



PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification PP 2006/02

Profil de Protection Application VPN cliente (PP-VPNC)

Paris, le 11 juillet 2006.

*Le Directeur central de la sécurité des
systèmes d'information*

Patrick Pailloux
[ORIGINAL SIGNE]



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	6
1.5. EXIGENCES D'ASSURANCE	6
1.6. OBJECTIFS DE SECURITE SUR L'ENVIRONNEMENT	7
1.6.1. Objectifs de sécurité sur l'environnement de développement	7
1.6.2. Objectifs de sécurité sur l'environnement opérationnel	7
2. L'EVALUATION	9
2.1. CENTRE D'EVALUATION	9
2.2. COMMANDITAIRE	9
2.3. REFERENTIELS D'EVALUATION	9
2.4. EVALUATION DU PROFIL DE PROTECTION	9
3. CONCLUSIONS DE L'EVALUATION.....	10
3.1. RAPPORT TECHNIQUE D'EVALUATION	10
3.2. RESULTATS D'EVALUATION	10
3.3. RECOMMANDATIONS ET LIMITATIONS D'USAGE	10
3.4. SYNTHESE DES RESULTATS	10
3.5. RECONNAISSANCE EUROPEENNE (SOG-IS)	11
3.6. RECONNAISSANCE INTERNATIONALE (CC RA)	11
ANNEXE 1. NIVEAUX D'ASSURANCE PREDEFINIS.....	12
ANNEXE 2. REFERENCES	13

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'accord¹, 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 signataires², 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 Application VPN cliente

Référence : PP-VPNC¹

Version : 1.0

Date : avril 2006

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Labs

5, rue du Bailliage

78000 Versailles

1.3. Description du profil de protection

1.3.1. Généralités

Le profil de protection a été rédigé dans le cadre d'un marché du SGDN/DCSSI. Il est le résultat de réunions avec les utilisateurs et les développeurs de ce type de produit.

Ce profil de protection est conforme aux préconisations pour la qualification de produits de sécurité au niveau standard selon la version 3.0 des CC [QS-QR].

1.3.2. Périmètre de la cible d'évaluation

La cible d'évaluation définie dans le profil de protection [PP] correspond à une application VPN présente sur un poste client. Ce profil de protection complète ainsi le profil « Chiffreur IP » ([PPnc0502]) qui spécifie les exigences sécuritaires d'une passerelle VPN.

L'application VPN cliente permet d'établir un lien de communication entre un équipement nomade ne disposant pas nécessairement d'une adresse prédictible (de type ordinateur portable connecté via un fournisseur d'accès ou via un réseau d'entreprises) et une passerelle VPN placée à l'entrée du réseau privé d'une organisation. Ce lien de communication peut potentiellement utiliser un réseau public non sûr, comme Internet, et des moyens d'accès extrêmement variés (tel que Wi-Fi), exposant ainsi le lien de communication à de nombreuses menaces qui imposent sa sécurisation. Les technologies « VPN » assurent l'obtention d'une sécurité des échanges réseaux équivalente à celle fournie par une liaison point à point, physiquement et logiquement dédiée.

¹ Lors de sa phase de développement, ce Profil de Protection était identifié par la référence : PU-2005-RT-454-1.2.2.

Le type de TOE¹ considéré est un client de type IPsec, mais les développeurs de produits implémentant un client VPN SSL pourront s'inspirer au besoin du présent PP pour la rédaction de la cible de sécurité de leur produit.

1.4. Exigences fonctionnelles

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

- Confidentiality of exported data (FCO_CED.1)
- Confidentiality of imported data (FCO_CID.1)
- Export of data and/or security attributes (FCO_ETC.1)
- Integrity of exported data without recovery (FCO_IED.1)
- Integrity of imported data without recovery (FCO_IID.1)
- Import without security attributes (FCO_ITC.1)
- Import with security attributes (FCO_ITC.2)
- Access control (FDP_ACC.1)
- Security attribute initialisation (FDP_ISA.1)
- TSF authentication (FIA_SUA.1)
- User authentication by TSF (FIA_UAU.1)
- User identification (FIA_UAU.2)
- User identification (FIA_UID.2)
- User-subject binding (FIA_USB.1)

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 **EAL2² augmenté des composants d'assurance suivants** :

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

¹ Target Of Evaluation

² Annexe 1 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

Tableau 1 - Augmentations

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

** *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

1.6.1. Objectifs de sécurité sur l'environnement de développement

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

- La TOE doit être évalué au niveau de qualification standard défini par la DCSSI; dans [QS-QR]; soit un EAL2 augmenté des exigences d'assurance, ADV_TDS.3, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1 et AVA_VAN.3. Par ailleurs, la description du design -ADV_TDS.3- et de l'implémentation -ADV_IMP.1- des mécanismes cryptographiques est requise (OED.EAL).

1.6.2. Objectifs de sécurité sur l'environnement opérationnel

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

- Les administrateurs doivent être de confiance et formés aux tâches qu'ils ont à réaliser sur la TOE (OE.ADMIN) ;
- L'utilisateur est formé à l'utilisation de la TOE et sensibilisé à la sécurité, en particulier sur les risques liés à la divulgation des informations qu'il détient et qui lui permettent de s'authentifier auprès du système de chiffrement (OE.UTILISATEUR) ;
- L'équipement de téléadministration centralisé doit se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs. Sa disponibilité devra par ailleurs être assurée et son bon fonctionnement régulièrement contrôlé (OE.EQUIPEMENT_TELEADMINISTRATION) ;
- Le chiffreur IP avec lequel l'application VPN cliente communique doit permettre de tracer les activités qui ont eu lieu sur le lien VPN. Il devra par ailleurs activer des alarmes de sécurité permettant de remonter vers un administrateur de sécurité toute violation des politiques de sécurité VPN sur le lien considéré (OE.CHIFFREUR_IP) ;
- Le composant du système de chiffrement réalisant l'authentification de l'utilisateur et de l'administrateur de sécurité doit être qualifié (au moins) au

niveau standard tel que défini par la DCSSI dans [QS-QR] (OE.COMPOSANT_AUTHENTIFIANT) ;

- La machine hôte sur laquelle est exécutée l'application VPN cliente doit être saine, protégée et configurée de manière à garantir sa sécurité et celle des données qu'elle héberge. En particulier, elle assure l'intégrité de l'application VPN cliente qu'elle héberge (OE.MACHINE) ;
- Seuls les administrateurs peuvent réaliser les tâches d'administration relatives à l'application VPN cliente -installation, configuration, mise à jour et désinstallation- (OE.DROITS_UTILISATEURS) ;
- La configuration de la machine hébergeant l'application VPN cliente doit protéger les communications sur les liens VPN des impacts pouvant résulter de communications en clair de la machine via différents canaux physiques ou logiques (OE.CONFIGURATION) ;
- L'environnement de la TOE doit permettre de maîtriser les communications vers et depuis l'extérieur de la machine hôte qui ne transitent pas par la TOE (OE.COMM) ;
- La configuration de la machine hôte hébergeant l'application VPN cliente doit rendre impossible l'export hors de la machine par l'utilisateur des clés cryptographiques secrètes ou privées importées ou générées dans la TOE (OE.EXPORT_CLES) ;
- La gestion des identifications/authentifications des différents utilisateurs d'une machine multi-utilisateurs doit être prise en compte par l'environnement de la TOE (OE.MULTI-UTILISATEURS) ;
- L'environnement doit permettre de réinitialiser la TOE dans un état sûr (OE.REINITIALISATION) ;
- Les clés cryptographiques, générées à l'extérieur de la TOE, qui sont injectées dans la TOE doivent avoir été générées en suivant les recommandations spécifiées dans le référentiel de cryptographie de la DCSSI [CRYPTO] pour le niveau de résistance standard (OE.CRYPTO) ;
- L'accès aux différents composants du système de chiffrement doit être restreint grâce à une gestion de clés cryptographiques -secret partagé, infrastructure à clé publique,...- associée à une politique de sécurité VPN (OE.ACCES).

2. L'évaluation

2.1. Centre d'évaluation

AQL Groupe SILICOMP

1 rue de la châtaigneraie
CS 51766
F 35513 Cesson Sévigné Cedex
France

Téléphone : +33 (0)2 99 12 50 00

Adresse électronique : cesti@aql.fr

2.2. Commanditaire

SGDN/DCSSI

51 boulevard de La Tour-Maubourg
75007 Paris

Adresse électronique : certification.dcssi@sgdn.pm.gouv.fr

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC] et 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	Derived 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. Résultats 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	Derived 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.

La TOE se situe dans le contexte d'un système de chiffrement composé de machines hôtes hébergeant l'application VPN cliente, de chiffreurs IP et d'équipements d'administration (ou de télégestion) pouvant héberger des services de mise à jour des politiques de sécurité VPN. La formulation des hypothèses de [PP] montre l'importance de ces équipements environnant, il est donc raisonnable de penser que l'équipement d'administration et la passerelle VPN (chiffreur IP) sur lesquelles la TOE s'appuie pour fonctionner seront des produits de confiance, éventuellement certifiés indépendamment.

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 Application VPN cliente (PP-VPNC) 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]	<p>Critères Communs pour l'évaluation de la sécurité des technologies de l'information:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Méthodologie d'évaluation de la sécurité des technologies de l'information:</p> <ul style="list-style-type: none"> ▪ Evaluation Methodology, June 2005, version 3.0, revision 2, ref CCMB-2005-07-004.
[RTE]	Profil de protection VPNC - Rapport Technique d'Evaluation - Activité APE, version 1.1, réf TDL002-VPNC-RTE-1.1, SILICOMP-AQL
[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
[CRYPTO]	Mécanismes de cryptographie : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard. Version 1.02, 19 novembre 2004. DCSSI.
[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

La reproduction de ce document sans altérations ni coupures est autorisée.