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-2008/20

Système Equant IPVPN

Paris, le 8 juillet 2008,

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ Ti 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

Référence du rapport de certification **DCSSI-2008/20**
Nom du système **Système Equant IPVPN**
Référence/version du système **Version 1.0**
Conformité à un profil de protection **Néant**
Critères d'évaluation et version **Critères Communs version 3.0**
Niveau d'évaluation **EAL 2 augmenté** **ALC_FLR.1**
Développeur **France Telecom – Orange Business Services** **9 rue du Chêne Germain, BP 91235, 35512 Cesson Sévigné, France**
Commanditaire **France Telecom – Orange Business Services** **9 rue du Chêne Germain, BP 91235, 35512 Cesson Sévigné, France**
Centre d'évaluation **Silicomp-AQL** **1 rue de la châtaigneraie, CS 51766, 35513 Cesson Sévigné Cedex, France** **Tél : +33 (0)2 99 12 50 00, mél : cesti@aql.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 système

1.1. Présentation du système

L'évaluation a porté sur le « Système Equant IPVPN, Version 1.0» développé par France Telecom – Orange Business Services.

Ce système est destiné à offrir des réseaux privés virtuels (VPN : Virtual Private Network), cloisonnés entre eux ainsi qu'avec l'Internet. Il est disponible actuellement dans 146 pays. Cette solution centralisée fournit une infrastructure simplifiée de communication, fonctionnant 24h/24, 7j/7 permettant aux clients de travailler d'où ils le souhaitent, tout en choisissant le type de connexion qu'ils souhaitent. Ces réseaux privés virtuels sont basés sur la technologie MPLS/VPN (Multi protocol Label Switching/ Virtual Private Networks).

1.2. Description du système évalué

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

1.2.1. Architecture

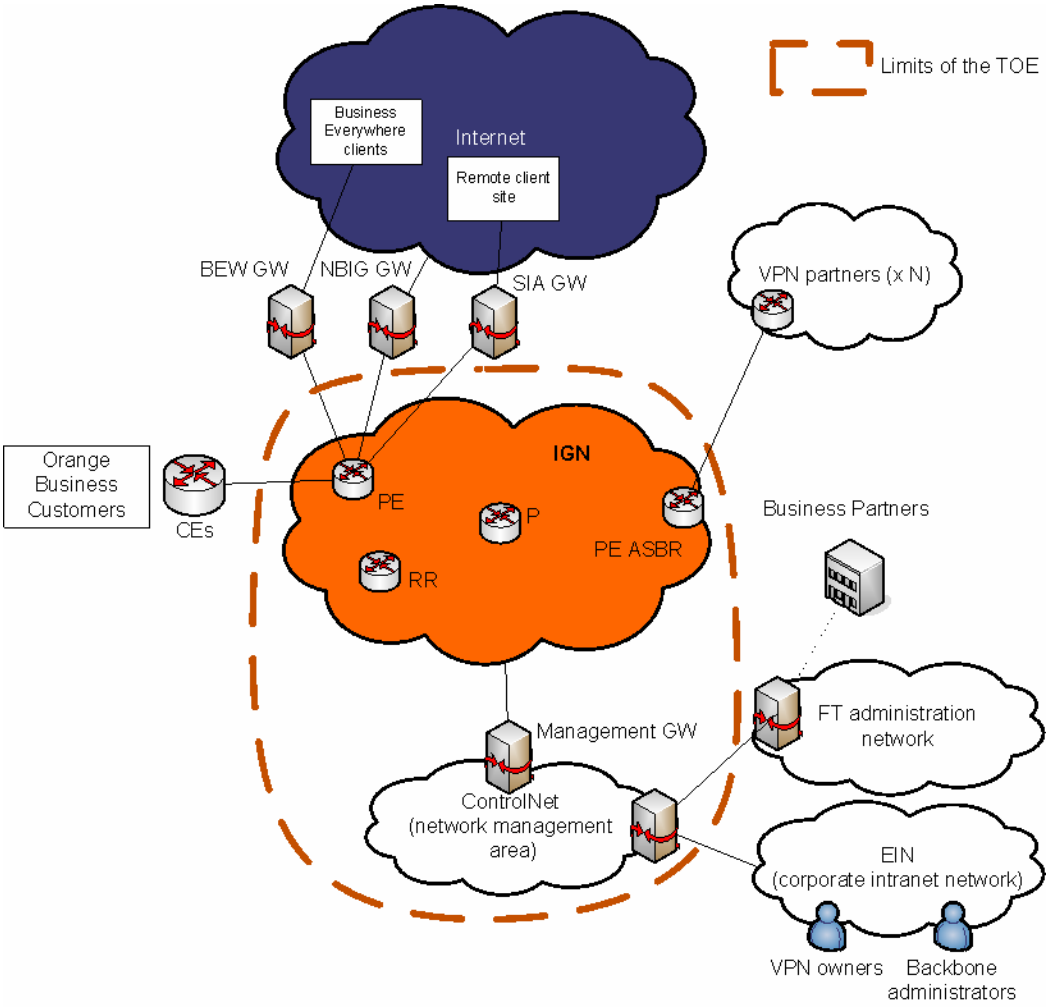
La TOE est un système qui permet de relier des sites d'entreprises distants par des réseaux privés virtuels (VPN).

Le système complet est constitué des principaux éléments suivants :

- L'*IP Global Network (IGN)* qui correspond au réseau international d'Orange Business Services, dédié aux flux VPN des entreprises clientes. C'est un backbone basé sur la technologie MPLS/VPN. Ce réseau est composé de routeurs Provider (P routers), de routeurs Provider Edge (PE routers), de routeurs PE Autonomous System Border Route (ASBR PE) et de Route Reflectors (RR). Ce réseau est en permanence sous surveillance grâce à des outils d'audit et de monitoring (SAFE et Netforensics) qui permettent aux équipes en charge de la surveillance du système de détecter et de réagir lorsque des incidents interviennent.
- Le *ControlNet* qui est un réseau dédié aux activités d'administration de l'IGN ; il est l'unique moyen d'atteindre les PE pour gérer leur configuration, ainsi que celle des VPN. Ce réseau héberge l'ensemble des outils de gestion de l'IGN. L'administration de la TOE est réalisée par les équipes d'Equant via ce réseau sécurisé. Cependant, dans certains cas, la TOE offre la possibilité de faire réaliser la maintenance des équipements IP directement par leurs fournisseurs (maintenance de niveau 4).
- Les *interfaces avec les clients du service Equant IPVPN* : les réseaux des entreprises clientes sont connectés à l'IGN à travers des routeurs CE (Client Edge), localisés dans leurs locaux et connectés aux routeurs PE. Il est à noter que ces routeurs, localisés dans les sites des clients, ne peuvent pas être considérés comme faisant partie des VPN, seule l'interface de raccordement d'un client au niveau du PE fait partie du VPN.

- Les *interfaces avec les partenaires VPN* : ces interfaces sont utilisées pour étendre le système IPVPN à des zones géographiques non couvertes par le réseau IGN d'Orange Business Services.
- Les *passerelles vers l'Internet* : les passerelles Business Everywhere Gateway (BEG GW), Secure ISP Access Gateway (SIA GW) et Network Based Internet Gateway (NBIG GW) correspondent aux différents types de passerelles de l'IGN vers Internet.

La figure suivante fournit une vue d'ensemble du système global et identifie les limites de la TOE.



1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le système sont :

- le cloisonnement des VPN clients entre eux ;
- l'intégrité des routeurs du backbone et leur contrôle d'accès ;
- des interfaces appropriées avec les partenaires VPN (pour les VPN qui doivent être étendus à des zones non couvertes par Orange Business Services);
- pour les clients NBIG (Network Based Internet Gateway) et SIA (Secure Internet Service Provider Access), une interconnexion contrôlée de leur VPN avec Internet.

1.2.3. Identification du système

La version évaluée de la TOE est la version la 1.0.

S'agissant d'une évaluation système, la version de la TOE n'est pas identifiable directement par les utilisateurs finaux.
L'ensemble des composants (tant matériels que logiciels) de la version évaluée, et sur lesquels les tests de cette évaluation ont été menés, est consigné dans la liste de configuration disponible dans [CONF].
La cible de sécurité [ST] identifie également, au chapitre 1.4, les différents types d'éléments qui composent la TOE.

Le CESTI a analysé les procédures d'ingénierie et de dimensionnement du backbone mises en œuvre par Orange Business Services [EVOLUTION] et a également vérifié qu'elles étaient effectivement utilisées.
Cette évaluation permet donc de confirmer que le développeur dispose de mesures adéquates pour faire évoluer le dimensionnement de ce système afin de garantir son maintien en conditions opérationnelles.

1.2.4. Cycle de vie

Le cycle de vie du système est le suivant :

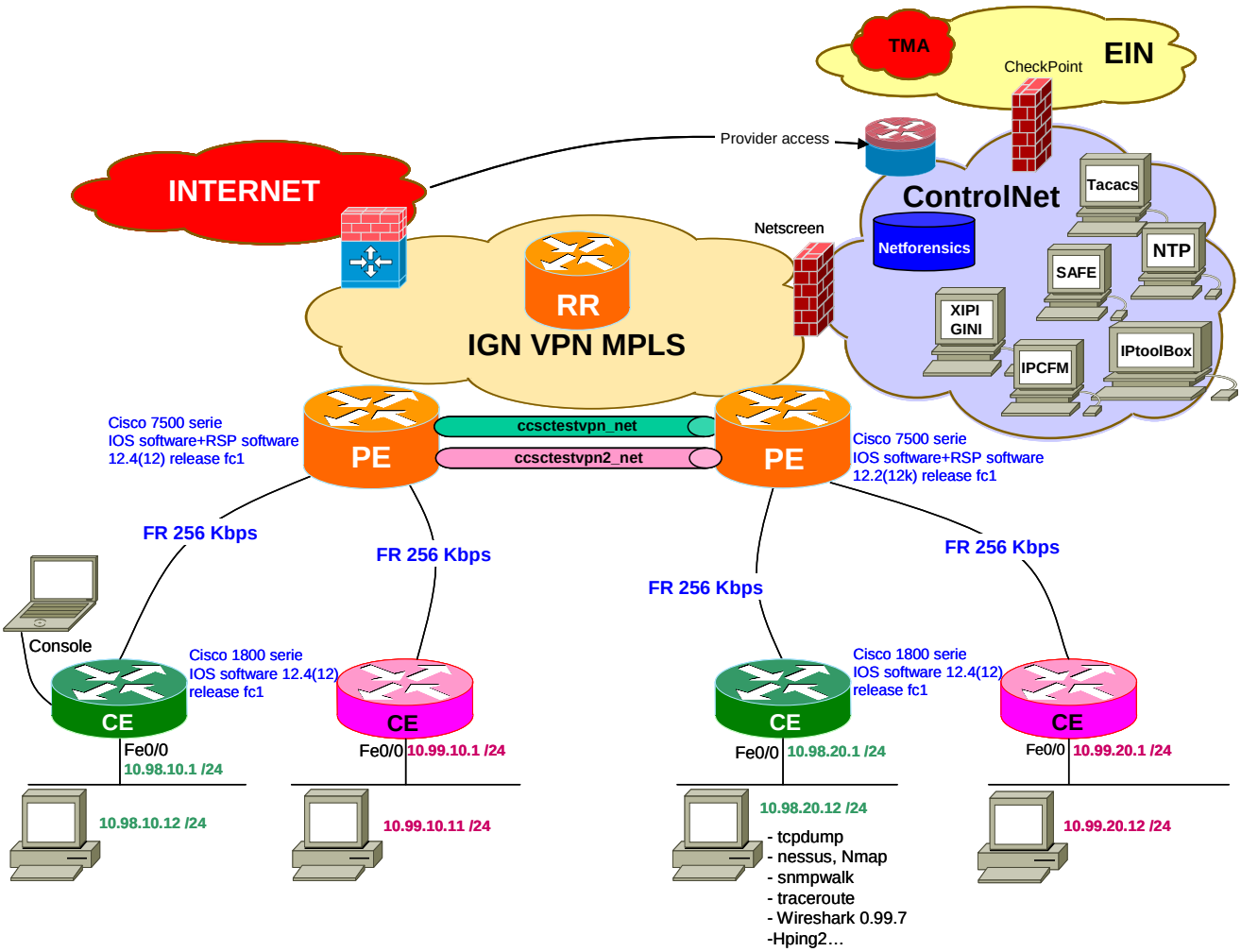
- le développement du système correspond à la phase d'intégration des différents composants
- l'installation correspond au déploiement (installation, configuration) des composants de la TOE
- l'utilisation correspond :
    - au déploiement des composants hors TOE (installation, configuration),
    - à l'utilisation du système.

1.2.5. Configuration évaluée

Comme mentionné ci-dessus, le présent certificat porte également sur les évolutions du dimensionnement du système mises en œuvre conformément au document [EVOLUTION].

La plate-forme de test, mise à disposition par le développeur, est représentative de la TOE. Elle est constituée d'une part par l'ensemble du réseau opérationnel (ControlNet et IGN, P, PE, RR compris) et d'autre part de quatre routeurs CE affectés uniquement à l'évaluateur (au même titre qu'un client) configurés conformément au guide d'administration des routeurs CE [CONF CE], section 4.

La plateforme de test utilisée dans le cadre de cette évaluation est décrite dans la figure suivante.



2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.0** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour répondre aux spécificités d'une évaluation système, la note d'application [EVAL-SYS] a été appliquée.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 6 juin 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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 système « Système Equant IPVPN, Version 1.0» 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 système spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du système 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 :

- ***OE.ControlledPhysicalAccess :*** France Telecom/Equant doit protéger l'accès aux locaux accueillant les composants de la TOE. Les clients de ce service doivent protéger l'accès aux locaux accueillant les routeurs CE fournis par France Telecom/Equant.
- ***OE.ProvidersAccesses :*** afin de permettre la réalisation de certaines opérations de maintenance, les fournisseurs des équipements du backbone doivent pouvoir avoir accès à la TOE. De même que tout autre administrateur, les équipes des fournisseurs doivent être authentifiées et leur accès sera restreint au strict nécessaire. Seul un accès en lecture doit leur être fourni.
- ***OE.CapableAdministrators :*** les administrateurs de la TOE doivent être formés à l'utilisation des applications et outils qu'ils doivent mettre en œuvre. Ces administrateurs sont de confiance, ils ne sont pas considérés comme étant des attaquants potentiels volontaires.
- ***OE.AutonomousSystem :*** les flux de données des VPN clients, à partir d'un routeur PE vers un autre, ne peuvent circuler qu'au travers de la TOE. Les VPN internationaux ne peuvent être étendus qu'au travers d'interconnexion avec les partenaires locaux de France Telecom.
- ***OE.RemoteAdministrationAccess :*** les opérations d'administration distantes, en dehors des heures ouvrables, sont réalisées au travers d'un réseau d'administration interne. Les moyens mis en œuvre pour sécuriser ce type d'accès doivent permettre l'authentification des opérateurs, et garantir la confidentialité et l'intégrité des données échangées.
- ***OE.VPNExtensionServices :*** les entités de France Telecom qui gèrent les services BEW, SIA et NBIG sont responsables du bon paramétrage des comptes clients.

- ***OE.ServersManagement :*** l'administration des équipements de ControlNet qui ne participent pas directement à la réalisation de fonctions de sécurité ne doit pas compromettre la sécurité du service fourni.
- ***OE.PasswordsManagement :*** les mots de passe des administrateurs doivent être générés, stockés et distribués de façon à garantir qu'ils ne sont connus que par leurs détenteurs.
- ***OE.OperationsAndMaintenance :*** France Telecom/Equant doit utiliser et maintenir les applications de la TOE de façon sécurisée.
- ***OE.ControlAtProductionTime :*** les opérateurs réalisant les opérations de production des VPN doivent réaliser des contrôles pour s'assurer que les accès fournis correspondent effectivement aux demandes clients.

Conformément à la note d'application [EVAL-SYS], l'audit des sites de déploiement de la TOE et la vérification de la mise en œuvre des mesures de protection organisationnelles n'ont pas été réalisés dans le cadre de cette évaluation (en effet, ce n'est pas l'objet d'une évaluation CC qui adresse principalement des mesures de sécurité TI). Il est donc à la charge des utilisateurs de ce certificat de s'assurer que les sites de déploiement de la TOE respectent effectivement les mesures de sécurité étudiées dans le cadre de cette évaluation. L'utilisateur de ce certificat pourra pour se faire s'appuyer, par exemple, sur les normes suivantes : ISO27001 / ISO17799 / BS7799.
Les mesures de sécurité étudiées dans le cadre de cette évaluation sont listées dans le tableau ci-dessous, [SECPHY-DEV] correspondant aux mesures de sécurité applicables aux sites d'Orange Business Services hébergeant la TOE et [SECPHY-USER] correspondant aux mesures applicables aux sites des clients ayant accès au système.

Objectifs de sécurité	**[SECPHY-DEV]**	**[SECPHY-USER]**
OE.ControlledPhysicalAccess	[Physical Security Controls]	[SECPHY-USER]
OE.ProvidersAccesses	[ProviderAccess Management] [Third party access Management]	
OE.CapableAdministrators	[Equant Security Policy] [Services Basics Learning Programmes]	
OE.AutonomousSystem	[Equant Security Policy] [Services Basics Learning Programmes]	
OE.RemoteAdministrationAccess	[NUAR Registration Procedure]	
OE.ServersManagement	[ESSC – Implementation Solaris]	
OE.PasswordsManagement	[NUAR Registration Procedure] [Password Security Policy]	
OE.OperationAndMaintenance	[Equant Security Policy] [Services Basics Learning Programmes]	
OE.ControlAtProductionTime	[Equant Security Policy] [Services Basics Learning Programmes]	

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, la République de Corée, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du système

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le système	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Architectural design with domain separation and non-bypassability
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**2**	Security-enforcing functional specification
	ADV_IMP				**1**	1	**2**	**2**		
	ADV_INT					**2**	**3**	**3**		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**1**	Basic 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		**2**	**3**	**4**	4	**5**	5	**2**	Use of a CM system
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**2**	Parts of the TOE CM coverage
	ADO_DEL		**1**	1	**1**	1	1	**1**	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2		
	ALC_FLR								**1**	Basic flaw remediation
	ALC_LCD			1	**1**	**1**	1	**2**		
	ALC_TAT				**1**	**2**	**3**	3		
ASE Security Target Evaluation	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	**1**	Evidence of coverage
	ATE_DPT			**1**	2	**3**	3	**4**		
	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	**2**	Vulnerability analysis

Annexe 2. Références documentaires du système évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - « Security target for the Equant IPVPN service – international perimeter », ref. SRVG-6QCGH2, version 3P6, 30/05/08 Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Equant IPVPN - Public security target for the Equant IPVPN service – international perimeter », ref. AGUI-7F8GPQ, version 1.0, 02/06/08
[RTE]	Rapport technique d'évaluation : - « PAMPLEMOUSSE - Rapport Technique d'Evaluation », ref. TPC320-RTE01, version 1.03, 06/06/08
[CONF]	« PAMPLEMOUSSE Project – ALC_CMS.2 &ALC_CMC.2 – Configuration management procedures », ref. MEXT-76LCGV, version 1P5, 22/02/08
[GUIDES]	Guide d'installation du système : - Production et test d'acceptation des VPN : « PAMPLEMOUSSE Project ALC_DEL.1 – Service Delivery Procedure », ref. MEXT-77CGDG, version 1P3 du 22/02/08 Guide «chapeau » : « AGD_PRE.1 & AGD_OPE.1 – Guidance documents », ref. MEXT-77CGCH, version 1P3 du 02/06/08 qui référence entre autres les documents [SECPHY-DEV]: - [Equant Security Policy] : «Equant Security Policy», ref. POL-SEC-CS-003, version 3, March 2002 - [ESSC – Implementation Solaris] : «ESSC Security standard implementation for Solaris 8, 9 & 10 », ref. ESSC-SESM-SOL-01, version 0.4, 08/08/2007 - [NUAR Registration Procedure] : «NUAR Registration Procedure», ref. NA, version1.2, 11/18/02 - [Password Security Policy] : « FT Group Password Security Policy », ref. n.a, version 1.0, 06/29/2005 - [Physical Security Controls] : «Photo ID and Facility Access Control Policy», ref. EM-SM-0008, version 1.3, 30/10/07 - [ProviderAccess Management] : «Equipment Supplier Access Security Policy», ref. POL-SEC-NS-09, version 2.4, 26/10/07 - [Services Basics Learning Programmes] : « Orange Business Services - Services Basics Learning Programme Trainee's Guide », ref. n.a, version 3.0, August 2007 - [Third party access Management] : «Third Party Access Security Policy», ref. POL-SEC-NS-11, version 1.6, 30/10/07
[SECPHY-USER]	« IP VPN Service - Security Policy », ref. POL-SEC-NS-07, version 2.8, July 2006 (plus particulièrement le chapitre 5.5)

[EVOLUTION]	« ENDD – RSND EUMA / Circuit & Design - Network trunking scalability", ref. n.a, version 1.0, 05/05/08
[CONF CE]	« IP VPN - Configuration guide », ref. IOPINFO/INF 001118, version 1P0, 21/02/2006
RFC 4364	RFC 4364 BGP/MPLS IP Virtual Private Network (VPNs)

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, June 2005, version 3.0, revision 2, ref CCMB-2005-07-001; Part 2: Security functional components, July 2005, version 3.0, revision2, ref CCMB-2005-07-002; Part 3: Security assurance components, July 2005, version 3.0, revision 2, ref CCMB-2005-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2005, version 3.0, revision2, ref CCMB-2005-07-004.
[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.
[EVAL-SYS]	«Note d'application – Interprétation des CC pour les évaluations de systèmes», version 1 draft 5, 4 juillet 2007.