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 DCSSI-PP 2008/04 du profil de protection « Application de chiffrement de données à la volée sur mémoire de masse » (ref : PP-CDISK-CCv3.1, version 1.4)

Paris, le 1 octobre 2008

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[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 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

Référence du rapport de certification

DCSSI-PP 2008/04

Nom du profil de protection

Application de chiffrement de données à la volée sur mémoire de masse

Référence/version du profil de protection

Référence : PP-CDISK-CCv3.1 / Version 1.4

Critères d'évaluation et version

Critères Communs version 3.1, révision 2

Niveau d'évaluation imposé par le PP

EAL 3 augmenté

ALC_FLR.3, AVA_VAN.3

Rédacteur

Trusted Labs

5 rue du bailliage, 78000 Versailles, France

Commanditaire

DCSSI

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

Centre d'évaluation

Silicomp-AQL

4 rue de la châtaignieraie - CS 51766, 35517 Cesson Sevigné Cedex, 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, 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. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Profil de protection – Application de chiffrement de données à la volée sur mémoire de masse.
Référence, version : PP-CDISK-CCv3.1, version 1.4.
Date : Août 2008.

1.2. Rédacteur

Ce profil de protection a été rédigé par :

Trusted Labs

5 rue du bailliage
78000 Versailles
France

1.3. Description du profil de protection

Le produit défini dans le profil de protection [PP] est un composant logiciel qui, installé sur un poste de travail, est destiné à assurer l'écriture (et la lecture, respectivement) de données à protéger sur une ou plusieurs mémoires de masse du poste de travail, par le biais d'un chiffrement (et déchiffrement, respectivement) à la volée par une ou plusieurs clés cryptographiques suivant l'implémentation. L'objectif premier du produit est ainsi de protéger les données enregistrées par les utilisateurs légitimes sur les disques ou partitions dédiés, en cas de vol de leur support ou de la machine les contenant.

Le produit défini dans le présent profil de protection [PP] peut avoir deux configurations possibles :

- configuration « avec génération de clé », si le produit génère lui-même les clés cryptographiques ;
- configuration « sans génération de clé », si le produit reçoit les clés cryptographiques d'un tiers de confiance.

Ce profil de protection [PP] 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 [PP], communes aux deux configurations sont les suivantes :

- Cryptographic operation (FCS_COP.1) ;
- Subset access control (FDP_ACC.1) ;
- Security attribute based access control (FDP_ACF.1) ;
- Subset residual information protection (FDP_RIP.1) ;
- User authentication before any action (FIA_UAU.1) ;
- User identification before any action (FIA_UID.1) ;
- Management of security attributes (FMT_MSA.1) ;
- Static attribute initialisation (FMT_MSA.3) ;
- Failure with preservation of secure state (FPT_FLS.1) ;

Le profil de protection [PP] définit une exigence fonctionnelle de sécurité supplémentaire pour la configuration « avec génération de clé » :

- Cryptographic key generation (FCS_CKM.1) ;

Toutes les exigences fonctionnelles du profil de protection [PP] 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 **EAL3[1] 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

4 rue de la Châtaigneraie – CS 51766
35517 Cesson-Sévigné Cedex
France

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 12 août 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. 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'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 :

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[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] 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 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 3 +	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**	**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**	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		**2**	**3**	**4**	4	**5**	5	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**3**	Implementation representation CM coverage
	ADO_DEL		**1**	1	**1**	1	1	**1**	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			1	**1**	**1**	1	**2**	**1**	Developer defined life-cycle model
	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	**2**	Analysis of coverage
	ATE_DPT			**1**	2	**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	**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, ref CCMB-2006-09-001, révision 1; Part 2: Security functional components, September 2007, version 3.1, ref CCMB-2007-09-002, révision 2; Part 3: Security assurance components, September 2007, version 3.1, ref CCMB-2007-09-003, révision 2.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, ref CCMB-2007-09-004, révision 2.
[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
[PP]	Profil de protection Application au chiffrement de données à la volée sur mémoire de masse, ref. PP-CDISK-CCv3.1, version 1.4 de août 2008.
[RTE]	Rapport Technique d'Evaluation – Projet PP-CDISK, réf: SPM033-CDISK-RTE, version 1.2 du 12 août 2008.
[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.