADV_IMP.1*	Implementation representation of the TSF
ALC_FLR.3	Systematic flaw remediation
ALC_TAT.1	Well-defined development tools
AVA_VAN.3	Focused vulnerability analysis

Tableau 1 - Augmentations

** Le composant ADV_IMP.1 est raffiné de la façon suivante : The sample of the implementation representation shall contain all the cryptographic mechanisms of the TOE.*

*** Le composant ADV_TDS.3 est raffiné de la façon suivante : The description of the design of the TSF in terms of modules could be limited to the cryptographic mechanisms of the TOE.*

Le composant ADV_TDS.3** étant moins « exigeant » que ADV_TDS.3, seule une conformité au composant ADV_TDS.2 peut-être reconnue au titre des accords de reconnaissance.

Toutes les exigences d'assurance du profil de protection sont extraites de la partie 3 des Critères Communs [CC].

1.6. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité sur l'environnement du profil de protection sont les suivants :

- OE_administrateurs_de_confiance
- OE_usager_non_privilégié
- OE_livraison_sûre
- OE_maîtrise_configuration
- OE_ressources_disponibles
- OE_poste_sûr
- OE_contexte_sûr
- OE_type_environnement
- OE_filtrage_total
- OE_poste_utilisateurs
- OE_protection_physique

2. L'évaluation

2.1. Centre d'évaluation

Oppida

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

Téléphone : +33 (0)1 30 14 19 00

Adresse électronique : cesti@oppida.fr

2.2. Commanditaire

Direction Centrale de la Sécurité des Systèmes d'Information

51, boulevard de la Tour-Maubourg
75700 Paris SP.

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.4. Evaluation du profil de protection

L'évaluation du profil de protection a été menée sur la base des exigences de la classe APE définie dans la partie 3 des Critères Communs [CC] :

Class APE	Security Target evaluation
APE_INT.1	PP introduction
APE_CCL.1	Conformance claims
APE_SPD.1	Security problem definition
APE_OBJ.2	Security objectives
APE_ECD.1	Extended components definition
APE_REQ.2	Security requirements

Tableau 2- Composants d'assurance de la classe APE

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats détaillés de l'évaluation du profil de protection.

3.2. Niveau d'évaluation

Pour tous les composants de la classe APE, les verdicts suivants ont été émis :

Class APE	Protection profile evaluation	
APE_INT.1	PP introduction	réussite
APE_CCL.1	Conformance claims	réussite
APE_SPD.1	Security problem definition	réussite
APE_OBJ.2	Security objectives	réussite
APE_ECD.1	Extended components definition	réussite
APE_REQ.2	Security requirements	réussite

Tableau 3 - Composants et verdicts associés

3.3. Recommandations et limitations d'usage

Le certificat d'un profil de protection ne s'applique qu'à la version évaluée du profil de protection.

3.4. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le profil de protection Profil de Protection Pare-feu Personnel identifié au paragraphe 1.1 du présent rapport **est conforme** aux exigences de la classe APE. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

3.5. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

3.6. Reconnaissance internationale (CC RA)

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

Annexe 1. Niveaux d'assurance prédéfinis

Classe	Famille	Composants d'assurance par niveau d'évaluation							
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	QS
Development	ADV_ARC		1	1	1	1	1	1	**1**
	ADV_FSP	1	2	3	4	5	5	6	**2**
	ADV_IMP				1	1	2	2	**1***
	ADV_INT					2	3	4	
	ADV_SPM						1	1	
	ADV_TDS		1	2	3	4	5	6	**3****
Guidance documents	AGD_OPE	1	1	1	1	1	1	1	**1**
	AGD_PRE	1	1	1	1	1	1	1	**1**
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5	**2**
	ALC_CMS	1	2	3	4	5	5	5	**2**
	ALC_DEL		1	1	1	1	1	1	**1**
	ALC_DVS			1	1	1	2	2	**1**
	ALC_FLR								**3**
	ALC_LCD				1	2	2	3	
	ALC_TAT				1	2	3	3	**1**
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1	**1**
	ASE_ECD	1	1	1	1	1	1	1	**1**
	ASE_INT	1	1	1	1	1	1	1	**1**
	ASE_OBJ	1	2	2	2	2	2	2	**2**
	ASE_REQ	1	2	2	2	2	2	2	**2**
	ASE_SPD		1	1	1	1	1	1	**1**
	ASE_TSS	1	1	1	1	1	1	1	**1**
Tests	ATE_COV		1	2	2	2	3	3	**1**
	ATE_DPT			1	1	2	2	3	
	ATE_FUN		1	1	1	1	2	2	**1**
	ATE_IND	1	2	2	2	2	2	3	**2**
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5	**3**

* Le composant ADV_IMP.1 est raffiné de la façon suivante : The sample of the implementation representation shall contain all the cryptographic mechanisms of the TOE.
** Le composant ADV_TDS.3 est raffiné de la façon suivante : The description of the design of the TSF in terms of modules could be limited to the cryptographic mechanisms of the TOE.

Annexe 2. Références

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, June 2005, version 3.0, revision 2, ref CCMB-2005-07-001; ▪ Part 2: Security functional requirements, July 2005, version 3.0, revision 2, ref CCMB-2005-07-002 ; ▪ Part 3: Security assurance requirements, July 2005, version 3.0, revision 2,ref CCMB-2005-07-003.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Evaluation Methodology, June 2005, version 3.0, revision 2, ref CCMB-2005-07-004
[QS-QR]	Définition des paquets d'assurance pour la qualification standard et la qualification renforcée suivant les CC version 3 – Document du 8 février 2006
[RTE]	PP-PFP Rapport de fin de tâche APE, réf: OPPIDA/CESTI/AIK/548/3.0, version 3.0 du 2 juin 2006.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr