Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0306-2005

for

Cisco VoIP Telephony Solution

Version 1.0

from

Cisco Systems, Inc.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn

Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0306-2005

for

Cisco VoIP Telephony Solution

Version 1.0

from

Cisco Systems, Inc.

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.4 revision 256 including draft interpretation #1 - #17* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.4, revision 256.*

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0012-2005**
Functionality:	**BSI-PP-0012-2005 conformant** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL1**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, May 12th, 2005

The Vice President of the Federal Office
for Information Security

Hange L.S.

Common Criteria

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

According to the decree issued by the Bundesministerium des Innern (Federal Ministry of the Interior) on 22. February 2005 the BSI is authorised to issue certificates for the CC version 2.4.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.4, revision 256 (see also Internet: http://www.bsi.bund.de)
- Common Methodology for IT Security Evaluation (CEM), Version 2.4, revision 256 with draft interpretations #1 - #17 (see also Internet: http://www.bsi.bund.de)
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005 and India in April 2005.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Cisco VoIP Telephony Solution, Version 1.0 has undergone the certification procedure at BSI.

The evaluation of the product Cisco VoIP Telephony Solution, Version 1.0 was conducted by TNO-ITSEF BV. The TNO-ITSEF BV is an evaluation facility (ITSEF)[5] recognised by BSI.

The sponsor, vendor and distributor is:

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134, USA

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 12.05.2005.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance, please refer to the excerpts from the criteria at the end of the Certification Report.

[5] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-18.

The product Cisco VoIP Telephony Solution, Version 1.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +049 228/9582-111.

Further copies of this Certification Report can be requested from the vendor[6] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[6] Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134, USA

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

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 tampering and interference by being well designed, produced and tested.

The IT product **Cisco VoIP Telephony Solution, Version 1.0** consisting of Cisco Call Manager (version 4.1(2)), Cisco Unity (version 4.0(4)), Cisco 7960 VoIP Telephone (version 7.0(2)), Cisco 7970 Telephone (version 6.0(2)) and Cisco 2685XM-V Router (version 12.3(10)) was evaluated by TNO-ITSEF BV. The evaluation was completed on 27.04.2005. The TNO-ITSEF BV is an evaluation facility (ITSEF)[7] recognised by BSI.

The sponsor, vendor and distributor is

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134, USA

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part3

[7] Information Technology Security Evaluation Facility

for details). The TOE meets the assurance requirements of assurance level EAL1 (Evaluation Assurance Level 1).

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 conformant as shown in the following table.

SFRs	Component-Name
FAU_GEN.1	Security audit data generation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_UID.2	User identification before any action
FIA_UAU.1	Timing of authentication
FIA_UAU.2	User authentication before any action
FMT_MSA.1	Management of security attributes
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FPT_SEP.1	TSF domain separation

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target [6], chapter 5.

These Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Functions	Description
Restricting access to certain telephone numbers	The administrator is allowed 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.

Voice mail	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. 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.
Managing telephones	The TOE only allows the modification of phone data by S.ADMIN who must firstly supply the correct logon credentials before the TSF allows the telephones to be managed.
Identifying users	The TOE differentiates between 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. 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.
Logging and auditing	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 through the administrator interface.
Self-protection	The TOE has been carefully designed, implemented and tested and therefore provides adequate self protection. It is not possible to configure the TSF except via the administrator interface provided by the TOE to S.ADMIN.

Note: The given descriptions are summaries of the security functions. For more information, please refer to the Security Target [6], chapter 6.

1.3 Strength of Function

A strength of function-claim is no more part of the CC in version 2.4.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

Not applicable for a CC, version 2.4 Low Assurance Security Target.

1.5 Special configuration requirements

When the TOE shall be used in the evaluated configuration the protocol ‘HTTPS‘ always has to be enabled.

1.6 Assumptions about the operating environment

Not applicable for a CC, version 2.4 Low Assurance Security Target.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The TOE is the **Cisco VoIP Telephony Solution, Version 1.0** consisting of Cisco Call Manager (version 4.1(2)), Cisco Unity (version 4.0(4)), Cisco 7960 VoIP Telephone (version 7.0(2)), Cisco 7970 Telephone (version 6.0(2)) and Cisco 2685XM-V Router (version 12.3(10)).

3 Security Policy

The TOE is a VoIP telephony solution which provides all the technology required to build up an IP-based telephony system. 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 tampering and interference.

4 Assumptions and Clarification of Scope

4.1 Environmental assumptions

The definition of assumptions is not applicable for CC version 2.4 and EAL1. Instead of assumptions the objectives which the operational environment of the TOE shall be conformant to (defined in the PP [8]) are listed here:

OE.PHONE_LOCATION	The operational environment of the VoIP phones shall be a general office-type environment: physical access is restricted to office personnel, visitors and the like.
OE.AGENT_LOCATION	The operational environment of the Call Control Agent and the Voice Mail System shall be a general server room environment: physical access will be restricted to authorised administrative personnel.
OE.NETWORK	The Operational Environment shall contain an IP-network.
OE.NW_FEATURES	If required, the IP-Network shall ensure that: - VoIP traffic will not be able to monopolise the IPNetwork to the point that other network traffic is hindered; - Other network traffic will not be able to monopolise the IP-Network to the point that VoIP traffic is hindered; - VoIP traffic will not be able to connect to some (or all) office equipment

4.2 Clarification of scope

This chapter is not applicable for CC version 2.4 Low Assurance Security Targets as there is no definition of threats in the PP [8] and ST [6].

5 Architectural Information

Because of the EAL-level (EAL1) this evaluation does not include ADV_HLD. Please refer to figure 1 in chapter 1.4.1 of the ST [6], which presents a graphical overview of the different components of the TOE.

6 Documentation

Administration Documentation

General Administration documentation

- Commentary and Configuration Guidelines for Implementation of the IPT System Evaluated Common Criteria 2.4 EAL 1, version 1.0, dated February 23, 2005. [9]

Administration documentation for Cisco call manager

- Cisco CallManager Administration Guide, Release 4.1(2), OL-6503-01 (ccmigration_09186a00802deadf.pdf) [10]
- Cisco CallManager Serviceability Administration Guide, Release 4.1(2), Text Part Number: OL-6508-01. [11]
- Cisco CallManager 4.1(2) Call Detail Record Definition, Text Part Number: OL-5435-01. [12]
- Cisco CallManager Security Guide, Release 4.1(2), Text Part Number: OL-6501-01 (ccmigration_09186a00802e406e.pdf) [13]
- Installing Cisco Call manager, Release 4.1(2), 78-16711-01,(cm412ins.pdf) [14]
- Cisco CallManager System Guide, Release 4.1(2), Text Part Number: OL-6504-01. [15]

Administration documentation for IP Phones

- Cisco IP phone 7970 Administration guide for Cisco Call Manager 4.0, Text Part Number: OL-4314-02 [16]
- Cisco IP Phone Administration Guide for Cisco CallManager 4.1, Cisco IP Phone Models 7960G and 7940G (ccmigration_09186a008024f5ab.pdf) [17]

Administration documentation for Cisco Unity

- Unity System Administration Guide (With Microsoft Exchange) Rele ase 4.0(4), May 25, 2004 (ccmigration_09186a008022c97e.pdf) [18]
- Cisco Unity Installation Guide (With Microsoft Exchange) 4.0(4), Release 4.0(4), May 25, 2004 Text Part Number: OL-5851-01 (ccmigration_09186a008022b8b6.pdf) [19]

- Cisco IOS Security Configuration Guide Release 12.2, Text Part Number: 78-11747-01 [20]

Administration documentation for Cisco 2651XM-V

- Cisco 2600 Series Routers Hardware Installation Guide, Text Part Number: OL-2171-05 [21]
- 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, Text Part Number: OL-2485-15 [22]
- Software Configuration Guide For Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers, Text Part Number: OL-1957-04 [23]

User Documentation

User documentation for Cisco Unity

- Cisco Unity User Guide Release 4.0(3) (With Microsoft Exchange), September 5, 2003 Text Part Number: OL-4727-01 [24]

User documentation for IP Phones

- Cisco IP Phone 7960 User Guide. [25]
- Cisco IP Phone 7970 User Guide License and Warranty. Text Part Number: 78-15630-02 [26]

7 IT Product Testing

On this EAL-level (EAL1) only independent evaluator test have to be conducted.

7.1 Testing Approach

Tests are executed according to the test specification of the evaluation facility. The tests are built upon the TOE security function interfaces as defined in the Functional Specification. The TOE security function interfaces are:

Interface	Purpose
Unity / LAN interface	Interconnecting the different components of the TOE through the supporting LAN.
Call manager / LAN interface	
Phone/ LAN interface	
Router/LAN interface	
Call manager-unity / Human interface	Management of the TOE by the TOE administrator.
Router/Human interface	
Router/PSTN interface	Connecting the TOE to an external public telephone network
Phone / Human interface	Allowing the user to interface with the TOE. (for phone calls and voice mail)

The objectives for the tests are derived from the security functions and are:

- To check the restriction of IP phone users access to certain telephone numbers.
- To check the identification and authentication of users who wish to access the TOEs' voice mail services.
- To check the management of IP Phones.
- To check the provision of systems traces through alarms, system traces and call information.

Protection of the TOE itself and the security functions it offers by being well designed, implemented and tested.

7.2 Test Configuration

The testing took place at Cisco's premises in Herndon, Virginia, USA. The used test configuration was commensurate with the descriptions in the ST [6].

7.3 Test Depth and Results

The test effort is commensurate with the functional specification and covers all TSFI.

The results of the developer testing showed that the security functionality performs as expected.

This means that the developer has showed that:

- The TOE restricts IP phone users access to certain telephone numbers.
- The TOE enforces the identification and authentication of users who wish to access the TOEs' voice mail services.
- The TOE provides for the management of IP Phones.
- The TOE provides systems traces system traces and call information.
- The TOE protects itself by being well defined, developed and tested as required by this evaluation.

8 Evaluated Configuration

Component	Hardware Version	Software Version in the TOE
Cisco IP Telephone	7960G	7.0(2)
Cisco IP Telephone	7970G	6.0(2)
Cisco Call Manager	N/A	4.1(2)
Cisco Unity	N/A	4.0(4)
Cisco Router	2651XM -V	12.3(10)

The following supporting hardware and software was used:

- A LAN, to link the various components of the TOE
- A Cisco MCS7800 rack mounted server for Cisco Call Manager
- A Cisco MCS7800 rack mounted server for Cisco Unity

Call Manager and Unity both run on a Microsoft Windows 2000 server installation, pre-configured by Cisco with the required software. The version number of the OS installation was identified during the test version 2.6sr5. The installation includes Java Runtime 1.4.2-04 and Microsoft SQL server 2000.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the scheme [3] and all interpretations and guidelines of the scheme [4] as relevant for the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL1 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		Verdict
Security Target evaluation	CC Class ASE	PASS
Conformance claims	ASE_CCL.1	PASS
Extended components definition	ASE_ECD.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives for the operational environment	ASE_OBJ.0	PASS
Security requirements	ASE_REQ.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Capabilities	ACM_CAP.1	PASS
Delivery and operation	CC Class ADO	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Functional specification	ADV_FSP.1	PASS
Representation correspondence	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Tests	CC Class ATE	PASS
Independent testing	ATE_IND.1	PASS

The evaluation has shown that:

- the TOE is conform to the Protection Profile BSI-PP-0012-2005
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL1

The results of the evaluation are only applicable to the Cisco VoIP Telephony Solution, Version 1.0 consisting of Cisco Call Manager (version 4.1(2)), Cisco Unity (version 4.0(4)), Cisco 7960 VoIP Telephone (version 7.0(2)), Cisco 7970 Telephone (version 6.0(2)) and Cisco 2685XM-V Router (version 12.3(10)) (see also chapter 2 of this report).

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The customer is recommended to read the general administration documentation called 'Commentary and Configuration Guidelines for Implementation of the IPT System Evaluated Common Criteria 2.4 EAL 1, version 1.0, dated February 23, 2005.' before installation of the TOE.

The 'HTTPS' protocol always has to be enabled when the TOE shall be used in the evaluated configuration.

11 Security Target

For the purpose of publishing, the Security Target [6] of the target of evaluation (TOE) is provided within a separate document.

12 Definitions

12.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
HTTPS	Hyper Text Transfer Protocol Secure sockets
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
ST	Security Target
VoIP	Voice over IP

TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.4, revision 256

[2] Common Methodology for Information Technology Security Evaluation (CEM), Version 2.4, revision 256

[3] BSI certification: Procedural Description (BSI 7125)

[4] Applicaton Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-0306-2005, Version 1.6, 14. March 2005 , Low Assurance Security Target for a Cisco VoIP Telephony System, Cisco Systems, Inc..

[7] Evaluation Technical Report, Version 3.0, 14. March 2005

[8] Protection Profile BSI-PP-0012-2005

Guidance Documentation

General Administration documentation

[9] Commentary and Configuration Guidelines for Implementation of the IPT System Evaluated Common Criteria 2.4 EAL 1, version 1.0, dated February 23, 2005.

Administration documentation for Cisco call manager

[10] Cisco CallManager Administration Guide, Release 4.1(2), OL-6503-01 (ccmigration_09186a00802deadf.pdf)

[11] Cisco CallManager Serviceability Administration Guide, Release 4.1(2), Text Part Number: OL-6508-01.

[12] Cisco CallManager 4.1(2) Call Detail Record Definition, Text Part Number: OL-5435-01.

[13] Cisco CallManager Security Guide, Release 4.1(2), Text Part Number: OL-6501-01 (ccmigration_09186a00802e406e.pdf)

[14] Installing Cisco Call manager, Release 4.1(2), 78-16711-01, (cm412ins.pdf)

[15] Cisco CallManager System Guide, Release 4.1(2), Text Part Number: OL-6504-01.

Administration documentation for IP Phones

[16] Cisco IP phone 7970 Administration guide for Cisco Call Manager 4.0, Text Part Number: OL-4314-02

[17] Cisco IP Phone Administration Guide for Cisco CallManager 4.1, Cisco IP Phone Models 7960G and 7940G (ccmigration_09186a008024f5ab.pdf)

Administration documentation for Cisco Unity

[18] Unity System Administration Guide (With Microsoft Exchange) Rele ase 4.0(4), May 25, 2004 (ccmigration_09186a008022c97e.pdf)

[19] Cisco Unity Installation Guide (With Microsoft Exchange) 4.0(4), Release 4.0(4), May 25, 2004 Text Part Number: OL-5851-01 (ccmigration_09186a008022b8b6.pdf)

[20] Cisco IOS Security Configuration Guide Release 12.2, Text Part Number: 78-11747-01

Administration documentation for Cisco 2651XM-V

[21] Cisco 2600 Series Routers Hardware Installation Guide, Text Part Number: OL-2171-05

[22] 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, Text Part Number: OL-2485-15

[23] Software Configuration Guide For Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers, Text Part Number: OL-1957-04

User documentation for Cisco Unity

[24] Cisco Unity User Guide Release 4.0(3) (With Microsoft Exchange), September 5, 2003 Text Part Number: OL-4727-01

User documentation for IP Phones

[25] Cisco IP Phone 7960 User Guide.

[26] Cisco IP Phone 7970 User Guide License and Warranty. Text Part Number: 78-15630-02

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 5.4)

The conformance claim indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance claim contains a CC conformance claim that:

a) describes to which version of the CC the TOE or PP claims conformance

b) describes the conformance to Part 2 (security functional requirements) as either:

- **Part 2 conformant** - A PP or TOE is Part 2 conformant if all SFRs are based only upon functional components in CC Part 2, or
- **Part 2 extended** - A PP or TOE is Part 2 extended if at least one SFR is not based upon functional components in CC Part 2.

c) describes the conformance to Part 3 (security assurance requirements) as either:

- **Part 3 conformant** - A PP or TOE is Part 3 conformant if all SARs are based only upon assurance components in CC Part 3, or
- **Part 3 extended** - A PP or TOE is Part 3 extended if at least one SAR is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:.

- Package name Conformant - A PP or TOE is conformant to a predefined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- Package name Augmented - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance claim may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Evaluation assurance levels (chapter 4)

„The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview (chapter 4.1)

Table 2 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 4.3)

Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.

Assurance components

EAL1 provides a basic level of assurance by a limited Security Target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

The analysis is supported by independent testing of the TSF.

This EAL provides a meaningful increase in assurance over unevaluated IT.

ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.0	Security objectives for the operational environment
ASE_REQ.1	Security requirements
ASE_TSS.1	TOE summary specification
ACM_CAP.1	Capabilities
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_RCR.1	Representation correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_IND.1	Independent testing

This page is intentionally left blank.