PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification PP 2006/01

Profil de Protection Application de chiffrement de données à la volée sur mémoire de masse (PP-CDISK)

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

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 Application de chiffrement de données à la volée sur mémoire de masse
Référence : PP-CDISK[1]
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 (TOE) considérée dans ce PP est un logiciel permettant de protéger en confidentialité les données enregistrées sur une partie au moins de la mémoire persistante de stockage d'une machine (ou, plus généralement, sur un support de stockage éventuellement amovible), dans les deux cas suivants :

1) la TOE est hors fonctionnement ;
2) la TOE est en fonctionnement mais sans qu'un utilisateur légitime ne se soit authentifié à la TOE.

Les menaces relatives au cas de la TOE en fonctionnement avec un utilisateur légitime authentifié à la TOE ne seront donc pas considérées dans le présent PP.
L'objectif principal est donc de couvrir le vol de la machine. Néanmoins, les risques de la phase opérationnelle vis-à-vis du service de protection des données en confidentialité rendu par le produit devront être couverts (comme, par exemple, l'écriture d'informations

[1] Lors de sa phase de développement, ce Profil de Protection était identifié à l'aide de la référence : PU-2005-RT-480-1.5.

confidentielles sur des zones non chiffrées ou l'écriture de la clé en clair sur une mémoire persistante). La confidentialité des données sur la mémoire de masse doit ainsi être garantie quels que soient les états successifs de la machine lors de la phase opérationnelle (mise en veille, arrêt brutal, …).

Deux configurations sont prises en compte dans le Profil de Protection :
- Application de chiffrement de données à la volée sur mémoire de masse avec génération de clé ;
- Application de chiffrement de données à la volée sur mémoire de masse sans génération de clé.

Chacune des deux configurations correspond à un type de produit spécifique, selon que la TOE génère elle-même les clés de chiffrement (configuration « avec génération de clé ») ou bien qu'elle les reçoit d'un tiers de confiance (configuration « sans génération de clé »).

La TOE est supposée fonctionner sur tout type de matériel informatique gérant une mémoire de masse. Elle s'appuie sur le système d'exploitation (OS) ou le micrologiciel (firmware) présent pour communiquer avec les applications clientes et l'utilisateur. Suivant les cas, les pilotes (drivers) de l'OS seront utilisés par la TOE pour accéder à la mémoire de masse ou bien la TOE fera elle-même office de pilote, si elle est distribuée sous cette forme (bibliothèque applicative).

1.4. Exigences fonctionnelles

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

1.4.1. Exigences applicables aux deux configurations

- Access control with automatic modification of security attributes (FDP_ACC.2)
- Security attribute initialisation (FDP_ISA.1)
- Management of security attributes (FDP_MSA.1)
- User authentication by TSF (FIA_UAU.1)
- Anonymous users (FIA_UID.1)
- User identification (FIA_UID.2)
- User-subject binding (FIA_USB.1)
- User registration with storage of authentication (FIA_URE.2)
- TSF-initiated termination of binding (FIA_TOB.1)
- User-initiated termination of binding (FIA_TOB.2)
- Fault tolerance (FPT_FLT.1)

1.4.2. Exigences liées à la génération des clés

- Random number generation (FMI_RND.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 **EAL2**[1] **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

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 :

- L'environnement de développement doit assurer le niveau de qualification standard défini par la DCSSI dans [QS-QR]; soit un EAL2 augmenté des exigences d'assurance ADV_IMP.1*, ADV_TDS.3**, ALC_DVS.1, ALC_TAT.1, ALC_FLR.3 et AVA_VAN.3. Par ailleurs, la description de l'implémentation des mécanismes cryptographiques est requise (ADV_IMP.1*, composant raffiné), et la description de la TOE en modules peut se limiter à ces mêmes mécanismes cryptographiques (ADV_TDS.3**, composant raffiné).

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

1.6.2. Objectifs de sécurité sur l'environnement opérationnel

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

Objectifs applicables aux deux configurations :

- Lorsque l'utilisateur est authentifié, l'environnement opérationnel doit assurer la confidentialité des données sensibles, des clés et des données d'authentification. Note d'application : L'équipement doit apporter des protections efficaces contre l'écoute illicite et la transmission non autorisée de données (pare-feu correctement configuré, antivirus avec base de données à jour, « anti-spyware », etc.). Les applications installées sur l'équipement ne doivent pas perturber le bon fonctionnement de la TOE. Ainsi, les opérations que peut faire l'utilisateur sur les fichiers protégés par la TOE, surtout au travers de ses applications, ne doivent pas entrainer de copies totales ou partielles de ces fichiers en dehors de la TOE, sauf lorsqu'il l'a clairement demandé ou lorsque c'est une conséquence claire de l'opération demandée. La configuration de la machine/système/compte utilisateur/application doit confiner les fichiers protégés au sein même de la TOE, notamment en ce qui concerne les fichiers temporaires ou de travail des applications (OE.ENV_OPERATIONNEL.1) ;
- L'utilisateur ne doit accéder à ses données sensibles que lorsqu'il se trouve dans un environnement de confiance (lorsqu'il se trouve seul ou avec des personnes ayant le besoin d'en connaître) (OE.ENV_OPERATIONNEL.2).

Objectifs applicables à la configuration sans génération de clé :

- L'environnement opérationnel de la TOE génère des clés de chiffrement de manière et de nature conformes aux exigences du référentiel de la DCSSI [CRYPTO] (OE.ENV_OPERATIONNEL.3) ;
- L'environnement opérationnel de la TOE fournit les clés générées dans le cadre de l'objectif OE.ENV_OPERATIONNEL.3 en assurant leur intégrité, leur confidentialité et leur authenticité (OE.ENV_OPERATIONNEL.4).

2. L'évaluation

2.1. 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

2.2. 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.
Tout rédacteur de cible de sécurité devra apporter une attention particulière à la particularité de ce profil de protection, qui décrit deux configurations : « avec génération de clé » et « sans génération de clé ».
Les deux configurations introduites dans le profil de protection visent à couvrir deux types de produits courants tout en gardant un maximum de souplesse pour la rédaction d'une cible : les produits orientés « mono-poste », générant les clés de chiffrement par eux-mêmes, et les produits orientés « grande organisation », fonctionnant en coopération avec une serveur de clé centralisé, pouvant par exemple faire office de séquestre.
Dans tous les cas, le principe est d'assurer que la qualité des clés générées est d'un niveau suffisant pour que la TOE puisse contrer la menace du vol d'un disque. Dans le cas de la configuration « avec génération », les algorithmes de génération des clés font partie du périmètre de la TOE et sont donc évalués avec le produit ; dans le cas « sans génération », la formulation des hypothèses pointe explicitement sur l'importance de la génération des clés, et il est raisonnable de penser que l'utilisateur devra s'appuyer sur un produit de confiance, éventuellement certifié 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 de chiffrement de données à la volée sur mémoire de masse (PP-CDISK) 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 CC

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.
[RTE]	Profil de protection CDISK - Rapport Technique d'Evaluation - Activité APE, référence : TDL002-CDISK-RTE-1.1 version 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