OmniPCX Enterprise Common Criteria Security Target

ALCATEL-LUCENT
Enterprise Product Group
March 2010

Ref: 3EU_29000_0019_DEZZA_03

Table of Content

1. ST introduction

1.1 ST reference

Title: CC/MLE: public version of the Security Target

Reference: 3EU_29000_0019_DEZZA

Author: Alcatel-Lucent.

Evaluation assurance level: EAL2 augmented with ADV_HLD.2, ALC_DVS.1, ALC_FLR.3, AVA.MSU.1, AVA_VLA.1.

1.2 CC conformance claim

This security target and the evaluation that will be performed on the TOE are compliant with requirements of the ISO/IEC 15408:2005 standard (Common Criteria version 2.3). [CC]

1.3 TOE reference

The commercial name of the TOE is OmniPCX Enterprise solution including the OmniPCX enterprise release 9.0 and the 4760 release 5.0.

The OmniPCX Enterprise software (release 9.0 like any other release) is composed of both the OmniPCX Enterprise Call Server software and the OmniPCX Enterprise Media Gateway software.

The OmniVista 4760 software (release 5.0 like any other release) is composed of both the OmniVista 4760 Server software and the OmniVista 4760 client software.

The TOE specific versions are:

TOE component	Software release
OmniPCX Enterprise	
Call Server software	H1.301.27.b
Media Gateway software	H1.301.27.b
OmniVista 4760	
Server software	R5.0.07.05+PatchM
Client software	R5.0.07.05+PatchM

1.4 TOE overview

The Alcatel-Lucent OmniPCX Enterprise solution is an integrated, interactive communications solution for medium-sized businesses and large corporations. The solution combines traditional telephone functions with support for Internet-based telephony (VoIP).

The objective of this evaluation is to assess the confidence an owner can have that a properly configured system is protected against toll theft from unauthorized users and that this risk won't increase over time when properly administered. To this effect the evaluation will focus specifically on the new risk represented by IP phones and their users to ensure that:

- The TOE can enforce an access policy to the phone network and additional services;
- Access control policy to the TOE configuration information can be enforced;

The TOE provides the following key services:

1.4.1 Call services

The Alcatel-Lucent OmniPCX Enterprise solution enables 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).

The call services are also available for the users allowed access to Direct Inward Service Access (DISA). The DISA service allows a caller external to the OmniPCX Enterprise to use telephone services that are normally reserved to internal users.

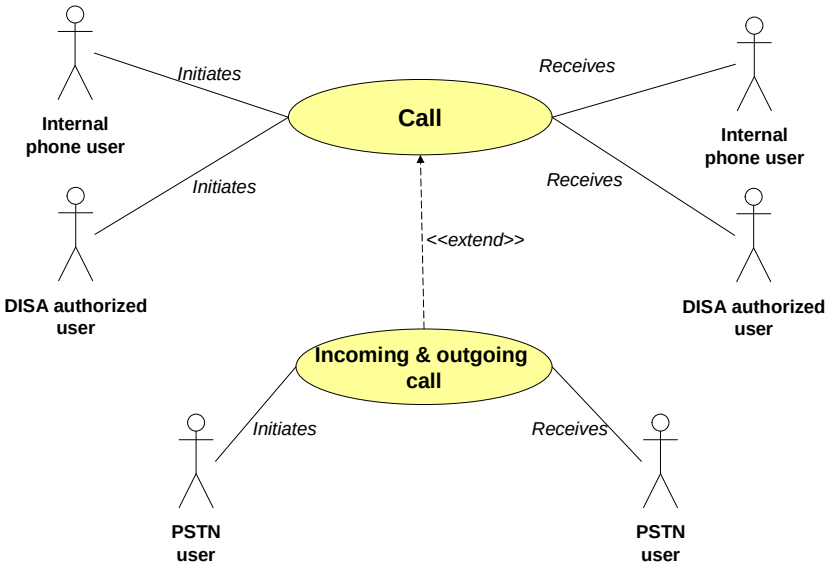

Figure 1 Call services UML use case diagram

Sensitive data handled for the Call services are: *users' conversations, phone calls information (source, destination, date,…)*.

1.4.2 Access to voice mail services

Voice mail services are offered on the OmniPCX Enterprise solution.

The voice mail services are also available for the DISA authorized users.

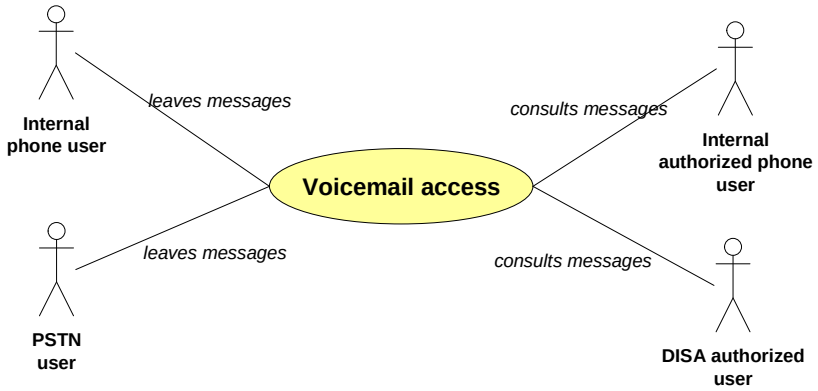

Figure 2 Voice mail services UML use case diagram

Sensitive data handled for the Voice mail services are: *voice mail messages*.

1.4.3 Telephony Administration services

Several administration services are provided by the OmniPCX Enterprise solution. For the security target, the only role operating these services is the telephony administrator. In operation, it is possible to share responsibilities and to split the telephony administrator profile into several profiles.

1.4.3.1 Users management

The telephony administrator can manage lists of IP phones sets and list of users.

1.4.3.2 Calls control

Controls can be set for all calls. Calls control services include:

Incoming and Outgoing Call Control

Various OmniPCX Enterprise services enable incoming calls (from the public network) and outgoing calls (to the public network) to be monitored. These services are based on use of the following mechanisms:

1. Connection Classes of Service (COS), used to allow or prohibit calls between terminations (sets and trunks). In the OmniPCX Enterprise, each termination (set or trunk) has a Connection COS. A table (that can be configured) specifies, for each COS, the COSs to which a call is authorized to be made.

2. Transfer Classes of Service, which is based on the same principle as Connection Classes of Service. For each COS, a table specifies the COSs to which call transfer is authorized.

3. External access COSs (Public network access COSs), used to authorize or prohibit outgoing calls according to their destination (call restrictions/discrimination). Call restrictions (discrimination) are based on analysis of the first digits dialed by the user to determine call type. Depending on the number requested and system status (day, night, etc.), the call may be accepted or not.

DISA Call Control

A class of incoming calls may be subject to specific monitoring. This is the case for calls using the DISA service.

1.4.3.3 Monitoring Call Costs

Using the OmniPCX Enterprise Accounting application, any call (incoming, outgoing, internal, transit) may be the subject of a cost record. Analysis of the data contained in the record allows OmniPCX Enterprise calls to be checked.

Accounting offers various types of monitoring:

1. Monitoring over a specific period: Records are stored in a database for subsequent processing (financial report or external accounting).

2. Permanent monitoring (or real-time printout): Records are progressively printed as calls are completed. This gives an immediate view of call flow.

3. Targeted monitoring: Records are supervised by an attendant according to a specific filter (user, user group, number of charge units, call duration, etc.). The results are output to a printer.

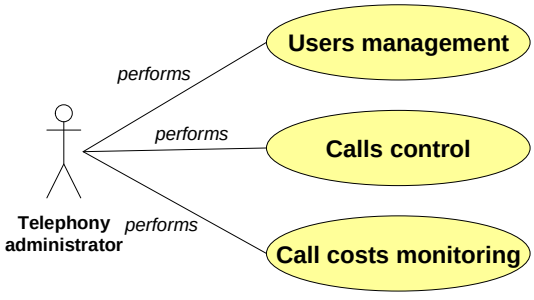

Figure 3 Administration services UML use case diagram

Sensitive data handled for the Administration services are: *configuration data, phone calls information (source, destination, date,…).*

2. TOE description

2.1 TOE elements

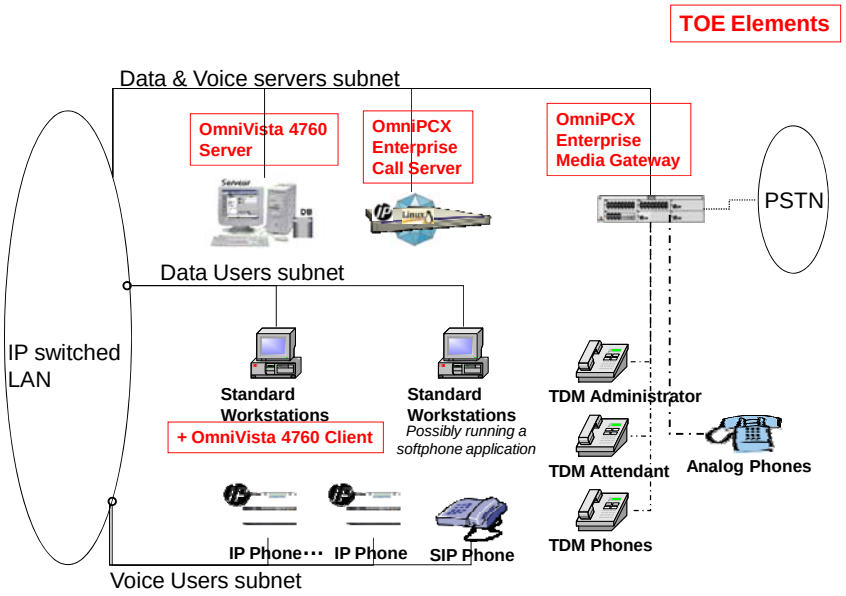

Figure 4 TOE elements

The TOE is composed of:

- The OmniPCX Enterprise Call server:

  The Call Server provides the telephonic services (call switching, 4645 voice mail application etc…) and centralizes the management and monitoring of the accompanying network elements (IP phones, Media Gateway).

  Configuration of services and network elements is performed on the Call Server using the Alcatel-Lucent OmniVista 4760 management platform. It can also be performed through a command line application accessed locally through a serial console or remotely through the LAN.

  The Call Server is an application suite running on an x86-based hardware architecture. Its operating system is based on a hardened Linux kernel with extensions to support real-time constraints and integrating the latest security patches. The run-time execution environment contains the minimal set of standard Linux services.

  The Call server is located on the Voice Servers subnet.

Call server key services and related TSF are provided by software only, therefore the OmniPCX hardware is out of the scope of the TOE.

- The OmniPCX Enterprise Media gateway:

  The media gateway is the gateway between the IP world and the traditional PSTN world and supports digital (TDM) and/or analog phones.

  Running on an x86 architecture its operating system is based on a hardened real-time Linux kernel kept up to date with the latest security patches[1].

  The Media gateway supports 2 different classes of physical interfaces:
  a) Analog and digital trunks connected to PSTN network and/or other PBXs;
  b) Analog and digital end-points (phones and faxes) giving end-users access to the offered services.

  The Media gateway is located on the Voice Servers subnet.

  Media gateway key services and related TSF are provided by software only, therefore the OmniPCX hardware is out of the scope of the TOE.

- The OmniVista 4760 Server:

  The OmniVista 4760 is an application suite enabling a telephony administrator to administer a set of Alcatel-Lucent OmniPCX Enterprise systems from one central OmniVista 4760 server.

  A single OmniVista 4760 server can administer many thousands of OmniPCX Enterprise systems working either in standalone mode or organized to form one or more network of PBXs. Communications between the OmniVista 4760 Server and one OmniPCX Enterprise system is carried over IP to the Call Servers component of the OmniPCX Enterprise system using the SSH, SFTP and CMIP protocols.

  The global architecture of the OmniVista 4760 product is a client/server architecture, whose server part is installed on Microsoft Windows Server 2003 and can support several OmniVista 4760 clients.

  The application suite comprises many modules:
  - The Enterprise directory
  - The PCX configuration, or network of PCXs
  - The Taxation, Observation of traffic and Channel on IP
  - The Taxation report
  - The Alarm management

[1] The OmniPCX security developer of the project analyses the security alert. When an alert impacts it, the matching security patch is included into the OmniPCX source environment, so that next production will integrate the patch. Business Partners are constantly aware of new delivered patches and will perform all the necessary update operation.

- The PCXs topology and PCXs network
- A Job scheduler
- A Maintenance tool for backup and restoration of databases

The OmniVista 4760 Server is located on the Voice Servers subnet.

PC hardware and Windows 2003 running OmniVista 4760 Server have no relation with the TSF “access to telephony administration”. Therefore OmniVista 4760 Server PC hardware and Windows 2003 operating system are not part of the TOE.

- The OmniVista 4760 Client:

  The 4760 Client application provides the User Interface of the OmniVista 4760 product. It can be installed on many types of Windows systems.

  The OmniVista 4760 Client is located on the Data Users subnet.

  PC hardware and Windows operating system running OmniVista 4760 Client have no relation with the TSF “access to telephony administration”. Therefore OmniVista 4760 Client PC hardware and the Windows operating system are not part of the TOE.

Calls can also be done using software applications installed on workstations (“softphone applications”).

The proprietary phones (either IP or digital) or softphones are very basic: all telephonic processing is done on the Call Server. The phone sets send simple hook and keypress events to the Call Server and receive from it display and media commands by mean of the proprietary NOE protocol over IP for IPTouch phones and UA protocol over twisted pair for TDM phones. Media flows over IP occur directly over the RTP protocol with the other communication endpoint. The phone sets and the softphone applications are therefore out of the scope of the TOE.

All the elements of the TOE are interconnected by an IP based LAN. For the evaluation, the IP network is divided in three different IP subnets interconnected by a network infrastructure element working at layer 3 of the ISO OSI model. The Voice and Data endpoints are isolated in distinct IP subnetworks. Likewise the servers are in their own IP subnet as well.

The three subnets are the following:

a) The Voice Servers subnet including the Call server, the media gateways and the 4760 server;

b) The Voice Users subnet including the IP phones;

c) The Data Users subnet including the users' workstations. Some of these workstations will run instances of the OmniVista 4760 client application used for the administration of the telephony.

The interconnecting network elements control the flows exchanged between the subnets and routes only authorized flows (see A.SEPARATION_NETWORKS).

2.2 Roles

2.2.1 Internal authorized IP phones users

The internal authorized users are the users initiating and receiving calls through their IP phones.

2.2.2 DISA authorized users

The DISA authorized users are the users allowed to use the DISA service to access Call services and Voice mail services from a public phone accessing the enterprise phone system over the PSTN network.

2.2.3 Telephony administrators

The telephony administrators are in charge of the maintenance of the telephony network, telephony user database, and telephony facilities and services.

They are also responsible for applications as enterprise directory maintenance, accounting management, accounting reports, and telephony network or traffic supervision.

The telephony administrator uses the OmniVista 4760 client or the serial console of the equipments to perform its activities.

2.3 Description of services provided by the TOE elements

2.3.1 Call services

A basic phone-to-phone call is performed in 4 steps:

- Phone unlocking: anyone can pickup the phone handset and dial any emergency number whether the phone has been locked or not (P.PHONE_LOCK). On phone whose locking mechanism has not been activated anyone can dial any phone number. On phones whose locking mechanism has been activated the user picking up the handset has first to enter the phone unlock password before dialing a non-emergency number.

– Call setup: the calling party phone set sends to the Call Server the information identifying (phone number) the called party. The Call Server controls the right (P.CALL_CONTROL) for the calling party to call the called party and if authorized rings the called party phone set. After the called party goes off hook the Call Server sends back to the calling party a command to establish a voice channel directly with the called party. A reciprocal command is sent to the called party identifying the calling party.

– Communication: If both parties are IP phones, a direct full-duplex voice channel is established between them. This direct full-duplex voice channel is established with a media-gateway converting the media stream if one of the parties is over the PSTN network or an internal digital or analog phone connected to this media-gateway. The Call Server is not involved during this phase of the phone communication.

– Call teardown: the Call Server is informed whenever one of the parties hangs up. The Call Server then sends to both parties commands to tear down the voice channel.

DISA authorized users appear as being located on the PSTN with the same calling rights as if calling from their allocated phone set.

2.3.2 Voice mail services

The 4645 Voice mail system stores voice mail messages on the Call server. Read access to the voice mails is performed using the phone sets.

DISA authorized users can also access their Voice mail messages from PSTN as if calling from their allocated phone set.

2.3.3 Administration services

The administration of the Call server can be performed through command line interface or through the OmniVista 4760 solution.

The command line interface can be used either locally or remotely. Local access to the command line interface is done through use of the Call Server serial console[2].

Remote access to the command line interface is done through one of these means:

- modem connected to the serial line. This can only be used temporarily for a specific intervention for a limited time. Modem and its connections shall be removed once the intervention is finished. Standard security measures have to be used (e.g. callback). **This configuration is not part of the TOE.**

- telnet connection over IP. This is possible only when the Call Server is explicitly configured to allow unsecured management connections. By default the Call Server allows only

[2] Shall respect the security constraints: in local physically protected.

secured remote console access, this is the configuration recommended by Alcatel. **This configuration is not part of the TOE.**

- SSH connection over IP. By default the Call Server only accepts secured remote console connections. The preferred configuration and management interface is through the OmniVista 4760 application and use of remote console connection –even secured- is allowed only coming from the OmniVista 4760 server. **This is the configuration supported by the TOE.**

- eRMA service over a PSTN connection: either an incoming data connection over ISDN or over an analog phone line a modem on the remote site can attempt a PPP connection only when explicitly allowed in the Call Server configuration. This service is turned off by default. Same precaution recommendations as for modem use apply when this service is used (see above). **For the evaluation, the eRMA service is not activated.**

3. TOE Security environment

3.1 Assets and security needs

The TOE services and sensitive data identified in chap. 1 are the assets to be protected.

3.1.1 Security needs for services

	Availability	Integrity	Confidentiality
Call services	X		
Voice mail services	X	X	
Administration services		X	

In addition, it is important that the telephony infrastructure can not be used as an entry point for the internal IP network. Therefore it can be considered that all the services provided by the other elements of the internal IP network are also assets to be protected in integrity.

3.1.2 Security needs for sensitive data

	Availability	Integrity	Confidentiality
Users' conversations	X		
Phone calls information (source, destination, date,…)	X	X	
Voice mail messages	X	X	X
Telephony configuration data	X	X	

Traditional telephony technologies like TDM and analog phones did provide a level of communication confidentiality and integrity deemed sufficient for many years by carrying the user's

conversation on a specific wiring and enclosed in locked cabinets. With these technologies, a malicious person having a physical access to the phone cables could perform illicit actions such as impersonating the users or tapping the communications.

VoIP technology offers the same level of security (confidentiality and integrity) provided some good practices are obeyed: proper dimensioning of the network elements carrying Voice users subnet traffic, layer 2 and 3 switches carrying the Voice Users subnet traffic are enclosed in locked cabinets, those layer 2 switches are resilient to MAC flooding attacks that otherwise would make them behave like Ethernet hubs.

With those practices enforced, users' conversations made with the TOE benefit from the same level of confidentiality and integrity as provided by a traditional PBX system. Where aggravated risks against communication confidentiality are identified Alcatel-Lucent provides additional confidentiality solution with Security Modules that are out of the scope of the TOE.

3.2 Assumptions

3.2.1 Assumptions about the architecture

A.SEPARATION_NETWORKS

The network is separated in three different subnets: Voice servers / Voice users / Data users. The flows are transmitted between these subnets by network equipments (routers, switches) according to the standard IP routing principles. Additional control may be exercised by using additional features sometimes found in switches, routers or using specific equipment (firewalls).

A.SOFTPHONE_DATA_USERS_SUBNET

Softphones, when deployed, are connected to the data users subnet like any other data workstations.

3.2.2 Assumptions about the Voice Server subnet

A.SECURE_VOICE_SERVERS_SUBNET

The Voice Servers subnet is located in a physically secured location. Physical access to the cables and to the equipments is controlled and restricted preventing any tampering. The Call server, its serial console, the 4760 Server and the Media gateway are installed in this secured location.

3.2.3 Assumptions about the Voice Users subnet

A.PROTECTION_VOICE_USERS_SUBNET

Good practices for the protection of “traditional” telephony networks are applied. Network elements carrying voice traffic are enclosed in locked cabinets.

Attacks from malicious persons having a physical access to the Voice users subnet are out of the scope of the security target because it has been considered that the VoIP technology is deployed in an environment following the good practices.

For the VoIP technology, additional products are available to counter such attacks (e.g. 802.1x authentication of the VoIP terminal plugged into the Voice Users subnet). These products are out of the scope of the TOE.

3.2.4 Assumption about the 4760 installation

A.FALSIFICATION_OF_DATA

A malicious person having access to the Data User subnet cannot modify (e.g. by forging or replaying data) or delete the configuration data exchanged between the 4760 client and the 4760 server because an IPSEC tunnel is operated between the client and the server.

A.PROTECTION_ADMIN_WORKSTATIONS

A malicious person cannot physically access any workstation used by telephony administrators because physical access to those workstations is permanently restricted.

3.2.5 Assumptions about the Telephony administrators

A.TRAINING

Telephony administrators are trained and do not performs mistakes when configuring the system.

A.TRUSTED_ADMIN

Telephony administrators are trusted and do not perform illicit acts such as unauthorized modification of configuration parameters, installation of illicit programs or deletion of activity logs.

3.3 Threats

For the evaluation, the following profiles are considered as potential attackers of the TOE:

- Malicious internal user = malicious persons (authorized users or persons having a temporary physical access) having access to a workstation connected to the Data User subnet;

- Malicious external user = malicious persons connected to PSTN.

Both attacker profiles are characterized by a good general knowledge in computers, relatively sparse resources available (computing and bandwidth), lack of intimate knowledge of the working of the TOE. The profiles may have access to the documentation delivered to Alcatel-Lucent Business Partners.

Their have a moderate motivation: mostly tax avoidance or theft, more rarely denial of service on the attacked TOE (for example to retaliate or lowering the victim company's public image in case of disgruntled former employee). Likewise access to confidential information is seldom the motive as this can be accomplished by better known and more easily deployed means (e.g. wiretapping).

Specifically the malicious external user has all its accesses to PSTN mediated through a carrier by using a phone or a modem: it has not direct access to the PSTN trunks entering the PBX and thus cannot craft ISDN packets thanks to physical security of trunks and communication lines implemented by the carrier.

3.3.1 Network intrusion

T.INTERNAL_NETWORK_INTRUSION

A malicious person having access to the Data User subnet gains illicit access to the Call server, to the media gateways or to the 4760 server in order to alter their functionality, to modify handled sensitive data or to try to gain illicit access to another element (servers, workstations) of the internal networks.

T.EXTERNAL_NETWORK_INTRUSION

A malicious person connected to PSTN gains illicit access to the Call server, to the media gateways or to the 4760 server in order to alter their functionality, to modify handled sensitive data or to try to gain illicit access to another element (servers, workstations) of the internal networks.

3.3.2 Denial of Service

T.INTERNAL_SYSTEM_FLOODING

A malicious person having access to the Data User subnet sends an abnormal amount of requests to the OmniPCX Enterprise Call Server or OmniVista applications or to the other services running on the TOE elements in order to perform a denial of service of the equipment.

T.EXTERNAL_SYSTEM_FLOODING

A malicious person connected to PSTN sends an abnormal amount of requests to the OmniPCX Enterprise Media Gateway, targeting call and/or voice mail services, in order to perform a denial of service of the equipment.

3.3.3 Threats related to the Telephony administrators

T.USURPATION_OF_ACCESS_RIGHTS-TELEPHONY_ADMIN

A malicious person having access to the Data user subnet impersonates an authorized telephony administrator in order to use his access rights to perform illicit acts (unauthorized access to information, unauthorized modification of services configuration parameters).

3.3.4 Threats related to the DISA authorized users

T.USURPATION_OF_ACCESS_RIGHTS-DISA_USERS

A malicious person connected to PSTN networks impersonates an authorized DISA user in order to illicitly use his services (calls, voice mail,…).

3.4 Organizational security policy

3.4.1 Evaluation requirements

None

3.4.2 Security services provided by the TOE

P.CALL_CONTROL

The telephony administrator must be able to define and to manage list of telephone number that can communicates together (call baring).

The TOE must also provide the capability to record calls information for audit purpose or for costs monitoring purpose.

P.VOICEMAIL_ACCESS_CONTROL

The access to the Voice mails must be controlled and limited to the owner of the voice mail.

P.PHONE_LOCK

The users must be able to lock their phone set to forbid another person to use the phone set to perform outgoing calls.

4. Security objectives

4.1 Security objectives for the TOE

4.1.1 Security objectives for the Call Server

OT.IDENTIFICATION_AUTHENTICATION-DISA_USERS

The TOE shall identify and authenticate the DISA users before allowing any action.

OT.ACCESS_CONTROL-DISA_USERS

The TOE shall restrict the DISA access to authenticated DISA users.

OT.IDENTIFICATION_AUTHENTICATION-VOICEMAIL

The TOE shall identify and authenticate the Voice mail users.

OT.ACCESS_CONTROL-VOICEMAIL

The TOE shall restrict the access to the Voice mail.

OT.HARDENING-CALL_SERVER_APPLICATION

The call server application must be hardened in order to avoid any network tampering or denial of service.

OT.HARDENING-CALL_SERVER_OS

The operating system on which the Call server is running and the other services running on the server must be hardened in order to avoid any network tampering or denial of service of the equipments.

OT.ACCESS_CONTROL-SSH

The TOE shall restrict the access to the command line administration interface (SSH) to the OmniVista 4760 server.

OT.ACCOUNTING-TELEPHONY_ADMIN

The TOE shall record the telephony administrator's actions on the call server.

OT.CALL_CONTROL

The telephony administrator must be able to define and to manage list of telephone numbers that can communicate together.

OT.ACCOUNTING-DISA

The TOE shall record the DISA access activity and generate an alarm in case of repetition of authentication failures.

OT.ACCOUNTING-CALLS

The TOE shall record the calls information.

OT.PHONE_LOCK

The users must be able to lock their phone set to forbid another person to use the phone set to perform outgoing calls.

4.1.2 Security objectives for the Media gateways

OT.HARDENING-MEDIA_GW_APPLICATION

The media gateways application must be hardened in order to avoid any network tampering or denial of service.

OT.HARDENING-MEDIA_GW_OS

The operating system on which the media gateways are running and the other services running on the gateways must be hardened in order to avoid any network tampering or denial of service of the equipments.

4.1.3 Security objectives for the 4760 Server

OT.IDENTIFICATION_AUTHENTICATION-TELEPHONY_ADMIN

The TOE shall identify and authenticate the telephony administrators before allowing any action.

OT.ACCESS_CONTROL-TELEPHONY_ADMIN

The TOE shall restrict the access to the telephony administration functions to authenticated telephony administrators.

4.1.4 Security objectives for the Evaluation

None

4.2 Security objectives for the environment

4.2.1 Security objectives for the architecture

OE.SEPARATION_NETWORKS

The network must be separated in three different subnets: Voice servers / Voice users / Data users. The flows transmitted between these subnets must be controlled by network equipments (routers, switches) in order to stop a subset of inter-subnet network attacks (e.g. spoofing).

The authorized IP flows on the **voice users subnet** are:

- Signaling flows between the phone sets and the OXE Call Server;
- Media flows between the phone sets (internal phone calls), between the phone sets and the media gateway (PSTN calls or calls with DECT phones and other non-IP phones like TDM phones), between the phone sets and the OXE Call Server during recording and playback of voice messages.

The authorized IP flows on the **data** users subnet are:

- The application flows already identified in the customer's pre-existing network security policy;
- The IPsec flows between the workstations running the 4760 client and the 4760 server.

The authorized IP flows on the **voice** servers subnet are:

- Signaling flow between the Media gateway and the Call Server, between the hard phones and the Call Server;
- Media flows between the Media gateway and the Call Server (case of a TDM phone user leaving or receiving a voice mail message), between the hard phones and the Media gateway (external calls) or Call Server (voice mail);
- Management flows between the 4760 server and the Call Server;
- The IPsec flows coming from the 4760 client applications going to the 4760 server.

On those three IP subnets no other IP flow is allowed going to or coming from the 4 TOE elements. Enforcement of this rule is based on the following information:

- Source IP address
- Destination IP address
- Transport protocol
- Source port
- Destination port.

OE.SOFTPHONE_DATA_USERS_SUBNET

When softphones are deployed, they are connected to the data users subnet which shall benefit from the same physical protection as the voice user subnet (refer to OE.PROTECTION_VOICE_USERS_SUBNET).

The softphones introduce the following additional IP flows on the **voice users subnet**:

- Media flows between the soft phones and hard phone sets during internal phone calls.

The additional IP flows on the **data** users subnet are:

- Signaling flows between the softphone applications and the Call Server;
- Media flows between the softphone applications (for internal phone calls), between the softphones and hardware phone sets (internal calls), between the softphones and the media gateway (PSTN calls or calls with non-IP phones like TDM phones), between the softphones and the OXE Call Server during recording and playback of voice messages.

The additional IP flows on the **voice** servers subnet are:

- Signaling flow between the softphones and the Call Server;
- Media flows between the softphones and the Media gateway (external calls or calls to TDM or DECT phones), between the softphones and the Call Server when leaving or reading a voice mail message.

On those three IP subnets no other IP flow than mentioned in objective OE.SEPARATION_NETWORKS and objective OE.SOFTPHONE_DATA_USERS_SUBNET is allowed going to or coming from the 4 TOE elements. Enforcement of this rule is based on the following information:

- Source IP address
- Destination IP address
- Transport protocol
- Source port
- Destination port.

4.2.2 Operational security objectives

OE.CONFIGURATION_REVIEW

Periodic review of the configuration of the TOE elements must be performed in order to detect any tampering and illicit modifications.

OE.REVIEW_LOGS

Periodic reviews of the logs (calls, DISA access, administration of the Call server) generated by the TOE must be performed in order to detect any illicit activity.

OE.DISA_DEACTIVATION

In case of DISA authentication failures (it could be a sign of attack attempts), the telephony administrator must deactivate the DISA service.

OE.BACKUP

Periodic configuration backup must be performed in order to mitigate the impact of an intrusion or of a mistake when configuring the TOE elements.

The OmniVista 4760 server provides maintenance application in order to backup/restore two kind of data that are:

– backup/restore PCX database included management, accounting, voice guide, and system configuration. This data can also be backed up/restored from the Call Server by using the command line interface.

– backup/restore OmniVista 4760 databases included system and company directories, alarms and accounting database.

On the OmniVista 4760 server these operations can be immediate or scheduled.

4.2.3 Security objectives for the Voice Servers subnet

OE.SECURE_VOICE_SERVERS_SUBNET

The Voice Servers subnet must be located in a physically secured location. Physical access to the cables and to the equipments (including the Call Server serial console) must be controlled and restricted preventing any tampering. The Call server, the OmniVista 4760 server and the Media gateway are installed in this subnet.

4.2.4 Security objectives for the Voice Users subnet

OE.PROTECTION_VOICE_USERS_SUBNET

Good practices for the protection of “traditional” telephony networks must be applied: they require physical protection against access by unauthorized persons for all network equipments and wiring all the way down to the wall plug. Applied to the TOE, those good practices are:

- The core network switching equipment is either inside the datacenter and benefits from its physical protection or may be outside the datacenter in a physically protected area whose access is restricted to authorized personnel only. Example: a closet whose door is closed with a key lock;
- Aggregation and distribution network equipment (LAN switches) are located in closets with a door locked by a key lock;
- All cabling between core and aggregation/distribution switches are physically protected in pipes;
- Cables between the last distribution switch and the wall-mounted socket are in false ceilings or underneath a raised floor in a place difficult to inconspicuously access for a human.

4.2.5 Security objectives for the telephony administrators

OE.TRAINING

Telephony administrators must be trained not to perform mistakes when configuring the system. The first and foremost mistake they must avoid is to keep the default passwords in the shipped systems that well publicized on the Internet.

OE.TRUSTED_ADMIN

Personal qualification procedures must be used in order to trust the telephony administrators and all personnel having:

- an account on the 4760 server and client workstations and/or the OXE Call Server;
- physical access to a workstation that ran or is running the 4760 client application.

4.2.6 Security objectives for the 4760 server and 4760 client operating systems

OE.HARDENING-4760_CLIENT_OS

The operating system on which the 4760 client is running and the other services running on the server must be hardened in order to avoid any network tampering of the equipment.

OE.IPSEC_TUNNEL

The Microsoft Windows IPSEC tunnel on the 4760 Server and the 4760 Client must be activated.

The secure IP communication by IPSEC permits: a mutual authentication of the machines, an encrypted exchange, a non-repudiation of the packets (check that the sender is the real correspondent), a message non-alteration protection.

OE.HARDENING-4760_SERVER_OS

The operating system on which the 4760 server is running and the other services running on the server must be hardened in order to avoid any network tampering of the equipment.

OE. PROTECTION_ADMIN_WORKSTATIONS

Physical access to the identified workstations on which the 4760 Client runs is restricted to trusted administrators. Those workstations are dedicated to administrators only: no other user can physically access those workstations or otherwise log onto them.

4.3 Security objectives rationale

The complete justification of the security problem coverage by the security objectives is available in Annex A: Justification of the TOE security environment coverage by the security objectives.

5. IT Security requirements

5.1 Security functional requirements for the TOE

All functional security requirements are extracted from the CC Part 2 [CC].

Operations on security requirements are underlined.

The TOE shall identify and authenticate the DISA users before allowing any action.

FIA_UAU.2-DISA users: User authentication before any action

FIA_UAU.2.1: The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement: applicable to DISA users

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2-DISA users: User identification before any action

FIA_UID.2.1: The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Refinement: applicable to DISA users

Dependencies: No dependencies.

The TOE shall restrict the DISA access to authenticated DISA users.

FDP_ACC.1-DISA: Subset access control

FDP_ACC.1.1: The TSF shall enforce the DISA access control policy on DISA access.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1-DISA: Security attributes based access control

FDP_ACF.1.1: The TSF shall enforce the DISA access control policy to objects based on the following:

Object: DISA access

Attributes: list of authorized DISA users

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Only authenticated DISA users are allowed to use the DISA access.

FDP_ACF.1.3: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

The authenticated user shall be member of the list of authorized DISA users.

FDP_ACF.1.4: The TSF shall explicitly deny access of subjects to objects based on the the rules:

The authenticated user is not member of the list of authorized DISA users.

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FMT_MSA.3-DISA: Static attributes initialization

FMT_MSA.3.1: The TSF shall enforce the Administration access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow the Telephony administrator to specify alternative initial values to override the default values when an object or information is created.

Refinement: applicable to the list of authorized DISA users

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.1-DISA Management of security attributes

FMT_MSA.1.1: The TSF shall enforce the Telephony administration access control policy to restrict the ability to modify the security attributes List of authorized DISA users to Telephony administrators.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_SMF.1-DISA Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions:

Management of DISA users

Dependencies: No dependencies.

The TOE shall identify and authenticate the Voice mail users.

FIA_UAU.1-Voicemail users: Timing of authentication

FIA_UAU.1.1: The TSF shall allow access to Voice mail portal on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2: The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement: applicable to Voice mail users

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1-Voicemail users: Timing of identification

FIA_UID.1.1: The TSF shall allow access to Voice mail portal on behalf of the user to be performed before the user is identified.

FIA_UID.1.2: The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement: applicable to Voice mail users

Dependencies: No dependencies.

The TOE shall restrict the access to the Voice mail.

FDP_ACC.1-Voice mail: Subset access control

FDP_ACC.1.1: The TSF shall enforce the Voice mail access control policy on Voice mail.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1-Voice mail: Security attributes based access control

FDP_ACF.1.1: The TSF shall enforce the Voice mail access control policy to objects based on the following:

Object: Voice mail

Attributes: Owner

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Only the owner of the voice mail shall have access to the Voice messages.

FDP_ACF.1.3: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

The authenticated user shall the owner of the Voice mail.

FDP_ACF.1.4: The TSF shall explicitly deny access of subjects to objects based on the rules:

The authenticated user is not the owner of the Voice mail.

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FMT_MSA.3-Voice mail: Static attribute initialisation

FMT_MSA.3.1: The TSF shall enforce the Telephony administration access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow the Telephony administrator to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.1-Voice mail: Management of security attributes

FMT_MSA.1.1: The TSF shall enforce the Telephony administration access control policy to restrict the ability to modify the security attributes Owner to Telephony administrators.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_SMF.1-Voice mail: Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions:

Management of Voice mails

Dependencies: No dependencies.

The call server application must be hardened in order to avoid any network tampering or denial of service.

FPT_SEP.1-Call server application: TSF domain separation

FPT_SEP.1.1: The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2: The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

The operating system on which the Call server is running and the other services running on the server must be hardened in order to avoid any network tampering or denial of service of the equipments.

FPT_SEP.1-Call server OS: TSF domain separation

FPT_SEP.1.1: The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2: The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

The TOE shall restrict the access to the administration interfaces (SSH) of the Call server to the 4760 server.

FDP_ACC.1-SSH: Subset access control

FDP_ACC.1.1: The TSF shall enforce the SSH access control policy on Call server.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1-SSH: Security attributes based access control

FDP_ACF.1.1: The TSF shall enforce the SSH access control policy to objects based on the following:

Object: Call server

Attributes: List of authorized SSH connections

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Only authorized equipments can initiate a SSH connection with the Call server.

FDP_ACF.1.3: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

The equipment shall be member of the list of authorized SSH connections.

FDP_ACF.1.4: The TSF shall explicitly deny access of subjects to objects based on the rules:

The equipment is not member of the list of authorized SSH connections.

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FMT_MSA.3-SSH: Static attribute initialisation

FMT_MSA.3.1: The TSF shall enforce the Telephony administration access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow the Call server system administrator to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_SMR.1-CS admin: Security roles

FMT_SMR.1.1: The TSF shall maintain the roles Call server administrator.

FMT_SMR.1.2: The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1-CS admin: Timing of identification

FIA_UID.1.1: The TSF shall allow access to the Call server system files on behalf of the user to be performed before the user is identified.

FIA_UID.1.2: The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement: applicable to the call server system administrators

Dependencies: No dependencies.

FMT_MSA.1-SSH: Management of security attributes

FMT_MSA.1.1: The TSF shall enforce the Telephony administration access control policy to restrict the ability to modify the security attributes List of authorized SSH connections to Telephony administrators.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_SMF.1-SSH: Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions:

Management of Call server SSH connections

Dependencies: No dependencies.

The TOE shall record the telephony administrator's actions on the call server.

FAU_GEN.2-Administration: User identity association

FAU_GEN.2.1: The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation, FIA_UID.1 Timing of identification

FAU_GEN.1-Administration: Audit data generation

FAU_GEN.1.1: The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) telephony administrator's actions on the call server.

FAU_GEN.1.2: The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, none.

Dependencies: FPT_STM.1 Reliable time stamps

The telephony administrator must be able to define and to manage list of telephone numbers that can communicate together.

FDP_ACC.1-Call baring: Subset access control

FDP_ACC.1.1: The TSF shall enforce the Call baring policy on Call server.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1-Call baring: Security attributes based access control

FDP_ACF.1.1: The TSF shall enforce the Call baring policy to objects based on the following:

Object: users

Attributes: List of bared connections

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Only authorized connections can be initiated by the users

FDP_ACF.1.3: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

The destination of the calls is not member of the list of bared connections.

FDP_ACF.1.4: The TSF shall explicitly deny access of subjects to objects based on the rules:

The destination of the calls is member of the list of bared connections.

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FMT_MSA.3-Call baring: Static attribute initialisation

FMT_MSA.3.1: The TSF shall enforce the Telephony administration access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow the Telephony administrator to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.1-Call baring: Management of security attributes

FMT_MSA.1.1: The TSF shall enforce the Telephony administration access control policy to restrict the ability to modify the security attributes List of bared connections to Telephony administrators.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_SMF.1-Call baring: Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions:

Management of users list of bared connections

Dependencies: No dependencies.

The TOE shall record the DISA access activity and generate an alarm in case of repetition of authentication failures.

FAU_GEN.2-DISA: User identity association

FAU_GEN.2.1: The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation, FIA_UID.1 Timing of identification

FAU_GEN.1-DISA: Audit data generation

FAU_GEN.1.1: The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) DISA access.

FAU_GEN.1.2: The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, none.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAA.1-DISA: Potential violation analysis

FAU_SAA.1.1: The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of authentication failures known to indicate a potential security violation;

b) nothing else

Dependencies: FAU_GEN.1 Audit data generation

FAU_ARP.1-DISA: Security alarms

FAU_ARP.1.1 The TSF shall take the action to raise an alarm to the telephony administrator upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

The TOE shall record the calls information.

FAU_GEN.2-calls: User identity association

FAU_GEN.2.1: The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation, FIA_UID.1 Timing of identification

FAU_GEN.1-calls: Audit data generation

FAU_GEN.1.1: The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) calls information.

FAU_GEN.1.2: The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, none.

Dependencies: FPT_STM.1 Reliable time stamps

FPT_STM.1 Reliable time stamps

FPT_STM.1.1: The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

FIA_UID.2-Calls: User identification before any action

FIA_UID.2.1: The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Refinement: applicable for the IP phones

Dependencies: No dependencies.

The users must be able to lock their phone set to forbid another person to use the phone set to perform outgoing calls.

FDP_ACC.1-Phone lock: Subset access control

FDP_ACC.1.1: The TSF shall enforce the Phone access control policy on IP phones.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1-Phone lock: Security attributes based access control

FDP_ACF.1.1: The TSF shall enforce the Phone access control policy to objects based on the following:

Object: IP phones

Attributes: Phone set password

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

The phone set password is required to use the IP phone when it is locked.

FDP_ACF.1.3: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

The password typed by the user is the phone set password.

FDP_ACF.1.4: The TSF shall explicitly deny access of subjects to objects based on the rules:

The password typed by the user is not correct.

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FMT_MSA.3-Phone lock: Static attribute initialisation

FMT_MSA.3.1: The TSF shall enforce the Telephony administration access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow the Telephony administrator to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.1-Phone lock: Management of security attributes

FMT_MSA.1.1: The TSF shall enforce the Telephony administration access control policy to restrict the ability to modify the security attributes enabling/disabling of the lock/unlock feature to Telephony administrators.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_SMF.1-Phone lock-admin: Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions:

Management of enabling/disabling of the phone lock/unlock feature

Dependencies: No dependencies.

FMT_SMF.1-Phone lock-user: Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions:

Change of the phone set password by the user

Dependencies: No dependencies.

The media gateways application must be hardened in order to avoid any network tampering or denial of service.

FPT_SEP.1-Media gateway application: TSF domain separation

FPT_SEP.1.1: The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2: The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

The operating system on which the media gateways are running and the other services running on the gateways must be hardened in order to avoid any network tampering or denial of service of the equipments.

FPT_SEP.1-Media gateway OS: TSF domain separation

FPT_SEP.1.1: The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2: The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

The TOE shall identify and authenticate the telephony administrators before allowing any action.

FIA_UAU.2-Telephony admin: User authentication before any action

FIA_UAU.2.1: The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2-Telephony admin: User identification before any action

FIA_UID.2.1: The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

The TOE shall restrict the access to the telephony administration functions to authenticated telephony administrators.

FDP_ACC.1-Administration: Subset access control

FDP_ACC.1.1: The TSF shall enforce the Telephony administration access control policy on the Telephony administration functions.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1-Administration: Security attributes based access control

FDP_ACF.1.1: The TSF shall enforce the Administration access control policy to objects based on the following:

Object: Telephony administration functions

Attributes: Access Control Lists

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Only authenticated telephony administrators can perform telephony administration functions.

FDP_ACF.1.3: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

The authenticated telephony administrator is member of the function ACL.

FDP_ACF.1.4: The TSF shall explicitly deny access of subjects to objects based on the rules:

The authenticated telephony administrator is not member of the function ACL.

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FMT_MSA.3-Administration: Static attribute initialisation

FMT_MSA.3.1: The TSF shall enforce the Telephony administration access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow the Telephony administrator to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_SMR.1-Telephony admin: Security roles

FMT_SMR.1.1: The TSF shall maintain the roles Telephony administrator.

FMT_SMR.1.2: The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_MSA.1-Administration: Management of security attributes

FMT_MSA.1.1: The TSF shall enforce the Telephony administration access control policy to restrict the ability to modify the security attributes Administration functions ACLs to Telephony administrators.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_SMF.1-Administration: Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions:

Management of administration functions ACLs

Dependencies: No dependencies.

5.2 Minimum Strength of TOE Security Functions

The minimum strength for the TOE security functions is: **SOF-High**.

5.3 Security assurance requirements for the TOE

All assurance security requirements are extracted from the CC Part 3 [CC]. The targeted assurance level is EAL2 augmented with ADV_HLD.2, ALC_DVS.1, ALC_FLR.3, AVA.MSU.1, AVA_VLA.1.

This results in the following CC assurance components:

ACM_CAP.2	Authorization controls

ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ALC_FLR.3	Systematic flaw remediation
ATE_COV.1	Analysis of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.1	Examination of guidance
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

5.4 Security requirements for the IT environment

No specific security requirements are defined for the IT environment.

5.5 Security requirements rationale

The complete justification of the TOE security objectives coverage by the security functional requirements is available in Annex B: Justification of the TOE security objectives coverage by the security requirements.

6. TOE summary specification

6.1 OmniPCX Enterprise Call server security functions

6.1.1 Access control to DISA

The use of the DISA feature is restricted to a list of authorized users. Before granting the DISA access, users are identified and authenticated through a password-based mechanism.

The Strength of the function is: SOF-High.

6.1.2 Access control to Voice mail

The access to the Voice mails is restricted using password mechanisms.

The Strength of the function is: SOF-High.

6.1.3 Access control to SSH

The access to the SSH administration interfaces of the Call server is restricted for the evaluation to the OmniVista 4760 server.

The list of the equipments authorized to connect to the SSH service is managed by the Call server system administrator himself identified and authenticated by the Call server.

The Strength of the function is: SOF-High (for the authentication of the administrator).

6.1.4 Phone lock

First level control concerns set use. A user can lock his set to forbid or to restrict access to it. When the set is locked and anyone wants to use it to make an outgoing call or use phone services, a password is requested.

Second level control is provided by the set password. When an external user enters the password of a locked set but makes several consecutive errors while doing this, access to the set is refused. The external user cannot then make personal use of the set to place outgoing calls or use telephone services.

The Strength of the function is: SOF-High.

6.1.5 Identification of IP phones

In order to perform access control (call baring) and accounting of calls, the Call server identifies each phone set with its MAC address.

6.1.6 Call baring

The telephony administrator defines and manages list of telephone numbers a user may call.

6.1.7 Accounting calls

Any call (incoming, outgoing, internal, transit) may be the subject of a cost record: caller number, caller node, called number, ticket type (local, private network), charged user, start time, end time, length are recorded by the call server. Clock synchronization can be achieved using public telephonic network connection or through IP using NTP protocol.

Calls records are then exported to the 4760 server for storage and consultation in a SYBASE database.

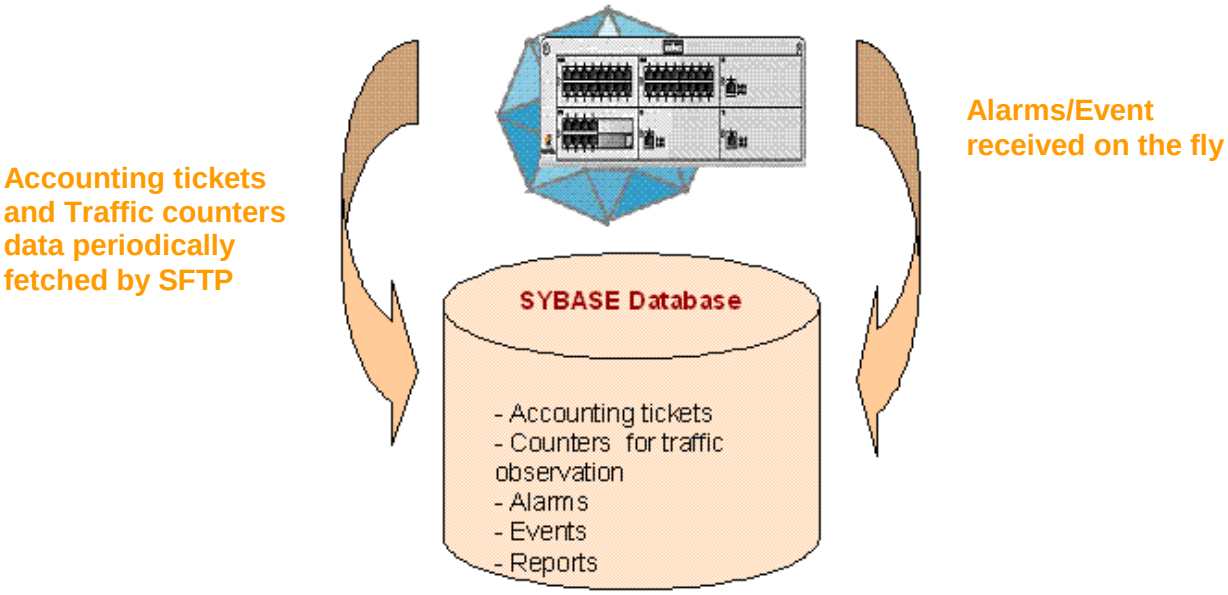

Figure 5 Accounting database

6.1.8 Accounting DISA

DISA accesses are recorded like any other calls (see 6.1.8) with a special marker enabling to specifically track DISA accesses and detect any illicit connection.

6.1.9 Accounting CS administration

The Call Server records performed administrative actions.

6.1.10 Call server hardening

The design of the Call server application and the configuration of the underlying operating system (Linux) and other services running on the call server have been hardened in order to resist to attempts of network tampering or of denial of service.

6.1.11 Telephony management

The telephony management includes:

- The management of DISA users and access;
- The management of the Voice mails users and storage;
- The management of the phone locks call baring and accounting.

The Strength of the function is: SOF-High.

6.2 OmniPCX Enterprise Media gateways security functions

6.2.1 Media gateways hardening

The design of the media gateways application and the configuration of the underlying operating system (Linux) and other services running on the gateways have been hardened in order to resist to attempts of network tampering or of denial of service.

6.3 OmniVista 4760 Server security functions

6.3.1 Telephony management user interface

OmniVista 4760 offers a graphical user interface (GUI) to the OmniPCX Telephony management described in chapter 6.1.11:

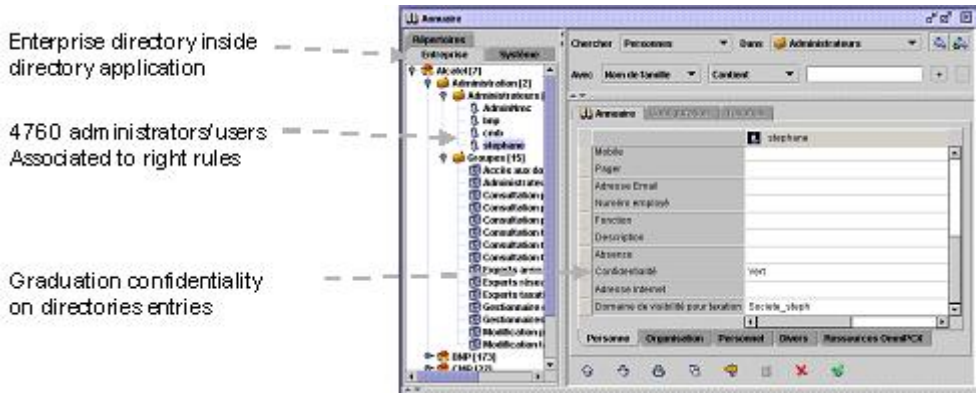

Figure 6 Management of administrators profiles interface

This GUI is the preferred management interface.

6.3.2 Access control to telephony administration functions

Telephony administrators are identified and authenticated through the 4760 client interface.

The 4760 client authenticates the telephony administrator by querying a LDAP server hosted by the 4760 server. The access to the 4760 client is itself protected by the Windows operating system logon process.

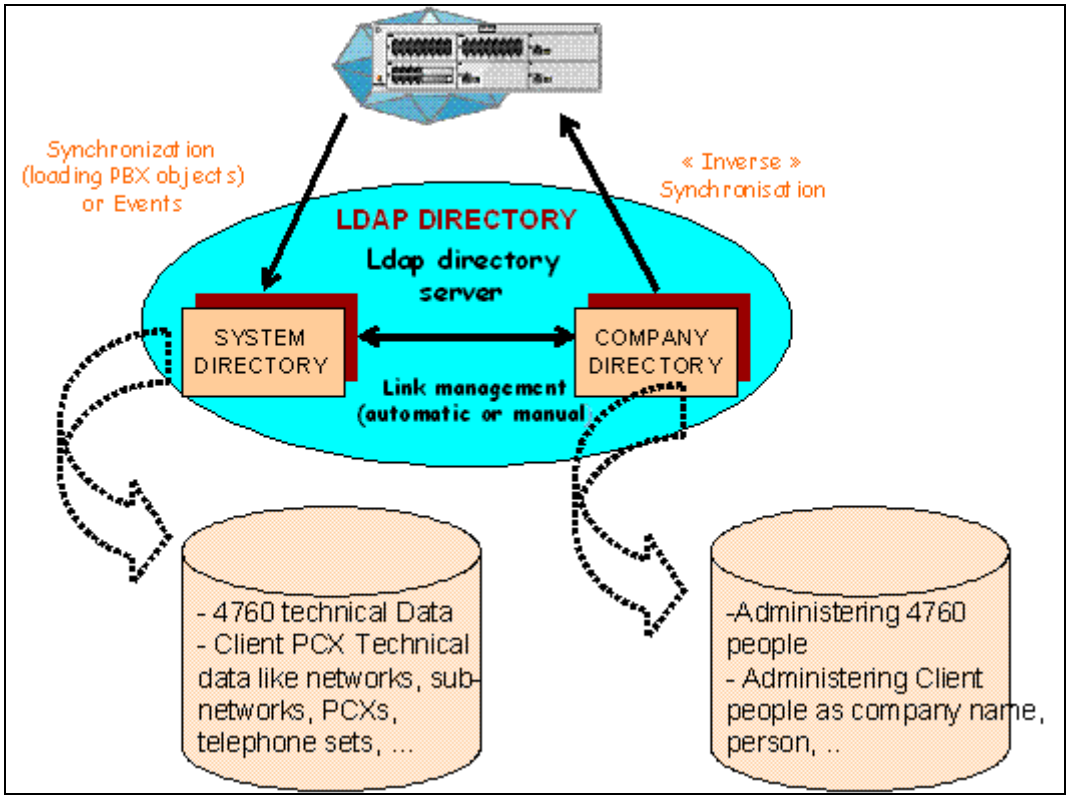

Figure 7 LDAP database

Then, the access to the telephony administration functionality depends on the profile of the authenticated administrator. Profiles are attached to users registered in the LDAP database hosted by the 4760 server. For all objects contained in the database, access rights are defined: green, orange, red depending on their criticality.

Telephony administrators access to the different OmniVista 4760 applications depends on whether or not the user belongs to groups with the appropriate access rights. These groups may be predefined or customized. Members of a group with access rights to the OmniVista 4760 security feature may customize these groups and assign individuals to them.

There are 16 predefined access groups. These groups can only be viewed by members of the Administrators group. By default, all the groups are empty.

1) “Administrators” group: Members of this group have access to all OmniVista 4760 applications without any restrictions.

2) “Accountants” group: Members of this group have access only to OmniVista 4760 features linked with Accounting and Traffic analysis operation.

3) “Accounting experts” group: Members of this group only have access to OmniVista 4760 features linked with Accounting and Traffic analysis administration and operation.

4) “Mask data access” group: The members of this group can generate reports with unmasked data.

5) “Simplified configuration” group: Members of this group have access to the Configuration application with Normal level rights and to the PCX with Access Profile 10. This group is intended for the task of managing the attendant.

6) “Network managers” group: Members of this group have access to all OmniVista 4760 features linked to network operations.

7) “Network experts” group: Members of this group have access to all OmniVista 4760 applications but have limited access to features linked to network administration.

8) “Directory experts” group: Members of this group have access to all OmniVista 4760 features linked to Company directory administration.

9) “Partial view of green list” group: Access to the Directory application with Partial view of green list level rights. Members can view: All System directory objects, Non-personal attributes of all green list records in the Company directory.

10) “Partial view of orange list” group: Access to the Directory application with Partial view of orange list level rights. Members can view: All System directory objects, Non-personal attributes of all green or orange list records in the Company directory.

11) “Partial view of red list” group: Access to the Directory application with Partial view of red list level rights. Members can view: All System directory objects, Non-personal attributes of green, orange, or red list records in the Company directory

12) “Total view of green list” group: Access to the Directory application with Total view of green list level rights. Members can view: All System directory objects, All attributes of all green list records of the Company directory

13) “Total view of orange list” group: Access to the Directory application with Total view of orange list level rights. Members can view: All System directory objects, All attributes of all green or orange list records in the Company directory

14) “Total view of red list” group: Access to the Directory application with Total view of red list level rights. Members can view: All System directory objects, All attributes of green, orange, or red list records in the Company directory

15) “Partial modification of company directory” group: Access to the Directory application with Partial modification of company directory level rights. Members can: View all objects in the System directory, View, create, edit, or delete non-personal attributes of all Company directory records

16) "Total modification of company directory" group: Access to the Directory application with Total Modification of company directory level rights. Members can: View all objects in the System directory, View, create, edit, or delete all attributes of all Company directory records

17) “Directory Security configuration” group: Access to

- Audit application with read only access level: can read everything
- Configuration application with normal access level: can read or modify all attributes
- Directory application with “Partial view of green list “ access level
- Reporting application with read only access level can see and generates reports
- Scheduler application with read only level access: can only see result of scheduled tasks

The Strength of the function is: SOF-High.

6.4 Assurance measures

6.4.1 Configuration Management

Alcatel-Lucent uses a configuration management system to assure the integrity of the TOE during its development and to track all evolutions of the TOE.

6.4.2 Delivery and Operation

Procedures are defined and applied to assure a correct delivery, installation, generation, and start-up of the TOE.

6.4.3 Development

The design of the TOE is decomposed in several layers including Functional specifications and high-level design.

6.4.4 Guidance Documents

Guidance for the operation and for the administration of the TOE is available.

6.4.5 Life Cycle Support

Life-cycle support is defined and applied for establishing discipline and control in the processes of refinement of the TOE during its development and maintenance.

6.4.6 Tests

Functional tests are performed on the TOE during its development. Functions tests covered all the security functions.

6.4.7 Vulnerability Assessment

Vulnerability assessment is performed by Alcatel-Lucent during the development in order to assure that all identified vulnerabilities have been addressed during the design of the TOE.

7. PP claims

This security target is based on with the VoIP Infrastructure Protection profile [PP VoIP].

8. References

CC	Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, ref. ISO/IEC 15408-1:2005(E) - Part 2: Security functional requirements, ref. ISO/IEC 15408-2:2005(E) - Part 3: Security assurance requirements, ref. ISO/IEC 15408-3:2005(E)
PP VoIP	Low Assurance Protection Profile for VoIP Infrastructure, version 1.1, 14th March 2005, certificate BSI-PP-0012

Annex A: Justification of the TOE security environment coverage by the security objectives

Coverage of security objectives

	A.SEPARATION_NETWORKS	A.SOFTPHONE_DATA_USERS_SUBNET	A.SECURE_VOICE_SERVERS_SUBNET	A.PROTECTION_VOICE_USERS_SUBNET	A.FALSIFICATION_OF_DATA	A.PROTECTION_ADMIN_WORKSTATIONS	A.TRAINING	A.TRUSTED_ADMIN	T.INTERNAL_NETWORK_INTRUSION	T.EXTERNAL_NETWORK_INTRUSION	T.INTERNAL_SYSTEM_FLOODING	T.EXTERNAL_SYSTEM_FLOODING	T.USURPATION_OF_ACCESS_RIGHTS-TELEPHONY_ADMIN	T.USURPATION_OF_ACCESS_RIGHTS-DISA_USERS	P.CALL_CONTROL	P.VOICEMAIL_ACCESS_CONTROL	P.PHONE_LOCK
OT.IDENTIFICATION_AUTHENTICATION-DISA_USERS														X			
OT.ACCESS_CONTROL-DISA_USERS										X		X		X			
OT.IDENTIFICATION_AUTHENTICATION-VOICEMAIL																X	
OT.ACCESS_CONTROL-VOICEMAIL																X	
OT.IDENTIFICATION_AUTHENTICATION-TELEPHONY_ADMIN													X				
OT.ACCESS_CONTROL-TELEPHONY_ADMIN													X				
OT.ACCOUTING_TELEPHONY_ADMIN													X				
OT.HARDENING-CALL_SERVER_APPLICATION									X	X	X	X					
OT.HARDENING-CALL_SERVER_OS									X	X	X	X					
OT.ACCESS_CONTROL-SSH													X				
OT.CALL_CONTROL															X		
OT.ACCOUTING_DISA										X				X	X		
OT.ACCOUTING_CALLS															X		
OT.PHONE_LOCK																	X
OT.HARDENING-MEDIA_GW_APPLICATION									X	X	X	X					
OT.HARDENING-MEDIA_GW_OS									X	X	X	X					
OE.SEPARATION_NETWORKS	X								X		X						
OE.SOFTPHONE_DATA_USERS_SUBNET		X															
OE.SECURE_VOICE_SERVERS_SUBNET			X														

	A.SEPARATION_NETWORKS	A.SOFTPHONE_DATA_USERS_SUBNET	A.SECURE_VOICE_SERVERS_SUBNET	A.PROTECTION_VOICE_USERS_SUBNET	A.FALSIFICATION_OF_DATA	A.PROTECTION_ADMIN_WORKSTATIONS	A.TRAINING	A.TRUSTED_ADMIN	T.INTERNAL_NETWORK_INTRUSION	T.EXTERNAL_NETWORK_INTRUSION	T.INTERNAL_SYSTEM_FLOODING	T.EXTERNAL_SYSTEM_FLOODING	T.USURPATION_OF_ACCESS_RIGHTS-TELEPHONY_ADMIN	T.USURPATION_OF_ACCESS_RIGHTS-DISA_USERS	P.CALL_CONTROL	P.VOICEMAIL_ACCESS_CONTROL	P.PHONE_LOCK
OE.PROTECTION_VOICE_USERS_SUBNET				X													
OE.CONFIGURATION_REVIEW									X	X	X	X					
OE.REVIEW_LOGS									X	X			X		X		
OE.DISA_DEACTIVATION														X			
OE.BACKUP									X	X	X	X					
OE.TRAINING							X										
OE.TRUSTED_ADMIN								X									
OE.HARDENING-4760_CLIENT_OS									X	X	X	X					
OE.IPSEC_TUNNEL					X												
OE.HARDENING-4760_SERVER_OS									X	X	X	X					
OE. PROTECTION_ADMIN_WORKSTATIONS						X											

Rationale of coverage for the assumptions

Assumptions	Rationale of coverage
A.SEPARATION_NETWORKS	The assumption is directly covered by OE.SEPARATION_NETWORKS.
A.SOFTPHONE_DATA_USERS_SUBNET	The assumption is directly covered by OE.SOFTPHONE_DATA_USERS_SUBNET.
A.SECURE_VOICE_SERVERS_SUBNET	The assumption is directly covered by OE.SECURE_VOICE_SERVERS_SUBNET.
A.PROTECTION_VOICE_USERS_SUBNET	The assumption is directly covered by OE.PROTECTION_VOICE_USERS_SUBNET.
A.FALSIFICATION_OF_DATA	The assumption is directly covered by OE.IPSEC_TUNNEL.
A. PROTECTION_ADMIN_WORKSTATIONS	The assumption is directly covered by OE.

Assumptions	Rationale of coverage
	PROTECTION_ADMIN_WORKSTATIONS
A.TRAINING	The assumption is directly covered by the OE.TRAINING objective.
A.TRUSTED_ADMIN	The assumption is directly covered by the OE.TRUSTED_ADMIN objective.

Rationale of coverage for the threats

All the threats have to be covered by security objectives. These security objectives can be related to:

- the prevention or the protection from the threat: the objective is that the threat does not occur;
- the detection of the occurrence of the threat;
- the mitigation of the impact of the occurrence of the threat. Even if the occurrence of the threat is not detected, measures could exist to limit the impact of a potential occurrence.

Threats	Rationale of coverage
T.INTERNAL_NETWORK_INTRUSION	Prevention & Protection: The first line of protection is provided by the network equipments located in the IP switched LAN assuring the separation of the subnets (OE.SEPARATION_NETWORKS). The call server can be protected against attempts of network tampering by hardening the code of the application (OT.HARDENING-CALL_SERVER_APPLICATION) and the code of the Linux on which it is running (OT.HARDENING-CALL_SERVER_OS). The operating system on which the 4760 server is running must be hardened in order to avoid any network tampering. (OE.HARDENING-4760_SERVER_OS) The Media gateway has been protected against attempts of network tampering by hardening the code of the application (OT.HARDENING-MEDIA_GW_APPLICATION) and the code of the Linux on which it is running (OT.HARDENING-MEDIA_GW_OS). The operating system on which the 4760 client is running must be hardened in order to avoid any network tampering. (OE.HARDENING-4760_CLIENT_OS) Detection: Periodic configuration audit should permit to detect any tampering.

Threats	Rationale of coverage
	(OE.CONFIGURATION_REVIEW) The record and the control (OE.REVIEW_LOGS) of the Call server administration activity should permit to detect any illicit connections. Impact mitigation: Periodic backup should permit to re-install authorized configuration in case of tampering. (OE.BACKUP)
T.EXTERNAL_NETWORK_INTRUSION	Prevention & Protection: The first line of defense is provided by the DISA access control mechanisms (OT.ACCESS_CONTROL-DISA_USERS). These mechanisms should limit the connection to authorized users. The call server can be protected against attempts of network tampering by hardening the code of the application (OT.HARDENING-CALL_SERVER_APPLICATION) and the code of the Linux on which it is running (OT.HARDENING-CALL_SERVER_OS). The operating system on which the 4760 server is running must be hardened in order to avoid any network tampering. (OE.HARDENING-4760_SERVER_OS) The Media gateway is protected against attempts of network tampering by a hardened application code (OT.HARDENING-MEDIA_GW_APPLICATION) and Linux code on which it is running (OT.HARDENING-MEDIA_GW_OS). The operating system on which the 4760 client is running must be hardened in order to avoid any network tampering. (OE.HARDENING-4760_CLIENT_OS) Detection: The record (OT.ACCOUNTING-DISA) and the control (OE.REVIEW_LOGS) of the DISA activity should permit to detect any illicit connections. Periodic configuration audit should also permit to detect any tampering. (OE.CONFIGURATION_REVIEW) Impact mitigation: Periodic backup should permit to re-install authorized configuration in case of tampering. (OE.BACKUP)
T.INTERNAL_SYSTEM_FLOODING	Prevention & Protection: The first line of protection is provided by the network equipments located in the IP switched LAN assuring the separation of the subnets (OE.SEPARATION_NETWORKS). The call server can be protected against attempts of DoS by hardening the code of the application (OT.HARDENING-CALL_SERVER_APPLICATION) and of the Linux on which it is running (OT.HARDENING-CALL_SERVER_OS). The operating system on which the 4760 server is running must be hardened in order to avoid any DoS. (OE.HARDENING-

Threats	Rationale of coverage
	4760_SERVER_OS) The media gateways can be protected against attempts of DoS by hardening the code of the application (OT.HARDENING-MEDIA_GW_APPLICATION) and of the Linux on which it is running (OT.HARDENING-MEDIA_GW_OS). The operating system on which the 4760 client is running must be hardened in order to avoid any network tampering. (OE.HARDENING-4760_CLIENT_OS) Detection: The detection is obvious because users cannot initiate or receives calls. Periodic configuration review should also permit to detect any illicit modifications. (OE.CONFIGURATION_REVIEW) Impact mitigation: - Periodic backup should permit to re-install stable system to mitigate flooding impact. (OE.BACKUP)
T.EXTERNAL_SYSTEM_FLOODING	Prevention & Protection: For DISA calls the first line of defense is provided by the DISA access control mechanisms (OT.ACCESS_CONTROL-DISA_USERS). These mechanisms should limit the connection to authorized users.. The call server can be protected against attempts of DoS by hardening the code of the application (OT.HARDENING-CALL_SERVER_APPLICATION) and of the Linux on which it is running (OT.HARDENING-CALL_SERVER_OS). The operating system on which the 4760 server is running must be hardened in order to avoid any DoS. (OE.HARDENING-4760_SERVER_OS) The media gateways can be protected against attempts of DoS by hardening the code of the application (OT.HARDENING-MEDIA_GW_APPLICATION) and of the Linux on which it is running (OT.HARDENING-MEDIA_GW_OS). The operating system on which the 4760 client is running must be hardened in order to avoid any network tampering. (OE.HARDENING-4760_CLIENT_OS) Detection: The detection is performed in the Media gateway which alerts the Call Server resulting in a notification sent to the OmniVista 4760 server. Periodic configuration review should also permit to detect any illicit modifications. (OE.CONFIGURATION_REVIEW) Impact mitigation: - Periodic backup should permit to re-install stable system to mitigate flooding impact. (OE.BACKUP)
T.USURPATION_OF_ACCES	Prevention & Protection:

Threats	Rationale of coverage
S_RIGHTS-TELEPHONY_ADMIN	At the level of the Call server, the access to the administration interfaces (SSH) must be restricted to the OmniVista 4760 server. (OT.ACCESS_CONTROL-SSH) At the level of the OmniVista 4760 server, the access to the services administration functions must be restricted to authenticated telephony administrators. (OT.IDENTIFICATION_AUTHENTICATION-TELEPHONY_ADMIN for the authentication and OT.ACCESS_CONTROL-TELEPHONY_ADMIN for the access control to the functions). Detection: At the level of the Call server, it must be possible to record the telephony administrator's actions in order to detect any modification not performed by the authorized administrator (OT.ACCOUNTING-TELEPHONY_ADMIN) and to control it (OE.REVIEW_LOGS). Impact mitigation: -
T.USURPATION_OF_ACCESS_RIGHTS-DISA_USERS	Prevention & Protection: The Call Server must restrict the access to the DISA services to authenticated users. (OT.IDENTIFICATION_AUTHENTICATION-DISA_USERS for the authentication and OT.ACCESS_CONTROL-DISA_USERS for the access control to DISA services). Detection: The telephony administrator is alerted when more the 3 authentication failures to access DISA service have occurred within a specific time frame. (OT.ACCOUNTING-DISA) Impact mitigation: In case of authentication failures, it is possible for the telephony administrator to deactivate the DISA service. (OE.DISA_DEACTIVATION)

Rationale of coverage for the OSP

OSP	Rationale of coverage
P.CALL_CONTROL	The OSP is directly covered by the OT.CALL_CONTROL objective for the management of the access lists and by OT.ACCOUNTING-DISA, OT.ACCOUNTING-CALLS and OE.REVIEW_LOGS for the record and the control of the audit tracks.
P.VOICEMAIL_ACCESS_CONTROL	The OSP is directly covered by the OT.IDENTIFICATION_AUTHENTICATION-VOICEMAIL and OT.ACCESS_CONTROL-VOICEMAIL.
P.PHONE_LOCK	The OSP is directly covered by the OT.PHONE_LOCK objective.

Annex B: Justification of the TOE security objectives coverage by the security requirements

Rationale of coverage of the security objectives for the TOE

Objectives	Rationale of coverage
OT.IDENTIFICATION_AUTHENTICATION-DISA_USERS	The objective is directly covered by FIA_UID.2 – DISA users for the identification and FIA_UAU.2 – DISA users for the authentication of the DISA users before allowing them to do any action.
OT.ACCESS_CONTROL-DISA_USERS	The objective is directly covered by FDP_ACC.1 – DISA and FDP_ACF.1 – DISA Access for the definition of the access control policy. The selection of these components requires the selection of their dependencies: – FMT_SMF.1-DISA, FMT_MSA.3-DISA and FMT_MSA.1-DISA for the management of the list of DISA users by the telephony administrator.
OT.IDENTIFICATION_AUTHENTICATION-VOICE_MAIL	The objective is directly covered by FIA_UID.1 – Voicemail users for the identification and FIA_UAU.1 – Voicemail users for the authentication of the users before to give access to their messages.
OT.ACCESS_CONTROL-VOICEMAIL	The objective is directly covered by FDP_ACC.1 – Voice mail and FDP_ACF.1 – Voice mail for the definition of the access control policy. The selection of these components requires the selection of their dependencies: – FMT_SMF.1- Voice mail, FMT_MSA.3- Voice mail and FMT_MSA.1- Voice mail for the management of the voice mails by the telephony administrator.
OT.HARDENING-CALL_SERVER_APPLICATION	The call server application must be resistant to any tampering or DoS (FPT_SEP.1-Call server application).
OT.HARDENING-CALL_SERVER_OS	The call server operating system must be resistant to any tampering or DoS (FPT_SEP.1-Call server OS).
OT.ACCESS_CONTROL-SSH	The objective is directly covered by FDP_ACC.1 – SSH and FDP_ACF.1 – SSH for the definition of the access control policy. The selection of these components requires the selection of their dependencies: – FMT_SMR.1-CS admin for the definition of the Call server system administrator and FIA_UID.1-CS admin for its identification; – FMT_SMF.1- SSH, FMT_MSA.3- SSH and FMT_MSA.1-SSH for the management of the SSH access list by the telephony administrator.

Objectives	Rationale of coverage
OT.ACCOUNTING-TELEPHONY_ADMIN	The Call server must record the administration actions and associated it with the identity of the telephony administrator (FAU_GEN.2-Administration, FAU_GEN.1 - Administration). It needs a reliable time source in order to time-stamp the events (FPT_STM.1 Reliable time stamps).
OT.CALL_CONTROL	The call control baring policy is defined by the FDP_ACC.1-Call baring and the FDP_ACF.1- Call baring components. The FMT_SMF.1-Call baring component permits to define the Call baring functions and FMT_MSA.3-Call baring and FMT_MSA.1-Call baring the management of the ACLs by the telephony administrator.
OT.ACCOUNTING-DISA	The Call server must record the DISA activity (FAU_GEN.1-DISA) and to associate the connections with a user (FAU_GEN.2 - DISA). In the case of authentication failures, the TOE must generate an alarm to the telephony administrator (FAU_SAA.1-DISA and FAU_ARP.1-DISA) It needs a reliable time source in order to time-stamp the events (FPT_STM.1 Reliable time stamps).
OT.ACCOUNTING-CALLS	The Call server must record the calls activity (FAU_GEN.1-calls): it associates the activity to an identified user (FAU_GEN.2-calls, FIA_UID.2-calls) It needs a reliable time source in order to time-stamp the events (FPT_STM.1 Reliable time stamps).
OT.PHONE_LOCK	The objective is directly covered by FDP_ACC.1 – Phone lock and FDP_ACF.1 – Phone lock for the definition of the access control policy. The selection of these components requires the selection of their dependencies: – FMT_SMF.1- Phone lock-admin, FMT_MSA.3- Phone lock and FMT_MSA.1- Phone lock for the management of the enabling/disabling of the lock/unlock feature by the telephony administrator and FMT_SMF.1-Phone lock-user for the change of the password by the user.
OT.HARDENING-MEDIA_GW_APPLICATION	The media gateway application must be resistant to any tampering or DoS (FPT_SEP.1-Media gateway application).
OT.HARDENING-MEDIA_GW_OS	The media gateway operating system must be resistant to any tampering or DoS (FPT_SEP.1-Media gateway OS).
OT.IDENTIFICATION_AUTHENTICATION-TELEPHONY_ADMIN	The objective is directly covered by FIA_UID.2 – Telephony admin for the identification and FIA_UAU.2 – Telephony admin for the authentication of the Telephony admin before allowing them to do any action.

Objectives	Rationale of coverage
OT.ACCESS_CONTROL-TELEPHONY_ADMIN	The objective is directly covered by FDP_ACC.1 – Administration and FDP_ACF.1 – Administration for the definition of the access control policy. The selection of these components requires the selection of their dependencies: – FMT_SMR.1 for the definition of the Telephony administrator role FMT_SMF.1-Administration, FMT_MSA.3- Administration and FMT_MSA.1- Administration for the management of the telephony administrator accounts.

Rationale for dependencies:

SFR dependencies

SFRs	Dependencies	Satisfaction/Rationale
FIA_UAU.2-DISA users	FIA_UID.1–DISA users	OK
FIA_UID.2-DISA users	-	OK
FDP_ACC.1-DISA	FDP_ACF.1-DISA	OK
FDP_ACF.1-DISA	FDP_ACC.1-DISA, FMT_MSA.3-DISA	OK
FMT_MSA.3-DISA	FMT_MSA.1-DISA, FMT_SMR.1-Telephony admin	OK
FMT_MSA.1-DISA	FDP_ACC.1-Administration, FMT_SMR.1-Telephony admin, FMT_SMF.1-DISA	OK
FMT_SMF.1-DISA	-	OK
FIA_UAU.1-Voicemail users	FIA_UID.1-Voicemail users	OK
FIA_UID.1-Voicemail users	-	OK
FDP_ACC.1-Voice mail	FDP_ACF.1- Voice mail	OK
FDP_ACF.1- Voice mail	FDP_ACC.1- Voice mail, FMT_MSA.3-Voice mail	OK
FMT_MSA.3- Voice mail	FMT_MSA.1- Voice mail, FMT_SMR.1-Telephony admin	OK
FMT_MSA.1- Voice mail	FDP_ACC.1-Administration, FMT_SMR.1-Telephony admin, FMT_SMF.1- Voice mail	OK
FMT_SMF.1- Voice mail	-	OK
FPT_SEP.1-Call server application	-	OK
FPT_SEP.1-Call server OS	-	OK

SFRs	Dependencies	Satisfaction/Rationale
FDP_ACC.1-SSH	FDP_ACF.1- SSH	OK
FDP_ACF.1- SSH	FDP_ACC.1- SSH FMT_MSA.3- SSH	OK
FMT_MSA.3- SSH	FMT_MSA.1- SSH, FMT_SMR.1-CS admin	OK
FMT_SMR.1-CS admin	FIA_UID.1-CS admin	OK
FIA_UID.1-CS admin	-	OK
FMT_MSA.1- SSH	FDP_ACC.1-Administration, FMT_SMR.1-CS admin, FMT_SMF.1-SSH	OK
FMT_SMF.1- SSH	-	OK
FAU_GEN.2-Administration	FAU_GEN.1-Administration, FIA_UID.1-CS admin	OK
FAU_GEN.1-Administration	FPT_STM.1	OK
FDP_ACC.1- Call baring	FDP_ACF.1- Call baring	OK
FDP_ACF.1- Call baring	FDP_ACC.1- Call baring FMT_MSA.3-Call baring	OK
FMT_MSA.3-Call baring	FMT_MSA.1-Call baring, FMT_SMR.1-Telephony admin	OK
FMT_MSA.1-Call baring	FDP_ACC.1-Administration, FMT_SMR.1-Telephony admin, FMT_SMF.1-Call baring	OK
FMT_SMF.1-Call baring	-	OK
FAU_GEN.2-DISA	FAU_GEN.1-DISA, FIA_UID.1-DISA users	OK
FAU_GEN.1-DISA	FPT_STM.1	OK
FAU_SAA.1-DISA	FAU_GEN.1-DISA	OK
FAU_ARP.1-DISA	FAU_SAA.1-DISA	OK
FAU_GEN.2-calls	FAU_GEN.1-calls, FIA_UID.1-Calls	OK
FAU_GEN.1-calls	FPT_STM.1	OK
FPT_STM.1	-	OK
FIA_UID.2-Calls	-	OK
FDP_ACC.1-Phone lock	FDP_ACF.1- Phone lock	OK
FDP_ACF.1- Phone lock	FDP_ACC.1- Phone lock FMT_MSA.3-Phone lock	OK
FMT_MSA.3- Phone lock	FMT_MSA.1- Phone lock, FMT_SMR.1-Telephony admin	OK
FMT_MSA.1- Phone lock	FDP_ACC.1-Administration, FMT_SMR.1-Telephony admin, FMT_SMF.1- Phone lock-admin	OK

SFRs	Dependencies	Satisfaction/Rationale
FMT_SMF.1- Phone lock-admin	-	OK
FMT_SMF.1- Phone lock-user	-	OK
FPT_SEP.1-Media gateway application	-	OK
FPT_SEP.1-Media gateway OS	-	OK
FIA_UAU.2-Telephony admin	FIA_UID.1-Telephony admin	OK
FIA_UID.2-Telephony admin	-	OK
FDP_ACC.1-Administration	FDP_ACF.1- Administration	OK
FDP_ACF.1- Administration	FDP_ACC.1- Administration FMT_MSA.3- Administration	OK
FMT_MSA.3- Administration	FMT_MSA.1- Administration, FMT_SMR.1-Telephony admin	OK
FMT_SMR.1-Telephony admin		
FMT_MSA.1- Administration	FDP_ACC.1-ADMIN, FMT_SMR.1-Telephony admin, FMT_SMF.1-Administration	OK
FMT_SMF.1-Administration	-	OK

SAR dependencies

SARs	Dependencies	Satisfaction/Rationale
ACM_CAP.2	-	OK
ADO_DEL.1	-	OK
ADO_IGS.1	AGD_ADM.1	OK
ADV_FSP.1	ADV_RCR.1	OK
ADV_HLD.2	ADV_FSP.1 ADV_RCR.1	OK
ADV_RCR.1	-	OK
AGD_ADM.1	ADV_FSP.1	OK
AGD_USR.1	ADV_FSP.1	OK
ALC_DVS.1	-	OK
ALC_FLR.3	-	OK
ATE_COV.1	ADV_FSP.1 ATE_FUN.1	OK
ATE_FUN.1	-	OK
ATE_IND.2	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	OK

SARs	Dependencies	Satisfaction/Rationale
AVA_MSU.1	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	OK
AVA_SOF.1	ADV_FSP.1 ADV_HLD.1	OK
AVA_VLA.1	ADV_FSP.1 ADV_HLD.2 AGD_ADM.1 AGD_USR.1	OK

The dependencies between the various assurance components are respected by this assurance level.

Annex C: Justification of the security requirements coverage by the TOE summary specification

Rationale of coverage of the security functional requirements

SFRs	Security functions
FIA_UAU.2-DISA users	Access control to DISA includes the authentication of the DISA users
FIA_UID.2-DISA users	Access control to DISA includes the identification of the DISA users
FDP_ACC.1-DISA	Access control to DISA includes the implementation of the access control policy
FDP_ACF.1-DISA	Access control to DISA includes the implementation of the access control policy
FMT_MSA.3-DISA	Telephony management includes the management of the security attributes
FMT_MSA.1-DISA	Telephony management includes the management of the security attributes
FMT_SMF.1-DISA	Telephony management includes the implementation of the management function
FIA_UAU.1-Voicemail users	Access control to Voice mail includes the authentication of the users
FIA_UID.1-Voicemail users	Access control to Voice mail includes the identification of the users
FDP_ACC.1-Voice mail	Access control to Voice mail includes the implementation of the access control policy
FDP_ACF.1- Voice mail	Access control to Voice mail includes the implementation of the access control policy
FMT_MSA.3- Voice mail	Telephony management includes the management of the security attributes
FMT_MSA.1- Voice mail	Telephony management includes the management of the security attributes
FMT_SMF.1- Voice mail	Telephony management includes the implementation of the management function
FPT_SEP.1-Call server application	Call server hardening includes the hardening of the application
FPT_SEP.1-Call server OS	Call server hardening includes the hardening of the OS
FDP_ACC.1-SSH	Access control to SSH includes the implementation of the access control policy
FDP_ACF.1- SSH	Access control to SSH includes the implementation of the access control policy
FMT_MSA.3- SSH	Access control to SSH includes the management of

SFRs	Security functions
	the security attributes
FMT_MSA.1- SSH	Access control to SSH includes the management of the security attributes
FMT_SMR.1-CS admin	Access control to SSH includes the definition of the CS system administrator role
FIA_UID.1-CS admin	Access control to SSH includes the identification of the CS system administrator
FMT_SMF.1- SSH	Access control to SSH includes the implementation of the management function
FAU_GEN.2-Administration	Accounting CS administration implements the audit track record
FAU_GEN.1-Administration	Accounting CS administration implements the audit track record
FDP_ACC.1- Call baring	Call baring includes the implementation of the Call baring policy
FDP_ACF.1- Call baring	Call baring includes the implementation of the Call baring policy
FMT_MSA.3- Call baring	Telephony management includes the management of the security attributes
FMT_MSA.1- Call baring	Telephony management includes the management of the security attributes
FMT_SMF.1- Call baring	Telephony management includes the implementation of the management function
FAU_GEN.2-DISA	Accounting DISA implements the audit track record
FAU_GEN.1-DISA	Accounting DISA implements the audit track record
FAU_SAA.1-DISA	Accounting DISA includes the monitoring of the audited events
FAU_ARP.1-DISA: Security alarms	Accounting DISA includes the alarm raising to the telephony administrator upon detection of a potential security violation.
FAU_GEN.2-calls	Accounting calls implements the audit track record
FAU_GEN.1-calls	Accounting calls implements the audit track record
FPT_STM.1	The time reference is required for Accounting calls, Accounting DISA and Accounting CS administration
FIA_UID.2-Calls	Identification of IP phones includes the identification of the IP phones
FDP_ACC.1-Phone lock	Phone lock includes the implementation of the access control policy
FDP_ACF.1- Phone lock	Phone lock includes the implementation of the access control policy

SFRs	Security functions
FMT_MSA.3- Phone lock	Telephony management includes the management of the security attributes
FMT_MSA.1- Phone lock	Telephony management includes the management of the security attributes
FMT_SMF.1-Phone lock-admin	Telephony management includes the management of enabling/disabling of the phone lock/unlock feature
FMT_SMF.1- Phone lock-user	Telephony management includes the implementation of the management function
FPT_SEP.1-Media gateway application	Media gateway hardening includes the hardening of the application
FPT_SEP.1-Media gateway OS	Media gateway hardening includes the hardening of the OS
FIA_UAU.2-Telephony admin	Access control to telephony administration functions includes the authentication of the administrator
FIA_UID.2-Telephony admin	Access control to telephony administration functions includes the identification of the administrator
FDP_ACC.1-Administration	Access control to telephony administration functions includes the implementation of the access control policy
FDP_ACF.1- Administration	Access control to telephony administration functions includes the implementation of the access control policy
FMT_MSA.3- Administration	Telephony management includes the management of the security attributes.
FMT_SMR.1-Telephony admin	Access control to telephony administration includes the definition of the Telephony administrator role
FMT_MSA.1- Administration	Telephony management includes the management of the security attributes.
FMT_SMF.1-Administration	Access control to telephony administration functions includes the management of administration functions ACLs

Rationale of coverage of the security assurance requirements

The assurance requirements are directly covered by the assurance measures associated to each class of the requirements (i.e. ACM, ADO, ADV, AGD, ALC, ATE, AVA).

www.alcatel-lucent.com