PREMIER MINISTRE

Secretariat General for National Defence

French Network and Information Security Agency

Certification Report ANSSI-CC-2010/15

OmniPCX Enterprise solution : OmniPCX Enterprise (release 9.0) and OmniVista 4760 (release 5.0) softwares

Paris, 7th April 2010,

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 ANSSI (French Network and Information Security Agency), 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
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.anssi@ssi.gouv.fr

Certification report reference **ANSSI-CC-2010/15**
Product name **OmniPCX Enterprise solution**
Product reference and version **OmniPCX Enterprise software, release 9.0** **OmniVista 4760 software, release 5.0**
Protection profile conformity **none**
Evaluation criteria and version **Common Criteria version 2.3** **compliant with ISO 15408:2005**
Evaluation level **EAL 2 augmented** **ADV_HLD.2, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1, VLA.2**
Developer **Alcatel-Lucent** **32 avenue Kleber, 92707 Colombes, France**
Sponsor **Alcatel-Lucent** **32 avenue Kleber, 92707 Colombes, France**
Evaluation facility **Oppida** **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France** **Phone: +33 (0)1 30 14 19 00, email : cesti@oppida.fr**

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 French Network and Information Security Agency 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 sponsors 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.

Content

1. The product

1.1. Presentation of the product

The evaluated product is the "OmniPCX Enterprise solution", composed of the "OmniPCX Enterprise software" release 9.0 and the "OmniVista 4760 software" release 5.0, developed by Alcatel-Lucent.
This product is an integrated communications solution for medium-sized businesses and large corporations. The solution combines traditional telephone functions with support for Internet-based telephony (VoIP).

1.2. Evaluated product description

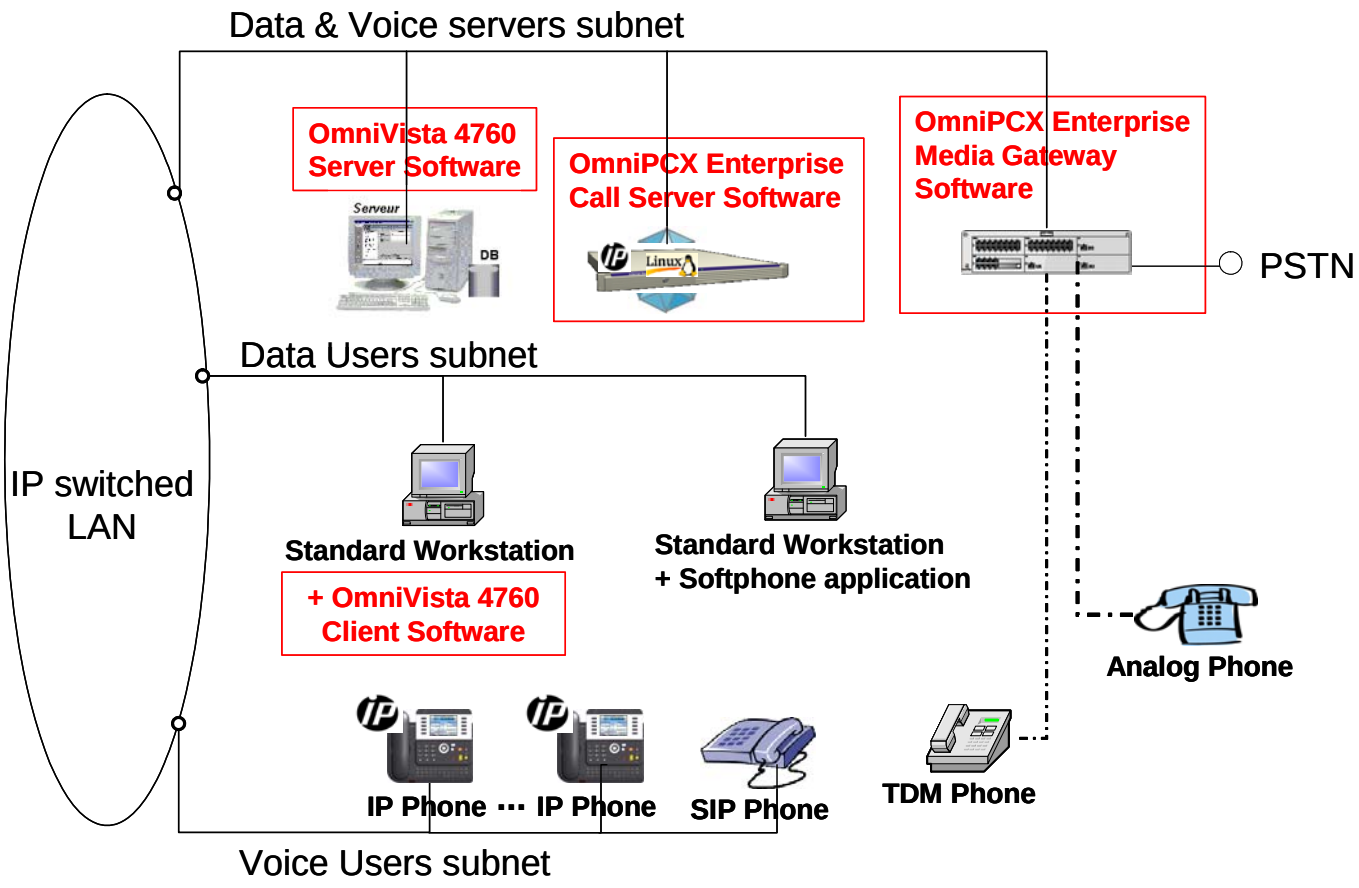
The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.
The security target is based on [PP VoIP].

1.2.1. Architecture

The TOE is composed of:
- The OmniPCX Enterprise System, itself composed of
    - The OmniPCX Enterprise Call Server (OXE Call Server) which provides the telephonic services such as call switching and voice mail application, it centralizes the management and monitoring of the accompanying telephonic elements on the enterprise LAN[1] such as IP phones for example
    - The OmniPCX Enterprise Media Gateway (OXE Media Gateway) which is the gateway between the IP world and the traditional PSTN[2] world and supports digital (TDM) and/or analog phones;
- The OmniVista 4760, itself composed of
    - The OmniVista 4760 Server Software (4760 Server Software) which is an application enabling to administer a set of Alcatel-Lucent OmniPCX Enterprise systems from one central server
    - The OmniVista 4760 Client Software (4760 Client Software) which provides the User Interface of the OmniVista 4760

[1] Local Area Network
[2] Public Swiched Telephone Network

The following figure identifies the different part of the product (framed blocs), and also its evaluated deployment.



For this evaluation:

- All the OmniPCX Enterprise software have been considered (the evaluation also took into account the operating system), only the hardware has been considered out of the scope of the evaluation as it doesn't contribute to the evaluated security functions;
- For the OmniVista 4760, only the applications developed by Alcatel-Lucent have been considered, the operating system and the hardware have been considered in the TOE environment as they don't contribute to the evaluated security functions (NB access to the workstation hosting the OmniVista 4760 components haven't been evaluated).

End users considered in this evaluation are

- Telephony administrators who directly interact with the product;
- Users of IP handsets connected to the enterprise internal network, the different type of handsets considered are IP Phones, SIP phones and Softphone applications;
- Users of analogs and TDM phones directly connected to the OXE Media Gateway or from the PSTN.

1.2.2. Evaluated services

The product provides mainly the following services:

- Call services which enable voice communications over the IP networks of the company as well as incoming calls (from the public network) and outgoing calls (to the public network); those services usually internal to the enterprise could be available from the public network PSTN with DISA[1] service;
- Access to voice mail services (also available for the DISA authorized users)
- Telephony Administration services which enable to manage IP phones sets and users of the previous services, they provide a calls control service of the incoming and outgoing calls that permit their accounting.

1.2.3. Product identification

The configuration list [CONF] identifies the product's constituent elements.

The full versions of the components of the certified product « OmniPCX Enterprise solution » are the followings:

- "OmniPCX enterprise", release 9.0
  - "OXE Call Server software", release H1.301.27.b
  - "OXE Media Gateway software", release H1.301.27.b
- "OmniVista 4760", release 5.0
  - "4760 Server software", release 5.0.07.05+ patch M
  - "4760 Client software", release 5.0.07.05+ patch M

The certified version of the product can be identified by the following elements:

- for OmniVista 4760,
  - the software version "4760.5.0.07.05" of both the client and server software is displayed from the 4760 Client application, whether this application is installed on the OmniVista 4760 Server or on a standard workstation, when selecting the "About" entry of the "Help" menu;
  - the patch identifier "4760-500705_PatchM_nmc50jar_Client=crms00171182" of the patch M of both client and server software is available in the [4760.5.0.07.05] section of the "%4760_INSTALL_DIR%\install\patch_history.ini" file; this patch M should be the latest patch installed;
- for OmniPCX Enterprise,
  - the release« R9.0 » and the version « H1.301.27.b » of the OXE Call Server and the OXE Media Gateway are displayed after a successful SSH[2] remote access from the workstation hosting the 4760 Server application

[1] Direct Inward Service Access
[2] Secure Shell

1.2.4. Life cycle

The product's life cycle is organised as follow

- Development of the OmniVista 4760 is only realised in Chennai, India;
- Most of the development of the OmniPCX Enterprise is done in Chennai. Internationalization of the GUI is developed in Shanghai. A few features are developed and supported in French R&D centers, for example: SIP stack in Brest, CS BIOS in Illkirch, Media Gateway firmware in Colombes;
- Support (patch development) of the OmniVista 4760 and OmniPCX Enterprise is only done in Chennai;
- Source code repository is donne in Chennai;
- Document repository is done in Colombes;
- Software's are all generated in Chennai.

As all critical operation related to the development of the evaluated softwares are done in Colombes and Chennai sites, only the following sites have been audited:

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,
India

1.2.5. Evaluated configuration

The testing platform used by the ITSEF is representative of the architecture described in the 1.2.1 section.

ITSEF's testing platform characteristics are the following:

- Both the LAN and the PSTN have been simulated;
- The OmniVista 4760 Server was running on a standard server with Windows XP SP2 running
- The OmniVista 4760 Client was running on a standard workstation with Windows XP SP2 running

NB : For the OmniPCX Enterprise, as only one hardware configuration (x86- - 32 bits INTEL based hardware) is delivered by Alcatel-Lucent, the software identification is sufficient to identify the hardware evaluated configuration

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC] and with the Common Evaluation Methodology [CEM].

2.2. Evaluation work

The evaluation technical report [ETR], delivered to ANSSI the 26th March 2010, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The product doesn't provide cryptographic mechanisms:

2.4. Random number generator analysis

The product doesn't provide Random number generator.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality of 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 product « OmniPCX Enterprise solution » : « OmniPCX enterprise » release 9.0 and « OmniVista 4760 » release 5.0, 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 product specified in chapter 1.2 of this certification report.

The user of the certified product shall respect the security objectives for the operational environment specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- The network must be separated in three different subnets: Voice servers / Voice users / Data users. The flows transmitted between these subnets must be controlled, based on IP address and port number, in order to restrict the authorised flows to the different elements of the product (OE.SEPARATION_NETWORKS, OE.SOFTPHONE_DATA_USERS_SUBNET)
- Periodic review of the configuration of the product elements and of the logs generated by the product must be performed (OE.CONFIGURATION_REVIEW, OE.REVIEW_LOGS);
- In case of recurring DISA authentication failures, the administrator must deactivate the DISA service (OE.DISA_DEACTIVATION);
- Periodic configuration backup must be performed (OE.BACKUP)
- The Voice Servers subnet, which have to host the OmniPCX Call Server, the OmniVista 4760 Serveur and the OmniPCX Media Gateway must be physically protected (OE.SECURE_VOICE_SERVERS_SUBNET);
- The Voice Users subnet which have to host the IP handsets and the Data Users subnet which have to host the Softphoe application must be physically protected (OE.PROTECTION_VOICE_USERS_SUBNET, OE.SOFTPHONE_DATA_USERS_SUBNET);
- Administrators must be trained to achieve their role (OE.TRAINING);
- Administrators and all personnel having an account on the product elements have to be trust (OE.TRUSTED_ADMIN);
- Access to the workstation on which the OmniVista 4760 Client runs must be restricted to trusted administrators, this workstation must be dedicated to administration functions (OE. PROTECTION_ADMIN_WORKSTATIONS);

- The operating systems on which the OmniVista 4760 Client and theOmniVista 4760 Server softwares are running must be hardened (OE.HARDENING-4760_CLIENT_OS, OE.HARDENING-4760_SERVER_OS);
- The Microsoft Windows IPSEC tunnel between the 4760 Server and the 4760 Client must be activated (OE.IPSEC_TUNNEL).

It is also recommended to install the workstation hosting the OmniVista 4760 Client software on the Voice Servers subnet in order to restrict the administrative function to that subnet.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 2+	Name of the component
ACM Configuration management	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 Delivery and operation	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 Development	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 Guidance	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 Life-cycle support	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**	Independant testing – sample
AVA Vulnerability assessment	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Examination of guidance
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - « OmniPCX Enterprise Common Criteria Security Target », reference 3EU_29000_0011_DEZZA, version 16 For the needs of publication, the following security target has been provided and validated in the evaluation: - « OmniPCX Enterprise R9.0 Common Criteria Security Target », reference 3EU_29000_0019_DEZZA, version 3
[ETR]	Evaluation technical report : - « Evaluation Technical Report - CALICOT PROJECT », reference OPPIDA/CESTI/CALICOT/RTE, version 1.2
[CONF]	OmniPCX Enterprise configuration list : - « OmniPCX Enterprise R9.0 : Software switch file », reference 3BA_50239_AAAB_DSZZA, version 6 - « H1.301.27.b read.me file », reference ref. [28] ~dhs3ccom/patch/h1/dyn_h1.301.27.b/read.me OmniVista 4760 configuration list : - « 4760 source code configuration list », reference ref. [27] 4760_5.0.07.05 Documentation configuration list : - « CC/MLE evaluation documentation plan », reference 3EU_29000_0004_AAZZA, version 12
[GUIDES]	Installation guidance: - « CC/MLE evidence: Installation, generation and start-up », reference 3EU_29000_0023_UUZZA, version 10 Administration guidance: - « CC/MLE evidence: Administration guidance », reference 3EU_29000_0024_UUZZA, version 12 User guidance: - « CC/MLE evidence: User guidance », reference 3EU_29000_0025_UUZZA, version 06
[PP VoIP].	Low Assurance Protection Profile for a Voice over IP Infrastructure, version 1.1, 14th March 2005 *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under refernce BSI-PP-0012-2005*

Annex 3. Certification references

Decree number 2002-535 dated 18th 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, 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. The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of CEM version 2.3 is identical to the international ISO/IEC 18045:2005.