



PREMIER MINISTRE

Secretariat General for National Defence  
Central Directorate for Information Systems Security

**Certification Report DCSSI-2008/20**  
**Equant IPVPN system**

*Paris, 8<sup>th</sup> of July 2008,*

**Courtesy Translation**



## Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.



Certification does not, however, constitute a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

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  
France

[certification.dcssi@sgdn.gouv.fr](mailto:certification.dcssi@sgdn.gouv.fr)

Reproduction of this document without any change or cut is authorised.

<i>Certification report reference</i>	<b>DCSSI-2008/20</b>
<i>System name</i>	<b>Equant IPVPN system</b>
<i>System reference</i>	<b>Version 1.0</b>
<i>Protection profile conformity</i>	<b>None</b>
<i>Evaluation criteria and version</i>	<b>Common Criteria version 3.0</b>
<i>Evaluation level</i>	<b>EAL 2 augmented ALC_FLR.1</b>
<i>Developer</i>	<b>France Telecom – Orange Business Services 9 rue du Chêne Germain, BP 91235, 35512 Cesson Sévigné, France</b>
<i>Sponsor</i>	<b>France Telecom – Orange Business Services 9 rue du Chêne Germain, BP 91235, 35512 Cesson Sévigné, France</b>
<i>Evaluation facility</i>	<b>Silicomp-AQL 1 rue de la châtaigneraie, CS 51766, 35513 Cesson Sévigné Cedex, France Phone: +33 (0)2 99 12 50 00, email : cesti@aql.fr</b>
<i>Recognition arrangements</i>	<div style="display: flex; justify-content: space-around; align-items: center;"><div style="text-align: center;"><b>CCRA</b> </div><div style="text-align: center;"><b>SOG-IS</b> </div></div>

# Introduction

## The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site [www.ssi.gouv.fr](http://www.ssi.gouv.fr).



# Content

<b>1. THE SYSTEM .....</b>	<b>6</b>
1.1. PRESENTATION OF THE SYSTEM.....	6
1.2. EVALUATED SYSTEM DESCRIPTION.....	6
1.2.1. <i>Architecture</i> .....	6
1.2.2. <i>Security services</i> .....	7
1.2.3. <i>System identification</i> .....	7
1.2.4. <i>Life cycle</i> .....	8
1.2.5. <i>Evaluated configuration</i> .....	8
<b>2. THE EVALUATION.....</b>	<b>10</b>
2.1. EVALUATION REFERENTIAL .....	10
2.2. EVALUATION WORK .....	10
<b>3. CERTIFICATION.....</b>	<b>11</b>
3.1. CONCLUSION .....	11
3.2. RESTRICTIONS .....	11
3.3. RECOGNITION OF THE CERTIFICATE .....	12
3.3.1. <i>European recognition (SOG-IS)</i> .....	12
3.3.2. <i>International common criteria recognition (CCRA)</i> .....	13
<b>ANNEX 1. EVALUATION LEVEL OF THE SYSTEM.....</b>	<b>14</b>
<b>ANNEX 2. EVALUATED SYSTEM REFERENCES.....</b>	<b>15</b>
<b>ANNEX 3. CERTIFICATION REFERENCES .....</b>	<b>17</b>

# 1. The system

## 1.1. Presentation of the system

The evaluated system is « Equant IPVPN system, Version 1.0» developed by France Telecom – Orange Business Services.

This system is designed to create Virtual Private Networks (VPN), isolated from each others and also from the Internet. Now available in 146 countries, this core solution provides a simplified communication infrastructure, which operates 24x7, anywhere customers do business, using their preferred type of connection. These virtual private networks are based on the MPLS/VPN technology (Multi protocol Label Switching/ Virtual Private Networks).

## 1.2. Evaluated system description

The security target [ST] defines in details the evaluated system, its evaluated security functionalities and its operation environment.

### 1.2.1. Architecture

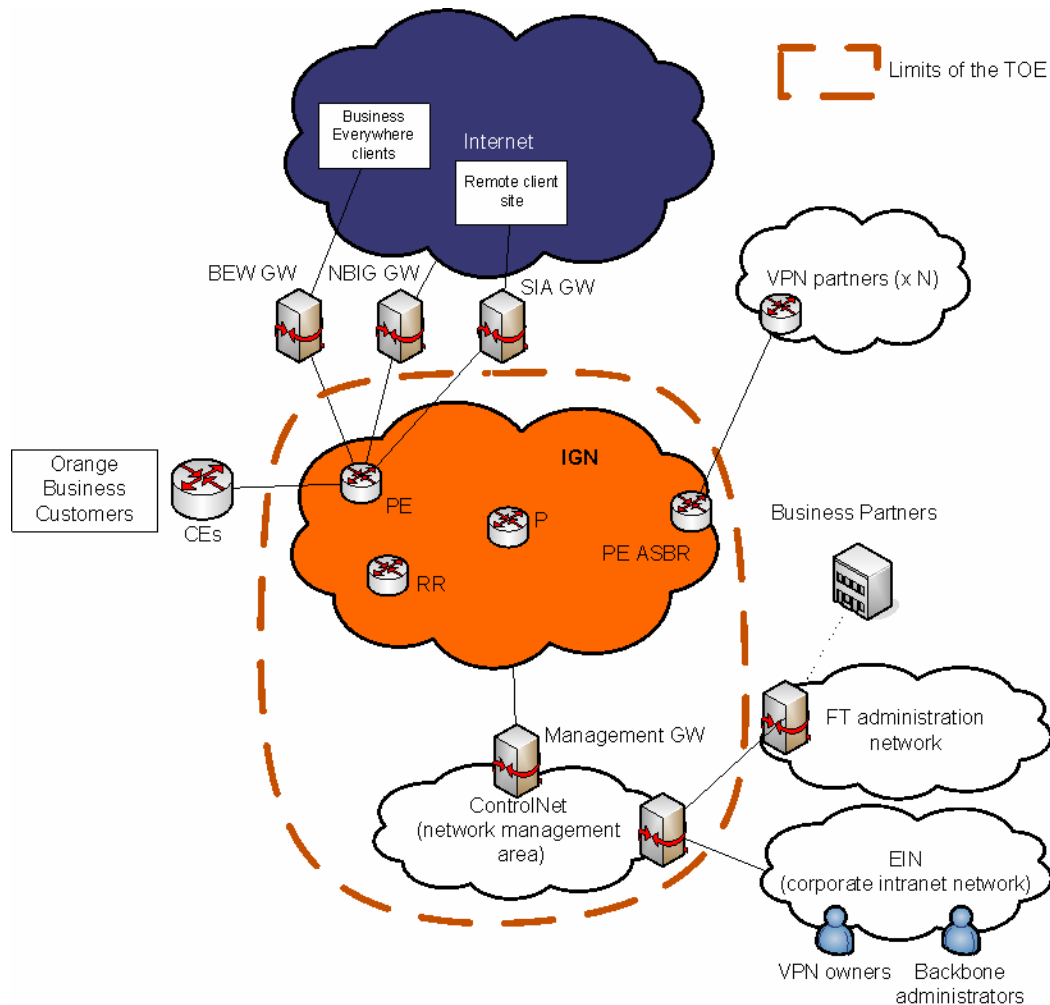
The TOE is a system that allows the interconnection of distant customers' sites based on a MPLS/VPN solution.

The whole system consists of the main following elements:

- *IP Global Network (IGN)* is the Orange Business Services' international network dedicated to enterprises' VPN flows. It is a backbone based on the MPLS/VPN technology. This network is composed of Provider routers (P routers), Provider Edge routers (PE routers), PE Autonomous System Border Route (ASBR PE) and Route Reflectors (RR). The IGN network is permanently under surveillance using audit and monitoring tools (SAFE and Netforensics) that allow the people in charge of the system supervision to detect incidents and to react appropriately;
- *ControlNet* is the dedicated administration network that constitutes a mandatory network access to reach the PEs in order to manage their configurations or the VPNs. This network hosts the various management applications. Administration of the TOE is realised by Equant staff on this secured administration network. However, in some cases, the TOE authorises staffs of companies that provide network equipment to perform level 4 support operation;
- *Interfaces with the customers of the Equant IPVPN service*: the customer networks are connected to the IGN through CE (Client Edge) routers located within their premises and connected to the PE routers. Note that the CE routers, which are located in the customers' premises, cannot be considered as supporting the VPNs, only the interface of the PE is part of the VPN;
- *Interfaces with VPN partners* this interface is used to extend the Equant IPVPN service to geographical areas that Orange Business Services's IGN does not cover;

- Gateways to the Internet Business Everywhere Gateway (BEG GW), Secure ISP Access Gateway (SIA GW) and Network Based Internet Gateway (NBIG GW) are the different types of gateway from the IGN to the internet.

The following figure presents a general overview of the whole system and identified the limits of the TOE



### 1.2.2. Security services

The system provides mainly the following security services:

- separation between customer VPNs (isolation);
- backbone router integrity and access control;
- proper interfaces with VPN partners (for VPNs that need to be extended to areas not covered by Orange Business Services);
- for the customers' NBIG (Network Based Internet Gateway) and SIA (Secure Internet Service Provider Access), controlled interconnection of their VPNs with the Internet.

### 1.2.3. System identification

The evaluated version of the TOE is version 1.0.

As the TOE considered here corresponds to a system, the TOE version cannot be directly identified by the end users.

The set of all software and hardware components that are making up the TOE and actually being under test for the evaluation are identified in the configuration list included in [CONF].

The security target [ST] also identifies the different types of components that compose the TOE at the chapter 1.4.

The Evaluation facility analysed the engineering procedures used by Orange Business Services to monitor the capacities of the TOE [EVOLUTION] and verified that they are actually applied.

Thus this evaluation allows confirming that the developer uses appropriate measures to upgrade the size of this system in order to guarantee its sustained working operational working condition.

#### ***1.2.4. Life cycle***

The system's life cycle is organised as follow:

- the development phase corresponds to the integration of the different TOE's components;
- the installation phase corresponds to the deployment (installation, configuration) of the TOE's components;
- the usage phase correspond to:
  - o the deployment (installation, configuration) of the non TOE's components,
  - o and the usage of the system.

#### ***1.2.5. Evaluated configuration***

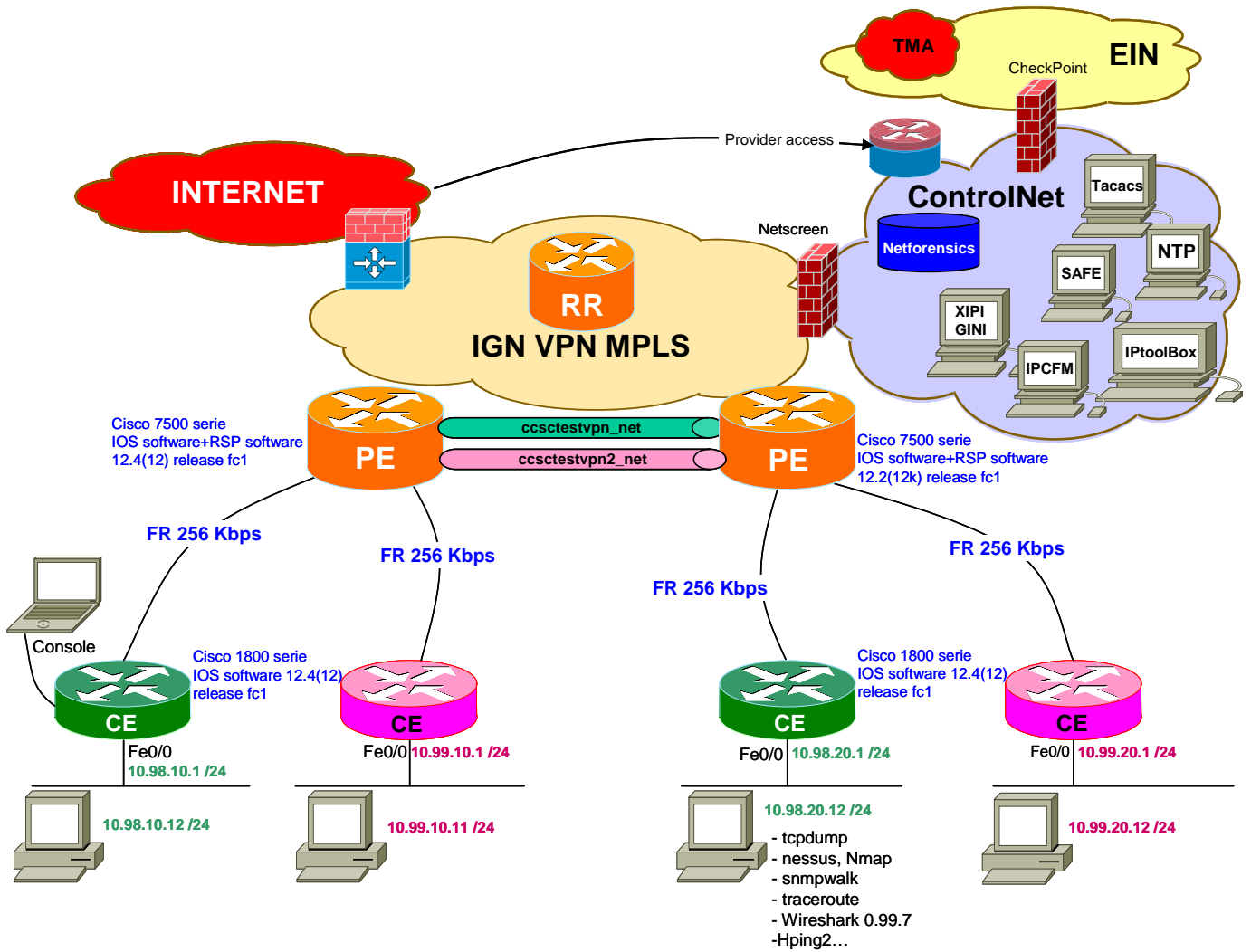
As mentioned above, this certificate is also valid for the evolution of the system performed according to the [EVOLUTION] document.

The test platform, provided by the developer, is representative of the TOE. It is composed of the operational network (ControlNet and IGN, with P, PE and RR) and of four CE routers allocated to the evaluator (like any client) which were configured according the CE administration guide [CONF CE], section 4.





The following picture describes the testing platform used by the evaluation facility.



## 2. The evaluation

### 2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.0** [CC], with the Common Evaluation Methodology [CEM].

In order to meet the specificities of a system evaluation, the [EVAL-SYS] application note have been applied.

### 2.2. Evaluation work

The evaluation technical report [ETR], delivered to DCSSI the 6<sup>th</sup> June 2008, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are “**pass**”.



## 3. Certification

### 3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the system “Equant IPVPN system, Version 1.0” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 2 augmented.

### 3.2. Restrictions

This certificate only applies on the system specified in chapter 1.2 of this certification report.

The user of the certified system shall respect the operational environmental security objectives summarized specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- ***OE.ControlledPhysicalAccess:*** France Telecom/Equant shall control the access to the premises hosting the appliances composing the TOE. The Customers shall control the access to the premises hosting the CE routers provided by France Telecom/Equant;
- ***OE.ProvidersAccesses:*** in order to allow maintenance operations, the TOE shall authorise providers' accesses. Like any other administrators, providers' staffs shall be authenticated and their accesses shall be restricted in terms of scope. Access shall only be granted in read only mode;
- ***OE.CapableAdministrators:*** the administrators of the system components shall be trained and capable to use the appliances and tools they use. The administrators are trusted people, they are not considered as threatening agents;
- ***OE.AutonomousSystem:*** Data flowing into a customer VPN, from a PE to another one, can only be exchanged within the TOE. International VPNs can only be extended through the interconnections with local partners;
- ***OE.RemoteAdministrationAccess:*** remote administration operations, out of working hours, are performed through the internal administration network. The means used to secure this type of access shall include an authentication of the operator, and guarantee confidentiality and integrity of exchanged data;
- ***OE.VPNExtensionServices:*** the entities of France Telecom that manage the services BEW, SIA and NBIG shall be responsible of the correct parameterization of the customers' accounts;
- ***OE.ServersManagement:*** the administration of the equipments of ControlNet which do not directly ensure security functions shall be performed in a manner ensuring the security of the provided services;
- ***OE.PasswordsManagement:*** the passwords of the administrators shall be generated, stored and distributed in a way ensuring that they are only known from their owner;

- **OE.OperationsAndMaintenance** : France Telecom/Equant shall operate and maintain the appliances constituting the TOE in a secure manner;
- **OE.ControlAtProductionTime** : at production time, the operators producing a VPN shall perform controls to make sure that the access produced is conformant to the customer request.

According to the application note [EVAL-SYS] the TOE deployment sites and the verification of the actual usage of the organisational security measures have not been audited during this evaluation (in fact it isn't the means of a CC evaluation which aimed mainly the IT security measures). Thus it is the responsibility of the certification report's user to make sure that the security measures studied during this evaluation are affectively applied in the TOE deployment premises To do so the certificate's user could rely, for example, on the following methodologies: ISO27001 / ISO17799 / BS7799.

The security measures studied during this evaluation are listed below, those that should be applied on Orange Business Services premise correspond to [SECPHY-DEV] and those that should be applied on the system's user premise correspond to [SECPHY-USER]

Security objectives	[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. Recognition of the certificate

#### 3.3.1. European recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].



The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement<sup>1</sup>, of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:



### **3.3.2. International common criteria recognition (CCRA)**

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries<sup>2</sup>, of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC\_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:



---

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

## Annex 1. Evaluation level of the system

Class	Family	Components by assurance level							Assurance level of the system	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL	Name of the component
ADV Development	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 Guidance	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 Life-cycle support	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 Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5	2	Vulnerability analysis



## Annex 2. Evaluated system references

[ST]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> <li>- « Security target for the Equant IPVPN service – international perimeter », ref. SRVG-6QCGH2, version 3P6, 30/05/08</li> </ul> <p>For the needs of publication, the following security target has been provided and validated in the evaluation:</p> <ul style="list-style-type: none"> <li>- « Equant IPVPN - Public security target for the Equant IPVPN service – international perimeter », ref. AGUI-7F8GPQ, version 1.0, 02/06/08</li> </ul>
[ETR]	<p>Evaluation technical report :</p> <ul style="list-style-type: none"> <li>- « PAMPLEMOUSSE - Rapport Technique d'Evaluation », ref. TPC320-RTE01, version 1.03, 06/06/08</li> </ul>
[CONF]	<p>« PAMPLEMOUSSE Project – ALC_CMS.2 &amp; ALC_CMC.2 – Configuration management procedures », ref. MEXT-76LCGV, version 1P5, 22/02/08</p>
[GUIDES]	<p>Installation guidance:</p> <ul style="list-style-type: none"> <li>- VPN production et acceptance test process: « PAMPLEMOUSSE Project ALC_DEL.1 – Service Delivery Procedure », ref. MEXT-77CGDG, version 1P3 du 22/02/08</li> </ul> <p>« AGD_PRE.1 &amp; AGD_OPE.1 – Guidance documents », ref. MEXT-77CGCH, version 1P3 du 02/06/08 that references [SECPHY-DEV] documents:</p> <ul style="list-style-type: none"> <li>- [Equant Security Policy] : «Equant Security Policy», ref. POL-SEC-CS-003, version 3, March 2002</li> <li>- [ESSC – Implementation Solaris] : «ESSC Security standard implementation for Solaris 8, 9 &amp; 10 », ref. ESSC-SESM-SOL-01, version 0.4, 08/08/2007</li> <li>- [NUAR Registration Procedure] : «NUAR Registration Procedure», ref. NA, version 1.2, 11/18/02</li> <li>- [Password Security Policy] : « FT Group Password Security Policy », ref. n.a, version 1.0, 06/29/2005</li> <li>- [Physical Security Controls] : «Photo ID and Facility Access Control Policy», ref. EM-SM-0008, version 1.3, 30/10/07</li> <li>- [ProviderAccess Management] : «Equipment Supplier Access Security Policy», ref. POL-SEC-NS-09, version 2.4, 26/10/07</li> <li>- [Services Basics Learning Programmes] : « Orange Business Services - Services Basics Learning Programme Trainee's Guide », ref. n.a, version 3.0, August 2007</li> <li>- [Third party access Management] : «Third Party Access Security Policy», ref. POL-SEC-NS-11, version 1.6, 30/10/07</li> </ul>
[SECPHY-USER]	<p>« IP VPN Service - Security Policy », ref. POL-SEC-NS-07, version 2.8, July 2006 (see chapter 5.5)</p>

[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)





### Annex 3. Certification references

Decree number 2002-535 dated 18 <sup>th</sup> April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, 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, revision 2, 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, revision 2, 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.