PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2010/16

OmniPCX Enterprise Solution : logiciels OmniPCX Enterprise (release 9.0) et OmniVista 4760 (release 5.0)

Paris, le 7 avril 2010,

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

Patrick Pailloux
[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.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-2010/16**
Nom du produit **OmniPCX Enterprise Solution**
Référence/version du produit **Logiciel OmniPCX Enterprise, release 9.0** **Logiciel OmniVista 4760, release 5.0**
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, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1**
Développeur **Alcatel-Lucent** **32, avenue Kleber, 92707 Colombes, France**
Commanditaire **Alcatel-Lucent** **32, avenue Kleber, 92707 Colombes, 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 :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « OmniPCX Enterprise Solution » composé des logiciels « OmniPCX Enterprise, release 9.0 » et « OmniVista 4760, release 5.0 » développés par Alcatel-Lucent.
Ce produit correspond à une solution de communication intégrée adaptée aux besoins des moyennes et grandes entreprises. Cette solution offre des fonctionnalités de téléphonie traditionnelle, ainsi que de voix sur IP (VoIP).

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
La cible de sécurité s'inspire du profil de protection [PP VoIP].

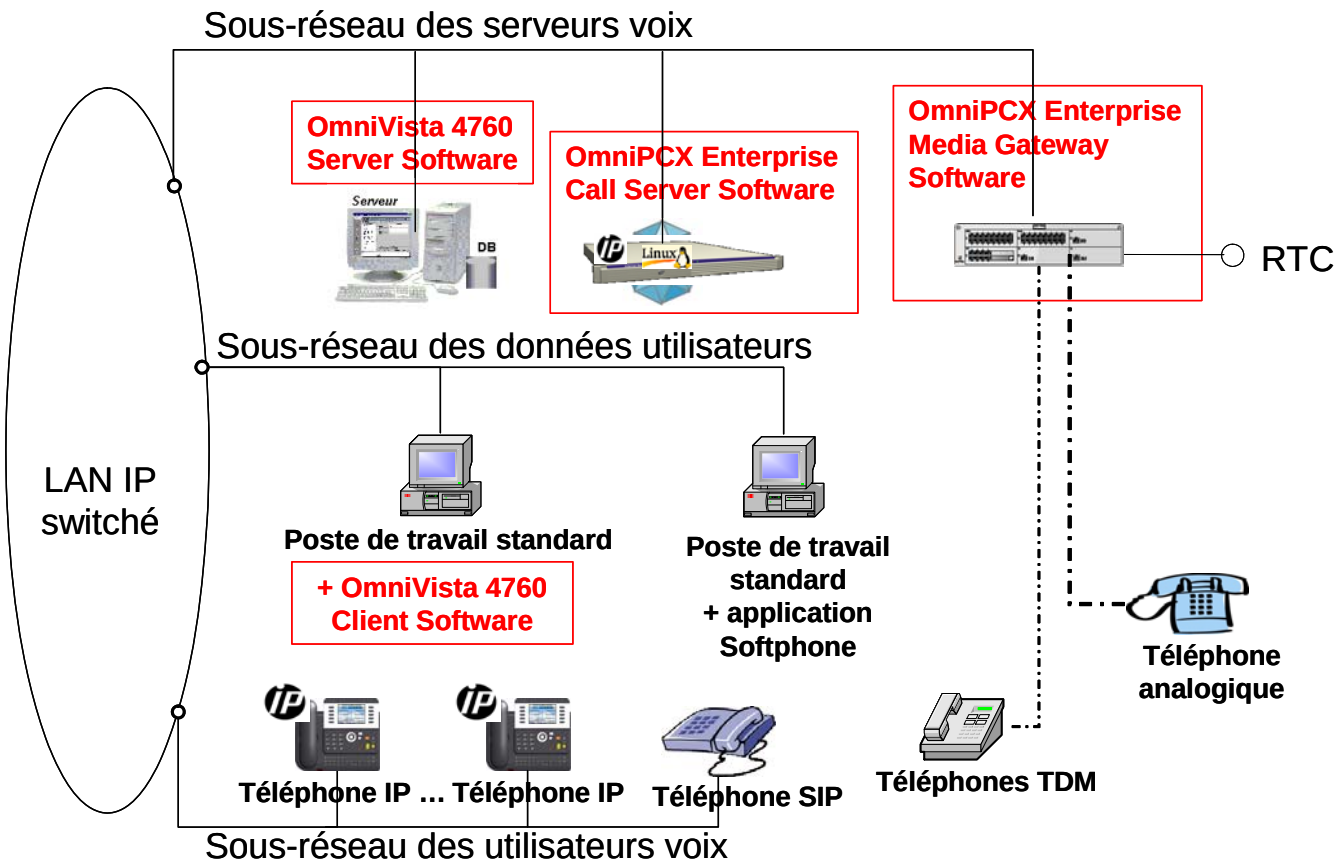
1.2.1. Architecture

Le produit est composé de :

- L'OmniPCX Enterprise, lui-même composé de :
  - L'OmniPCX Enterprise Call Server (ou OXE Call Server), qui fournit les services téléphoniques traditionnels tels que l'appel téléphonique, le transfert d'appel et la messagerie voix, et qui centralise la gestion et la supervision des éléments du système téléphonique présents sur le LAN[1] de l'entreprise comme, par exemple, les téléphones IP ;
  - L'OmniPCX Enterprise Media Gateway (ou OXE Media Gateway), qui correspond à la passerelle entre le monde IP de l'entreprise et le monde RTC[2] public, et permet l'utilisation de téléphones TDM[3] et de téléphones analogiques ;
- L'OmniVista 4760, lui-même composé de :
  - L'OmniVista 4760 Server Software (ou 4760 Server Software), qui correspond à une application permettant d'administrer un ensemble de systèmes OmniPCX Enterprise à partir d'un serveur central ;
  - L'OmniVista 4760 Client Software (ou 4760 Client Software), qui fournit l'interface graphique de OmniVista 4760, cette application cliente pouvant être installée sur le même poste que le serveur.

[1] Local Area Network
[2] Réseau Téléphonique Commuté (ou PSTN, Public Swiched Telephone Network)
[3] Time division multiplexing

La figure suivante identifie les différents éléments du produit (blocs encadrés) ainsi que son architecture de déploiement évaluée.



Pour l'évaluation

- l'ensemble des logiciels de l'OmniPCX Enterprise a été évalué (i.e. l'évaluation a également portée sur le système d'exploitation), la partie matérielle n'ayant pas été prise en compte car ne participant pas à la mise en œuvre des fonctions de sécurité ;
- pour l'OmniVista 4760, seules les applications développées par Alcatel-Lucent ont été évaluées, le système d'exploitation et la partie matérielle ayant été considérés dans l'environnement de l'évaluation, ceux-ci n'intervenant dans les fonctions de sécurité évalués (NB : l'accès aux postes hébergeant les composants de l'OmniVista 4760 n'a pas été évalué).

Les utilisateurs finaux identifiés dans le cadre de cette évaluation correspondent :

- aux administrateurs qui interagissent directement avec le produit ;
- aux utilisateurs d'équipements téléphoniques IP du réseau interne de l'entreprise, les postes téléphoniques considérés correspondant à des téléphones IP, à des téléphones SIP[1] et à des applications logiciels de téléphonie (Softphone) ;
- aux utilisateurs de postes téléphoniques analogiques ou de postes TDM[2] connectés directement sur l'OXE Media Gateway ou depuis le réseau public RTC.

[1] Session Initiation Protocol
[2] Time Division Multiplexing

1.2.2. Services évalués

Les principaux services fournis par le produit sont :

- des services d'appel qui permettent aux utilisateurs de réaliser des appels internes (communications voix sur le réseau IP interne de l'entreprise), d'émettre des appels sortants (vers le réseau public RTC), de recevoir des appels entrants (depuis le réseau public RTC), et de bloquer l'usage de téléphones ; ces services, normalement internes à l'entreprise, peuvent être mis à la disposition des utilisateurs depuis le réseau public RTC grâce au service Direct Inward Service Access (DISA) ;
- des services d'accès à la messagerie voix (pouvant être également mis à disposition des utilisateurs DISA) ;
- des services d'administration qui permettent de gérer les autorisations associées aux équipements téléphoniques et aux utilisateurs des services décrits ci-dessus ; ils offrent notamment un service de contrôle des appels entrants et sortants permettant leurs taxations.

1.2.3. Identification du produit

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

Les versions complètes des composants du produit « OmniPCX Enterprise Solution » certifié sont les suivantes :

- « OmniPCX Enterprise », release 9.0
  - « OXE Call Server software », version H1.301.27.b
  - « OXE Media Gateway software », version H1.301.27.b
- « OmniVista 4760 », release 5.0
  - « 4760 Server software », version 5.0.07.05+ patch M
  - « 4760 Client software », version 5.0.07.05+ patch M

La version certifiée du produit est identifiable par les éléments suivants :

- pour l'OmniVista 4760,
  - la version « 4760.5.0.07.05 » des logiciels client et serveur est affichée à partir l'application du 4760 Client, que cette dernière soit installée sur le 4760 Server ou sur un poste de travail standard, suite à la sélection dans le menu « Help » de l'entrée « About » ;
  - l'identifiant du patch M des logiciels client et serveur « 4760-500705_PatchM_nmc50jar_Client=crms00171182 » est fournie dans la section [4760.5.0.07.05] du fichier « %4760_INSTALL_DIR%\install\patch_history.ini », ce patch M devant correspondre à la dernière version de patch installée ;
- pour l'OmniPCX Enterprise,
  - la release « R9.0 » et la version « H1.301.27.b » de l'OXE Call Server et de l'OXE Media Gateway sont affichées suite à un accès distant SSH[1] depuis le poste accueillant l'application 4760 Server.

[1] Secure Shell

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement de l'OmniVista 4760 est uniquement réalisé sur le site de Chennai en Inde ;
- la majeure partie du développement de l'OmniPCX Enterprise est réalisée sur le site de Chennai. L'internationalisation des IHM est réalisée à Shanghai. Quelques fonctionnalités sont développées en France : la pile SIP à Brest, le BIOS de l'OXE Call Server à Illkirch et le firmware de l'OXE Media Gateway à Colombes ;
- le développement des correctifs (patch) de l'OmniVista 4760 et de l'OmniPCX Enterprise est réalisé sur le site de Chennai ;
- l'ensemble du code source est géré sur le site de Chennai ;
- l'ensemble de la documentation est géré sur le site de Colombes ;
- les logiciels du produit sont tous générés sur le site de Chennai.

Toutes les opérations critiques relatives au développement des logiciels évalués étant réalisées sur les sites de Colombes et Chennai, seuls les sites suivants ont été audités :

ALCATEL-LUCENT COLOMBES

32, avenue Kleber,
92707 Colombes,
France

ALCATEL-LUCENT INDIA LIMITED,

RR Tower III, Plot Super B1,
Thiruvika Industrial Estate, Guindy,
600032 Chennai,
Inde

1.2.5. Configuration évaluée

La plateforme de tests mis en œuvre par le CESTI est représentative de l'architecture de déploiement décrite en 1.2.1.

Les caractéristiques de cette plateforme sont les suivants :

- le LAN et le RTC ont été simulés ;
- l'OmniVista 4760 Server a été installé sur un serveur standard sous Windows XP SP2 ;
- l'OmniVista 4760 Client a été installé sur un poste de travail standard sous Windows XP SP2.

NB : Pour l'OmniPCX Enterprise, Alcatel-Lucent ne disposant que d'une unique configuration matérielle (architecture x86 - 32 bits INTEL), l'identification du logiciel suffit à identifier la configuration matérielle évaluée.

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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 26 mars 2010, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

Le produit ne comporte pas de mécanisme cryptographique.

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas.

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 « OmniPCX Enterprise Solution : logiciels OmniPCX Enterprise, release 9.0 et OmniVista 4760, release 5.0 » 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 produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- le réseau doit être séparé en trois sous-réseaux distincts : un sous-réseau « utilisateurs voix », un sous-réseau « serveurs voix » et un sous-réseau « données utilisateurs ». Les flux autorisés sur, et entre, ces sous-réseaux doivent être contrôlés sur la base des adresses IP et des numéros de port, notamment pour restreindre les flux autorisés vers chacun des composants du produit évalué (OE.SEPARATION_NETWORKS, OE.SOFTPHONE_DATA_USERS_SUBNET) ;
- des revues périodiques de la configuration du produit et des journaux générés par le produit doivent être réalisées (OE.CONFIGURATION_REVIEW, OE.REVIEW_LOGS) ;
- en cas de détection de blocages automatiques du service DISA trop répétés, l'administrateur doit désactiver le service DISA (OE.DISA_DEACTIVATION) ;
- des sauvegardes périodiques de configuration doivent être réalisées (OE.BACKUP) ;
- le sous-réseau « serveurs voix » qui accueille l'OmniPCX Call server, l'OmniVista 4760 Serveur et l'OmniPCX Media Gateway doit être physiquement protégé (OE.SECURE_VOICE_SERVERS_SUBNET) ;
- le sous-réseau « utilisateurs voix » qui accueille les téléphones IP et le sous-réseau « données utilisateurs » qui accueille les applications logicielles de téléphonie et l'OmniVista 4760 Client doivent être physiquement protégés (OE.PROTECTION_VOICE_USERS_SUBNET, OE.SOFTPHONE_DATA_USERS_SUBNET) ;
- les administrateurs doivent être formés à leur fonction (OE.TRAINING) ;
- les administrateurs et tout le personnel disposant de comptes sur les composants du produit doivent être de confiance (OE.TRUSTED_ADMIN) ;
- l'accès au poste sur lequel s'exécute l'OmniVista 4760 Client doit être restreint aux administrateurs de confiance, et ce poste doit être dédié à des fonctions d'administration (OE. PROTECTION_ADMIN_WORKSTATIONS) ;

- les systèmes d'exploitation sur lesquels sont exécutés les logiciels de l'OmniVista 4760 Client et de l'OmniVista 4760 Server doivent être durcis (OE.HARDENING-4760_CLIENT_OS, OE.HARDENING-4760_SERVER_OS) ;
- le mode IPSec tunnel entre les systèmes d'exploitation Windows sur lesquels s'exécutent l'OmniVista 4760 Client et l'OmniVista 4760 Server doit être activé (OE.IPSEC_TUNNEL).

De plus, il est recommandé d'installer le poste accueillant l'OmniVista 4760 Client sur le sous-réseau « serveurs voix » afin de limiter l'accès aux fonctions d'administration à ce sous-réseau.

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		
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2		
	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**	Indentification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3		
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	**1**	Developer vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - « OmniPCX Enterprise Common Criteria Security Target », référence 3EU_29000_0011_DEZZA, version 16 Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « OmniPCX Enterprise R9.0 Common Criteria Security Target », référence 3EU_29000_0019_DEZZA, version 3
[RTE]	Rapport technique d'évaluation : - « Evaluation Technical Report - CALICOT PROJECT », référence OPPIDA/CESTI/CALICOT/RTE, version 1.2
[CONF]	Liste de configuration OmniPCX Enterprise R9.0 - « OmniPCX Enterprise R9.0 : Software switch file », référence 3BA_50239_AAAB_DSZZA, version 6 - « H1.301.27.b read.me file », référence ref. [28] ~dhs3ccom/patch/h1/dyn_h1.301.27.b/read.me Liste de configuration OmniVista 4760 : - « 4760 source code configuration list », référence ref. [27] 4760_5.0.07.05 Liste de configuration documentaire : - « CC/MLE evaluation documentation plan », référence 3EU_29000_0004_AAZZA, version 12
[GUIDES]	Guide d'installation du produit : - « CC/MLE evidence: Installation, generation and start-up », référence 3EU_29000_0023_UUZZA, version 10 Guide d'administration du produit : - « CC/MLE evidence: Administration guidance », référence 3EU_29000_0024_UUZZA, version 12 Guide d'utilisation du produit : - « CC/MLE evidence: User guidance », référence 3EU_29000_0025_UUZZA, version 06
[PP VoIP].	Low Assurance Protection Profile for a Voice over IP Infrastructure, version 1.1, 14 mars 2005 *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0012-2005*

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.