PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2004/30

BULL Trustway VPN Appliance v3.01.06

Paris, le 21 septembre 2004

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[ORIGINAL SIGNE]

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.
Toutefois, la certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

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)

[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.

Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[1], 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 novembre 2003, 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 et le Japon ; 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 Norvège, les Pays-Bas, la Suède et la Turquie.

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le produit « Trustway Virtual Private Network » (appelé « TVPN » par la suite), en version 3.01.06, de l'offre « Trustway VPN Appliance », développée par BULL.

1.2. Développeur

Le produit est développé par :

BULL S.A.

Rue Jean Jaurès
BP 68
78340 les Clayes-sous-Bois
France

L'intégration du produit dans les boîtiers est effectuée par :

BULL S.A.

357, avenue Patton
BP 20845
49008 Angers Cedex 01
France

1.3. Description du produit évalué

1.3.1. Architecture

Le produit est constitué d'un boîtier comportant les éléments suivants :

- Une carte mère VIA C3,
- Un processeur Intel Celeron de 800Mhz,
- Un disque dur Fujitsu de 20Go,
- 128Mb de SDRAM PC100,
- Une carte PCI Trustway CC2000 « PCA3 » (carte version 76677843-104A, driver CC2000 version 76 678 027) et son logiciel embarqué (version B005), développés par BULL, et réalisant les opérations cryptographiques,
- Une alimentation,
- Un terminal permettant l'authentification de l'administrateur et le chargement initial des clés,
- Deux cartes Ethernet PRO100 & REALTEK 8139,
- Des leds pour indiquer l'activité du châssis,
- Un port série (utilisé pour l'administration locale).

Les applications suivantes sont installées sur le produit :

- Un système d'exploitation Linux (linux kernel 2.4.12),
- L'utilitaire Netfilter (inclus dans Linux),
- Le logiciel Tripwire (version 2.2.1),

- Le logiciel TVPN (version 3.01.06) incluant le protocole sécurisé d'échanges de données avec la station d'administration,
- le module logiciel d'administration locale.

Une description détaillée de l'architecture de l'application se trouve dans le document [HLD].

1.3.2. Cycle de vie

Le produit TVPN est développé par BULL sur son site des Clayes-sous-bois. Le produit TVPN est ensuite intégré et finalisé dans l'usine de BULL à Angers d'où il est livré aux clients finaux.

1.3.3. Périmètre et limites du produit évalué

Le produit évalué comprend le logiciel TVPN, le logiciel de la carte cryptographique, la partie logicielle implémentant le protocole de communication avec la station d'administration et le module logiciel d'administration locale.
En particulier, la station d'administration, le logiciel Tripwire et le système d'exploitation Linux ne font pas partie du périmètre d'évaluation.

2. L'évaluation

2.1. Commanditaire

BULL S.A.

Rue Jean Jaurès
BP 68
78340 les Clayes-sous-Bois
France

2.2. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.3. Centre d'évaluation

Oppida

13, route de la Minière – Bâtiment 134
78000 Versailles
France

Téléphone : +33 (0)1 30 83 27 95

Adresse électronique : cesti@oppida.fr

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation satisfont aux exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].

L'évaluation s'est déroulée de mai 2003 à août 2004.

2.5.1. L'environnement de développement

Le produit est développé sur le site de BULL situé à l'adresse :

Rue Jean Jaurès
BP 68
78340 les Clayes-sous-Bois
France

Le produit est intégré sur le site de Bull situé à l'adresse :

357, avenue Patton
BP 20845
49008 Angers Cedex 01
France

Les mesures de sécurité permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.
Un système de gestion de configuration est utilisé conformément au plan de gestion de configuration défini par le développeur du produit. La liste de configuration [LGC] identifie les éléments gérés par ce système. Les procédures de génération permettent par ailleurs de s'assurer que les bons éléments de configuration sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures de développement et de gestion de configuration a été effectuée par une visite des sites de Bull aux Clayes-sous-Bois et à Angers (cf Annexe 1 et 2).

2.5.2. La conception du produit

La classe d'assurance ADV définit les exigences de raffinement des fonctions de sécurité du produit depuis les spécifications globales présentes dans la cible de sécurité [ST] jusqu'à l'implémentation de ces fonctions.

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit :

- spécifications fonctionnelles (FSP),
- conception de haut-niveau (HLD),
- conception de bas-niveau (LLD) pour la partie cryptographique du produit,
- implémentation des fonctions de sécurité (IMP) pour la partie cryptographique du produit.

2.5.3. La livraison et l'installation

La livraison est considérée juste après le développement du produit. L'application est développée par Bull sur le site des Clayes-sous-bois. Elle est livrée à l'usine d'Angers sous la forme d'un CDROM, où elle est installée sur le boîtier. La livraison au client final se fait sous la forme d'un CDROM contenant le logiciel d'administration du TVPN, et du boîtier lui-même. La procédure de livraison utilisée [DEL] permet de connaître l'origine de la livraison et de détecter une modification du produit pendant la livraison, que ce soit pour la livraison du CDROM à l'usine d'Angers ou pour la livraison du produit à l'utilisateur final.

L'installation du produit correspond à l'installation la configuration du logiciel TVPN par le client final. Les procédures d'installation, de génération et de démarrage [ADM] permettent d'obtenir la configuration évaluée du produit.
Le logiciel d'administration ne fait pas partie du périmètre d'évaluation. Il a néanmoins été installé sur la plate-forme de test pour les besoins de l'évaluation. Le guide utilisé pour son installation et son utilisation est donné sous la référence [TDM].

2.5.4. La documentation d'exploitation

Du point de vue de l'évaluation, les administrateurs sont les personnes en charge de l'installation et de la configuration des boîtiers VPN. Les guides livrés à ces administrateurs [ADM] ont été fournis pour évaluation.
Du point de vue de l'évaluation, les utilisateurs sont les personnes transmettant des données via le VPN mis en place par les administrateurs. L'usage du VPN est transparent pour les utilisateurs et il n'y a donc pas de guide utilisateurs spécifique.
Le logiciel d'administration ne fait pas partie du périmètre d'évaluation. Il a néanmoins été installé sur la plate-forme de test pour les besoins de l'évaluation. Le guide administrateur utilisé pour son installation et son utilisation est donné sous la référence [TDM].

2.5.5. Les tests fonctionnels

L'évaluateur a vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit sont reliées à au moins un test fonctionnel dans la documentation de test.
Les tests ont été réalisés sur une plate-forme représentative du produit en exploitation comprenant deux boîtiers TRUSTWAY VPN (TVPN), une console d'administration TDM, un serveur Web IIS, trois PC portables et un PC servant de passerelle réseau.

2.5.6. L'analyse de vulnérabilité

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement prises en compte dans la conception du produit.
L'évaluateur a également réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré.
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élémentaire**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du produit Trustay VPN Appliance v3.01.06.

3.2. Niveau d'évaluation

Le produit Trustay VPN Appliance a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL2[1] augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_HLD.2	Security enforcing high-level design
ADV_LLD.1[2]	Descriptive low-level design
ADV_IMP.1[2]	Subset of the implementation of the TSF
ALC_DVS.1	Identification of security measures
ALC_TAT.1	Well-defined development tools
ALC_FLR.3	Systematic Flaw Remediation
AVA_MSU.1	Examination of guidance
AVA_VLA.2	Independent vulnerability analysis

Tableau 1 - Augmentations

Pour tous les composants, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite
Class ACM	**Configuration management**	
ACM_CAP.2	Configuration items	Réussite
Class ADO	**Delivery and operation**	

[1] Annexe 4 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].
[2] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

ADO_DEL.1	Delivery procedures	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite
Class ADV	**Development**	
ADV_FSP.1	Informal functional specification	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_IMP.1[1]	Subset of the implementation of the TSF	Réussite[1]
ADV_LLD.1[1]	Descriptive low-level design	Réussite[1]
ADV_RCR.1	Informal correspondence demonstration	Réussite
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
Class ALC	**Life cycle support**	
ALC_DVS.1	Identification of security measures	Réussite
ALC_FLR.3	Systematic Flaw Remediation	Réussite
ALC_TAT.1	Well-defined development tools	Réussite
Class ATE	**Tests**	
ATE_COV.1	Evidence of coverage	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_MSU.1	Examination of guidance	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.2	Independent vulnerability analysis	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** suivantes[2]. Les opérations sur ces exigences sont décrites dans la cible de sécurité [ST].

- Security alarms (FAU_ARP.1),
- Audit data generation (FAU_GEN.1),
- Potential violation analysis (FAU_SAA.1),
- Audit review (FAU_SAR.1),
- Protected audit trail storage (FAU_STG.1),
- Cryptographic key generation (FCS_CKM.1),
- Cryptographic key distribution (FCS_CKM.2),
- Cryptographic key destruction (FCS_CKM.4),
- Cryptographic operation (FCS_COP.1),

[1] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS
[2] Annexe 3 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- Complete access control (FDP_ACC.2),
- Security attributes based access control (FDP_ACF.1),
- Subset information flow control (FDP_IFC.1),
- Simple security attributes (FDP_IFF.1),
- Subset residual information protection (FDP_RIP.1),
- Basic data exchange confidentiality (FDP_UCT.1),
- Data exchange integrity (FDP_UIT.1),
- Authentication failures handling (FIA_AFL.1),
- User attribute definition (FIA_ATD.1),
- User authentication before any action (FIA_UAU.2),
- User identification before any action (FIA_UID.2),
- Management of security functions behavior (FMT_MOF.1),
- Management of security attributes (FMT_MSA.1),
- Static attribute initialisation (FMT_MSA.3),
- Management of TSF data (FMT_MTD.1),
- Management of limits on TSF data (FMT_MTD.2),
- Security management roles (FMT_SMR.1),
- Reliable time stamps (FPT_STM.1),
- TSF testing (FPT_TST.1),
- Trusted Path (FTP_TRP.1).

3.4. Résistance des fonctions

Seules les fonctions d'authentification ont fait l'objet d'une estimation du niveau de résistance.
Le niveau de résistance des fonctions de sécurité est jugé **élevé** (**SOF-High**).

3.5. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI suivant la procédure [CRY/I/01].

3.6. Reconnaissance européenne (SOG-IS)

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

3.7. Reconnaissance internationale (CC RA)

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

3.8. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.9) ainsi que les recommandations se trouvant dans les guides administrateur [ADM et TDM].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

3.9. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST § 4.2] :

- le produit (incluant la partie matérielle et le système d'exploitation linux) 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 ;
- la station d'administration doit être protégée par des mesures physiques et organisationnelles de sécurité. Son accès doit être réservé aux personnes autorisées. Les cartes à puce d'installation doivent être stockées et transmises à l'administrateur local de façon sécurisée. La politique de sécurité du réseau doit être définie de façon appropriée. Le produit doit être configuré conformément à cette politique. La station d'administration doit fournir des services de confidentialité et de sécurité afin d'assurer la protection des dialogues administratifs avec les boîtiers VPN ;
- le produit doit utiliser un système de clé créé 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 bien à une date planifiée, en mettant à jour la configuration du produit (et des autres systèmes).
- le produit doit mettre en oeuvre une configuration correcte de Tripwire qui vérifie périodiquement l'intégrité du logiciel réalisant les fonctions de sécurité du produit.

3.10. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le produit Trustay VPN Appliance v3.01.06, identifié au paragraphe 1.1 et décrit au paragraphe 1.3 du présent rapport, **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Visite du site de Bull S.A. aux Clayes sous Bois

Le site de développement de Bull S.A. situé rue Jean Jaurès, BP 68, 78340 les Clayes-sous-Bois, France, a fait l'objet, dans le cadre de l'évaluation du produit Trustay VPN Appliance v3.01.06, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_CAP.2) ;
- la livraison : **ADO** (ADO_DEL.1) ;
- le support au cycle de vie : **ALC** (ALC_DVS.1).

La visite par le centre d'évaluation a permis de conclure que les critères sont satisfaits sur ce site. Le rapport de visite se trouve sous la référence [Visite].

Annexe 2. Visite du site de Bull S.A. à Angers

Le site de développement de Bull S.A. situé au 357, avenue Patton, BP 20845, 49008 Angers Cedex 01, France, a fait l'objet, dans le cadre de l'évaluation du produit Trustay VPN Appliance v3.01.06, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la livraison : **ADO** (ADO_DEL.1),
- le support au cycle de vie : **ALC** (ALC_DVS.1).

La visite par le centre d'évaluation a permis de conclure que les critères sont satisfaits sur ce site. Le rapport de visite se trouve sous la référence [Visite].

Annexe 3. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont données à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles du produit.

Class FAU	**Security audit**
Security audit automatic response	
FAU_ARP.1	*Security alarms* Le produit doit entreprendre des actions (spécifiées dans la cible de sécurité [ST]) dans le cas où une violation potentielle de la sécurité est détectée.
Security audit data generation	
FAU_GEN.1	*Audit data generation* Ce composant définit le niveau des événements auditables et spécifie la liste des données que chaque enregistrement doit contenir.
Security audit analysis	
FAU_SAA.1	*Potential violation analysis* Le produit doit implémenter un seuil de détection élémentaire, défini selon une règle fixée (spécifiée dans la cible de sécurité [ST]).
Security audit review	
FAU_SAR.1	*Audit review* Le produit doit offrir aux utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]) la capacité de lire certaines informations (spécifiées dans la cible de sécurité [ST]) à partir des enregistrements d'audit.
Security audit event storage	
FAU_STG.1	*Protected audit trail storage* Les enregistrements d'audit doivent être protégés contre une suppression ou une modification non autorisées.
Class FCS	**Cryptographic support**
Cryptographic key management	
FCS_CKM.1	*Cryptographic key generation* Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiées qui peuvent être basées sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.2	*Cryptographic key distribution* Le produit doit distribuer des clés cryptographiques conformément à une méthode de distribution spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.4	*Cryptographic key destruction* Le produit doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques

	spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Information flow control policy	
FDP_IFC.1	*Subset information flow control* Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information, lesquelles sont spécifiées dans la cible de sécurité [ST] pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'informations.
Information flow control functions	
FDP_IFF.1	*Simple security attributes* Ce composant impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la fonction et décrit comment les attributs de sécurité sont choisis par la fonction.
Residual information protection	
FDP_RIP.1	*Subset residual information protection* Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets lors de l'allocation ou de la désallocation de la ressource.
Inter-TSF user data confidentiality transfer protection	
FDP_UCT.1	*Basic data exchange confidentiality* Ce composant a pour but de fournir une protection vis-à-vis de la divulgation de données de l'utilisateur lorsqu'elles sont transférées.
Inter-TSF user data integrity transfer protection	
FDP_UIT.1	*Data exchange integrity* Ce composant concerne la détection d'erreurs liées à des modifications, suppressions, insertions et rejeux des données de l'utilisateur transmises.
Class FIA	**Identification and authentication**
Authentication failures	
FIA_AFL.1	*Authentication failure handling* Le produit doit être capable d'arrêter le processus d'établissement d'une session après un nombre spécifié de tentatives d'authentification infructueuses d'un utilisateur. Il doit aussi, après la clôture du processus d'établissement d'une session, être capable de désactiver le compte de l'utilisateur ou le point d'entrée (e.g. station de travail) à partir duquel les tentatives ont été faites jusqu'à ce qu'une condition définie par un administrateur se réalise.
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.

User authentication	
FIA_UAU.2	*User authentication before any action* Les utilisateurs doivent s'authentifier avant que toute action ne soit autorisée.
User identification	
FIA_UID.2	*User identification before any action* Les utilisateurs doivent s'identifier avant que toute action ne soit autorisée.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Management of TSF data	
FMT_MTD.1	*Management of TSF data* Les utilisateurs autorisés peuvent gérer les données des fonctions de sécurité du produit.
FMT_MTD.2	*Management of limits on TSF data* Ce composant spécifie l'action à entreprendre lorsque les valeurs limites des données sont atteintes ou dépassées.
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiés dans la cible de sécurité [ST]).
Class FPT	**Protection of the TSF**
Time stamps	
FPT_STM.1	*Reliable time stamps* Le produit doit fournir un horodatage fiable.
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.
Class FTP	**Trusted path/channels**
Trusted path	
FTP_TRP.1	*Trusted path* Un chemin de confiance entre le produit et un utilisateur doit être fourni pour un ensemble d'événements défini. Soit l'utilisateur soit le produit initie le chemin de confiance.

Annexe 4. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 5. Références documentaires du produit évalué

[ST]	Bull Trustway VPN Appliance - ISO15408 - Security Target, Référence : version 1.6 du 03/03/2004 BULL S.A.
[HLD]	Spécifications globales de l'appliance TrustWay VPN, Référence : TVPN-003-FR, révision 1.1 BULL S.A.
[LGC]	Liste de configuration de l'appliance TrustWay VPN, Référence : D00P011 v1.0 BULL S.A.
[ADM]	Manuel d'Installation et d'Utilisation - TrustWay VPN/Devices, Référence : D00U007 v3.3, BULL S.A.
[TDM]	Manuel d'installation et d'utilisation - TrustWay Domain Manager, Référence : version 08 de Novembre 2003 BULL S.A.
[Visite]	ANNEXE : Tâche ALC_DVS, Référence : OPPIDA/CESTI/ALTAÏR/ALC.001/1, Oppida
[DEL]	Processus de livraison de l'appliance TrustWay VPN, Référence : TVPN-005-FR, révision 1.1 BULL S.A.
[RTE]	Rapport Technique d'Evaluation, Référence : OPPIDA/CESTI/ALTAÏR/RTE/1.1 Oppida

Annexe 6. 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.
[CRY/I/01]	Instruction CRY/I/01 Analyse des mécanismes cryptographiques, DCSSI.
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, August 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, August 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, August 1999, version 2.1, réf: CCIMB-99-033. Le contenu des Critères Communs version 2.1 est identique à celui de la Norme Internationale ISO/IEC 15408:1999, comportant les trois documents suivants : ▪ ISO/IEC 15408-1: Part 1 Introduction and general model ; ▪ ISO/IEC 15408–2: Part 2 Security functional requirements ; ▪ ISO/IEC 15408–3: Part 3 Security assurance requirements.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, August 1999, version 1.0, ref CEM- 99/045.
[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