



PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

**Rapport de certification DCSSI-PP 2008/08
du profil de protection
« Chiffreur IP »
(référence PP-CIP-3.1, version 1.9)**

Paris, le 22 août 2008

*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, 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 nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

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



<i>Référence du rapport de certification</i>	DCSSI-PP 2008/08
<i>Nom du profil de protection</i>	Chiffreur IP
<i>Référence/version du profil de protection</i>	Référence : PP-CIP-3.1 / Version 1.9
<i>Critères d'évaluation et version</i>	Critères Communs version 3.1
<i>Niveau d'évaluation imposé par le PP</i>	EAL 3 augmenté ALC_FLR.3, AVA_VAN.3
<i>Rédacteur</i>	Trusted Labs SAS 5 rue du Bailliage, 78000 Versailles, France
<i>Commanditaire</i>	DCSSI 51, boulevard de la Tour-Maubourg ,75700 Paris 07 SP, France
<i>Centre d'évaluation</i>	Silicomp-AQL 1 rue de la châtaigneraie, CS 51766, 35513 Cesson Sévigné Cedex, France Tél : +33 (0)2 99 12 50 00, mél : cesti@aql.fr
<i>Accords de reconnaissance applicables</i>	<div style="display: flex; justify-content: space-around;"><div style="text-align: center;">CCRA </div><div style="text-align: center;">SOG-IS </div></div>

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



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	6
1.5. EXIGENCES D'ASSURANCE	7
2. L'EVALUATION	8
2.1. REFERENTIELS D'EVALUATION	8
2.2. COMMANDITAIRE	8
2.3. CENTRE D'EVALUATION	8
2.4. TRAVAUX D'EVALUATION	8
3. LA CERTIFICATION	9
3.1. CONCLUSIONS	9
3.2. RECOMMANDATIONS ET LIMITATIONS D'USAGE	9
3.3. RECONNAISSANCE EUROPEENNE (SOG-IS)	10
3.4. RECONNAISSANCE INTERNATIONALE (CC RA)	10
ANNEXE 1. NIVEAU D'EVALUATION.....	11
ANNEXE 2. REFERENCES.....	12

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Profil de protection Chiffreur IP - CC3.1

Référence, version : PP-CIP-3.1 / Version 1.9

Date : Juillet 2008

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Labs SAS

5 rue du Bailliage

78000 Versailles

France

1.3. Description du profil de protection

Le [PP] définit les exigences de sécurité pour une passerelle (ou « gateway ») d'un réseau privé virtuel (VPN).

Ces passerelles VPN sont placées aux entrées/sorties de réseaux privés, considérés comme sûrs, pour établir des liens de communication entre plusieurs de ces réseaux privés en utilisant un réseau public (comme Internet), considéré comme non sûr. Ces liens de communication entre plusieurs passerelles VPN, aussi appelé liens VPN, doivent être sécurisés pour que les données qui transitent entre les réseaux privés puissent être protégées vis-à-vis de tous les utilisateurs du réseau public.

Ce profil de protection se limite à définir des exigences de sécurité pour les passerelles VPN, qui permettent de faire communiquer des réseaux privés, et ne définit pas d'exigences de sécurité sur la partie VPN clients, qui permet d'établir des communications sécurisées entre équipements nomades (PC, portables) ou entre des équipements nomades et des réseaux privés. Cette partie est couverte par ailleurs par le PP « Application VPN cliente ».

Ce profil de protection est conforme aux préconisations de la 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 de produits sur la base du présent profil.

1.4. Exigences fonctionnelles

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

- Security alarms (FAU_ARP.1)
- Audit data generation (FAU_GEN.1)
- Potential violation analysis (FAU_SAA.1)
- Audit review (FAU_SAR.1)



- Selectable audit review (FAU_SAR.3)
- Protected audit trail storage (FAU_STG.1)
- Cryptographic key access (FCS_CKM.3)
- 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)
- Export of user data without security attributes (FDP_ETC.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Import of user data without security attributes (FDP_ITC.1)
- Subset residual information protection (FDP_RIP.1)
- Basic data exchange confidentiality (FDP_UCT.1) ;
- Data exchange integrity (FDP_UIT.1)
- User authentication before any action (FIA_UAU.2)
- User identification before any action (FIA_UID.2)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Management of TSF data (FMT_MTD.1) ;
- Specification of management functions (FMT_SMF.1)
- Security roles (FMT_SMR.1)
- Reliable time stamps (FPT_STM.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 **EAL3¹ augmenté des composants d'assurance suivants** :

Composants	Descriptions
ALC_FLR.3	Systematic flaw remediation
AVA_VAN.3	Focused vulnerability analysis

Tableau 1 - Augmentations

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

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

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Commanditaire

Direction centrale de la sécurité des systèmes d'information

51 boulevard de la Tour-Maubourg
75700 Paris 07 SP
France

2.3. Centre d'évaluation

SILICOMP-AQL

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

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 15 juillet 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives à la classe d'exigences d'assurance APE sont à « **réussite** ».



3. La certification

3.1. Conclusions

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. Recommandations et limitations d'usage

Une cible de sécurité se réclamant conforme au PP peut présenter des fonctionnalités supplémentaires non prises en compte par ce PP : pare-feu (ou « firewall »), serveur d'authentification, passerelle anti-virus,... Les fonctionnalités additionnelles et leur implémentation ne doivent pas remettre en cause les exigences du présent PP. Lors de la rédaction d'une cible de sécurité se réclamant conforme à ce profil de protection, ces fonctionnalités sont parfaitement exprimables et, le cas échéant, la cible pourra faire référence à tout autre profil de protection les couvrant.

Ce profil de protection définit les exigences sur la configuration minimale d'un chiffreur IP qui comprend l'administration locale du chiffreur IP. Trois autres configurations peuvent être envisagées à partir des deux options suivantes, disponibles dans l'annexe A du [PP] :

- l'administration à distance des chiffreurs IP en plus de l'administration locale ;
- la négociation dynamique d'une partie des contextes des politiques de sécurité appliquées par les chiffreurs IP.

La méthodologie Critères Communs ne permettant pas l'évaluation d'un profil avec options, il a été choisi d'évaluer la configuration minimale et de définir les éléments (menaces, hypothèses, OSP, objectifs et exigences) spécifiques à chaque option en notes d'application. Ces notes d'application contiennent aussi l'argumentaire d'associations entre ces éléments uniquement pour la configuration maximale (administration à distance et négociation dynamique) afin de conserver le travail réalisé dans une version précédente du profil de protection.

Une cible de sécurité se réclamant conforme au PP et incluant une ou deux options définies dans les notes d'application doit prendre en compte les éléments et argumentaires de ces notes d'application (cf. annexe A du [PP]).

3.3. 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 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 :



3.4. 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 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 Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni, la Suède.

² 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, la République de Corée, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation

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 3+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	3	3	Functional specification with complete summary
	ADV_IMP				1	1	2	2			
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	2	2	Architectural design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC		2	3	4	4	5	5	3	3	Authorisation controls
	ALC_CMS	1	2	3	4	5	5	5	3	3	Implementation representation CM coverage
	ADO_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	1	1	Identification of security measures
	ALC_FLR									3	Systematic flaw remediation
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3			
ASE Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	2	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing - sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	3	3	Focused vulnerability analysis

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.	
[CPP/P/01]	Procédure CPP/P/01 Certification de profils de protection, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[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.
[PP]	Profil de protection - Chiffreur IP - CC3.1, Référence : PP-CIP-3.1 version 1.9, Juillet 2008
[RTE]	Rapport Technique Evaluation du PP CIP, version 1.1, Référence : SPM033C1-CIP- RTE-1.1
[QUA-STD]	Processus de qualification d'un produit de sécurité – Niveau standard, N°549/SGDN/DCSSI/SDR, Version 1.1 du 18 mars 2008,
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version courante, voir www.ssi.gouv.fr .
[REF-KEY]	Gestion des clés cryptographiques - Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard, version courante, voir www.ssi.gouv.fr
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version courante, voir www.ssi.gouv.fr