Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2014/89

TheGreenBow VPN Client

(Version : 5.22.005)

Paris, le 10 décembre 2014

Le directeur général de l'agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD
[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 doit 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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), 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 et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-2014/89**
Nom du produit **TheGreenBow VPN Client**
Référence/version du produit **Version 5.22.005**
Conformité à un profil de protection **[PP VPNC]**
Critères d'évaluation et version **Critères Communs version 3.1 révision 3**
Niveau d'évaluation **EAL 3 augmenté** **ALC_FLR.3, AVA_VAN.3**
Développeur **TheGreenBow** **28 rue de Caumartin, 75009 Paris, France**
Commanditaire **TheGreenBow** **28 rue de Caumartin, 75009 Paris, France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, 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 modifié. Ce décret indique que :

- L'agence nationale 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 le logiciel « TheGreenBow VPN Client », version 5.22.005, développé par la société TheGreenBow.

Ce produit est une application logicielle offrant le service de client VPN (Virtual Private Network) IPSec (Internet Protocol Security). Un client VPN IPSec permet l'établissement d'une connexion sécurisée avec une passerelle IPSec par laquelle transitent des flux chiffrés qui sont protégés en confidentialité et en intégrité.

1.2. Description du produit

1.2.1. Introduction

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

Cette cible de sécurité est conforme au profil de protection [PP VPNC]. Cette conformité est de type démontrable. Le problème de sécurité décrit dans la cible de sécurité est plus restrictif que celui décrit dans [PP VPNC] car le produit évalué ne permet pas l'administration à distance.

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable selon les moyens suivants :

- lors de l'installation du produit, en effectuant un clic droit sur le nom du fichier d'installation « `TheGreenBow_VPN_Certified_2013.exe` » et en regardant dans « Propriétés », dans l'onglet « Détails ». La version du produit doit être la suivante : 5.22.005.
- en cours d'utilisation, le nom commercial de la TOE (« TheGreenBow VPN Certified 2013 ») doit être inscrit dans la bannière du logiciel et dans la fenêtre « A propos ». La version exacte peut être consultée dans cette même fenêtre.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- protection des flux en confidentialité et intégrité via l'établissement d'un tunnel IPsec ;
- authentification des utilisateurs et des administrateurs.

1.2.4. Architecture

L'architecture du produit est définie par la figure ci-dessous :

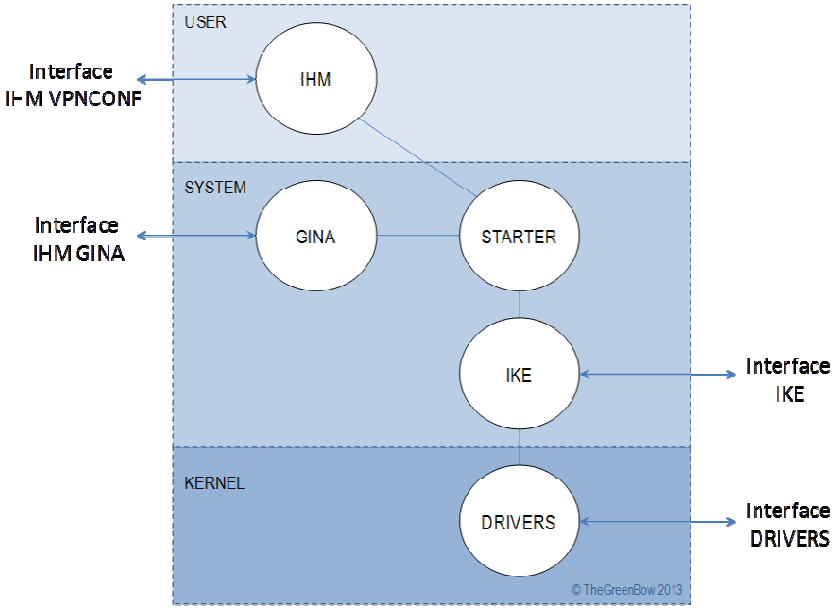

Figure 1 - Architecture du produit

Le produit est constitué des éléments suivants :

- **IHM (Interface Homme Machine)** : ce sous-système a pour rôle la gestion des interactions avec l'utilisateur (préalablement authentifié par le système d'exploitation Windows) ;
- **GINA (*Graphical Identification and Authentication*)** : ce sous-système a pour rôle l'ouverture et la fermeture des tunnels VPN avant l'authentification Windows de l'utilisateur ;
- **STARTER** : ce sous-système a pour rôle la gestion des communications entre l'IHM, le *GINA* et l'IKE, la surveillance des processus, la gestion du mot de passe administrateur avec l'IHM ;
- **IKE (*Internet Key Exchange*)** : ce sous-système a pour rôle d'assurer la négociation des tunnels et des clés ;
- **DRIVERS** : ce sous-système a pour rôle l'interception des flux entrants et sortants pour l'application de la politique de sécurité VPN.

1.2.5. Cycle de vie

La production de la TOE est organisée en étapes (gates) décrites ci-dessous.

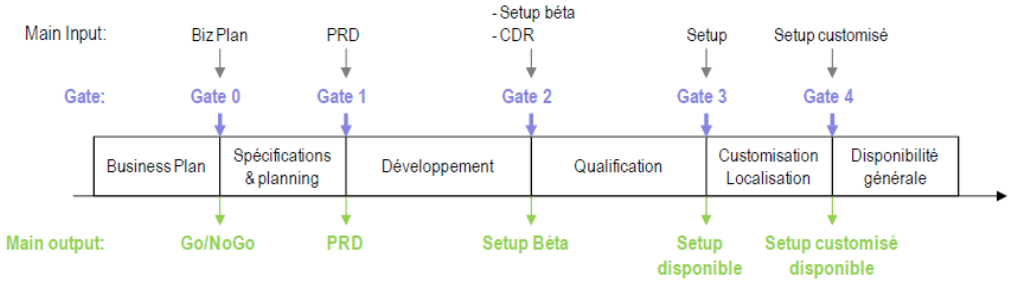

Figure 2 - Etapes de la production

Pour chaque étape, les différents acteurs sont les suivants :

Contributeurs	Gate 0	Gate 1	Gate 2	Gate 3	Gate 4
Product Management	X	X	X	X	X
Sales	X	X		X	X
Marketing	X	X		X	
Support		X		X	
Qualification		X	X	X	
Engineering (R&D)		X	X	X	X

Figure 3 - Acteurs impliqués dans la production

Le produit a été développé sur le site suivant :

TheGreenBow

28 rue de Caumartin
75009 Paris
France

Pour l'évaluation, l'évaluateur a considéré les rôles suivants :

- UTILISATEUR : C'est l'usager de la machine hébergeant la TOE et utilisant l'application VPN cliente pour accéder à un réseau privé. Cet utilisateur peut envoyer/recevoir des informations vers/de ce réseau privé à travers un lien VPN établi entre l'application VPN cliente et la passerelle IPSec ;
- ADMINISTRATEUR SYSTEME ET RESEAU: C'est l'administrateur responsable de la machine hébergeant la TOE. Il configure les paramètres de la machine (comme les comptes utilisateurs), les paramètres réseaux de l'application VPN cliente et les paramètres systèmes qui sont liés aux contextes réseaux opérationnels, mais ne définit pas les politiques de sécurité VPN. Cet administrateur n'interagit pas directement avec la TOE. Ce rôle a uniquement pour vocation de configurer le système d'exploitation hébergeant la TOE ;
- ADMINISTRATEUR SECURITE : C'est l'administrateur responsable de la gestion des éléments de sécurité de la TOE. Il est chargé de distribuer les clés dans l'application VPN cliente et d'importer les politiques de sécurité VPN qui seront appliquées par l'application VPN cliente.

1.2.6. Configuration évaluée

La plateforme de test mise en œuvre par le CESTI correspond à la configuration suivante :

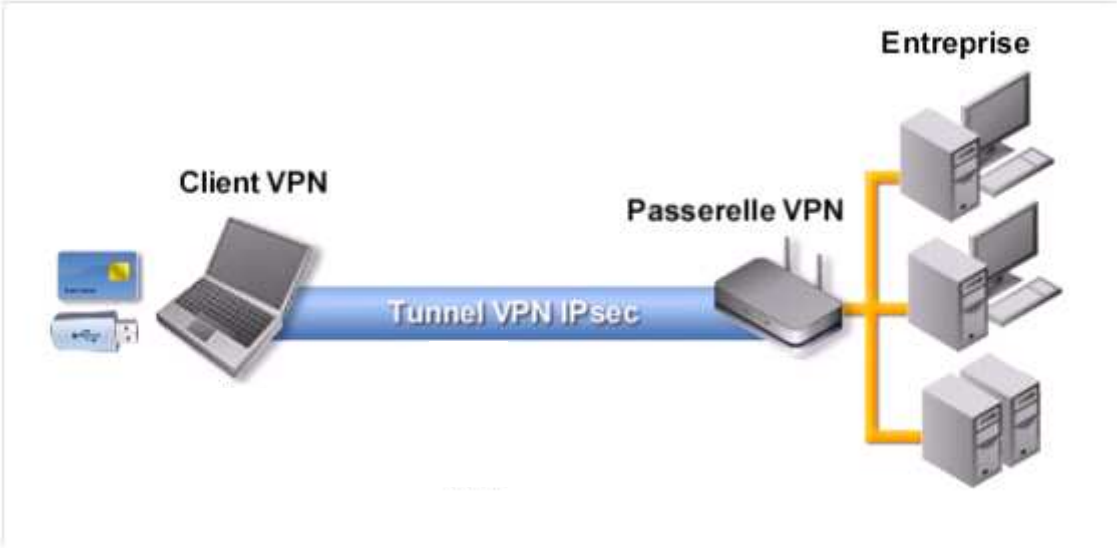

Figure 4 - Plateforme de tests

Les tests ont été réalisés sur l'environnement d'exploitation suivant :

- un PC sur lequel est installé le client VPN TheGreenBow et s'exécutant sur l'un des systèmes d'exploitation suivant :
  - Windows XP SP3 (architecture 32 bits) ;
  - Windows Seven (architecture 32 bits) ;
  - Windows Seven (architecture 64 bits) ;
- une passerelle VPN sur laquelle est installé un logiciel (StrongSwan U5.0.4/K3.2.0.4-amd64) qui permet de monter un tunnel IPSec avec le client VPN TheGreenBow ;
- une machine, correspondant à un serveur connecté sur une interface réseau de la passerelle VPN ;
- une machine (sous distribution Linux Debian 7 64 bits) émulant un routeur positionné sur Internet et qui permet de vérifier le bon fonctionnement du NAT-T ;
- un token servant de support de certificats.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC], et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 07/10/2014, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI. Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

2.4. Analyse du générateur d'aléas

Le produit comporte un générateur d'aléas entrant dans le périmètre d'évaluation. Ce générateur a fait l'objet d'une analyse. Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que les générateurs ne souffrent pas de défauts majeurs de conception. Conformément au document [REF], la sortie des générateurs matériels de nombres aléatoires subit un retraitement algorithmique de nature cryptographique.

3. La certification

3.1. Conclusion

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.

Ce certificat atteste que le produit « TheGreenBow VPN Client », version 5.22.005, soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- privilégier le mode d'authentification X-AUTH ;
- ne pas sauvegarder d'informations sensibles dans les politiques VPN. En particulier, le guide utilisateur préconise de :
    - ne pas importer de certificat dans la configuration et privilégier l'utilisation d'un certificat sur support amovible ou du magasin de certificat Windows ;
    - ne pas utiliser de clé pré-partagée (PSK - *pre-shared key*) et en particulier ne pas utiliser le mode agressif (*aggressive mode*) ;
    - privilégier l'emploi d'une PKI (*Public Key infrastructure)* qualifiée, dans la mesure du possible.
- utiliser des algorithmes forts et conformes à l'annexe B-1 du RGS :
    - AES 128/192/256 pour les algorithmes IKE - Chiffrement et ESP – Chiffrement ;
    - SHA-256 pour les algorithmes IKE - Authentification et ESP - Authentification ;
    - DH14 (2048 bits) comme Groupe de clé IKE et comme groupe PFS.
- le poste de travail doit être sécurisé, maintenu à jour de tous les correctifs de vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées.
- l'utilisateur ne doit pas posséder de privilèges sur le poste de travail permettant l'installation d'un debugger ;
- il est nécessaire que les utilisateurs soient sensibilisés à la complexité attendue d'un mot de passe ;
- les mots de passe des utilisateurs et des administrateurs doivent être gérés par une politique de création et de contrôle des mots de passe conforme aux recommandations de l'ANSSI ;
- sous Windows XP, une attention particulière de l'utilisateur doit être portée sur la protection physique de l'accès au poste.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance 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'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et 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, le Pakistan, les Pays-Bas, la République de Corée, 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	**1**	**2**	**3**	**4**	4	**5**	5	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**3**	Implementation representation CM coverage
	ALC_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**	1	**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 documentaires du produit évalué

[ST]	*Cible de Sécurité CC / Application VPN cliente : TheGreenBow VPN Client* - Version : 1.6, - Référence : CDS-TGB-CC, - Date : 20/06/2014.
[RTE]	*Rapport Technique d'Evaluation THEGREENBOW* - Version : 2.0, - Référence : OPPIDA/CESTI/THEGREENBOW/RTE/2.0, - Date : 02/10/2014.
[ANA-CRY]	*Expertise cryptographique - TheGreenBow VPN Client v5.2* - Version : 2.0, - Référence : OPPIDA/CESTI/THEGREENBOW/CRYPTO/2.0, - Date : 28/05/2014.
[CONF]	Liste de configuration du produit : - tgbvpn_eval_delivery_3.1.
[GUIDES]	Guides de déploiement du produit : - TheGreenBow VPN Certified 2013 – Guide de Déploiement, Référence : tgbvpn_ug_deployment_fr, Version 1.6 de mars 2014, TheGreenBow. - TheGreenBow IPsec VPN Client – Guide de Déploiement – Options PKI, Référence : tgbvpn_ug_deployment_pki_fr, Version 1.1 de novembre 2012, TheGreenBow. Guide d'utilisation du produit : - TheGreenBow VPN Certified 2013 – Guide Utilisateur, Référence : tgbvpn_ug_fr, Version 1.6 de mars 2014, TheGreenBow.
[PP VPNC]	*PP Application VPN cliente* - version : 1.3 - référence : PP-VPNC-CCv3.1 - date : 10/07/2008

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, Septembre 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_3), voir www.ssi.gouv.fr.