Low Assurance Security Target for a Cisco VoIP Telephony System

Security Target
Version 1.6
March 14, 2005

Document Control

Preparation

Action	Name	Date
Prepared by:	Rob Hunter of TNO-ITSEF BV on behalf of Cisco	14 March 2005

Release

Version	Date Released	Change Notice	Pages Affected	Remarks
1.2	29-11-04	n/a	All	Initial version of rewrite by ITSEF
1.3	16-12-04	n/a	All	Modified after evaluator comments and site visit
1.4	17-01-05	n/a	All	Modified after first round BSI certifier comments
1.5	25-02-05	n/a	All	Modified after second round BSI certifier comments
1.6	14-03-05	n/a	All	Modified after third round BSI certifier comments

Distribution List

Name	
1.	BSI
2.	BSI
3.	TNO-ITSEF BV

Document Information

Version number report	1.6
Certification ID	BSI-DSZ-CC-0306
Scheme	BSI
Sponsor	BSI
Evaluation Lab Evaluation Lab address	TNO-ITSEF BV Delftech Park 1 2628XJ Delft The Netherlands
Target of Evaluation (TOE)	Cisco VoIP Telephony System
TOE reference name	Cisco VoIP Telephony System
CC-EAL number	1
Report title	Low Assurance Security Target for a Cisco VoIP Telephony System
Report reference name	LAST-Cisco VoIP Telephony System-1.6

TABLE OF CONTENTS

1 SECURITY TARGET INTRODUCTION 8

1.1 ST REFERENCE 8
1.2 TOE REFERENCE 8
1.3 TOE OVERVIEW 8
1.4 TOE DESCRIPTION 9
1.4.1 Physical Scope and Boundaries 9
1.4.2 Logical Scope and Boundaries 14

2 CONFORMANCE CLAIMS 16

2.1 CONFORMANCE CLAIM 16
2.2 PROTECTION PROFILE CLAIM 16
2.3 PACKAGE CLAIM 16

3 DEFINITION OF TERMS 17

3.1 DEFINITION OF SUBJECTS, INFORMATION AND OPERATIONS 17
3.1.1 Subjects 17
3.1.2 Operations 17
3.1.3 Objects 17

4 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT .. 18

5 SECURITY REQUIREMENTS 19

5.1 EXTENDED COMPONENTS DEFINITION 19
5.2 SFRS 19
5.2.1 Restricting access to certain telephone numbers 19
5.2.2 Voice mail 19
5.2.3 Managing telephones 19
5.2.4 Identifying users 20
5.2.5 Logging and auditing 20
5.2.6 Self-protection 20
5.3 SARS 21

6 TOE SUMMARY SECTION 22

6.1 TOE SECURITY FUNCTIONS 22
6.1.1 Restricting access to certain telephone numbers 22
6.1.2 Voice mail 22
6.1.3 Managing telephones 23
6.1.4 Identifying users 23
6.1.5 Logging and auditing 23
6.1.6 Self-protection 23

LIST OF TABLES

Table 1: Components and Software in the TOE 10
Table 2: Physical Definition of 7970G Components 11
Table 3: Physical Definition of 7970G Touch Screen Components 11
Table 4: Physical Definition of 7960G Components 12

LIST OF FIGURES

Figure 1: Front View of the Cisco IP Phone 7970G.....11
Figure 2: Front View of the Cisco IP Phone 7960G.....12

References

[VOIP-PP] Low Assurance Protection Profile for a VoIP Infrastructure, Version 1.1, 14th March 2004.

The following references can be downloaded from the developers website.

[CDR-DEF] Cisco CallManager 4.1(2) Call Detail Record Definition pages 11-28 inclusive.

[CM_ADMIN] Cisco CallManager Administration Guide, Release 4.1(2).

[CM_TRACE] Cisco CallManager Serviceability Administration Guide, Release 4.1(2).

[UNITY_USER] Cisco Unity User Guide Release 4.0(3).

[CISCO-CC] Commentary and Configuration Guidelines for Implementation of the IPT System Evaluated Common Criteria 2.4 EAL 1, dated feb 23rd, 2005, version 1.0

1 Security Target Introduction

1.1 ST Reference

This is the Low Assurance Security Target for a
Cisco VoIP Telephony System 1.6, BSI, March 14th, 2005

1.2 TOE Reference

The TOE reference is defined as the 'Cisco VoIP Telephony System Version 1.0' and is the collective reference for the TOE components as described in section 1.4

1.3 TOE overview

The VoIP Telephony System provides all the technology required to replace a traditional Private Branch Exchange (PBX) with an Internet Protocol (IP) -based solution. The System includes Cisco IP-based telephones (IP phones), Cisco CallManager (Cisco's PBX call-agent - CCM), a Cisco Voice Gateway router and Cisco Unity for voice messaging. The IP phones combine the functions of a traditional telephone with an Ethernet connection. Cisco CallManager is a software-based call processing agent that extends enterprise telephony features and functions to packet telephony network devices. Cisco Unity is a Windows 2000-based communications solution that provides voice mail and unified messaging (voice to text-based systems).

The TOE provides the following security functionality:

- Access to certain phone numbers can be restricted.
- Access to Voice mail in order to listen to messages and delete them is only allowed after successful user identification and authentication.
- The administrator can only manage the TOE after successful user identification and authentication.
- The TOE generates audit records for each telephone call and for audit enabling/disabling.
- The TOE security functionality protects itself from tempering and interference by being well designed, produced and tested.

The following non TOE hardware, software or firmware is required by the TOE components in order for the TOE to operate as described in this Security Target:

- Cisco CallManager requires a Cisco MCS7800 server platform (a rack mounted PC) with Microsoft Windows 2000 server running: Sun JRE, Microsoft SQL Server 2000 updated with SP3a (or later)
- Cisco Unity (Voicemail) requires a Cisco MCS7800 server platform (a rack mounted PC) with Microsoft Windows 2000 server running: Sun JRE, Microsoft SQL Server 2000 updated with SP3a (or later)
- The TOE requires an underlying IP based network for data transport.

- A standard PC equipped with a web browser that supports HTTPS to Cisco CallManager and Cisco Unity over the LAN and a serial connection to the Cisco Voice Gateway router via a terminal emulator such as Hyper terminal is needed to administer the TOE.

The other TOE components are self contained and do not require supporting hardware, software or firmware to operate.

1.4 TOE description

The TOE is a Cisco VoIP System composed of IP phones, a Cisco CallManager, a Cisco Unity and a Cisco Voice Gateway router to connect the infrastructure to the Public Switched Telephone Network (PSTN). The goal of this VoIP System is to provide telephony services over an IP network. An IP-based network is the backbone of the TOE, and carries the IP packets between the distinct pieces of the System.

The major Security Features that are provided by the TOE are:

- The restriction of IP phone users access to certain telephone numbers.
- Identification and authentication of users who wish to access the TOEs' voice mail services.
- The management of IP Phones.
- The provision of systems traces through alarms, system traces and call information.
- Protection of itself and the security functions it offers by being well designed, implemented and tested.

1.4.1 Physical Scope and Boundaries

IP Telephony enables calls to be made between IP phones, as well as between an IP-based phone and a traditional PSTN telephone. The components for a VoIP System are shown in Figure 1.

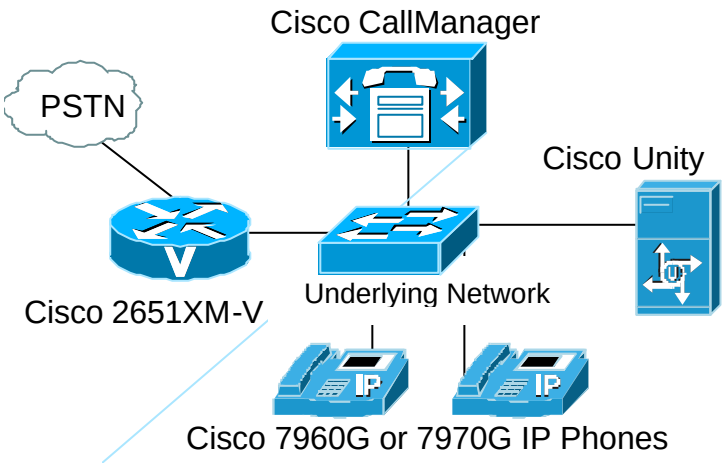


Figure 1: The Cisco VoIP system – note that that network is not part of the TOE.

A minimum of two Cisco IP phones (type 7960G or 7970G) are required to place calls between IP-based phones.

Cisco CallManager (CCM) is a central entity that provides call control and configuration management for the IP Phones. The CCM provides the core functionality to provide call set-up and route calls throughout the network to voice gateways and voice mail systems.

The Cisco Unity system provides IP-based voicemail storage.

The Cisco 2651XM-V voice gateway router provides access and data conversion to and from the PSTN and the IP network.

The version numbers for the components that together form the TOE are:

Component	**Software Version in the TOE**
Cisco IP Telephone 7960G	7.0(2)
Cisco IP Telephone 7970G	6.0(2)
Cisco CallManager	4.1(2)
Cisco Unity	4.0(4)
Cisco 2651XM-V	12.3(10)

Table 1: Components and Software in the TOE

1.4.1.1 IP Phones

Two different IP phone models are included in the TOE: Cisco IP Phone 7960G and 7970G. The main difference between the two models is the inclusion of a color screen on the 7970, its touch screen capabilities, and its support for user-defined LCD backgrounds. Both phones are self contained operational units.

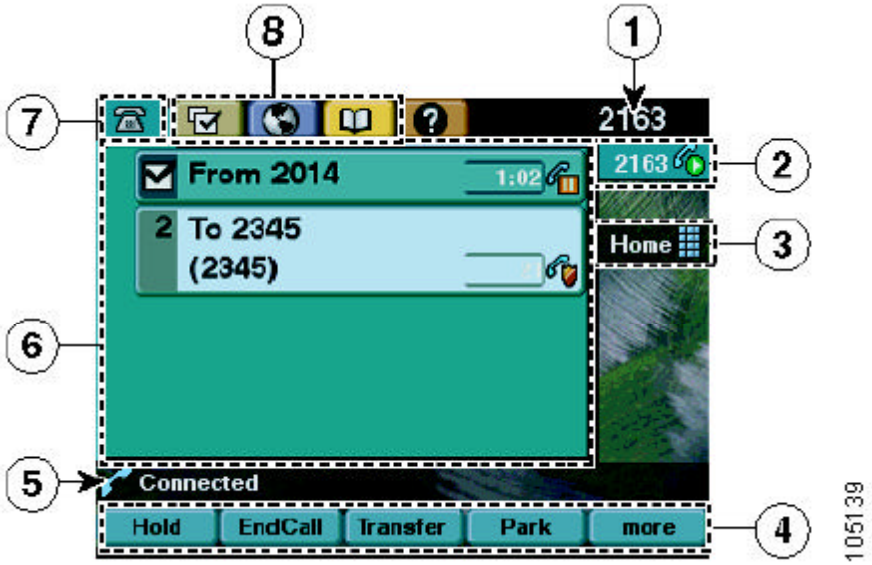
Cisco IP phones are full-featured telephones that provide voice communication over an IP-based network.

The 7970G IP Phone

Figure 1: Front View of the Cisco IP Phone 7970G

1	Programmable buttons	10	Toggles the speaker phone on and off
2	Foot stand button	11	Toggles mute on and off
3	Display button	12	Toggles the headset on and off
4	Messages (voicemail)	13	Navigation button
5	Directories button	14	Keypad
6	Help	15	Soft keys
7	Settings	16	Handset Light Strip
8	Services	17	Touch screen
9	Volume		

Table 2: Physical Definition of 7970G Components



1	Primary Line	2	Line Area and Call Overview
3	Programmable button labels	4	Soft key labels
5	Status	6	Call activity
7	Phone tab	8	Feature tab

Table 3: Physical Definition of 7970G Touch Screen Components

The 7960G IP Phone

Figure 2: Front View of the Cisco IP Phone 7960G

1	Handset light strip, indicates an incoming call or voice message	10	Toggles mute on and off
2	LCD Screen	11	Toggles the headset on and off
3	Model Type	12	Volume
4	Programmable buttons	13	Services
5	Foot stand button	14	Messages (voicemail)
6	Directories button	15	Scroll
7	Help	16	Keypad
8	Settings	17	Soft keys
9	Speaker		

Table 4: Physical Definition of 7960G Components

1.4.1.2 Cisco CallManager

The operating system that hosts the CCM application is a turn-key, pre-configured version of Microsoft Windows 2000 Server that runs on Cisco's MCS7800 server hardware. It includes the following software packages:

- Sun Microsystem Java Runtime Environnent (JRE)
- Microsoft SQL Server 2000
- Microsoft SQL Server 2000 Service Pack 3a (or later)

The "Cisco CallManager Operating System Optional Security Settings" are applied to the Cisco CallManager before the Cisco CallManager is placed into production.

1.4.1.3 Cisco Unity

The operating system that hosts the Cisco Unity application is a turn-key, pre-configured version of Microsoft Windows 2000 Server that runs on Cisco's MCS7800 server hardware. It includes the following software packages:

- Sun Microsystem Java Runtime Environnent (JRE)
- Microsoft SQL Server 2000
- Microsoft SQL Server 2000 Service Pack 3a (or later)

The "Cisco CallManager Operating System Optional Security Settings" are applied to the Cisco Unity before the Cisco Unity is placed into production.

1.4.1.4 Cisco 2651XM-V

The Cisco 2651XM-V router (Gateway) provides the interface between the TOE and the PSTN. The Cisco 2651XM-V is a self contained operational unit that is administered by attaching a console or PC running terminal emulation software to a port on the rear of the router.

1.4.1.5 Associated Documentation

Administration Documentation

General Administration Documentation
Commentary and Configuration Guidelines for Implementation of the IPT System Evaluated Common Criteria 2.4 EAL 1, dated feb 23rd, 2005, version 1.0

Administration Documentation for the Cisco CallManager
Cisco CallManager Administration Guide, Release 4.1(2).
Cisco CallManager Serviceability Administration Guide, Release 4.1(2).
Cisco CallManager Security Guide Version 4.1(2)
Installing Cisco CallManager Release 4.1(2)

Administration Documentation for the IP Phones
Cisco IP Phone 7970 Administration Guide for Cisco CallManager
Cisco IP Phone Model 7960G and 7940G Administration Guide for Cisco CallManager Release 4.1

Administration Documentation for Cisco Unity
Cisco Unity System Administration Guide (With Microsoft Exchange), Release 4.0(4)
Cisco Unity Installation Guide (With Microsoft Exchange), Release 4.0(4)
Cisco IOS Security Configuration Guide Version 12.2

Administration Documentation for the Cisco 2651XM-V
Cisco 2600 Series Routers Hardware Installation Guide
Cisco Network Modules Hardware Installation Guide for Cisco 2600 Series, Cisco 2800 Series, Cisco 3600 Series, Cisco 3700 Series, Cisco 3800 Series, and Cisco MWR 1941-DC Routers
Software Configuration Guide For Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers
Cisco IOS Security configuration guide

User Documentation

User Documentation for Cisco Unity
Cisco Unity User Guide Release 4.0(3).

User Documentation for the IP Phones
Cisco IP Phone 7970 User Guide
Cisco IP Phone 7960 User Guide

1.4.2 Logical Scope and Boundaries

The Logical Scope and Boundary of the TOE is the following:

1. The software in the 7970G and 7960G IP Phones.
2. The Cisco CallManager software that implements TOE functionality. Note that the underlying operating system, SQL server etc. is excluded.
3. The Cisco Unity software that implements TOE functionality. Note that the underlying operating system, SQL server etc. is excluded.
4. The Cisco 2651XM-V router software (IOS operating system).

1.4.2.1 IP Phones

Cisco IP phones contain software that provide voice communication over an IP-based network. The software is self contained and does not provide any TSF functionality that must be administered.

1.4.2.2 Cisco CallManager

Cisco CallManager software version 4.1(2) provides an IP telephony call-processing solution that guides the other TOE components in routing calls and is self protecting. It does not rely on underlying components to provide security functionality. A web interface to the configuration database enables secure remote device and system configuration using the HTTPS (SSL/TLS) protocol. Hyper Text Markup Language (HTML) based online help is also available for administrators.

1.4.2.3 Cisco Unity

Cisco Unity allows users to listen to their voice messages, send voice messages to other users, and customize settings such as personal greetings. With Cisco Unity the user can set up an automated attendant that answers and routes incoming calls.

The Web Administrator provides an interface to create or modify user accounts, configure messaging options, assign classes of service, record greetings, and run reports. Cisco Unity is administered via the same web interface that is used to administer the Cisco CallManager. It does not rely on underlying components to provide security functionality.

Users access their voice messages on Cisco Unity through the IP Phone.

1.4.2.4 Cisco 2651XM-V

The Cisco 2651XM-V router (Gateway) runs a version of the IOS software that is administered by attaching a console or PC running terminal emulation software to a port on the rear of the router.

2 Conformance claims

2.1 Conformance claim

This Security Target is EAL1 conformant and claims conformance to:
Common Criteria for Information Technology Security Evaluation
- Parts I and III, version 2.4, revision 256 and v2.4 Draft Interpretation[1] #1-#17 dated February 24, 2005.
- Parts II, version 2.1 including Final Interpretations as of date 2003-12-31.

2.2 Protection Profile claim

This ST (and TOE) claims conformance to the following PP:

Low Assurance Protection Profile for a VoIP Infrastructure 1.1, TNO-ITSEF BV, March 14th 2005.

2.3 Package claim

This ST is EAL1 conformant. The EAL1 package contains no uncompleted operations. As no SARs were added to EAL1, the SARs in this ST are consistent with EAL1.

[1] V2.4 Draft Interpretation #n are interpretations that are made during the v2.4 Trial Period. They address problems with CC v2.4 as they occur.

3 Definition of Terms

3.1 Definition of subjects, information and operations

This section is added to define the terms that are used in the SFRs.

3.1.1 Subjects

The subjects are defined in [VOIP-PP]. This Security Target does not define any additional subjects for the TOE.

3.1.2 Operations

The operations are defined in [VOIP-PP]. This Security Target does not define any additional operations for the TOE.

3.1.3 Objects

The objects are defined in [VOIP-PP]. This Security Target does not define any additional objects for the TOE.

4 Security Objectives for the Operational Environment

The Security Objectives for the Operational Environment are defined in [VOIP-PP]. This Security Target does not define any additional Security Objectives for the Operational Environment for the TOE.

5 Security Requirements

5.1 Extended components definition

As this ST does not contain extended security requirements, there are no extended components to define.

5.2 SFRs

The SFRs are grouped for easy understanding:

- Restricting access to certain telephone numbers
- Voice mail
- Managing telephones
- Identifying users
- Logging and auditing
- Self-protection

5.2.1 Restricting access to certain telephone numbers

The reader is referred to [VOIP-PP] for the SFRs relating to restricting access to certain telephone numbers:

- Subset access control (FDP_ACC.1)
- Security attribute based access control (FDP_ACF.1)
- Management of TSF data (FMT_MTD.1)

5.2.2 Voice mail

Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1	The TSF shall allow **no voice mail related actions**[2] on behalf of the user to be performed before **S.USER** is authenticated.
FIA_UAU.1.2	The TSF shall require **S.USER** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of **S.USER**.

5.2.3 Managing telephones

The reader is referred to [VOIP-PP] for the SFRs relating to managing telephones:

- Management of TSF data (FMT_MSA.1)
- User authentication before any action (FIA_UAU.2)

[2] [VOIP-PP] defines this SFR as 'The TSF shall allow all actions except R.GET_VMAIL , R.DEL_VMAIL, [assignment: other actions] on behalf' etc. etc. The user cannot access the Cisco Unity voicemail functions without first identifying themselves. These functions include R.GET_VMAIL and R.DEL_VMAIL. Please see [UNITY_USER] for more information.

5.2.4 Identifying users

The reader is referred to [VOIP-PP] for the SFRs relating to identifying users:

- Security roles (FMT_SMR.1)
- User identification before any action (FIA_UID.2)

5.2.5 Logging and auditing

FAU_GEN.1 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) **Registration of a new S.IN_PHONE, details of calls made by S.IN_PHONE as described in the document [CDR-DEF], modification of the configuration of S.IN_PHONE, failed authentication events and no other specifically defined auditable events**[3]**.**

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.**

FAU_SAR.1 Audit review[4]

FAU_SAR.1.1 The TSF shall provide **administrators** with the capability to read **audit information** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.6 Self-protection

FPT_SEP.1 TSF domain separation

[3] The comma before the word 'and' in 'and no other' was removed for grammatical reasons.

[4] Application Note: The following text is taken from [VOIP-PP] *"Application Note: This PP does not prescribe what is actually done with the generated audit data. The ST author should add FAU_SAR, FAU_SAA and/or FAU_ARP requirements where necessary to describe his specific solution."*. The author of this Security Target interprets in inclusion of the words 'where necessary' and the comma between FAU_SAR and FAU_SAA to mean that either FAU_SAR or FAU_SAA should be chosen where necessary and the inclusion of FAU_ARP is optional.

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.

5.3 SARs

The Security Assurance Requirements are defined in [VOIP-PP]. This Security Target does not define any additional security assurance requirements for the TOE.

6 TOE Summary Section

In this section, the manner in which the TOE implements the SFRs that are defined in chapter 5 is given.

6.1 TOE Security Functions

The TOE Security Functions are defined as:

- Restricting access to certain telephone numbers
- Voice mail
- Managing telephones
- Identifying users
- Logging and auditing
- Self-protection

In order to use the security functions provided by the TOE, the S.ADMIN must first log onto the Cisco CallManager via a web browser interface. Data communication between the Cisco CallManager web server that the administrator interfaces with via his browser is encrypted by using a HTTPS connection.

Only administrators who supply the correct log-in credentials as defined during the Cisco CallManager installation process can access the TOE security functions as S.ADMIN. In addition, the S.USER is required to log-on to the TOE in order to use voicemail functionality. They do this via their phone keypad.

6.1.1 Restricting access to certain telephone numbers

This security function helps implement the SFRs by allowing the administrator to restrict access to certain telephone number by defining 'Route Patterns'. Only S.ADMIN can define these as he is required to identify and authenticate himself first. S.ADMIN creates Route Patterns in order to define how the Cisco CallManager handles dialled number requests that S.USER can enter (i.e. the administrator may wish to block attempts to dial international numbers). S.ADMIN can define a pattern that represents a specific number and choose whether to block or allow S.USER dialled number requests that match the specified pattern via the 'Route Option' field.

More information can be found in the 'Device Configuration – Cisco IP Phone Configuration', Page 57-1 of [CM_ADMIN].

6.1.2 Voice mail

This security function helps implement the SFRs as in order to access voice mail, the S.USER associated with the phone device must log onto the Cisco Unity voicemail server. They can do this by calling the Cisco Unity voicemail server. This can be from a different telephone number than their own. The logon procedure requires the S.USER to enter their phone number followed by a '#'. They are then prompted to enter their password followed by a '#'. When successfully authenticated, they can listen to stored voicemail messages and delete them via menu interface that the user navigates through by using the phone keypad.

More information about the S.USER logon procedure can be found in the section ‘Working With Cisco Unity By Phone’, Page 3-2 of [UNITY_USER].

6.1.3 Managing telephones

This security function helps implement the SFRs as the TOE only allows the modification of phone data by the S.ADMIN who must firstly supply the correct logon credentials before the TSF allows the telephones to be managed.

Before an IP phone can be used it must be added to the Cisco CallManager. The phone is identified in the Cisco CallManager based on its network card MAC address. Once a phone has been added to the Cisco CallManager, it can be assigned a Directory Entry which gives the telephone device an actual telephone number.

Detailed information about how telephones can be managed and the data that defines the phone in the Cisco CallManager can be found in the ‘Device Configuration’ section of the Cisco CallManager Administration Guidance.
[PHONE-DEF].

6.1.4 Identifying users

This security function helps implement the SFRs by ensuring that the TOE differentiates between the S.USER and S.ADMIN roles. It does this by requiring administrators to supply the correct logon credentials in order to identify and authenticate themselves. The interface to the administrator functionality is via an HTTPS secured HTML interface. The web server that provides the interface requires correct logon credentials before access is given to TSF administrative functions.

All non-administrators are regarded by the TOE as users who interface with the TOE via the phone. The telephone keypad provides the interface provides the interface that S.USER uses to provide the correct logon credentials before access is given to the TSF administered voice mail functionality.

6.1.5 Logging and auditing

This security function helps implement the SFRs as the TOE is able to record audit information in the form of a traces, alarms and Call Descriptor Records (CDR) records. S.ADMIN is able to configure the TOE to log the information required by [VOIP-PP] through the administrator interface.

More information about logging and auditing is described in [CM_TRACE]. More information about Call Descriptor Records can be found in [CDR-DEF].

6.1.6 Self-protection

This security function helps implement the SFRs as the TOE has been carefully designed, implemented and tested and therefore provides adequate self protection that meets the requirements made by [VOIP-PP]. It is not possible to configure the TSF except via the administrator interface provided by the TOE to S.ADMIN.