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-CSPN-2008/02

Blancco Data Cleaner+ version 4.8

Paris, le 12/11/2008

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification devrait être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par la Direction centrale de la sécurité des systèmes d'information (DCSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

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-CSPN-2008/02

Nom du produit

Blancco Data Cleaner+ version 4.8

Référence/version du produit

Version 4.8

Critères d'évaluation et version

CERTIFICATION SECURITE DE PREMIER NIVEAU (CSPN, Phase expérimentale)

Développeur(s)

Blancco OyLtd.
Länsikatu 15
80110 Joensuu
Finlande

Commanditaire

Blancco France
29/31 rue du Chemin de fer
59100 – Roubaix
France

Centre d'évaluation

Amossys
Espace Performance 3, bâtiment M1 35769 Saint Grégoire, France
Tél : +33 (0)2 99 23 15 79, mél : frederic.remi@amossys.fr

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 disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Blancco Data Cleaner+ version 4.8 » développé par la société Blancco.

Il est conçu pour assurer un service d'effacement sécurisé de disques durs et implémente pour ce faire plusieurs algorithmes d'effacement correspondant à des référentiels nationaux et internationaux.

Le produit est disponible en 3 versions différentes :

- *Standalone* : le produit est gravé sur un CD ou présent dans une disquette. Il n'est dépendant d'aucune autre installation. Il nécessite la disponibilité d'un support externe au PC pour sauvegarder les rapports d'effacement.

- *Network* : le produit peut être gravé ou démarré à partir du réseau à l'aide d'une carte réseau supportant le protocole de boot réseau PXE. La carte réseau détecte le serveur DHCP Blancco et charge le produit en mémoire. Ce serveur peut être local (« Blancco LAN Server » ou « Blancco WAN Server ») ou hébergé par la société Blancco (www.blanccoservice.com).

- *Combined* : cette version est une fusion des deux précédentes. Si la machine sur laquelle s'installe le logiciel ne détecte pas de serveur « Blancco » dans le réseau de la machine, il passe en mode *Standalone*.

1.2 Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☐ 3 - firewall
☒ **4 - effacement de données**
☐ 5 - administration et supervision de la sécurité
☐ 6 - identification, authentification et contrôle d'accès
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☐ 9 - stockage sécurisé
☐ 10 - matériel et logiciel embarqué
☐ 99-Autres

1.2.2 Identification du produit

Le n° de version du produit certifié (version 4.8) est visible en haut à droite de l'écran lorsque l'application est démarrée ainsi que dans les rapports générés par l'application.

1.2.3 Services de sécurité

Blancco Data Cleaner+ version 4.8 fournit une fonction d'effacement de données secteur par secteur en réécrivant la totalité du disque. Cette réécriture est régie de deux façons:

1. Standards prédéfinis : certifiés par des agences de sécurité et des gouvernements, leur configuration varie en fonction des pays et standards de sécurité dans lesquels ils ont été validés (voir ci-après).

2. Standards personnalisés : l'utilisateur choisit comment l'effacement sera effectué.

Ces deux types de standard sont régis par une configuration à deux paramètres :

- le nombre de passages : le nombre de réécritures complètes du disque ;
- le motif d'écrasement : la valeur hexadécimale écrite dans chaque secteur du disque.

Certains des standards prédéfinis définissent si une vérification est obligatoire ou optionnelle après l'effacement. Cette vérification est faite par le produit après chaque effacement et est confirmée dans le rapport d'effacement.

Les standards prédéfinis présents dans le logiciel sont :

Les standards prédéfinis	**Nombre de réécritures**	**Vérification**
Air Force System Security Instructions 5020	4	Obligatoire
Bruce Shneier's algorithm	7	/
HMG Infosec Standard No: 5 (baseline)	1	Optionnel
HMG Infosec Standard No: 5 (enhanced)	3	Obligatoire
Navy Staff Office Publication (NAVSO P-5239-26) for RLL	3	Obligatoire
OPNAVINST 5239.1A	3	Obligatoire
Peter Gutmann's algorithm	35	/
The National Computer Security Center (NCSC-TG-025)	4	Obligatoire
U.S. Department of Defense Sanitizing (DOD 5220.22-M)	3	Obligatoire
U.S. Army AR380-19	3	Obligatoire
German Standard BSI/VSITR	7	/
National Security Agency 130-1	3	Obligatoire
U.S. Department of Defense Sanitizing (DOD 5220-22-M ECE)	7	Obligatoire

Le tableau ci-dessous définit les références des algorithmes :

Identifiant d'algorithme	Algorithme
A1_MASK	Masque (0xff, 1 passe)
A2_HMG1	HMG Infosec Standard, the baseline standard
A3_HMG2	HMG Infosec Standard, the enhanced standard
A4_PG	Peter Gutmann's algorithm
A5_BS	Bruce Schneier's algorithm
A6_DOD1	US Department of Defense Sanitizing (DOD 5220.22-M)
A7_NAVY	Navy Staff Office Publication (NAVSO P-5239-26) for RLL
A8_NCSC	The National Computer Security Center (NC SC-TG-025)
A9_AIR	Air Force System Security Instruction 5020
A10_UA	US Army AR380-19
A11_VSITR	VSITR-Standard/BSI-Method
A12_OPNAV	OPNAVINST 5239_1A
A13_NSA	NSA 130-1
A14_DOD2	DOD 5220.22-MECE
A15_BL	Blancco RSD

Tableau 1 Références des algorithmes

En outre, le produit dispose d'outils de détection permettant la suppression de données dans des zones normalement non accessibles telles que HPA (Host Protected Areas) et DCO (Device configuration Overlay), ainsi que le support des secteurs altérés et réaffectés.

1.2.4 Configuration évaluée

Le périmètre de l'évaluation concerne le logiciel Blancco Data Cleaner+ version 4.8 complet, en version *Network, Combined* et *Standalone*, avec toutes ses fonctions de sécurité.

Le serveur « Blancco – LAN Server » est en dehors du périmètre de la cible mais a été mis en œuvre pour évaluer les versions *Network* et *Combined* du produit. Les considérations liées à la sécurité (et en particulier à l'intégrité) des échanges entre le serveur et le client comportant le disque à effacer sortent en particulier du cadre de la présente évaluation.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de Sécurité de Premier Niveau en phase expérimentale. Les références des documents se trouvent en annexe 2.

2.2 Charge de travail prévue et durée de l'évaluation

La charge de travail prévue lors de la demande de certification était conforme à la charge de travail préconisée dans [CSPN] pour un produit ne comportant pas de mécanismes cryptographiques, soit 20 hommes x jour. L'évaluation s'est déroulée de mi-juillet 2008 à début septembre 2008.

2.3 Travaux d'évaluation

Ce paragraphe apporte des compléments sur la cible de sécurité [ST] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1 Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1 Spécification de besoin du produit

Conforme à [ST].

2.3.1.2 Biens sensibles manipulés par le produit

Conforme à [ST].

2.3.1.3 Description des menaces contre lesquelles le produit apporte une protection

Conforme à [ST]. L'évaluateur a complété la cible en présentant les différents chemins permettant à un attaquant de stocker des informations dans des zones non accessibles ou non utilisées par le système ou l'utilisateur.

2.3.1.4 Fonctions de sécurité

Conforme à [ST].

2.3.1.5 Utilisateurs typiques

Conforme à [ST].

2.3.2 Installation du produit

2.3.2.1 Plate-forme de test

Le mode *stand-alone* ne nécessite aucune installation particulière. Les modes de fonctionnement *server* et *combined* nécessitent l'installation d'un serveur. La partie serveur a été installée sur un système d'exploitation Windows 2003 Server SP2. Elle nécessite l'utilisation d'une base de données (Access ou SQL). L'évaluateur a utilisé la base de données Access disponible dans Windows 2003 Server SP2.

Afin d'avoir des résultats représentatifs du marché, les tests portent sur des disques IDE et SATA de différents formats et capacité. A ce titre, les disques durs utilisés pour les tests sont plus ou moins récents (voire très ancien pour le disque dur Fujitsu).

Identifiant de disques	HPA	DCO	Connecteur	Constructeur	Capacité	Référence produit
S1	X	X	SATA	Western Digital	320 Go	WD3200AAJS
I2	X		IDE	Fujitsu	8.45 Go	MPE3084AE
S3	X	X	SATA	Maxtor	160 Go	STM3160815AS
S4	X	X	SATA	Maxtor	250 Go	7Y250M00672RA
I5	X	X	IDE	Western Digital	320 Go	WD3200AAJB

Tableau 2 : **Liste des disques durs utilisés**

Des tests ont été réalisés sur des cartes mères différentes, afin d'observer le comportement du produit face à des *chipsets* différents.

Identifiant de carte mère	Constructeur	Chipset	Connecteurs supportés	Référence produit
M1	ASUS	Intel P35 / ICH9R	SATA / IDE	P5K Deluxe
M2	Jetway	Intel	IDE	J-78XAN
M3	MSI	AMD690 / SB600	SATA / IDE	K9AGM2
M4	MSI	AMD780 / SB700	SATA / IDE	K9A2GM

Tableau 3 : Liste des cartes mères utilisées

2.3.2.2 Particularités de paramétrage de l'environnement

Les tests sont réalisés de la manière suivante :

- remplissage du disque dur ;
- paramétrage du disque dur afin de créer des zones HPA et/ou DCO ;
- effacement ;
- vérification.

Deux méthodes de remplissage, décrites ci-après, ont été utilisées :

Méthode 1. La première méthode permet de vérifier si le produit se fonde sur les partitions du disque dur pour réaliser l'opération d'effacement.

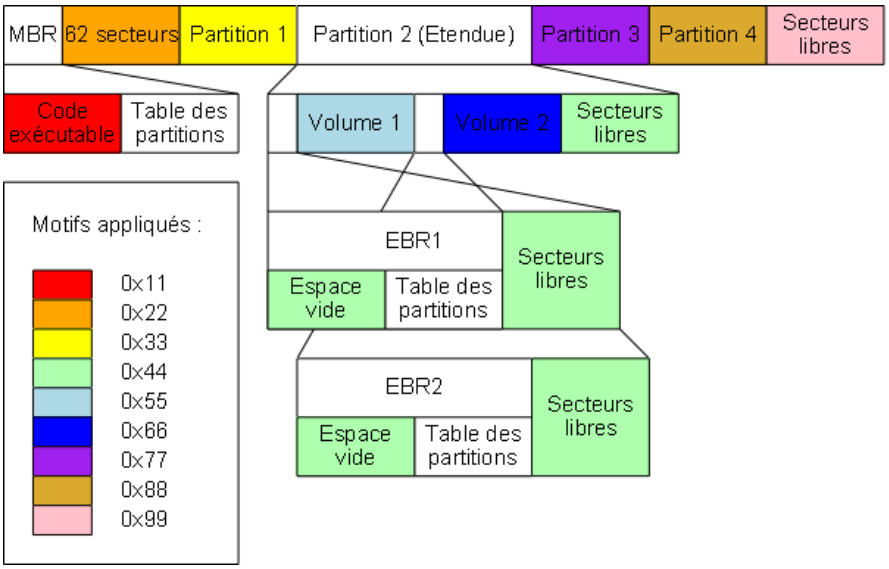

Figure 1 : Méthode 1 de remplissage

Méthode 2. La deuxième méthode correspond à un remplissage classique des partitions.

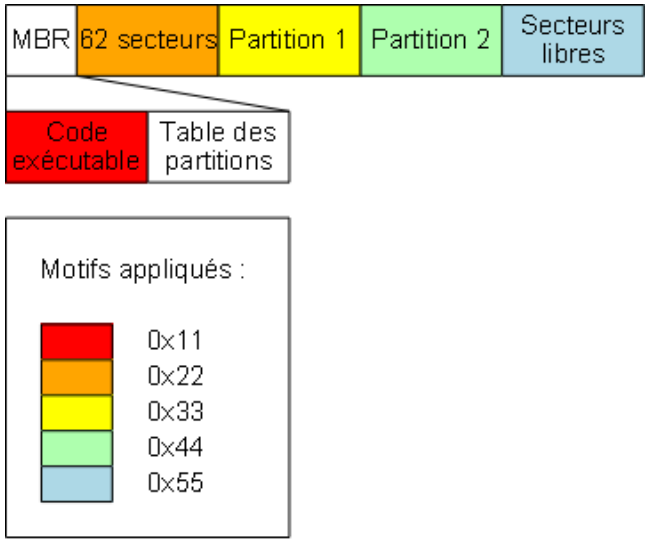

Figure 2 : Méthode 2 de remplissage

Une fois le disque rempli, certaines partitions sont supprimées afin de simuler des espaces non utilisés. Pour la première méthode de remplissage, les partitions supprimées sont :

- le volume 2 qui simule une zone d'espace libre dans une partition étendue ;
- la partition 3 qui simule une zone d'espace libre après les partitions ;
- la partition 4 qui sera cachée par le mécanisme HPA.

Pour la deuxième méthode, la partition supprimée est la partition 2 :

- les secteurs libres à la fin du disque dur seront cachés par le mécanisme DCO ;
- la partition 2 sera cachée par le mécanisme HPA.

Certaines options du BIOS peuvent empêcher le produit de détecter les zones HPA et DCO. Pour cela, les BIOS des PCs de tests sont configurés afin de :

- désactiver la reconnaissance automatique des disques durs ;
- utiliser le mode compatibilité des contrôleurs SATA.

2.3.2.3 Options d'installation retenues pour le produit

Néant.

2.3.2.4 Description de l'installation et des non-conformités éventuelles

Il n'a pas été relevé de non-conformité.

2.3.2.5 Durée de l'installation

Aucune installation n'est nécessaire pour la version *stand-alone*. Pour les modes de fonctionnement *server* et *combined*, l'installation du serveur dure environ 30 minutes.

2.3.2.6 Notes et remarques diverses

Les durées d'effacement des disques suivant la méthode d'effacement sont inscrites dans le tableau suivant :

Test	Algorithme	Carte mère	ID DD	Capacité en Go	Durée du remplissage	Durée de l'effacement (min)
TEST-001	A1_MASK	M1	S1	320	109	64
TEST-002	A5_BS	M3	S3	160	55	299
TEST-003	A8_NCSC	M3	S4	250	85	345
TEST-004	A15_BL	M1	S3	160	55	42
TEST-005	A6_DOD1	M3	I2	8,45	29	108
TEST-006	A4_PG	M3	I2	8,45	29	168
TEST-007	A2_HMG1	M2	I2	8,45	29	5
TEST-008	A3_HMG2	M2	I2	8,45	29	17
TEST-009	A6_DOD1	M3	I5	320	109	261
TEST-010	A4_PG	M3	I5	320	109	3055
TEST-011	A7_NAVY	M1	S4	250	85	259
TEST-012	A9_AIR	M1	S3	160	55	170
TEST-013	A10_UA	M3	I5	320	109	261
TEST-014	A1_MASK	M1	S3	160	55	42
TEST-015	A1_MASK	M3	I5	320	109	87
TEST-016	A11_VSITR	M3	I5	320	109	611
TEST-017	A12_OPNAV	M3	S3	160	55	128
TEST-018	A13_NSA	M3	I5	320	109	261
TEST-019	A14_DOD2	M1	S4	250	85	604
TEST-020	A1_MASK	M1	S3	160	30	32

Remarque : la vitesse d'écriture d'un disque varie de 5Mo/s à 50Mo/s selon le disque dur utilisé.

2.3.3 Analyse de la conformité

2.3.3.1 Analyse de la documentation

La documentation est claire et lisible et permet de prendre en main le produit aisément. Les différentes étapes de l'installation du serveur et de l'utilisation du produit sont bien détaillées. Pour l'installation du serveur, le guide est illustré par des captures d'écran afin d'aider l'utilisateur.
Contrairement à ce qui est indiqué en page 13 du document « Client_Software_v48_User_Manual_FR.pdf », le logiciel n'avertit pas l'utilisateur lorsqu'il détecte et efface une zone HPA.

2.3.3.2 Revue du code source

Le code source n'a pas été fourni.

2.3.3.3 Fonctionnalités testées

L'analyse de la conformité du produit a pour objectif de vérifier les fonctionnalités :
- d'effacement ;
- de détection et de retrait des limitations imposées par les mécanismes HPA et DCO.

2.3.3.4 Fonctionnalités non testées

Concernant la réallocation des secteurs défectueux, Blancco indique que le produit est en mesure de les effacer. Blancco utiliserait les commandes définies par la norme ATA prévues à cet effet. La commande ATA utilisée est « SECURE ERASE UNIT » en mode « Enhanced Erase mode ». L'effacement est possible dans la mesure où le disque dur supporte cette commande.

L'évaluateur ne disposant d'outil de *debug* de l'éditeur n'a pu pas vérifier l'efficacité de cette fonction.

2.3.3.5 Synthèse des fonctionnalités testés / non testées et des non-conformités

Les résultats des tests concernant la conformité sont détaillés dans ce tableau :

Test	Mode	Algorithme	HPA	DCO	LBA28	Type	ID DD	Carte mère	Motif	Résultat
TEST-001	Stand alone	A1_MASK	X			SATA	S1	M1	0xff	OK
TEST-002	Stand alone	A5_BS	X			SATA	S3	M3	Aléa	OK
TEST-003	Stand alone	A8_NCSC	X	X		SATA	S4	M3	Aléa	OK
TEST-004	Stand alone	A15_BL			X	SATA	S3	M1	0x00	OK
TEST-005	Stand alone	A6_DOD1	X			IDE	I2	M3	0x7f	NOK
TEST-006	Stand alone	A4_PG	X			IDE	I2	M3	Aléa	NOK
TEST-007	Stand alone	A2_HMG1	X			IDE	I2	M2	0x00	NOK
TEST-008	Stand alone	A3_HMG2	X			IDE	I2	M2	0x6b	NOK

Test	Mode	Algorithme	HPA	DCO	LBA28	Type	ID DD	Carte mère	Motif	Résultat
TEST-009	Stand alone	A6_DOD1	X	X		IDE	I5	M3	0x50	OK
TEST-010	Stand alone	A4_PG			X	IDE	I5	M3	Aléa	OK
TEST-011	LAN Server	A7_NAVY	X			SATA	S4	M1	Aléa	OK
TEST-012	LAN Server	A9_AIR	X	X		SATA	S3	M1	0xaa	OK
TEST-013	LAN Server	A10_UA	X	X		IDE	I5	M3	0x55	OK
TEST-014	LAN Server	A1_MASK			X	SATA	S3	M1	0xff	OK
TEST-015	LAN Server	A1_MASK			X	IDE	I5	M3	0xff	OK
TEST-016	Combine	A11_VSITR	X	X		IDE	I5	M3	0xC1	OK
TEST-017	Combine	A12_OPNAV	X	X		SATA	S3	M3	0xb6	OK
TEST-018	Combine	A13_NSA			X	IDE	I5	M3	0x00	OK
TEST-019	Combine	A14_DOD2			X	SATA	S4	M1	0x21	OK
TEST-020	Stand alone	A1_MASK				SATA	S3	M1	0xff	OK

Tableau 2 : Résultats des tests de conformité

Les tests 5, 6, 7, 8 portants sur le disque IDE Fujitsu n'ont pas donné entièrement satisfaction car le produit n'a pas détecté de zone HPA.

2.3.3.6 Avis d'expert sur le produit

La documentation et les rapports d'effacement sont complets et très lisibles.

Le produit est conforme à ses spécifications, sauf pour un disque dur d'ancienne génération (Fujitsu) fonctionnant selon la norme ATA-5[1] pour lequel un problème a été détecté sur la gestion de la zone HPA.

2.3.4 Analyse de la résistance des mécanismes et des fonctions

2.3.4.1 Liste des fonctions testées et résistance

La résistance du produit est déterminée par sa capacité à effacer entièrement un disque dur.

A la fin de chaque effacement, l'évaluateur a vérifié que les données ont bien été effacées. Pour cela, l'outil « *hexedit* » qui permet de visualiser le contenu d'un disque dur a été utilisé. La vérification a été faite par échantillonnage. Les zones observées étaient :

- les adresses qui contiennent les extrémités des partitions effacées ;
- les zones habituellement non utilisées par les systèmes (la zone de 62 secteurs après le MBR, les secteurs à la fin du disque dur).

[1] Le problème semble provenir d'un défaut de gestion de la norme ATA-5 dans cette version du produit. Le développeur annonce que ce problème devrait être corrigé à partir de la version 4.9.

Les résultats des tests sont tous positifs à l'exception des non-conformités constatées au point 2.3.3.5.

Test	Mode	Algorithme	Type	ID DD	Carte mère	Résultat
TEST-001	Stand alone	A1_MASK	SATA	S1	M1	OK
TEST-002	Stand alone	A5_BS	SATA	S3	M3	OK
TEST-003	Stand alone	A8_NCSC	SATA	S4	M3	OK
TEST-004	Stand alone	A15_BL	SATA	S3	M1	OK
TEST-005	Stand alone	A6_DOD1	IDE	I2	M3	NOK
TEST-006	Stand alone	A4_PG	IDE	I2	M3	NOK
TEST-007	Stand alone	A2_HMG1	IDE	I2	M2	NOK
TEST-008	Stand alone	A3_HMG2	IDE	I2	M2	NOK
TEST-009	Stand alone	A6_DOD1	IDE	I5	M3	OK
TEST-010	Stand alone	A4_PG	IDE	I5	M3	OK
TEST-011	LAN Server	A7_NAVY	SATA	S4	M1	OK
TEST-012	LAN Server	A9_AIR	SATA	S3	M1	OK
TEST-013	LAN Server	A10_UA	IDE	I5	M3	OK
TEST-014	LAN Server	A1_MASK	SATA	S3	M1	OK
TEST-015	LAN Server	A1_MASK	IDE	I5	M3	OK
TEST-016	Combine	A11_VSITR	IDE	I5	M3	OK
TEST-017	Combine	A12_OPNAV	SATA	S3	M3	OK
TEST-018	Combine	A13_NSA	IDE	I5	M3	OK
TEST-019	Combine	A14_DOD2	SATA	S4	M1	OK
TEST-020	Stand alone	A1_MASK	SATA	S3	M1	OK

Tableau 3 : Résultats des tests de résistance

2.3.4.2 Avis d'expert sur la résistance des mécanismes

Le mécanisme d'effacement est efficace. Il n'a pas été possible de relire une information utile après effacement avec les moyens utilisés (utilitaires logiciels de lecture de disque), sauf dans le cas des tests 005 à 008. Le risque qu'un attaquant parvienne à exploiter le mécanisme HPA de certains disques durs pour soustraire des informations sensibles à l'effacement effectué existe. Ce risque est jugé du même ordre que celui lié au fait qu'un disque dur puisse posséder des mécanismes non connus du logiciel Blancco dont l'emploi (éventuellement frauduleux) pourrait conduire au non effacement de certaines données par le produit (voir recommandation 3 paragraphe 2.3.6.2).

2.3.5 Analyse des vulnérabilités (conception, construction…)

2.3.5.1 Liste des vulnérabilités connues

L'évaluateur a consulté différentes sources afin d'identifier d'éventuelles vulnérabilités spécifiques à ce produit et en particulier :

Site	Adresse
National Institute of Standards and Technology (NIST)	http://nvd.nist.gov
The Open Source Vulnerability Database (OSVDB)	http://osvdb.org
SECUNIA	http://secunia.com
FrSIRT	http://www.frsirt.com
Security Focus	http://www.securityfocus.com
US-CERT	http://www.kb.cert.org

Ces sites ne rapportent aucune vulnérabilité connue concernant le produit.

2.3.5.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Hormis un problème concernant la zone HPA sur un disque d'ancienne génération (Fujitsu) fonctionnant selon la norme ATA-5 (voir test I2 dans le Tableau 3 : Résultats des tests de résistance). Pour plus de précisions, voir en 2.3.3.6), aucune vulnérabilité n'a été mise en évidence durant l'évaluation.

2.3.6 Analyse de la facilité d'emploi et préconisations

2.3.6.1 Avis d'expert sur la facilité d'emploi

Il n'a pas été identifié de cas où l'utilisation du produit aurait des conséquences ambigües sur la sécurité (par exemple, effacement non réalisé alors que l'utilisateur pourrait croire qu'il l'a été). D'une manière générale, le produit est simple à utiliser, facile à configurer et bien documenté.

L'utilisateur est fortement incité à se familiariser avec la documentation et suivre les recommandations d'emploi.

Toutefois, une indication concernant la détection et l'effacement des zones HPA et DCO des disques durs serait de nature à rassurer l'utilisateur sur la bonne prise en compte de ces zones dans les opérations d'effacement.

2.3.6.2 Recommandations pour une utilisation sûre du produit

Recommandation 1 :
L'utilisation de cette version du produit pour effacer des disques durs anciens fonctionnant selon la norme ATA-5 n'est pas recommandée du fait du risque de non-reconnaissance d'une éventuelle zone HPA.

Recommandation 2 :
Il convient d'utiliser ce produit avec les plate-formes listées dans le document [LISTE] (Liste des équipements supportés par le produit). Si l'équipement n'est pas dans la liste, il est recommandé à l'utilisateur de se renseigner auprès de la société Blancco ou de réaliser ses propres tests pour qualifier la plate-forme.

Recommandation 3 :
Les tests réalisés ont montré que la fonctionnalité du produit était correctement et efficacement réalisée (au problème près mentionné dans la recommandation 1). L'utilisation d'un tel produit est donc utile pour effacer des disques avant que ceux-ci ne soient réattribués ou réformés dès lors qu'ils sont susceptibles d'avoir mémorisé de l'information sensible. Il convient néanmoins de préciser les points suivants :

- les disques durs disposent de fonctionnalités de plus en plus évoluées qui masquent ou peuvent masquer la structure réelle du disque au processus utilisateur. Si ces fonctionnalités permettent de faciliter et d'améliorer la gestion du disque par les systèmes d'exploitation, elles sont également susceptibles d'être génératrices de vulnérabilités pouvant compromettre la confidentialité d'informations que l'on pourrait croire effacées. Il est probable que dans ce cas, l'information non effacée représentera une très faible portion de l'information que mémorisait le disque mais l'utilisateur doit être conscient qu'il existe potentiellement ce risque résiduel ;
- la présente évaluation n'a fait appel qu'à des moyens logiques (logiciels de lecture / écriture utilisant l'interface standard du disque) pour effectuer les vérifications d'effacement des données. Il n'a pas été utilisé de moyens techniques dédiés pour vérifier au plus près du support physique l'existence d'informations résiduelles non effacées.

Pour ces raisons, l'usage de ce produit dans le cadre de la réforme d'un disque dur ayant contenu des informations classifiées de défense n'est pas couvert par ce certificat.

Recommandation 4 :
Les versions *Network* et *Combined* (option de chargement du logiciel par le réseau) doivent être utilisées dans un environnement de confiance où des mesures organisationnelles permettant de couvrir la menace d'attaque par le milieu et de modification du code du logiciel chargé sur la machine cible sont mises en œuvre. Si ces mesures ne sont pas mises en place, l'utilisation de la version *Standalone* est alors préconisée. Dans tous les cas, il est nécessaire d'assurer l'intégrité des supports de stockage du logiciel Blancco Data Cleaner+ de manière à prévenir tout risque de piégeage (ou de remplacement) de ce logiciel par un attaquant.

Recommandation 5 :
En cas d'anomalie (message d'erreur non prévu, durée de l'effacement anormalement courte), il convient de relancer l'opération depuis le début.

Recommandation 6 :
En cas de crash du disque en cours d'effacement, il faut considérer qu'il n'a pas pu être effacé et envisager une destruction physique du disque.

2.3.7 Accès aux développeurs

L'évaluateur a bénéficié d'un support technique réactif et compétent.

2.4 Analyse de la résistance des mécanismes cryptographiques

Le produit évalué ne comporte pas de mécanismes cryptographiques.

2.5 Analyse du générateur d'aléas

Les tests sur la cryptographie se sont concentrés sur le générateur d'aléa du produit qui est utilisé dans plusieurs contextes :

- génération des identifiants de rapports ;
- génération de données d'effacement.

Les tests ont porté sur la génération d'aléa pour les données d'effacement. 500Mo d'aléa issus de la dernière passe d'effacement de l'algorithme « Navy Staff Office Publication (NAVSO P-5239-26) for RLL » ont été utilisés comme données d'entrée pour les tests.

Les résultats des tests statistiques sont tous positifs et l'aléa produit est assimilable à de l'aléa pur.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles en vigueur, avec la compétence et l'impartialité requise pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Blancco Data Cleaner+ version 4.8 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST].

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST], suivre les recommandations énoncées dans le présent rapport de certification au paragraphe 2.3.6.2 ainsi que celles se trouvant dans les guides fournis [GUIDES] avec le produit.

Annexe 1. Références documentaires du produit évalué

[CDS]	Cible_de_securité_Blancco_Data_Cleaner+_V4.8, version 1, révision 3, 30 avril 2008
[RTE]	BLA001-RTE-1.10, version 1, révision 1, 29 septembre 2008.
[GUIDES]	Guide d'installation du produit : .BLS_v47_MSI_Installation_Manual_for_Windows_2003_Server_FR.pdf ; .BLS_v47_Manual_Installation_for_Windows_2003_Server_FR.pdf. Guides d'utilisation : .BLS_v47_User_Manuel_FR.pdf ; .Client_Software_v48_User_Manual_FR.pdf.
[LISTE]	Blancco - Client 4.8 Hardware support

Annexe 2. Références liées à la certification

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.	
[CER/P/01]	Procédure CSPN-CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2.4, phase expérimentale, n°915/SGDN/DCSSI/SDR/CCN, 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1.4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1.3.