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-2009/01

BULL TrustWay VPN Line :
- TVPN v4.05.02
- TCRX/TCRX2 v4.05.01

Paris, le 2 avril 2009

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 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 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

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

Référence du rapport de certification

DCSSI-2009/01

Nom du produit

BULL TrustWay VPN Line :
- TVPN v4.05.02
- TCRX/TCRX2 v4.05.01

Référence/version du produit

v4.05.02 / b205 pour TVPN
v4.05.01 / c020 pour TCRX/TCRX2

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 2 augmenté

ADV_HLD.2, ADV_IMP.1*, ADV_LLD.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1*, AVA_MSU.1, AVA_VLA.2

***appliqués aux exigences FCS**

Développeur

Bull SAS

Rue Jean Jaurès – BP 68, 78340 Les Clayes sous Bois, France

Commanditaire

Direction Générale de la Gendarmerie Nationale

1, bd Théophile Sueur, 93110 Rosny sous Bois, France

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France

Tél : +33 (0)1 30 14 19 00, mél : cesti@oppida.fr

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

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est constitué des trois boîtiers de l'offre BULL TrustWay VPN Line développée par Bull SAS :

- le boîtier TVPN (Trustway Virtual Private Network) version 4.05.02,
- le boîtier TCRX (Trustway Chiffreur Routeur d'eXtrémité) version 4.05.01,
- le boîtier TCRX2 (2ème modèle du TCRX) version 4.05.01.

Ces boîtiers sont utilisés pour relier entre eux des réseaux internes à protéger au travers d'un réseau externe non protégé. Ils permettent ainsi de constituer des réseaux privés virtuels VPN (*Virtual Private Network*) au travers de réseaux publics tels qu'Internet, de façon à préserver la confidentialité et l'intégrité des données échangées entre des systèmes distants.

1.2. Description du produit évalué

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

1.2.1. Identification du produit

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

La version certifiée du produit contient les éléments identifiables suivants :

- pour le boîtier TVPN :
  - le logiciel TVPN v4.05.02 ;
  - la carte PCA3 de version 76677843-309 A de firmware v5.5 et son logiciel embarqué b205 ;
- pour le boîtier TCRX :
  - le logiciel TCRX v4.05.01 ;
  - la carte cryptographique 76679897-106A avec un processeur cryptographique Altera EP1C20F324C8N et son logiciel embarqué c020 ;
- pour le boîtier TCRX2 :
  - le logiciel TCRX v4.05.01 ;
  - la carte cryptographique 76680490-105A avec un processeur cryptographique Altera EP1C20F324C8N et son logiciel embarqué c020.

Ces versions peuvent être vérifiées à l'aide de la station d'administration TDM (cf. §1.2.3).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- confidentialité et intégrité des données en mode tunnel ;
- passage des flux en clair uniquement dans la mémoire de la TOE (pas d'écriture sur le disque dur) ;
- confidentialité et intégrité des dialogues d'administration ;
- confidentialité et intégrité des configurations ;
- alerte et destruction des trames en cas de données non authentifiables ;
- intégrité du logiciel ;
- blocage de la transmission en mode clair ;
- contrôle des correspondants autorisés à communiquer ;
- filtrage de ports ;
- filtrage d'adresses ;
- protection anti-rejeu des flux d'administration;
- gestion des clés ;
- gestion des configurations ;
- alarmes et supervision.

1.2.3. Architecture

L'architecture matérielle du produit est la suivante :

- pour le boîtier TVPN :
  - une carte mère ASROCK I775 GV s775 FSB800 ;
  - un processeur Intel Celeron D 331 2.66Ghz s775 ;
  - un disque dur 160go PATA Maxtor 8M ;
  - 512 Mo de mémoire RAM 400Mhz CL3 ;
  - une carte PCA3 version 76677843-309A de firmware v5.5 et son logiciel embarqué b205 développé par BULL, et réalisant les opérations cryptographiques ;
  - deux interfaces Ethernet ;
  - des leds pour indiquer l'activité du châssis ;
  - un port série (utilisé pour l'administration locale) ;
  - une alimentation ;
- pour le boîtier TCRX :
  - un processeur réseau Intel EGLXT973QCA3V ;
  - une carte cryptographique 76679897-106A avec un processeur cryptographique Altera EP1C20F324C8N et son logiciel embarqué c020 ;
  - deux interfaces Ethernet ;
  - des leds pour indiquer l'activité du châssis ;
  - un port série (utilisé pour l'administration locale) ;
- pour le boîtier TCRX2 :
  - un processeur réseau Intel EGLXT973QCA3V ;
  - une carte cryptographique 76680490-105A avec un processeur cryptographique Altera EP1C20F324C8N et son logiciel embarqué c020 ;
  - deux interfaces Ethernet ;
  - des leds pour indiquer l'activité du châssis ;
  - un port série (utilisé pour l'administration locale) ;
  - une alimentation intégrée dans le boîtier.

L'architecture logicielle du produit est la suivante :

- pour le boîtier TVPN :
  - un logiciel TVPN v4.05.02 ;
  - un logiciel b205 ;
  - un système d'exploitation Linux (linux kernel 2.4.24) ;
  - un utilitaire Netfilter (inclus dans Linux) ;
  - un logiciel Tripwire (version 1.2.2) ;
  - un module logiciel d'administration locale ;
- pour les boîtiers TCRX et TCRX2 :
  - un logiciel TCRX v4.05.01 ;
  - un logiciel c020 ;
  - un système d'exploitation Linux (linux kernel 2.4.24) ;
  - un utilitaire Netfilter (inclus dans Linux) ;
  - un logiciel Tripwire (version 1.2.2) ;
  - un module logiciel d'administration locale.

Localement, le produit est relié à un terminal externe (SafePad, non représenté sur le schéma ci-après) qui est nécessaire pour l'authentification de l'administrateur et pour le chargement initial des clés.

Le produit s'utilise au sein d'une architecture type illustrée ci-après :

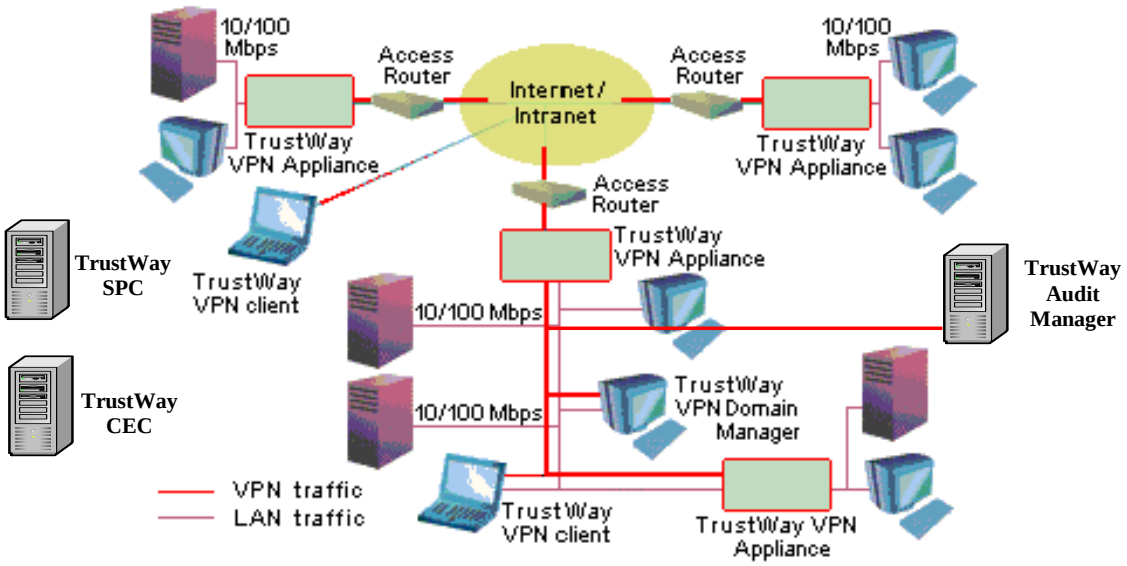

Figure 1 – Using architecture

Sur ce schéma, le produit est désigné par TrustWay VPN Appliance.

On identifie également sur ce schéma différents équipements optionnels ne faisant pas partie du périmètre de l'évaluation, ils sont désignés par :

- logiciel VPN client ;
- station de personnalisation (SPC) ;
- centre d'élaboration de clés (CEC) ;
- station d'administration Trustway VPN Domain Manager (TDM) ;
- station d'audit Trustway Audit Manager (TAM) ;
- accès routeur.

Le TDM offre la possibilité de déclarer des serveurs complémentaires dans l'architecture réseau du produit :

- serveur syslog devant recevoir les messages d'alarmes syslog émis par le produit ;
- serveur de supervision snmp devant recevoir les traps snmp émis par le produit.

Ces équipements ne font pas partie du périmètre de l'évaluation (ils ne sont pas représentés sur le précédent schéma).

Les diverses fonctionnalités de tous ces équipements sont décrites dans la cible de sécurité [ST] ainsi que dans les guides d'administration (cf. [GUIDES]).

1.2.4. Cycle de vie

Le produit a été développé sur le site suivant :

Bull SAS - Les Clayes sous Bois

Rue Jean Jaurès – BP 68,
78340 Les Clayes sous Bois,
France

Le produit est ensuite intégré et finalisé sur le site de :

Bull BILS - Angers

357, avenue Patton
49008 Angers Cedex 01
France

Il n'y a pas de rôle utilisateur pour les fonctions de sécurité du produit.

1.2.5. Configuration évaluée

Le produit évalué comprend :

- les logiciels TVPN/TCRX ;
- les logiciels b205/c020 de la carte cryptographique ;
- la partie logicielle implémentant le protocole de communication avec la station d'administration ;
- le module logiciel d'administration locale.

Les éléments ci-après sont également présents dans le produit mais sont exclus du périmètre d'évaluation :

- le système d'exploitation Linux, ainsi que l'utilitaire Netfilter qui y est inclus ;
- le logiciel Tripwire.

Les éléments ci-après se trouvent en dehors du produit et sont exclus du périmètre d'évaluation, toutefois il faut noter qu'ils sont nécessaires à son fonctionnement :

- un terminal externe (SafePad) nécessaire à l'authentification de l'administrateur et au chargement initial des clés ;
- une station d'administration (TDM) ;
- une station d'audit (TAM).

Bien que le produit dispose de quatre modes (*drop, forward, IPSEC-transport, IPSEC-tunnel*), seul ce dernier mode est dans le périmètre de l'évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation du produit BULL Trustway VPN Appliance v3.01.06 certifié par la DCSSI (voir [2004/30]).

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 11 mars 2009, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu à la conclusion suivante : certains des mécanismes analysés n'atteignent pas le niveau standard défini dans le référentiel cryptographique de la DCSSI (Cf. [REF-CRY]).

Toutefois, 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 VLA visé.

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, l'offre BULL TrustWay VPN Line, développée par Bull SAS**,** se présentant sous la forme d'un des trois boîtiers suivants :

- boîtier TVPN (Trustway Virtual Private Network) version 4.05.02,
- boîtier TCRX (Trustway Chiffreur Routeur d'eXtrémité) version 4.05.01,
- boîtier TCRX2 (2ème modèle du TCRX) version 4.05.01,

soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 2 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit décrit 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] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- le produit doit être installé, configuré et maintenu (application des correctifs ou mises à jour sécuritaires du logiciel et du matériel) de façon à préserver l'intégrité et la confidentialité des données sensibles (c'est-à-dire les données de configuration et d'administration) et des données transitant dans le produit ;
- les administrateurs du produit doivent être non hostiles, correctement formés et doivent respecter les guides d'administration du produit. En particulier, les administrateurs autorisés sont authentifiés avant toute action réalisée sur les stations d'administration (TDM) ou d'audit (TAM). L'authentification est réalisée par les TDM et TAM au moyen de dispositifs hardware (*token*), au travers d'un canal sécurisé suivant des procédures d'authentification à base de cartes à puce ;
- tout équipement d'administration (TDM, CEC, TAM, SPC,…), incluant les données associées (e.g. CD-ROM contenant les clés, cartes à puce, …), et le boîtier TVPN doivent être protégés par des mesures physiques et logiques avec accès restreint aux seuls administrateurs autorisés. En particulier, le CEC et le SPC en charge de la génération des clés ne doivent être connectés à aucun réseau. La politique de sécurité du réseau général doit être définie de façon appropriée, en particulier, des équipements de filtrage doivent limiter au strict minimum les flux provenant d'une zone potentiellement hostile vers les équipements d'administration TDM et TAM, flux *udp* 69 (*tftp*) et *udp* 162 (*snmp*) en provenance d'adresses IP fixes, et le produit doit être configuré en accord avec cette politique. Le TDM et le TAM doivent fournir des services d'intégrité et de confidentialité pour assurer la protection des dialogues d'administration avec le produit ;

- le produit doit être personnalisé par la station SPC de façon à injecter les secrets spécifiques à un équipement particulier et pour un utilisateur particulier. Au cours de ce processus, l'équipement est cryptographiquement personnalisé et sera ainsi authentifiable lorsqu'il sera introduit sur le réseau utilisateur ;
- le produit doit utiliser un système de clés créées par la station d'administration pour sécuriser les flux de communication avec les autres systèmes. Toutes les données sensibles doivent être envoyées chiffrées en tant qu'éléments de configuration du produit (et des autres systèmes). Le renouvellement des clés peut être réalisé n'importe quand, ou à une date planifiée, en mettant à jour la configuration du produit (et des autres systèmes) ;
- le produit doit mettre en œuvre une configuration correcte du logiciel Tripwire qui vérifie périodiquement l'intégrité du logiciel réalisant les fonctions de sécurité du produit ;
- les clés cryptographiques distribuées au produit doivent avoir été générées et dimensionnées conformément aux recommandations du référentiel cryptographique de la DCSSI (cf. [REF-CRY]) pour le niveau standard ;
- les auditeurs du TDM, des serveurs syslog et des serveurs de supervision snmp doivent analyser régulièrement les fichiers d'audits. Ils sont en charge de la gestion des fichiers d'audits et de la détection des attaques ;
- l'administrateur doit gérer sur le TDM une liste noire de façon à contrôler (accepter ou interdire) l'introduction d'un équipement sur le réseau ;
- lors du retrait d'un équipement sur le réseau (e.g. pour raison de maintenance), l'administrateur doit dépersonnaliser l'équipement avant de l'envoyer au fabricant, et doit l'inclure dans la liste de révocation des stations TDM et TAM.

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 1999 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 E6 et CC EAL7. 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'Espagne, la Finlande, la France, la Grèce, 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 2+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2		
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**2**	Configuration items
	ACM_SCP			**1**	**2**	**3**	3	3		
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**1**	Delivery procedures
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**1**	Informal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**1***	Subset of the implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1***	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3		
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3	**1***	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**1**	Evidence coverage
	ATE_DPT			**1**	1	**2**	2	**3**		
	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_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Examination of guidance
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

*appliqués aux exigences FCS

Annexe 2. Références documentaires du produit évalué

[2004/30]	Certificat DCSSI délivré le 21 septembre 2004 pour le produit BULL Trustway VPN Appliance v3.01.06
[ST]	Cible de sécurité de référence pour l'évaluation : - BULL Trustway VPN Line - Security Target, - référence D00G007, - version 2.9 du 27 février 2009 (document référencé [IN.103] dans le [RTE])
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation – Projet ALTAIR2, - référence OPPIDA/CESTI/ALTAIR2/RTE/3, - version du 11/03/2009 (document référencé [OUT.037] dans le [RTE])
[ANA-CRY]	Rapport d'analyse des mécanismes cryptographiques : - cotation de mécanismes cryptographiques ALTAIR2, - référence 1438/SGDN/DCSSI/SDS/Crypto, - version 1 du 3 juillet 2008 (document référencé [IN.095] dans le [RTE])
[CONF]	Liste de configuration : - Liste de configuration des équipements TrustWay VPN, - référence D00P018, - révision 1.10 (document référencé [IN.102] dans le [RTE])
[GUIDES]	Guide d'installation et d'administration du produit : - Manuel d'installation TrustWay VPN et TrustWay CRX ou CRX2, - référence 86 F2 23ET, - version 02 (document référencé [IN.062] dans le [RTE]) - Manuel d'installation et d'utilisation TDM, - référence 86 F2 26ET, - version 03 (document référencé [IN.073] dans le [RTE]) Guide d'utilisation du produit : - TDM-TAM Journalisation, Description des enregistrements - référence 86 X2 31ET 00, - version de nov. 06 (document référencé [IN.045] dans le [RTE]) - Manuel de dépannage TrustWay VPN et TrustWay CRX ou CRX2, - référence 86 F2 27ET, - version 02 (document référencé [IN.049] dans le [RTE])

Annexe 3. 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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[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.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.