Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0540-2009

for

Avaya VoIP PBX System
based on the Communication Manager 5.1

from

Avaya GmbH & Co. KG

sponsored by

Avaya Inc.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0540-2009

Avaya VoIP PBX System
based on the Communication Manager 5.1

from	Avaya GmbH & Co. KG
sponsored by	Avaya Inc.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 1 augmented by ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1 and ADV_FSP.2

Common Criteria
Recognition
Arrangement

Common Criteria

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 (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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.

Bonn, 27 March 2009
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski
Abteilungspräsident

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

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.

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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

---

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 07 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

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

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 Avaya VoIP PBX System based on the Communication Manager 5.1 has undergone the certification procedure at BSI.

The evaluation of the product Avaya VoIP PBX System based on the Communication Manager 5.1 was conducted by CSC Deutschland Solutions GmbH. The evaluation was completed on 10 March 2009. The CSC Deutschland Solutions GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: Avaya GmbH & Co. KG

The sponsor is: Avaya Inc.
Avaya Inc. Headquaters
211 Mt. Airy Road
Basking Ridge, NJ 07920
USA

The product was developed by: Avaya GmbH & Co. KG
Kleyerstraße 94
60326 Frankfurt

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

[6] Information Technology Security Evaluation Facility

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. 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 and in the Security Target.

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

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Avaya VoIP PBX System based on the Communication Manager 5.1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Avaya GmbH & Co. KG
Kleyerstraße 94
60326 Frankfurt

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.

1 Executive Summary

The Target of Evaluation (TOE) is the Avaya VoIP PBX System based on the Communication Manager 5.1 (for detailed description of the scope of the TOE see chapter 2 of this report).

The TOE is a sophisticated communication system from Avaya which is based on the VoIP (Voice over IP) platform which mainly provides authentication, confidential communication and auditing. The system meets all demands from small companies with less than 100 employees to global enterprises with ten-thousands of employees on a single system to more than one million users on a single network.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 1 augmented by ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1 and ADV_FSP.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.3. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Function	Addressed issue
Authentication and access restrictions	Authentication of all human users and access restrictions to specific user roles.
Securing the confidentiality and integrity of communication data	Signalling data as well as media streams will be protected regarding confidentiality and integrity as long as they are inside the TSC.
Self-protection of the telephones and servers	The phones will only accept new configuration files with correct digital signature.
Logging of security relevant events	All security relevant events will be logged by the TOE servers.
Managing of user access restrictions	The user access to certain phone numbers may be restricted by the administrators.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.2 – 3.4.

The TOE is composed of up to six different components (see chapter 2 of this report), which all have several configuration options. Only some of these configuration options in each TOE component are security relevant. The guidance document “Security Configuration Guidelines of the certified system based on the Communication Manager

5.1” [15] lists all security relevant configuration options and describes in detail the configuration of the TOE which is covered by the certification.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

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 Target of Evaluation (TOE) is called:

Avaya VoIP PBX System based on the Communication Manager 5.1

In the following the TOE deliverables are outlined:

- The Avaya Communication Manager 5.1 which is running on the Avaya Media Server S8730
- The Avaya Media Gateway G650 exactly with the three modules listed below:
  - IPSI TN2312BP Firmware 44
  - C-LAN TN799DP Firmware 26
  - Medpro TN2602AP Firmware 41
- The Avaya SES Server 5.1 on the Avaya Media Server S8500C
- The following models of the Avaya one-X family together with protocol specific software application are part of the TOE:
  - 9630 for H.323 with software version 2.0
  - 9630 for SIP with software version 2.4
- The Avaya Secure Service Gateway (SSG) Version 3.1.22 on the Avaya Media Server S8500C.

The Avaya SSG is an optional component. The system also works without an Avaya SSG but remote-management by Avaya is then not possible.

The following guidance documents for each TOE part are part of the deliverables to the final customer. It must be mentioned that for each TOE server component all relevant documents are listed. This results in multiple listings of some documents.

Avaya Communication Manager

- The complete documentation for the Communication Manager is included on the Guidance CD “Communication Manager 5.0”, Publication Date: January 2008 [9] and structured as followed. In addition to this CD, there are additional documents available to support the user where indicated. Those documents are listed below and labelled by ID’s. Those documents can be downloaded from the Avaya support site (support.avaya.com).
- Overview
  - Integrated Management Overview, Release 4.0, Document-ID 14-601718, Issue 2, May 2007 [11]
- Design
  - All Covered by the Guidance CD “Communication Manager 5.0” [9]
- Implement
  - Avaya Remote Feature Activation (RFA) User Guide, Document-ID 03-300149, Issue 5.1, November 2007 [12]
- Maintain
  - All covered by the Guidance CD “Communication Manager 5.0” [9]
- User
  - All covered by the Guidance CD “Communication Manager 5.0” [9]
- System Management/Administer
  - Administration for Network Connectivity for Avaya Communication Manager, Document-ID 555-233-504, Issue 13, January 2008 [13]
  - SNMP Reference Guide for Avaya Communication Manager, Document-ID 03-602013, Issue 1.0, February 2007 [14]
  - Security Configuration Guidelines of the certified system based on the Communication Manager 5.1, Version 1.3, 17.02.2009 [15]
- The new and updated documentation for the CM Version 5.1 is included on the Guidance CD “Updated documents for the Communication Manager 5.1 CD Collection” [10]. Those documents can be downloaded from the Avaya support site (support.avaya.com).

Avaya 9630 Phone SIP

- Avaya one-X Deskphone SIP for 9630 IP-Telefon Quick Reference, Document-ID 16-601948 [16]
- Avaya one-X Deskphone SIP for 9630 IP-Telefon User Guide, Document-ID 16-601946 [17]
- Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 2.0, Document-ID 16-300698, Issue 5 [18]

- Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide, Release 2.0, Document-ID 16-300694, Issue 5, May 2008 [19]

Avaya 9630 Phone H.323

- Avaya one-X Deskphone Edition for 9630/9630 IP-Telefon Quick Reference, Document-ID 16-600913 [20]
- Avaya one-X Deskphone Edition for 9630/9630 IP-Telefon User Guide, Document-ID 16-300700 [21]

Avaya G650 Media Gateway

- Overview
  - All covered by the Guidance CD “Communication Manager 5.0” [9]
- Implement
  - All covered by the Guidance CD “Communication Manager 5.0” [9]
- Maintain
  - All covered by the Guidance CD “Communication Manager 5.0” [9]

Avaya Media Server

- Overview
  - All covered by the Guidance CD “Communication Manager 5.0” [9]
- Design
  - All covered by the Guidance CD “Communication Manager 5.0” [9]
- Implement
  - Job Aid: Upgrading Firmware on the BIOS - Avaya S8500 Media Server, Document-ID 03-300411, Issue 2, June 2005 [22]
- Maintain
  - All covered by the Guidance CD “Communication Manager 5.0” [9]
- System Management/Administration
  - Security the Avaya Communication Manager Media Servers, Issue 3, June 2005 [23]

Avaya SSG

- Secure Services Gateway (SSG) Documentation, Document ID 19-601378-4 [24]

Avaya SES

- All covered by the Guidance CD “Communication Manager 5.0” [9]

Due to being an EAL1+ evaluation the assurance family ALC_DEL is not in scope of this evaluation. Therefore, statements about the detailed delivery procedures and the scope of delivery can not be made. According to the developer the whole VoIP System will be delivered to the customer and will be installed and configured on site by Avaya service engineers according to the Security Target and the Guidance Documentation. The Guidance Documentation describes how to check that the TOE is configured according to the Security Target.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

Administrators have to enter a username-password-combination to access the TOE functions. Phone users have to enter their own phone number and a PIN to become authorized users in order to use the full allowed functionality of the phones.

The complete signalling data and media streams within the company internal LAN/WAN (TOE scope of control) are encrypted. Calls over the internet using the SIP trunk maybe encrypted, if supported by the provider but are outside the scope of this certification.

The TOE provides secure and dependable (trustworthy) mediation of sessions, i.e. caller party and called party of a call must be identified and authenticated and a call must only be mediated from the caller party to the called party.

The telephones protect themselves against unauthorized software updates and modification of its configuration by the use of digital signatures.

Security-relevant events will be logged.

Administrators can manage white- and black lists for telephone numbers, which means allowing and disallowing certain telephone numbers, for each authorized user.

Access for remote administrators by using the Avaya Secure Service Gateway (SSG) which is an optional part of the TOE is controlled by an identification & authentication process.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: Trustworthy administrators, availability of all required components, a carefully administered Configuration Server, timely analysis of the log files produced by the TOE, physical protection of the TOE by the environment, network protection mechanisms and responsible authorized users. Details can be found in the Security Target [6], chapter 3.2.

5 Architectural Information

The following figure shows the distribution of the different parts of the TOE over an internal network. The TOE parts are marked with red coloured boxes.

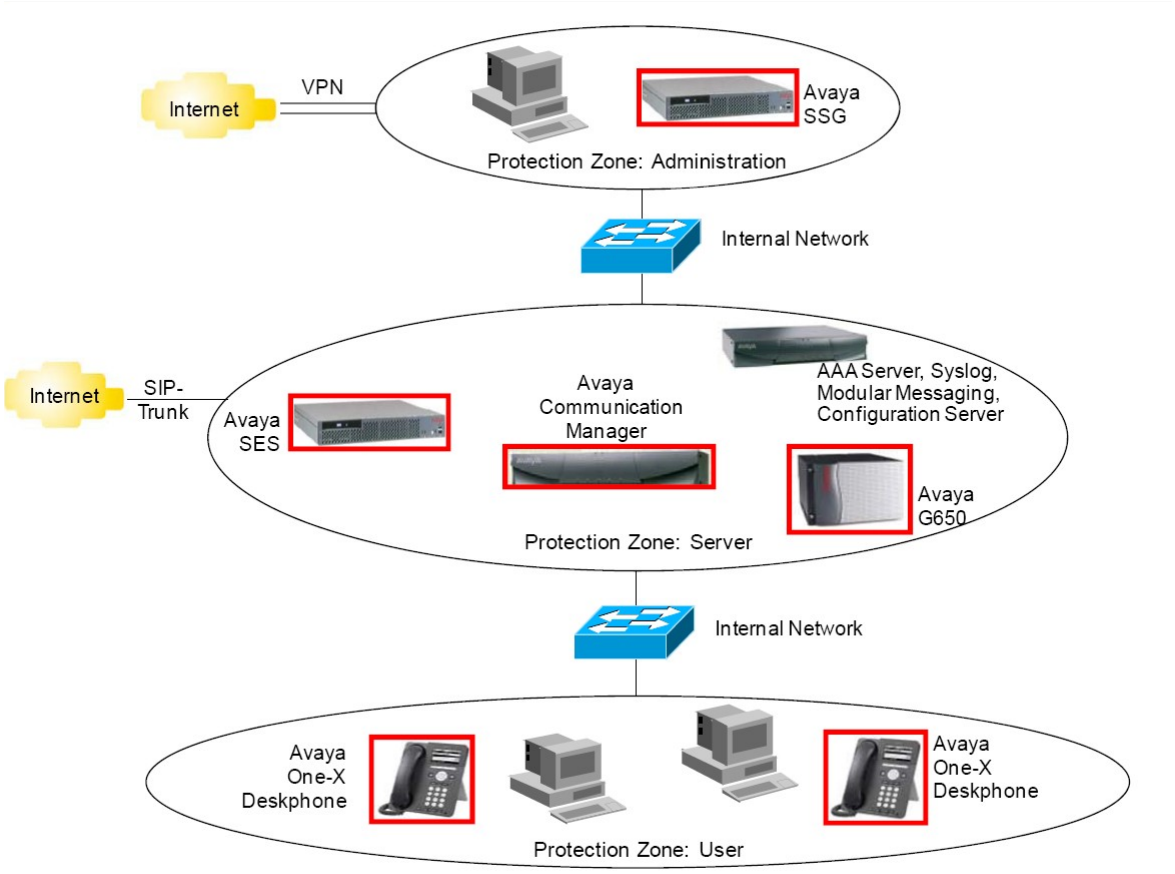

Figure 1: Structure of the VoIP System

The protection zone “User” contains all terminal devices like phones or computers. It should be remarked that only dedicated Avaya phones will be recognized as part of the certified system (see chapter 2 of this report). The phones can be used to enter the identification & authentication credentials of the human users and to make encrypted calls to other phones connected to this PBX. Calls over the internet (using the SIP trunk) to other phones cannot be encrypted. The phones itself are a trusted platform because they do not accept faked firmware or configuration data from unknown sources.

Between the protection zones “User” and “Server”, there are some network devices (hubs, switches, routers, maybe a firewall). These devices may implement some security features like IEEE 802.1X network device authentication. They are out of scope. Their existence and their security features can be assumed.

The protection zone “Server” contains the most important devices, the Avaya Media Gateways G650 (at least one, usually more), the Avaya Communication Manager and the Avaya SIP Enable Services (SES), which are all part of the TOE.
The servers are able to connect to other IP phones via the internal network, via the internet or via conventional telephone networks (PSTN, includes ISDN). The certified scenario just covers the communication over a company internal LAN/WAN and over the internet using a SIP trunk.

The Avaya Communication Manager is the actual centre of the communication. Here, the sessions will be mediated (signalling). Also here, client authentication (human users) will be performed and all security events are logged. The human users use the phones to enter their identification and authentication credentials. The phones register at the server after boot-up and prior to be ready-for-use.
The Avaya SES Server is a feature server for the modern SIP protocol. If SIP is used, the signalling information is protected by a TLS tunnel, which terminates at the SES server.
The Avaya Media Gateway G650 is just a “bridge” between the different network technologies and protocols (e.g. IP ↔ PSTN, or H.323 ↔ SIP). This includes that they have to perform the encryption and decryption of the media streams of a call for all participants of this call, if the phones do not use the same protocol or codec.
Additionally, the “Server” zone may contain additional servers like Modular Messaging, a Conferencing System, a central authentication Server, a Syslog Server (both here named as AAA Server) or client-specific application servers, which are all not part of the TOE. A Configuration Server, which is also located in the Server zone, stores the configuration files of the phones. This server is not part of the TOE but relevant for the operation.
Also here, the network devices like switches and routers are out of scope. This holds also valid for the connection to the internet (the SIP trunk) and the required network devices and firewalls.

Between the protection zones “Server” and “Administrator”, there are some network devices (hubs, switches, routers, maybe a firewall).

The protection zone “Administration” contains all systems and clients required for systems management (monitoring, administration). In general, these devices are not part of the TOE. As optional part of the TOE the Avaya Secure Service Gateway (SSG) is located in this zone. This device will be used as single-point-of-contact for the Avaya Support Centre, which provides remote administration services, so that the customer is always able to control all accesses to its system.
Avaya SSG enforces the access restrictions to the systems on network level configured by the customer’s administrator.

6 Documentation

The evaluated documentation as outlined in chapter 2 of this report is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 Independent Evaluator Testing

Due to the selected assurance level EAL1+ a rigorous test strategy is not adequate. Therefore, only simple tests and uncomplicated attacks are in scope of the test subset. Anyhow, the test strategy aims on covering all SFR's to an acceptable rate of coverage whereas coverage of external interfaces should be focused on not restricted interfaces. This means that tests of respective attacks against interfaces located in the server zone (see chapter 5 of this report) and protected by firewalls and physical means are limited to the minimum.

The TOE passed all evaluator tests. This means the verification of the complete and correct implementation of all TOE Security Functions and all TOE Security Functional Requirements was successful. The depth of testing was on the level of the external interfaces as required by ATE_IND.1.

7.2 Penetration Testing

According to the requirements of AVA_VAN.1 the evaluator did a research for common known vulnerabilities for this product or product type. The evaluator also performed penetration testing using penetration testing tools. The following penetration tests have been performed:

- The evaluators examined if it is possible to penetrate the phones via a various combination of key inputs. There were no vulnerabilities which allow unauthorised access to the management functions of the phone.
- Within a second test series the evaluators tested if an attacker may access the TOE exploiting a vulnerability of the used network protocols. No exploitable vulnerabilities of the network interfaces of the evaluated configuration could be identified.
- Moreover the evaluator examined the possibility to spoof the IP addresses of the TOE components in order to capture phone calls or login information. No vulnerabilities have been identified.
- Lastly, the evaluators analysed if an attacker may get access to the administrative interfaces of the TOE by applying brute-force attacks. The tests did not reveal any vulnerability.

8 Evaluated Configuration

The TOE is composed of up to six different components (see chapter 2 of this report), which all have several configuration options. Only some of these configuration options in each TOE component are security relevant. The guidance document "Security Configuration Guidelines of the certified system based on the Communication Manager 5.1" [15] lists all security relevant configuration options and describes in detail the configuration of the TOE which is covered by the certification. This guidance document will be delivered to the customer and is available on the Avaya support website (support.avaya.com).

The following major issues have to be considered:

- Encryption has to be enabled for all signalling data and media transfer within the company internal network. The protection of company external communication was not within the scope of the evaluation.
- The logging mechanisms have to be enabled.
- The identification and authentication mechanisms on all TOE components have to be securely configured.
- The certified scenario just covers company internal communication over a LAN/WAN and external calls over the internet using a SIP trunk. There is no external ISDN connection possible in the evaluated configuration.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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 (AIS) [4] as relevant for the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 1 package including the class ASE as defined in the CC (see also part C of this report)
- The components ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1 and ADV_FSP.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 1 augmented by
  ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1 and ADV_FSP.2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for: the cryptographic functions used in the TOE Security Functions “Securing the confidentiality and integrity of communication data” (AES 128) and “Self-protection of the telephones and servers” (SHA-1 and DSA-1024).

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2).

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in chapter 2 of this report contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Errichtungsgesetz

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

EAL Evaluation Assurance Level

IP Internet Protocol

ISDN Integrated Services Digital Network

IT Information Technology

ITSEC Information Technology Security Evaluation Criteria

ITSEF Information Technology Security Evaluation Facility

H.323 Packet-based multimedia communications systems (ITU-T recommendation)

LAN Local Area Network

PBX Private Branch Exchange

PP Protection Profile

PSTN Public Switched Telephone Network

SAR Security Assurance Requirement

SES SIP enable services

SF Security Function

SFP Security Function Policy

SFR Security Functional Requirement

SIP Session Initiation Protocol

SSG Secure Service Gateway

ST Security Target

TLS Transport Layer Security

TSC TOE Scope of Control

TOE Target of Evaluation

TSF TOE Security Functions

VoIP Voice over IP

WAN Wide Area Network

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

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

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

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

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

[5] German IT Security Certifcates (BSI 7148, BSI 7149), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-0540-2009, Version 1.11, 2009-02-19, Avaya VoIP PBX System Security Target, Avaya GmbH & Co KG

[7] Evaluation Technical Report, Version 1.0, 2009-03-10, Evaluation Technical Report BSI-DSZ-CC-0540, CSC Deutschland Solutions GmbH, (confidential document)

[8] Configuration list for the TOE, Version 1.0, 2009-03-09, Avaya VoIP PBX System Configuration List, Avaya GmbH & Co KG (confidential document)

[9] Guidance CD “Communication Manager 5.0”, Publication Date: January 2008

[10] Guidance CD “Updated documents for the Communication Manager 5.1 - CD Collection”, Publication Date: June 2008

[11] Integrated Management Overview, Release 4.0, Document-ID 14-601718, Issue 2, May 2007

[12] Avaya Remote Feature Activation (RFA) User Guide, Document-ID 03-300149, Issue 5.1, November 2007

[13] Administration for Network Connectivity for Avaya Communication Manager, Document-ID 555-233-504, Issue 13, January 2008

[14] SNMP Reference Guide for Avaya Communication Manager, Document-ID 03-602013, Issue 1.0, February 2007

[15] Security Configuration Guidelines of the certified system based on the Communication Manager 5.1, Version 1.3, 17.02.2009

[16] Avaya one-X Deskphone SIP for 9630 IP-Telefon Quick Reference, Document-ID 16-601948

[17] Avaya one-X Deskphone SIP for 9630 IP-Telefon User Guide, Document-ID 16-601946

[18] Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 2.0, Document-ID 16-300698, Issue 5

[19] Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide, Release 2.0, Document-ID 16-300694, Issue 5, May 2008

[20] Avaya one-X Deskphone Edition for 9630/9630 IP-Telefon Quick Reference, Document-ID 16-600913

[21] Avaya one-X Deskphone Edition for 9630/9630 IP-Telefon User Guide, Document-ID 16-300700

[22] Job Aid: Upgrading Firmware on the BIOS - Avaya S8500 Media Server, Document ID 03-300411, Issue 2, June 2005

[23] Security the Avaya Communication Manager Media Servers, Issue 3, June 2005

[24] Secure Services Gateway (SSG) Documentation, Document ID 19-601378-4

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

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

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

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

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex A.

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decompositon.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“ 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 CC 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 8.1)

“Table 1 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 7 of this CC 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.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.