Avaya VoIP PBX System

Security Target

Prepared by

Avaya GmbH & Co KG

Dieter Rohrdrommel
Kleyerstraße 94
60326 Frankfurt am Main
Germany

CSC Deutschland Solutions GmbH

Peter Rehäußer
Sandstr. 7-9
80335 München
Germany

Date 2009/02/19, Author: Peter Rehäußer (CSC Deutschland Solutions GmbH), Dieter Rohrdrommel (GCS/LE-PM),

Document History

Version	Date	Author	Remarks
0.1	2007/11/27	Peter Rehäußer	Initial Version
0.2	2007/12/14	Peter Rehäußer	Reviewed by Avaya USA, Comments of the evaluator
0.3	2007/12/18	Peter Rehäußer	2nd Review by Avaya and comments of the valuator
1.0	2008/01/08	Peter Rehäußer	3rd Review by Avaya
1.1	2008/04/18	Peter Rehäußer	Some updates due to findings in FSP
1.2	2008/06/03	Peter Rehäußer	Update of Assurance Requirements and TOE definition
1.3	2008/07/11	Dieter Rohrdrommel	Update to CM version 5.1
1.4	2008/07/23	Peter Rehäußer	Updates due to some BSI inquiries
1.5	2008/08/05	Peter Rehäußer	Update to cover separation of TOE and operating system in a better way.
1.6	2008/09/22	Peter Rehäußer	Updates due to some BSI inquiries
1.7	2008/10/17	Peter Rehäußer	Updates due to some test results
1.8	2008/12/10	Peter Rehäußer	Updates due to some BSI inquiries
1.9	2009/01/22	Peter Rehäußer	Updates due to new TOE definition
1.10	2009/02/17	Peter Rehäußer	Update of TOE guidance documents
1.11	2009/02/19	Peter Rehäußer	Updates due to some BSI inquiries

1 ST INTRODUCTION 5

1.1 ST REFERENCE 5
1.2 TOE REFERENCE 5
1.3 TOE OVERVIEW 7
1.3.1 USAGE AND MAJOR SECURITY FEATURES OF THE TOE 7
1.3.2 TOE TYPE 9
1.3.3 REQUIRED NON-TOE HARDWARE/SOFTWARE/FIRMWARE 10
1.4 TOE DESCRIPTION 11
1.4.1 PHYSICAL SCOPE OF THE TOE 11
1.4.2 LOGICAL SCOPE OF THE TOE 12
1.4.3 CONFIGURATION UNDER EVALUATION 14

2 CONFORMANCE CLAIM 15

2.1 CC CONFORMANCE CLAIM 15
2.2 PP CONFORMANCE CLAIM 15
2.3 PACKAGE CLAIM 15

3 SECURITY PROBLEM DEFINITION 16

3.1 DEFINITIONS 16
3.1.1 SUBJECTS 16
3.1.2 OBJECTS 17
3.1.3 INFORMATION 17
3.1.4 OPERATIONS 18
3.1.5 SECURITY ATTRIBUTES 18
3.2 ASSUMPTIONS 19
3.3 THREATS 20
3.4 ORGANIZATIONAL SECURITY POLICIES 21

4 SECURITY OBJECTIVES 22

4.1 SECURITY OBJECTIVES FOR THE TOE 22
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 23
4.3 RATIONALE FOR SECURITY OBJECTIVES 25
4.3.1 COVERAGE OF THE ASSUMPTIONS 26
4.3.2 COVERAGE OF THE THREATS 27
4.3.3 IMPLEMENTATION OF ORGANIZATIONAL SECURITY POLICIES 28

5 SECURITY REQUIREMENTS 29

5.1 CONVENTIONS 29
5.2 SECURITY POLICIES 29
5.2.1 AUDIT-EXPORT CONTROL POLICY 29

5.2.2 CALL-MEDIATION POLICY 30
5.2.3 USER ACCESS CONTROL POLICY 31
5.2.4 FIRMWARE-UPGRADE POLICY 32
5.3 SECURITY FUNCTIONAL REQUIREMENTS 33
5.3.1 SFR COVERING O.AUTHENTICATE 33
5.3.2 SFR COVERING O.CONFCLIENT 36
5.3.3 SFR COVERING O.DISCLOSE 38
5.3.4 SFR COVERING O.LOGEXPORT 41
5.3.5 SFR COVERING O.MEDIATION 44
5.3.6 SFR COVERING O.RESTRICTION 46
5.3.7 SFR COVERING O.SELFPROTECT 48
5.3.8 COMMON SFR 50
5.4 SECURITY ASSURANCE REQUIREMENTS 51
5.5 RATIONALE FOR THE SECURITY FUNCTIONAL REQUIREMENTS 52
5.6 RATIONALE FOR ASSURANCE REQUIREMENTS 55
5.7 RATIONALE FOR ALL NOT-SATISFIED DEPENDENCIES 56
5.7.1 SECURITY FUNCTIONAL REQUIREMENTS 56
5.7.2 SECURITY ASSURANCE REQUIREMENTS 57
6 TOE SUMMARY SPECIFICATION 59
6.1 COVERAGE OF THE SECURITY FUNCTIONAL REQUIREMENTS 59
7 ABBREVIATIONS 62
8 REFERENCES 63

1 ST Introduction

1.1 ST Reference

ST Name:	Avaya VoIP PBX System
Certification ID:	BSI-DSZ-CC-0540
ST Version:	1.11
Date:	2009/02/19
Applicant:	Avaya GmbH & Co KG
Authors:	Peter Rehäußer, CSC Deutschland Solutions GmbH
CC Version:	3.1

1.2 TOE Reference

The TOE consists of the following components and documents:

- 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 protocol specific software application on the telephone family Avaya One-X Deskphone.
  The following models of the Avaya One-X family are part of the TOE:
  - 9630 for H.323, software version 2.0
  - 9630 for SIP, 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.

- It is possible to extent some server with SAMP cards enabling emergency access options for administrators. These SAMP cards are not part of the TOE. Anyhow, these cards may be installed. It is assumed that the access options provided by these cards are sufficiently protected by the environment (e.g. physical protection, by network components, by the operating system).

  These TOE components are shown in Figure 1 below and marked with a red frame.

- The following guidance documents, which are part of the deliverables to the final customer:[1]
  - **Avaya Communication Manager**
    - The complete documentation for the Communication Manager is included on the Guidance CD "Communication Manager 5.0", Publication Date: January 2008 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 labeld 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
    - Design
      - All Covered by the Guidance CD "Communication Manager 5.0"
    - Implement
      - Avaya Remote Feature Activation (RFA) User Guide, Document ID 03-300149, Issue 5.1, November 2007
    - Maintain
      - All covered by the Guidance CD "Communication Manager 5.0"
    - User
      - All covered by the Guidance CD "Communication Manager 5.0"
    - System Management/Administer
      - Administration for Network Connectivity for Avaya Communication Manager, Document ID 555-233-504, Issue 13, January 2008
      - SNMP Reference Guide for Avaya Communication Manager, 03-602013, Issue 1.0, Feburary 2007
      - Security Configuration Guidelines of the certified system based on the Communication Manager 5.1 [SecureConfigG]
    - 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". 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 16-601948
    - Avaya one-X Deskphone SIP for 9630 IP-Telefon User Guide 16-601946
    - Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 2.0, 16-300698, Issue 5
    - Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide, Release 2.0, 16-300694, Issue 5, May 2008
  - **Avaya 9630 Phone H.323**
    - Avaya one-X Deskphone Edition for 9630/9630 IP-Telefon Quick Reference 16-600913
    - Avaya one-X Deskphone Edition for 9630/9630 IP-Telefon User Guide 16-300700

[1] It must be mentioned that for each TOE server component all relevant documents are listed. This results in multiple listings of some documents.

- **Avaya G650 Media Gateway**
  - Overview
    - All covered by the Guidance CD “Communication Manager 5.0”
  - Implement
    - All covered by the Guidance CD “Communication Manager 5.0”
  - Maintain
    - All covered by the Guidance CD “Communication Manager 5.0”
- **Avaya Media Server**
  - Overview
    - All covered by the Guidance CD “Communication Manager 5.0”
  - Design
    - All covered by the Guidance CD “Communication Manager 5.0”
  - Implement
    - Job Aid: Upgrading Firmware on the BIOS - Avaya S8500 Media Server, Document ID 03-300411, issue 2, June 2005
  - Maintain
    - All covered by the Guidance CD “Communication Manager 5.0”
  - System Management/Administration
    - Security the Avaya Communication Manager Media Servers, Issue 3, June 2005
- **Avaya SSG**
  - Secure Services Gateway (SSG) Documentation, Document ID 19-601378-4
- **Avaya SES**
  - All covered by the Guidance CD “Communication Manager 5.0”

1.3 TOE Overview

1.3.1 Usage and major security features of the TOE

The product is a sophisticated Communication System from Avaya which is based on the VoIP (Voice over IP) platform. The system meets all demands from small companies with less than 100 employees to global enterprises with ten-thousands of personals on a single system to more than one million users on a single network. It provides a wide range of Media Servers, IP-Phones and Application Server to optimize business communication and improve productivity. Avaya solutions are designed to meet highest security standards as end-to-end encryption and authentication of the devices and the users.

The figure below shows the structure of such a VoIP system.

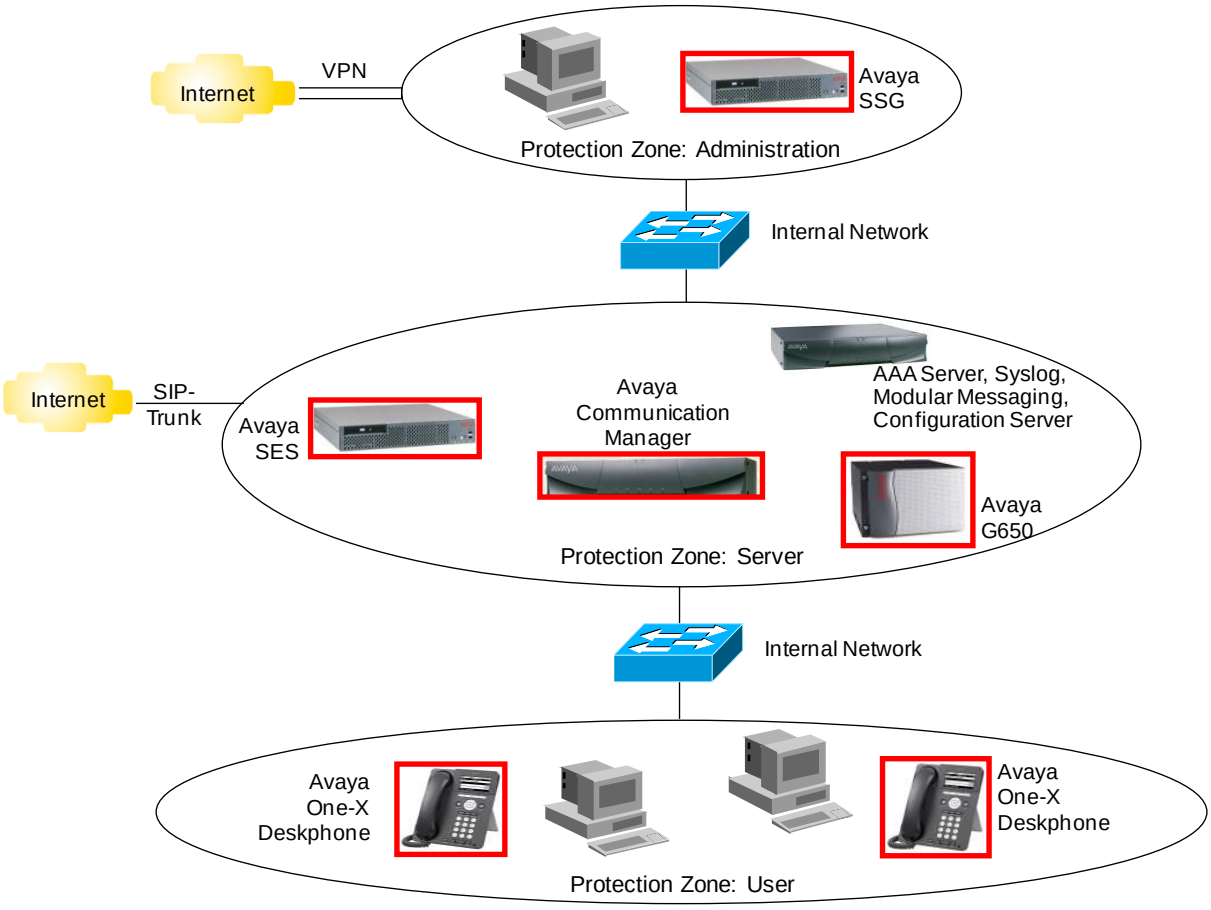

Figure 1 – Structure of the VoIP system

- The protection zone "**User**" contains all terminal devices like phones or computers. It should be remarked that only Avaya phones will be recognized as part of the certified system. 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[2] and the Avaya SIP Enable Services (SES), which are all part of the TOE.

[2] The complete appliance can be named as „Media Server". The software running on it is named „Communication Manager".

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 (signaling). 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 signaling 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. This holds especially valid for calls to external participants because external calls cannot be encrypted due to limitations of the Telecommunication service provider.

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 Center, 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.

1.3.2 TOE Type

The TOE is a VoIP PBX system and appropriate phones which mainly provide authentication, confidential communication and auditing.

1.3.3 Required non-TOE hardware/software/firmware

As shown in the Figure 1 above, there is some network equipment (switches, router, etc.) required to interconnect the different TOE parts and the environment. However, the TOE does not require any additional special hardware, software or firmware to implement or enforce its security features.

The Configuration Server seems to be relevant because it stores the configuration files of the phones. It is not required to have such a server because the phones need not to download new configuration files. They can store their configuration locally. The configuration server is especially not required to enforce any security function. However, a central management of the phones without such a server is not possible, whereas it is highly recommended to have such a server.

1.4 TOE Description

1.4.1 Physical Scope of the TOE

As listed in chapter 1.2 the TOE consists of hardware, several software components as well as guidance documents.

- The physical scope of the TOE is defined by the hardware components listed in chapter 1.2.
- The TOE consists of software modules (listed in chapter 1.2) which run on these hardware components.
- Finally, the physical scope of the TOE includes the guidance documents of all these hard- and software components as listed in chapter 1.2.

The functions of these TOE components are described in more detail in the following sections.

1.4.1.1 Avaya Communication Manager

Designed to run on a variety of Linux-based Media Servers, Communication Manager provides centralized call control for a resilient, distributed network of Avaya Media Gateways and a wide range of digital and IP-based communication devices.
Avaya Communication Manager provides an open SIP and H.323 model with full coverage of support of open API/SDK. This approach allows seamless integration of voice into other applications and flexibility to integrate third party endpoints and applications.
Avaya Communication Manager is in charge of the registration of the phones, the correct mediation of calls and the key management for the encryption of the calls (except calls based on SIP). Furthermore, the Communication Manager is in charge for logging of calls and the log-on of phones (users) to the system.

1.4.1.2 Avaya G650 Media Gateway

The G650 can accommodate a range of analog, digital, ISDN, and IP (over the LAN) phone station configurations, with voice transport options over IP, analog, TDM, or ATM. So, G650 is responsible for connecting the varied types of phone stations and conversion of the different protocols. This includes also the encryption and decryption of the calls, if possible and necessary. The configuration under evaluation only includes a company external connection over a SIP trunk.

1.4.1.3 Avaya SES Server

SIP Enablement Services (SES) is a Linux-based software application that is deployed as a network appliance on the Avaya S8500 Server series (short: SES Server). SIP Enablement Services adds support for Avaya's one-X™ Deskphone SIP 9630 telephones. The SES server is involved in the signaling of SIP calls and therefore also for the respective key management and the logging of the relevant events of these calls.

1.4.1.4 Avaya SSG Server

In order to support any service and maintenance tasks, the Avaya Global Service provides secured services platforms at the Avaya site as well as for the customer site. The Avaya SSG (Secure Service Gateway) which is located behind the customer's firewall is the central access point for all service requests from the Avaya Service Center. In addition to providing a point of outbound alarm aggregation for all maintained devices inside the customer network, the Avaya SSG serves as a platform for future value-added services.

A SSG is required at the customer's intranet to collect alarms from maintained devices and aggregate them into a single secure data stream to be sent to Avaya over a WAN connection. Once collected, the SSG sends the alarms to Avaya using HTTPS.

SSG uses the Red Hat Linux Enterprise Server 3.0 operating system, the Java SDK and a Postgres database. All TCP/UDP ports are closed unless required for normal operation.

Logging all events is critical to SSG security. User logins, product alarms, software and hardware events as well as network outages are all recorded in the SSG's event and alarm log.

The customer is able to enforce access control rules to the SSG. As example, the customer may allow or deny access to all products at the SSG with the ability to set one-time or recurring time-of-day access control restrictions for one or more devices. For example, the customer may deny remote access to all equipment in his call center during the business hours where the call volume is at its peak. SSG also enables the customer to view a real-time list of active sessions passing through the SSG and to terminate one or more of the active sessions if deemed suspicious or inappropriate.

1.4.1.5 Avaya One-X Desktop Phone 9630

The Avaya one-X Desktop Phone 9630 is an enterprise class VoIP phone and supports both H.323 and SIP protocol with two different models. The main security features of these phones are the ability to handle encrypted calls, to use only authentic firmware for an upgrade, to authenticate the Configuration Server prior of downloading the configuration file and to forward the human user authentication credentials to the Avaya Communication Manager.

1.4.2 Logical Scope of the TOE

The following security features define the logical scope of the TOE:

- **Authentication of human users.**
  The user has to enter his (personal) phone number and his PIN at the client phone. Subsequently, he becomes an authorized person and may use all (enabled) functions of the phone and the system and call all (allowed, not disallowed) telephone numbers.
  Administrators have to enter username/password to access the TOE functions. For all TOE servers except G650, this I&A procedure is covered by the operating system.
- **Securing the confidentiality of the signaling**. This includes services like call forwarding or inquiry call.

This also includes the simple conferencing function “MeetMe” implemented in the Communication Manager, the gateways and the phones.

Calls over the internet using the SIP trunk are excluded.

- **Securing the confidentiality of the media stream**, but only if there are no components involved which are not part of the TOE (e.g. external telephones or the modular messaging).

  This includes also the simple conferencing function “MeetMe” implemented in the Communication Manager, the gateways and the phones.

  Calls over the internet using the SIP trunk are excluded.
- **Secure and dependable (trustworthy) mediation of sessions,** caller party and called party of a call must be identified and authenticated; a call must only be mediated from the caller party to the called party. This includes services like call forwarding or inquiry call and the simple conferencing functions.

  The actual conferencing server and its services are out-of-scope.

  This service can only be provided to devices part of this PBX system. Phones connected over the internet to the system (using the SIP trunk) cannot be controlled.
- **Self-protection of the telephones** against unauthorized software updates and modification of its configuration.
- **Logging of security relevant events**
  - Identification/Authentication of a human user
  - Successful establishing of a connection
  - All administrative actions
- **Managing of white- and black lists** for telephone numbers, which means allowing and disallowing certain telephone numbers.
  - Separation between authenticated and not authenticated human users.
    e.g. emergency calls are also allowed for non authenticated users
  - Separation between groups of human users or single users.
    e.g. usually, users are not allowed to call to foreign countries but the companies president is allowed to do so.
- **Access Control for Remote Administrators** by using SSG (which is an optional part of the TOE).

In order to define the logical scope in detail, the following functions are **out of scope** of the TOE:

- Boarder protection of all external connections like SIP trunks or remote management connections.
- Conferencing Systems; they need an additional server component which is not part of the TOE.
- IEEE 802.1x functionalities; this may be implemented in the network equipment.
- Logging of the Identification/Authentication of server components against the phones.
  The phones are not capable to store audit information.
- Audit information will not automatically be deleted after expiry of their retention time. Possible data protection requirements are not considered in this Security Target.
- VPN Connections of remote access solutions for administrators

1.4.3 Configuration under Evaluation

This chapter defines in short terms the configuration of the complete system which is under evaluation:

- The system must be configured according to the specifications in [SecureConfigG].

2 Conformance Claim

2.1 CC Conformance Claim

The Security Target is based upon

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 1, CCMB-2006-09-001,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 2, CCMB-2007-09-002,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 2, CCMB-2007-09-003,

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

- part 2 conformant
- part 3 conformant
- evaluation assurance level (EAL) 1 augmented by ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1 and ADV_FSP.2

2.2 PP Conformance Claim

The Security Target does not claim conformance to a Protection Profile.

2.3 Package Claim

The Security Target does not claim conformance to a Package beside “EAL 1 augmented”.

3 Security Problem Definition

The Security Problem Definition describes assumptions about the operational environment in which the TOE is intended to be used and represents the conditions for the secure operation of the TOE.

3.1 Definitions

3.1.1 Subjects

(Authorized) Issuer of the Firmware	The issuer of the firmware is the person or company who signs the firmware by a digital signature by using his (personnel) digital certificate. Such an issuer is authorized, if his digital certificate is signed by the root authority the phones trust.
Administrator	A person who is responsible for administration of some or all hardware components or software applications on which the TOE bases and/or which build up the TOE. This includes also the operating systems and other services like a central authentication service or a firewall. Administrators have the authority and the (technical) permissions to access the hardware and software components and to perform administrative tasks on these components and data.
Attacker	An attacker may be an authorized or an unauthorized person who tries to use the system without permission or in an unintended way, to modify the system or to bother the functions of the system. It is assumed that attackers have at most basic attack potential because the VoIP information or the functionality of the phone system is usually not a very valuable good. Furthermore, the VoIP system (the TOE) is accessible from the local LAN and (using the SIP trunk) over the internet and is located in secured or at least standard office rooms (complex attacks/modifications are not possible). All logical remote access points are protected by firewalls and/or VPN gateways/connections.
Authenticated user	An authenticated user has successfully authenticated them against the TOE. An authenticated user must also be an authorized person.

Authorized Person	An authorized person is a user of the VoIP system who is authorized to make phone calls (to dedicated numbers or to all numbers except some defined numbers) or use other user-accessible services of the system. It is possible that a particular person is only authorized to make calls with his own phone number. So, for using this phone number and/or calling a special number the person is an authorized person; for using another phone number and/or calling another number this person is an unauthorized person.
Customer-Administrator	The Customer-Administrator is an underprivileged Administrator for SSG. This role is only able to manage the access permissions to the other TOE devices accessible through the SSG and the WAN connection of the SSG. The Customer-Administrator can also monitor all current activities on the SSG. This role does not have further permissions. A "normal" administrator also exists on SSG to manage all other issues of this device. It may be possible that one person is Administrator and Customer-Administrator.
Unauthorized Person	These are all people which are not administrators and not authorized persons.

3.1.2 Objects

Configuration Server	A server in the operational environment of the TOE which stores the configuration files for the phones. This server is located in the Server Zone and is protected by physical means and the access control of the operating system. The server provides a HTTP(S) interface for downloading the configuration files.
Gateway(s)	This term identifies the Avaya Media Gateways G650. This term is just an abbreviation.
Phone	The Avaya One-X Deskphone 9630 (both models).
TOE Servers	This definition includes "Avaya Communication Manager" (software), "Avaya Media Gateway G650" and the three listed printed boards (hardware), "Avaya SES Server" (software) and "Avaya SSG" (software). All other parts of the physical scope of the TOE are not included in this definition.

3.1.3 Information

Audit Data / Audit Information	These are the log information collected and stored by the TOE. Audit data contain e.g. logon failures of administrators, call information like start date/time, duration, called party number, calling party number, etc.

Blacklist	A list of phone numbers or patterns of phone numbers a phone/user/group of users are not allowed to call.
Media Stream	The data stream which transports the actual voice information.
Signaling data	The data stream which transports the signaling information required to establish the connection (e.g. the called party's phone number)
Whitelist	A list of phone numbers or patterns of phone numbers a phone/user/group of users are allowed to call.

3.1.4 Operations

Mediation	"Mediation" means that the server components of the TOE receive the signaling data and/or the media stream and forward them to the respective called party(ies). The TOE must not store the information permanently and must not forward the information to any other parties.
Receiving information	In the context of VoIP and telephones, "receiving" usually means listening to your phone.
Registration as unnamed	Unnamed Registration is the process a phone performs after its boot-up and if the user does neither start the login procedure within 60 seconds nor starts the login process with inserting his credentials. The phone connects to the Avaya Communication Manager and registers as unnamed. The Avaya Communication Manager now "knows" this phone. Unnamed Registration provides only a configurable set of functions, including e.g. emergency call. Until now the phone does not have a phone number. This number will be assigned to the phone when an authorized person has successfully identified & authenticated itself. (see "Full Registration")
Full Registration	Full Registration is reached when a human user has logged on with "his" phone extension and his private PIN.
Sending information	In the context of VoIP and telephones, "sending" usually means dialing a number or talking into the phone.

3.1.5 Security Attributes

Path name	A path name specifies the location of a file or directory on the storage of the operating system. For an Unix operating system a valid path name for audit information may be "/var/log/audit.log"

3.2 Assumptions

A.ADMIN All administrators are trustworthy and trained. Administrators do especially not pass their access credentials over to anyone else.

A.AVAILABLE All components are assumed to be sufficiently available or to be redundant. This includes also the bandwidth of the network for the VoIP traffic.

A.ConfServer The Configuration Server is assumed to be carefully administered. This means especially that the access to the configuration files is restricted by means of the operating system of this server.

A.DEVICES It is assumed that the user zone does only contain VoIP phone components. There are no conventional phones or fax machines located in this zone. Computers or other IT equipment is allowed.

A.ERRMONITORING It is assumed that all errors the applications, the media servers and gateways sent will be received, monitored and processed by an administrator in time.

A.LOCATION It is assumed that all phones of the user zone are located in a standard office environment and are always under supervision except short breaks, e.g. when the user is at the rest room. For longer breaks it is assumed that the access to the office room is restricted to authorized[3] persons by any other means (e.g. locked doors, doormen). So, no unauthorized **physical** modifications of the phones (e.g. disassembling, replacing, installation of an additional hardware component to the phone) or of the respective network connection (usually, the line between the phone and the plug socket) are possible.

A.PHYSICAL The components of the server and admin zone as well as the respective network equipment of these zones are physically protected by the environment (the rooms). The rooms are access controlled.

A.SECDEV The network components between the user zone and the server zone are able to and are configured to enforce the IEEE 802.1X hardware authentication of the client phone devices.
Further, it is assumed that only authorized phones are allowed to connect to the IP network to which the TOE is connected.

[3] „authorized" means here „authorized to access the room". This does not necessary include the permission to use the phones inside this room.

A.SECNET	If the System is connected to the Internet or any other untrusted (IP) network, the complete system is protected on protocol level (e.g. TCP/UDP/IP) by a firewall or equal products. Only the ports required for operation are opened. This holds also valid for the junction between user zone and server zone. (see Figure 1)
A.USER	The authorized persons do not pass their access credentials, if existent, over to other authorized or unauthorized persons.
A.VPN	If there is a remote access via SSG, the WAN connection is sufficiently protected by physical or logical means (e.g. VPN encryption as shown in Figure 1).

3.3 Threats

T.AccServer	An attacker gets direct **logical** access to TOE servers (on the level of the application) because the TOE servers provide such access points.[4]
T.CallDisc	An attacker is able to disclose the signaling traffic and/or the media streams, e.g. by rerouting the data, by sniffing the IP traffic or by using functions of the VoIP system (e.g. unnoticeable listening of calls).
T.CallPrev	An attacker is able to prevent the establishing of calls, e.g. by provoking IP address collisions with the servers.
T.ConfClient	An attacker modifies the **software** configuration parameter of a phone (e.g. by using the available hardware switches or available software options) in a short moment when the phone is not under supervision.
T.ConfServer	An attacker modifies the configuration data of the TOE servers, e.g. by direct modification or replacing of configuration files.
T.ConnServer	An attacker terminates/bothers/prevents/redirects the logical connection between the server zone and another IT system required for the (secure) operation of the system (e.g. a directory service), e.g. by rerouting the IP traffic or by provoking an IP address collision.
T.DoS	An attacker performs a DoS attack against the server components, e.g. with a high number of concurrent calls or a high number of concurrent phones which want to register at the server. An attacker performs a DoS attack against a phone or a server, e.g. with a high number of IP packages sent to its IP address.

[4] Please consider that this threat deals only with the logical access to the TOE servers, not with the logical access to the TOE environment like the underlying operating system. This is covered by OSP.OS.

T.LogDel	An attacker is able to delete or modify (parts of) the logs (e.g. call data records), e.g. by direct modification/erasure of the log files.
T.LogDisc	An attacker is able to disclose the logs (e.g. call data records), e.g. by direct read access to the log files.
T.Remote	An attacker is able to log into the system remotely by using the administrative interfaces of SSG. This attack may be possible if the attacker is already "inside" the VPN tunnel, e.g. when the attacker origins from the Avaya SSDP.
T.ReplaceClient	A virus, worm, trojan horse or other malware can be installed by an attacker on any client system, e.g. by modifying/replacing the software on the bootp/DHCP server or by faking the bootp/DHCP servers at all which stores the telephone applications for the clients.
T.ReplaceServer	An attacker modifies/replaces one or more server software components, e.g. by exploiting a vulnerability of the operating system of this server.
T.Replay	An attacker performs a replay attack against a TOE part by re-sending already captured IP packages. The attacker wants e.g. to spoof a server or phone or he wants to perform a DoS attack against a server or a phone in order to exploit a buffer-overflow vulnerability.
T.Unauth	An unauthorized person uses features (e.g. call forwarding, conferencing functions) of the VoIP-System for which he or she is not authorized. An unauthorized person causes a very high telephone invoice by calling expensive phone numbers, making long-distance calls or a lot of normal calls.

3.4 Organizational Security Policies

OSP.NETMONITOR	The network that the TOE is connected to will be monitored by the administrators for unapproved activities and/or attempts to attack network resources (including the parts of the TOE).
OSP.OS	The administrator(s) must take care about the secure configuration of the operating systems of all TOE components. This means especially, that they do not create unnecessary or unprotected accounts, give more permissions than required to an account, disable all accounts if they are not longer required and install all security patches to the system.

4 Security Objectives

4.1 Security Objectives for the TOE

O.Authenticate The TOE servers must require a successful and not replayable identification and authentication of the administrators before granting access to these components.[5]

The TOE must also require a successful and not replayable identification and authentication of the human users before considering the user as authorized person but some non-security critical functions (e.g. emergency call) are still available to unauthorized persons.

O.ConfClient The security attributes of the phones must only be configurable by administrators using trustworthy communication channels. Only non-security relevant parameters are possible to be changed by the user.

O.Disclose All signaling data and media streams between two or more phones must be protected against disclosure .

O.LogExport The TOE must store all log records in a storage secured by the operating system

O.Mediation The TOE must ensure that only the intended parties of a call can listen the call.

O.Restriction The TOE must provide an access control system for its users. The TOE must enable the administrators to configure the permissions the users shall have. This includes access permissions to features of the system, static assignment of a phone number to a user (identification of the user) and access restrictions to dedicated phone numbers.

O.SelfProtect The phones must check the integrity and authenticity of a software application before starting this software.

[5] Please consider that this objective deals only with securing the logical access to the TOE servers, not with securing the logical access to the TOE environment like the underlying operating system. This is covered by OE.ADMIN and OE.OS.

4.2 Security Objectives for the Operational Environment

OE.ADMIN	All administrators shall be trustworthy and trained. Administrators must especially not pass their access credentials over to anyone else. The administrator(s) must take care about the secure configuration of the operating systems of all TOE components. This means especially, that they do not create unnecessary or unprotected accounts, give more permissions than required to an account and disable all accounts if they are not longer required.
OE.AVAILABLE	All components must be sufficiently available or to be redundant. This includes also the bandwidth of the network for the VoIP traffic. The owner of the VoIP system is in charge of procuring/providing the respective technical environment.
OE.ConfServer	The Configuration Server shall be carefully administered. This means especially that the access to the configuration files shall be restricted to a minimum by means of the operating system of this server.
OE.DEVICES	The user zone must not contain conventional phones or fax machines.
OE.DoS	The operational environment must provide a sufficient protection of all TOE devices against DoS attacks. This can be implemented by technical means (e.g. filter on network devices) or by organizational mean (e.g. ongoing monitoring of network activities).
OE.ERRMONITORING	All errors the TOE servers sent will be received, monitored and processed by an administrator in time.
OE.LOCATION	All phones of the user zone must be located in a standard office environment and must always be under supervision except short breaks, e.g. when the user is at the rest room. For longer breaks the user must restrict the access to the office room to authorized[6] persons by any other means (e.g. locked doors, doormen).
OE.LOGOUT	When an authorized user leaves his place and leaves especially the phone without supervision, the user is required to prevent unauthorized usage of the phone, e.g. by log out from the phone.
OE.NETMONITOR	The network that the TOE is connected to must be monitored by the administrators for unapproved activities and/or attempts to attack network resources (including the parts of the TOE).
OE.PHYSICAL	The components of the server and admin zone as well as the respective network equipment of these zones must be physically protected by the environment (the rooms). The rooms must be access controlled.

[6] „authorized" means here „authorized to access the room". This does not necessary include the permission to use the phones inside this room.

OE.SECDEV	The network components between the user zone and the server zone must be configured to enforce the IEEE 802.1X hardware authentication of the client phone devices. Only authorized phones are allowed to connect to the IP network to which the TOE is connected.
OE.SECNET	If the System is connected to the Internet or any other untrusted (IP) network, the complete system must at least be protected on protocol level (e.g. TCP/UDP/IP) by a firewall or equal products. Some additional protections on higher protocol levels are advisable. Only these ports required for operation are allowed to pass the filter. The junction between user zone and server zone (see Figure 1) must also be protected by such a filter.
OE.USER	The authorized persons must be trained to not pass their access credentials, if existent, over to other authorized or unauthorized persons.
OE.VPN	If there is a remote access via SSG, the WAN connection must be sufficiently protected by physical or logical means (e.g. VPN encryption).

4.3 Rationale for Security Objectives

The following table maps the assumptions, threats and OSPs to the objectives for the TOE and the objectives for the operation environment. The mapping will be justified in the subsequent sections of this chapter.

	O.Authenticate	O.ConfClient	O.Disclose	O.LogExport	O.Mediation	O.Restriction	O.SelfProtect	OE.ADMIN	OE.AVAILABLE	OE.ConfServer	OE.DEVICES	OE.DoS	OE.ERRMONITORING	OE.LOCATION	OE.LOGOUT	OE.NETMONITOR	OE.PHYSICAL	OE.SECDEV	OE.SECNET	OE.USER	OE.VPN
A.ADMIN								X													
A.AVAILABLE									X												
A.ConfServer										X											
A.DEVICES											X										
A.LOCATION														X							
A.ERRMONITORING													X								
A.PHYSICAL																	X				
A.SECDEV																		X			
A.SECNET																			X		
A.USER																				X	
A.VPN																					X
T.AccServer	X																X				
T.CallDisc	X		X		X											X					
T.CallPrev													X			X					
T.ConfClient	X	X												X							
T.ConfServer								X									X				
T.ConnServer								X								X	X				
T.DoS												X	X			X					
T.LogDel	X			X				X									X				
T.LogDisc	X			X				X									X				
T.Remote	X							X											X		X
T.ReplaceClient							X							X							
T.ReplaceServer								X									X				
T.Replay	X											X				X					
T.Unauth	X	X				X								X	X						
OSP.OS								X													
OSP.NETMONITOR																X					

4.3.1 Coverage of the Assumptions

A.ADMIN	**OE.Admin** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.AVAILABLE	**OE.AVAILABLE** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.ConfServer	**OE.ConfServer** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.DEVICES	**OE.DEVICES** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.LOCATION	**OE.LOCATION** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.ERRMONITORING	**OE.ERRMONITORING** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.PHYSICAL	**OE.PHYSICAL** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.SECDEV	**OE.SECDEV** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.SECNET	**OE.SECNET** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.USER	**OE.USER** verbalized the assumption as objective and covers the assumption therefore completely and correctly.
A.VPN	**OE.VPN** verbalized the assumption as objective and covers the assumption therefore completely and correctly.

4.3.2 Coverage of the Threats

T.AccServer	**O.Authenticate** requires identification/authentication before any action at the servers – at each physical or logical interface. **OE.PHYSICAL** supports by hindering the access to the physical interfaces.
T.CallDisc	**O.Mediation** ensures that the VoIP system does not provide functions to listen a call unnoticed. **O.Authenticate** ensures that nobody can access the system (or at least the security critical parts) without authorization. **O.Disclose** ensures that the VoIP traffic will be end-to-end encrypted for the respective parties. **OE.NETMONITOR** supports by the fast identification of unapproved activities on the network.
T.CallPrev	**OE.ERRMONITORING** ensures that all errors (including errors of the operating system) the servers sent, will be monitored and processed by administrators in time. **OE.NETMONITOR** supports by the fast identification of unapproved activities on the network.
T.ConfClient	**OE.LOCATION** prevents physical modifications of the phones. **O.ConfClient** prevents the security-relevant configuration of the phone by unauthorized persons and **O.Authenticate** requires a successful identification and authentication before any security critical action.
T.ConfServer	**OE.PHYSICAL** ensures that a direct physical access to the servers by attackers is not possible. **OE.ADMIN** ensures well-trained administrators which do not bring the systems in an insecure state.
T.ConnServer	**OE.PHYSICAL** ensures that a direct physical access to the servers and the network equipment by attackers is not possible. **OE.ADMIN** ensures well-trained administrators which do not bring the systems in an insecure state. **OE.NETMONITOR** supports by the fast identification of unapproved activities on the network.
T.DoS	**OE.DoS** ensures that all servers and the phones are protected against a DoS attack. **OE.ERRMONITORING** supports the early identification of such an attack. **OE.NETMONITOR** supports by the fast identification of unapproved activities on the network.
T.LogDel	**O.Authenticate** in addition with **OE.ADMIN** ensure that only authorized person have access to the log files by using the appropriate TOE functions. **O.LogExport** ensures that the TOE stores all audit information in a storage protected by the operating system. **OE.ADMIN** enforces the protection of this storage logically. **OE.PHYSICAL** enforces the protection of this storage physically.

T.LogDisc	**O.Authenticate** in addition with **OE.ADMIN** ensure that only authorized person have access to the log files by using the appropriate TOE functions. **O.LogExport** ensures that the TOE stores all audit information in a storage protected by the operating system. **OE.ADMIN** enforces the protection of this storage logically. **OE.PHYSICAL** enforces the protection of this storage physically.
T.Remote	**OE.SECNET** and **OE.VPN** ensure that network based attacks against the SSG are without success. **O.Authenticate** in addition with **OE.ADMIN** ensure that only authorized person can log in from remote sites by using the optional SSG.
T.ReplaceClient	**OE.LOCATION** prevents modifications at the phones directly. **O.SelfProtect** ensures that the phones run only successfully authenticated software applications, even if the application origins from a valid server.
T.ReplaceServer	**OE.PHYSICAL** prevents physical modifications or replacements of the servers. **OE.ADMIN** ensures that the operating system is configured in a secure way and that this level of security will not decreased by insecure configuration.
T.Replay	**O.Authenticate** requires an identification/authentication mechanism which is resistant against replay attacks. **OE.DoS** protects against DoS attacks based on replayed packages. **OE.NETMONITOR** supports by the fast identification of unapproved activities on the network.
T.Unauth	**O.Restriction** implements an access control system which restricts the possibilities of the users. **O.Authenticate** enforces a successful identification and authentication before any action. **O.ConfClient** prevents circumvention of the access control by manipulations of the phone. **OE.LOGOUT** requires that users ensure that no one unauthorized can use the phone when he is absent and **OE.LOCATION** requires that physical access to the phone is restricted.

4.3.3 Implementation of Organizational Security Policies

OSP.OS	**OE.ADMIN** covers the requirement that the administrators must take care about the secure configuration of the TOE's systems.
OSP.NETMONITOR	**OE.NETMONITOR** verbalized the OSP as objective and covers the OSP therefore completely and correctly.

5 Security Requirements

5.1 Conventions

All operations performed on the Security Functional Requirements or the Security Assurance Requirements need to be identified. For this purpose the following conventions shall be used.

- **Assignments** *will be written italic*
- **Selections** will be written underlined
- **Refinements** **will be written bold**
- **Iterations** will only be performed on components level. The component ID defined by the Common Criteria (e.g. FDP_IFC.1) will be extended by an ID for the iteration (e.g. "(Export)"). The resulting component ID would be "FDP_IFC.1 (Export)".

5.2 Security Policies

The following sections define the security policies which must be enforced by the TSF.

5.2.1 Audit-Export Control Policy

This is an information flow control policy which defines the permissible information flow for exporting audit data record to outside of the TOE.

- All audit data records be generated by the TSF must be exported to a trusted storage platform.

It is assumed (A.PHYSICAL, A.ADMIN, OE.ADMIN, OE.OS) that the storage is access controlled by the underlying operating system or by any other means so that only administrators have read and write access to this information after the export. It is also assumed that only administrators have the permissions to configure the destination path to the trusted storage.

5.2.2 Call-Mediation Policy

This is an information flow control policy which defines which devices shall be enabled to be participants of a call.

- The TSF shall ensure that a call can only be received by these participants which are identified by the calling party (usually by entering the respective phone numbers of the intended called party).[7]
- If the intended called party has configured an automatic call-forwarding or has manually forwarded the call to another called party, only the caller party and the finally called party shall be able to be participants of the call.[8]
- It is permissible that a called party is also a caller party at the same time for virtually the same call. This happens if the called party extends the call to a conference call.
- The TSF shall ensure that all signaling information and media streams of different calls will be handled completely separated at all devices.

Furthermore, this policy also defines the procedures for ensuring the confidentiality of the signaling data and media streams:

- All signaling data and media streams managed by only the TOE devices shall be encrypted by using strong cryptographic algorithms appropriate for the respective communication protocol.
- Signaling data and media streams from and to a SIP-trunk may be transferred/received from the respective TOE servers to/from the network gateways unencrypted but only on the connection between the TOE servers and the gateway. All connections inside the scope of control of the TOE are encrypted.
- All (encrypted) data of one call must strictly be separated from all other data from other calls. This holds valid for all software and hardware components of the TOE. A logical separation, e.g. by using security attributes, is acceptable.
- The cryptographic keys for a particular session must be generated and managed in such a way that the keys keep confidential outside of this session.
  This means, the keys shall not be readable from outside of this session and the keys shall not be determinable from keys of another session or from other (security) attributes[9].
- The cryptographic keys for a particular session must be made unavailable when the information is not longer needed.
- The encrypted information shall only be transferred to the called party(ies) of the call.
- All (unencrypted) signaling data or media streams stored in the memory of this device shall immediately be made unavailable when the information is not longer needed for the actual communication.

---

[7] Covers a standard one-to-one call and a conference call build up by the originator's phone.

[8] This scenario can only be completely covered by the TSF, if the new called party is also a device in the scope of the TSF. However, the first called party, which has forwarded the call, shall not be able to listen the call after forwarding.

[9] Such "*security attributes*" may be the current time or date, the phone numbers of the participants, an ongoing number managed on this gateway, a deterministic (weak) random number generator, etc.

- The encrypted or unencrypted information shall not be stored on a permanent storage (e.g. hard disk).

5.2.3 User Access Control Policy

This is an access control policy which defines the access permissions of normal users of the phones.

- The administrator can configure whether the system requires a user authentication for special actions / phone numbers or not.
- The administrator can configure groups of users.
- The administrator can configure whether all users are allowed to dial dedicated numbers (whitelistening) whereas a preceding user identification/authentication is not required.
- The administrator can configure whether all users or groups of users are allowed to dial dedicated numbers (whitelistening) whereas a preceding user authentication is required.
- The administrator can configure whether all users or groups of users are not allowed to dial dedicated numbers (blacklistening) whereas a preceding user authentication is required

The access control follows the following policy:

1. Check all whitelists for the respective user.
   If the phone number to be called is included, access is granted.
2. Check all blacklists for the respective user.
   If the phone number to be called is included, access is denied.
3. If the called number was not found in the whitelist or the blacklist, the default behavior is
   - Internal calls are allowed
   - External calls are denied

5.2.4 Firmware-Upgrade Policy

When a phone has downloaded a new version of its firmware, the phone has to check the integrity and the authenticity of this firmware prior to installation.

For this purpose, the phone has to check the digital signature of the firmware.

- If the check of the signature shows that the firmware was modified, the phone does not accept the firmware, prints an error message and continues using the current version of the firmware.
- If the check of the signature shows that the firmware is integer but the phone could not verify the authenticity of the creator of the signature, the phone does not accept the firmware, prints an error message and continues using the current version of the firmware.
- If the check of the signature shows that the firmware is integer and the phone could verify the authenticity of the creator of the signature, the phone upgrades itself. During this time, an appropriate message will be displayed.

5.3 Security Functional Requirements

5.3.1 SFR covering O.Authenticate

5.3.1.1 FIA_UAU.2 (AdminServer) User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **Administrator and Customer-Administrator** to be successfully authenticated **against the TOE servers** before allowing any other TSF-mediated actions on behalf of that **Administrator or Customer-Administrator**.

5.3.1.2 FIA_UID.2 (AdminServer) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each **Administrator and Customer-Administrator** to be successfully identified **against the TOE servers** before allowing any other TSF-mediated actions on behalf of that **Administrator or Customer-Administrator**.

5.3.1.3 FIA_UAU.1 (UserServer) Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow *the TSF mediated actions defined in the User Access Control Policy* on behalf of the user to be performed before the user is authenticated.

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

5.3.1.4 FIA_UID.1 (UserServer) Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow *the TSF mediated actions defined in the User Access Control Policy* on behalf of the user to be performed before the user is identified.

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

***Application Note**: All these requirements regarding identification and authentication are refined to cover a particular I&A relation, e.g. the users against the TOE servers. All these requirements together cover all I&A relations of the TOE. So, these refinements should be considered as conformant to the CC definition of "Refinement".*

5.3.1.5 FIA_UAU.3 (UserServer) Unforgeable authentication

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.3.1 The TSF shall prevent use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall prevent use of authentication data that has been copied from any other user of the TSF.

5.3.1.6 FMT_SMF.1 (Server) Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions **on the TOE servers except the SSG**:

- *Management of Administrator Accounts*
- *Management of Phones*
- *Management of Features of the Phones (Configuration)*
- *Management of Encryption Settings for calls*

5.3.1.7 FMT_SMF.1 (SSG) Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions **on the SSG**:

- *Granting and revoking access permissions of external IP addresses to TOE servers identified by their internal IP addresses*
- *Function to cancel all active sessions and preventing new sessions*
- *Monitoring of all activities performed by the remote users logged in*

5.3.1.8 FMT_MTD.1 (Server) Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete the *accounts and access permissions* **of the TOE servers except the SSG** to *the administrators*.

5.3.1.9 FMT_MTD.1 (SSG) Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete the *access permissions* **of the SSG** to *Customer-Administrators*.

5.3.2 SFR covering O.ConfClient

5.3.2.1 FMT_MTD.1 (Phone) Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to modify the *security relevant phone configuration parameters* to *administrators*.

Application Note: *This requirement covers the local configuration of the phone by pressing dedicated key combinations. This does not cover the configuration of the phone via the configuration file.*
The default key combinations are only mentioned in the administrator guidance and shall be changed by the administrator after initial configuration. Therefore, the TOE is able to enforce this SFR.

5.3.2.2 FMT_SMR.1 (Phone) Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles

- *Administrator*
- *Authorized person*
- *Unauthorized person*

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

Application Note: *FMT_SMR.1 (Phone) defines which roles are to be managed by the phones itself.*

5.3.2.3 FMT_SMF.1 (Phone) Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions **on the phones**:

- *Upgrade of the firmware of the phone*
- *Configuration of IP parameters (e.g. Use of DHCP or static configuration, IP address of configuration server, default gateway, broadcast address, etc.)*

5.3.2.4 FIA_UAU.2 (ServerPhone) User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

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

5.3.2.5 FIA_UID.2 (ServerPhone) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each **Configuration Server** to be successfully identified **against the phone** before allowing any other TSF-mediated actions on behalf of that **Configuration Server**.

5.3.2.6 FTP_ITC.1 (ServerPhone) Inter-TSF trusted channel

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and **the Configuration Server** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the **phones** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

- *Download of phone configuration data.*

Application Note: *The identification of the configuration server is explicit by providing a digital certificate to establish the SSL tunnel. The identification of a phone is implicit because the individual phones do not have an "identity". They can just transfer their type and model (e.g. One-X 9630 for SIP).*

5.3.3 SFR covering O.Disclose

5.3.3.1 FDP_ITT.2 (Conf) Transmission separation by attribute

Hierarchical to: FDP_ITT.1 Basic internal transfer protection
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ITT.2.1 The TSF shall enforce the *Call-Mediation Policy* to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.2.2 The TSF shall separate data controlled by the SFP(s) when transmitted between physically-separated parts of the TOE, based on the values of the following:

- *IP addresses and TCP/UDP ports of source and destination*

Application Note: *This requirement shall ensure that the streams of the different calls will be logically separated during transfer.*

5.3.3.2 FDP_ETC.2 (Conf) Export of user data with security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1 The TSF shall enforce the *Call-Mediation Policy* when exporting **signaling data and media streams**, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the **signaling data and media streams** with the **signaling data's and media streams'** associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported **signaling data and media streams**.

FDP_ETC.2.4 The TSF shall enforce the following rules when **signaling data and media streams are** exported from the TOE:

- *H.323, H.235.5, SIP, SRTP and TLS shall be used*
- *All signaling data and media streams must be encrypted before exporting*
- *All signaling data and media streams must be assigned with an evidence for their authenticity.*

Application Note: *This requirement shall ensure that the streams of the calls will be exported to outside the TOE assigned with the respective encryption parameter and valid authenticity attributes.*
This SFR is limited to the TOE Scope of Control. The TSC can be defined as the network connections between the TOE components used for transmission. The TSC does e.g. not cover communication connections over the Internet using the SIP-Trunk. This implies that external calls (incoming and outgoing, using the SIP-Trunk) need not to be encrypted.

5.3.3.3 FDP_ITC.2 (Conf) Import of user data with security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1 The TSF shall enforce the *Call-Mediation Policy* when importing **signaling data and media streams**, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported **signaling data and media streams**.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the **signaling data and media streams** received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported **signaling data and media streams** is as intended by the source of the **signaling data and media streams**.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing **signaling data and media streams** controlled under the SFP from outside the TOE:

- *Right after import, verify the authenticity of the signaling data and media streams.*
- *Decrypt the signaling data and media streams after import but before further proceeding*

Application Note: *This requirement shall ensure that the streams of the calls will be imported from outside of the TOE assigned with the respective encryption parameter and valid authenticity attributes.*
This SFR is limited to the TOE Scope of Control. The TSC can be defined as the network connections between the TOE components used for transmission. The TSC does e.g. not cover communication connections over the Internet using the SIP-Trunk. This implies that external calls (incoming and outgoing, using the SIP-Trunk) need not to be encrypted.

5.3.3.4 FTP_ITC.1 (Conf) Inter-TSF trusted channel

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the TSF to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *the transfer of signaling data and media streams between the phones and the TOE servers.*

5.3.3.5 FPT_TDC.1 (Conf) Inter-TSF basic TSF data consistency

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *signaling data and media streams* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *H.323, H.235.5, SIP, RTP, SRTP and TLS* when interpreting the TSF data from another trusted IT product.

> ***Application** Note: "Another trusted IT product" may be another part of the TOE or the systems of the SIP-trunk provider.*

5.3.3.6 FDP_RIP.2 (Conf) Full residual information protection

Hierarchical to: FDP_RIP.1 Subset residual information protection
Dependencies: No dependencies.

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a **signaling data or media stream** is made unavailable upon the deallocation of the **signaling data or media stream** from all objects.

> ***Application Note:** This requirement shall ensure that the signaling data or media streams shall be made unavailable after receiving/generating at the first phone, mediation by the TOE servers and output/processing at another phone. This shall support the Non-Disclosure objective.*

5.3.4 SFR covering O.LogExport

5.3.4.1 FDP_ETC.1 (Export) Export of user data without security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1 The TSF shall enforce the *Audit-Export Control Policy* when exporting **audit information**, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the **audit information** without the **audit information**'s associated security attributes

5.3.4.2 FDP_IFC.1 (Export) Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the *Audit-Export Control Policy* on

- *Subjects: the TOE applications G650, SSG, Communciation Manager and SES; the underlying operating systems*
- *Information: Audit Information*
- *Operations: when an audit record was generated by G650, SSG, Communication Manager or SES this audit record shall be exported to the underlying operating system.*

5.3.4.3 FDP_IFF.1 (Export) Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the *Audit-Export Control Policy* based on the following types of subject and information security attributes:

- *Subjects: the TOE applications G650, SSG, Communication Manager and SES*
  - *Attribute: Path name to be used for storing the audit information*
- *Subjects: the underlying operating systems*
  - *Attributes: none*
- *Information: Audit Information*
  - *Attributes: none*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- *Storing of audit information: the TOE applications G650, SSG, Communication Manager and SES shall export and store the audit information to the reserved area provided by the operating system.*

FDP_IFF.1.3 The TSF shall enforce *no additional information flow control SFP rules*.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules:

- *none*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

- *none*

Application note: *FDP_IFC.1 (Export) and FDP_IFF.1 (Export) ensure that the TOE applications store their audit information on access protected areas provided by the underlying operating systems. It is not the function of the TOE to configure the access permissions or to verify whether the access permissions are restrictive. The administrators are in charge of configuring the system in a secure way (OE.ADMIN, OE.OS).*

5.3.4.4 FMT_MSA.3 (Export) Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *Audit-Export Control Policy* to provide *secure* default values for **the path names**.

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

***Application Note**: This requirement covers the initialization of the path where the TOE applications shall store their audit information. So, a "secure" default value means a path which exists and is access protected by default.*

5.3.4.5 FMT_MSA.1 (Export) Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the *Audit-Export Control Policy* to restrict the ability to modify the security attributes *path name* to *administrators*.

5.3.4.6 FMT_SMF.1 (Export) Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

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

- *For all TOE server applications the path name to be used for storing the audit information can by modified by administrators.*

5.3.5 SFR covering O.Mediation

5.3.5.1 FDP_IFC.1 (Mediation) Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the *Call-Mediation Policy* on

- *Subjects: the TOE applications running on the phones, the Communication Manager, the gateways and the SES*
- *Information: Signaling data or media streams*
- *Operations: sending, mediation and receiving of the information*

5.3.5.2 FDP_IFF.1 (Mediation) Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the *Call-Mediation Policy* based on the following types of subject and information security attributes:

- *Subjects: the TOE applications running on the phones, the Communication Manager, the gateways and the SES*
  - *Attributes: none*
- *Information: Signaling data or media streams*
  - *Attributes: calling party and called party(s) defined by the phone numbers*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- *The mediation rules and encryption rules defined in chapter 5.2.2 Call-Mediation Policy*

FDP_IFF.1.3 The TSF shall enforce *no additional information flow control SFP rules*.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules:

- *none*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

- *none*

5.3.5.3 FMT_MSA.3 (Mediation) Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *Call-Mediation Policy* to provide restrictive default values for **the called party number and the calling party number**.

FMT_MSA.3.2 The TSF shall allow *nobody* to specify alternative initial values to override the default values when **a new call is to be initialized**.

Application Note: *This requirement covers the secure initialization of the called party's phone number and the calling party's phone number of a new call. Nobody shall be able to modify these phone numbers.*

5.3.5.4 FMT_MSA.1 (Mediation) Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the *Call-Mediation Policy* to restrict the ability to change_default the security attributes *called party number* to *everybody*.

Application Note*: FMT_MSA.3 (Mediation) ensures that restrictive default values for the calling party's and the called party's phone number will be used for initialization. This requirement here allows everybody to specify the called party's number to be used for the call.*

5.3.5.5 FMT_SMF.1 (Mediation) Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

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

- *Configuration of capability characteristics*[10]

[10] Such features may be call forwarding, group calls, Restrictions of calls, etc.

5.3.6 SFR covering O.Restriction

5.3.6.1 FDP_ACC.1 (Restriction) Subset access control

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the *User Access Control Policy* on

- *Subjects: a phone identified by its number*
- *Objects: Phone numbers*
- *Operations: from a phone a phone number shall be called*

5.3.6.2 FDP_ACF.1 (Restriction) Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the *User Access Control Policy* to objects based on the following:

- *Subjects: a phone*
  - *Attributes: its phone number*
- *Objects: the called party of a call to be made*
  - *Attributes: its phone number*

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

- *The access control rules defined in chapter 5.2.3 User Access Control Policy*

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

- *The phone is authorized to call the intended called party number, if this phone number is stored in the Whitelist.*

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

- *The phone is not authorized to call the intended called party number, if this phone number is stored in the Blacklist.*

5.3.6.3 FMT_MSA.3 (Restriction) Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *User Access Control Policy* to provide *the configured* default values for **the default access control policy, the whitelists and the blacklists** that are used to enforce the SFP.

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

***Application Note**: This requirement covers the default access control policy of the system and the initialization of the white and black lists. Both are defined and can be configured according to the user access control policy.*

5.3.6.4 FMT_MSA.1 (Restriction) Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the *User Access Control Policy* to restrict the ability to modify the security attributes *default access control policy, whitelists, blacklists* to *administrators*.

5.3.6.5 FMT_SMF.1 (Restriction) Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

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

- *Modification of the default access control policy of the system*
- *Modification of the whitelists*
- *Modification of the blacklists*

5.3.7 SFR covering O.SelfProtect

5.3.7.1 FDP_IFC.1 (DigSig) Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the *Firmware-Upgrade Policy* on

- *Subjects: Phones, Issuer of the Firmware*
- *Information: new Firmware*
- *Operation: Firmware upgrade process*

5.3.7.2 FDP_IFF.1 (DigSig) Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the *Firmware-Upgrade Policy* based on the following types of subject and information security attributes:

- *Subjects: Phones*
  - *Attributes: none*
- *Subjects: Issuer of the Firmware*
  - *Attributes: Digital Certificate / its Public Key*
- *Information: new Firmware*
  - *Attributes: Digital Signature of the Issuer of the firmware*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- *The digital signature of the firmware demonstrates that the firmware is not modified and the issuer of the firmware can successfully be identified using its Digital Certificate / its Public Key.*

FDP_IFF.1.3 The TSF shall enforce *no additional information flow control SFP rules*.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules:

- *none*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

- *none*

5.3.7.3 FMT_MSA.3 (DigSig) Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *Firmware-Upgrade Policy* to provide *static* default values for **the certificates of authorized issuers of firmware** that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *firmware issuer* to specify alternative initial values to override the default values when an object or information is created.

Application Note: *These requirements enforce the check of the digital signature of the firmware for the phones. The phones have to check this "proof of origin" as protection against spoofing/modification of the firmware before upgrading the firmware to the downloaded version. The known (authorized) issuer of firmware are statically stored in the phone. Only a known issue can modify these values by upgrading the firmware.*
Actually, the digital certificates of the authorized issuer of the firmware are stored. These certificates are considered as trustworthy.

5.3.8 Common SFR

The following SFR support some of the TOE security objectives. For this reason, these SFR are not listed in any of the chapters above but here in this common chapter.

5.3.8.1 FMT_SMR.1 (Com) Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles

- *Customer-Administrator*
- *Administrator*
- *Authorized person*
- *Unauthorized person*

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

5.3.8.2 FAU_GEN.1 (Com) Audit data generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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)

- *Unnamed Registration of phones at the Communication Manager*
- *Identification/Authentication of a human user*
- *Establishing of a connection (caller party number, called party number)*
- *All administrative actions.*

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 (if applicable), 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,

- *For Connections: The phone number of the calling party and (if applicable), the phone number of the called party and date and time of the end of the call.*
- *For administrative actions: All commands be performed*

5.4 Security Assurance Requirements

This Security Target claims that the TOE as defined herein fulfills the requirements of the security requirements package EAL 1 augmented by ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1 and ADV_FSP.2.
See also chapter 2.3.

5.5 Rationale for the Security Functional Requirements

The following table provides a mapping from the SFR to security objectives for the TOE.

	O.Authenticate	O.ConfClient	O.Disclose	O.LogExport	O.Mediation	O.Restriction	O.SelfProtect
FIA_UAU.2 (AdminServer)	X						
FIA_UID.2 (AdminServer)	X						
FIA_UAU.1 (UserServer)	X						
FIA_UID.1 (UserServer)	X				S	S	
FIA_UAU.3 (UserServer)	X						
FMT_SMF.1 (Server)	X						
FMT_SMF.1 (SSG)	X						
FMT_MTD.1 (Server)	X						
FMT_MTD.1 (SSG)	X						
FMT_MTD.1 (Phone)		X					
FMT_SMR.1 (Phone)		X					
FMT_SMF.1 (Phone)		X					
FIA_UAU.2 (ServerPhone)		X					
FIA_UID.2 (ServerPhone)		X					
FTP_ITC.1 (ServerPhone)		X					
FDP_ITT.2 (Conf)			X		S		
FDP_ETC.2 (Conf)			X		S		
FDP_ITC.2 (Conf)			X		S		
FTP_ITC.1 (Conf)			X		S		
FPT_TDC.1 (Conf)			X		S		
FDP_RIP.2 (Conf)			X		S		
FDP_ETC.1 (Export)				X			
FDP_IFC.1 (Export)				X			
FDP_IFF.1 (Export)				X			
FMT_MSA.3 (Export)				X			
FMT_MSA.1 (Export)				X			
FMT_SMF.1 (Export)				X			
FDP_IFC.1 (Mediation)			S		X		
FDP_IFF.1 (Mediation)			S		X		
FMT_MSA.3 (Mediation)			S		X		
FMT_MSA.1 (Mediation)			S		X		
FMT_SMF.1 (Mediation)			S		X		
FDP_ACC.1 (Restriction)						X	
FDP_ACF.1 (Restriction)						X	
FMT_MSA.3 (Restriction)						X	
FMT_MSA.1 (Restriction)						X	
FMT_SMF.1 (Restriction)						X	
FDP_IFC.1 (DigSig)							X
FDP_IFF.1 (DigSig)							X
FMT_MSA.3 (DigSig)							X
FMT_SMR.1 (Com)	X			X	X	X	
FAU_GEN.1 (Com)	X				X	X	
AGD_OPE.1		S					
AGD_PRE.1		S					

X means “SFR covers this objective”

S means “SFR supports this objective”

O.Authenticate FMT_SMF.1 (Server) defines the management functions available at the TOE server components except SSG. FMT_SMF.1 (SSG) defines the management functions of SSG. FMT_MTD.1 (Server) restricts the access to the TOE server management functions (except SSG) to the administrator. FMT_MTD.1 (SSG) restricts the access to the SSG management functions to the Customer-administrator. FIA_UAU.2 (AdminServer) and FIA_UID.2 (AdminServer) enforces I&A at all TOE server components.

FIA_UAU.1 (UserServer) and FIA_UID.1 (UserServer) enforces I&A of the human users. FIA_UAU.3 (UserServer) protects this I&A against forgery.

FMT_SMR.1 (Com) defines all roles.

FAU_GEN.1 (Com) enforces logging of all security relevant events.

O.ConfClient FMT_SMF.1 (Phone) defines the security relevant management functions of the phone. FMT_MTD.1 (Phone) restricts the access to the security relevant phone management functions to the administrator. FMT_SMR.1 (Phone) defines all roles which are to be managed by the phones itself.

FTP_ITC.1 (ServerPhone) enforces a trusted channel between the Configuration Server and the phone which wants to read its configuration file. FIA_UAU.2 (ServerPhone) and FIA_UID.2 (ServerPhone) enforces a dependable identification and authentication of this configuration server (enforced by the phone).

AGD_OPE.1 and AGD_PRE.1 support this objective by requiring appropriate hints regarding a secure configuration in the guidance documents.

O.Disclose FDP_ETC.2 (Conf), FDP_ITC.2 (Conf) and FTP_ITC.1 (Conf) ensure that the signaling data and the media streams will always be encrypted before transfer. FPT_TDC.1 (Conf) ensures that the encrypted data can be interpreted at the called party's side.

FDP_ITT.2 (Conf) ensures that data of different calls will not be mixed up. FDP_RIP.2 (Conf) ensures that no confidential information keep left in one of the TOE servers.

FDP_IFC.1 (Mediation), FDP_IFF.1 (Mediation), FMT_MSA.3 (Mediation), FMT_MSA.1 (Mediation) and FMT_SMF.1 (Mediation) support this objective by enforcing a correct (dependable) mediation of the calls and their data.

O.LogExport FDP_IFF.1 (Export) defines a policy for the export of audit information to the underlying operating system. FDP_IFC.1 (Export) enforces this policy.

FMT_MSA.3 (Export) enforces secure default values for the export policy parameters. FMT_MSA.1 (Export) defines the permissions for managing these values, FMT_SMF.1 (Export) defines the management functions which allow the management of the values and FMT_SMR.1 (Com) defines the roles (Administrator) which are used to define the permissions.

FDP_ETC.1 (Export) determines the actual export.

O.Mediation FDP_IFF.1 (Mediation) defines a policy for the secure/dependable mediation of calls. FDP_IFC.1 (Mediation) enforces this policy.

FMT_MSA.3 (Mediation) defines the values for the mediation policy. FMT_MSA.1 (Mediation) defines the permissions for managing these values, FMT_SMF.1 (Mediation) defines the management functions which allow the management of the values and FMT_SMR.1 (Com) defines the roles (Administrator) which are used to define the permissions.

FAU_GEN.1 (Com) enforces logging of all security relevant events.

FDP_ITT.2 (Conf), FDP_ETC.2 (Conf), FDP_ITC.2 (Conf), FTP_ITC.1 (Conf), FPT_TDC.1 (Conf) and FDP_RIP.2 (Conf) support this objective by ensuring the confidentiality of the calls.

FIA_UID.1 (UserServer) supports the correct logging of the events because the user's identity is given indirectly by the phone number.

O.Restriction FDP_ACF.1 (Restriction) defines a user access control policy. FDP_ACC.1 (Restriction) enforces this policy.

FMT_MSA.3 (Restriction) defines the values for the access control policy. FMT_MSA.1 (Restriction) defines the permissions for managing these values, FMT_SMF.1 (Restriction) defines the management functions which allow the management of the values and FMT_SMR.1 (Com) defines the roles (Administrator) which are used to define the permissions.

FIA_UID.1 (UserServer) supports this objective because the user's identity can be mapped to a phone.

FAU_GEN.1 (Com) enforces logging of all security relevant events.

O.SelfProtect FDP_IFC.1 (DigSig) defines a policy regarding the firmware upgrade procedure of the phones. FDP_IFF.1 (DigSig) enforces this policy.

This policy enforces the phone to only upgrade its own firmware, if this new firmware was issued by an authorized issuer.

FMT_MSA.3 (DigSig) defines that the authentication information stored in the current firmware of the phones is static and cannot be modified except by an upgrade of the firmware.

This means, only an authorized issuer of a firmware is able to "produce" a firmware which will be considered as authentic. This means also, that only an authorized issuer can modify the authentication information regarding the authorized issuer. So, a complete chain of trust is established.

5.6 Rationale For Assurance Requirements

The evaluation assurance level (EAL) 1 augmented was selected because the vendor and its customers do not need a higher level of assurance and the expected attack potential against the system is at most basic.
The augmentations are selected in preparation of a possible future EAL2 evaluation.

5.7 Rationale for all not-satisfied Dependencies

5.7.1 Security Functional Requirements

The following table shows the resolved and not resolved dependencies of the SFR. All non-satisfied dependencies are justified in the right column of the table.

'--' means that there are no dependencies to be considered.

SFR	Dependencies	Justification
FIA_UAU.2 (AdminServer)	FIA_UID.1	Resolved (FIA_UID.2 (AdminServer))
FIA_UID.2 (AdminServer)	--	--
FIA_UAU.1 (UserServer)	FIA_UID.1	Resolved (FIA_UID.1 (UserServer))
FIA_UID.1 (UserServer)	--	--
FIA_UAU.3 (UserServer)	--	--
FMT_SMF.1 (Server)	--	--
FMT_SMF.1 (SSG)	--	--
FMT_MTD.1 (Server)	FMT_SMR.1	Resolved (FMT_SMR.1 (Com))
	FMT_SMF.1	Resolved (FMT_SMF.1 (Server))
FMT_MTD.1 (SSG)	FMT_SMR.1	Resolved (FMT_SMR.1 (Com))
	FMT_SMF.1	Resolved (FMT_SMF.1 (SSG))
FMT_MTD.1 (Phone)	FMT_SMR.1	Resolved (FMT_SMR.1 (Phone))
	FMT_SMF.1	Resolved (FMT_SMF.1 (Phone))
FMT_SMR.1 (Phone)	FIA_UID.1	Resolved (FIA_UID.1 (UserServer))
FMT_SMF.1 (Phone)	--	--
FIA_UAU.2 (ServerPhone)	FIA_UID.1	Resolved (FIA_UID.2 (ServerPhone))
FIA_UID.2 (ServerPhone)	--	--
FTP_ITC.1 (ServerPhone)	--	--
FDP_ITT.2 (Conf)	FDP_IFC.1	Resolved (FDP_IFC.1 (Mediation))
FDP_ETC.2 (Conf)	FDP_IFC.1	Resolved (FDP_IFC.1 (Mediation))
FDP_ITC.2 (Conf)	FDP_IFC.1	Resolved (FDP_IFC.1 (Mediation))
	FPT_TDC.1	Resolved (FPT_TDC.1 (Conf))
	FTP_ITC.1	Resolved (FTP_ITC.1 (Conf))
FTP_ITC.1 (Conf)	--	--
FPT_TDC.1 (Conf)	--	--
FDP_RIP.2 (Conf)	--	--
FDP_ETC.1 (Export)	FDP_IFC.1	Resolved (FDP_IFC.1 (Export))
FDP_IFC.1 (Export)	FDP_IFF.1	Resolved (FDP_IFF.1 (Export))
FDP_IFF.1 (Export)	FDP_IFC.1	Resolved (FDP_IFC.1 (Export))
	FMT_MSA.3	Resolved (FMT_MSA.3 (Export))
FMT_MSA.3 (Export)	FMT_MSA.1	Resolved (FMT_MSA.1 (Export))
	FMT_SMR.1	Resolved (FMT_SMR.1 (Com))
FMT_MSA.1 (Export)	FDP_IFC.1	Resolved (FDP_IFC.1 (Export))
	FMT_SMR.1	Resolved (FMT_SMR.1 (Com))
	FMT_SMF.1	Resolved (FMT_SMF.1 (Export))
FMT_SMF.1 (Export)	--	--
FDP_IFC.1 (Mediation)	FDP_IFF.1	Resolved (FDP_IFF.1 (Mediation))

FDP_IFF.1 (Mediation)	FDP_IFC.1	Resolved (FDP_IFC.1 (Mediation))
	FMT_MSA.3	Resolved (FMT_MSA.3 (Mediation))
FMT_MSA.3 (Mediation)	FMT_MSA.1	Resolved (FMT_MSA.1 (Mediation))
	FMT_SMR.1	Resolved (FMT_SMR.1 (Com))
FMT_MSA.1 (Mediation)	FDP_IFC.1	Resolved (FDP_IFC.1 (Mediation))
	FMT_SMR.1	Resolved (FMT_SMR.1 (Com))
	FMT_SMF.1	Resolved (FMT_SMF.1 (Mediation))
FMT_SMF.1 (Mediation)	--	--
FDP_ACC.1 (Restriction)	FDP_ACF.1	Resolved (FDP_ACF.1 (Restriction))
FDP_ACF.1 (Restriction)	FDP_ACC.1	Resolved (FDP_ACC.1 (Restriction))
	FMT_MSA.3	Resolved (FMT_MSA.3 (Restriction))
FMT_MSA.3 (Restriction)	FMT_MSA.1	Resolved (FMT_MSA.1 (Restriction))
	FMT_SMR.1	Resolved (FMT_SMR.1 (Com))
FMT_MSA.1 (Restriction)	FDP_ACC.1	Resolved (FDP_ACC.1 (Restriction))
	FMT_SMR.1	Resolved (FMT_SMR.1 (Com))
	FMT_SMF.1	Resolved (FMT_SMF.1 (Restriction))
FMT_SMF.1 (Restriction)	--	--
FDP_IFC.1 (DigSig)	FDP_IFF.1	Resolved (FDP_IFF.1 (DigSig))
FDP_IFF.1 (DigSig)	FDP_IFC.1	Resolved (FDP_IFC.1 (DigSig))
	FMT_MSA.3	Resolved (FMT_MSA.3 (DigSig))
FMT_MSA.3 (DigSig)	FMT_MSA.1	The list of the authorized issuer will not be managed by using “attributes”. So, no management roles or functions required.
	FMT_SMR.1	
FMT_SMR.1 (Com)	FIA_UID.2	Resolved (FIA_UID.2 (AdminServer))
FAU_GEN.1 (Com)	FPT_STM.1	The operational environment (e.g. a TOE external time server) shall provide a dependable time.

5.7.2 Security Assurance Requirements

SAR	Dependencies	Justification
ADV_FSP.2	ADV_TDS.1	NOT included because this EAL1 needs not to provide internal details of the TOE.
AGD_OPE.1	ADV_FSP.1	Resolved by hierarchical component ADV_FSP.2
AGD_PRE.1	--	--
ALC_CMC.1	ALC_CMS.1	Resolved
ALC_CMS.1	--	--
ASE_CCL.1	ASE_INT.1	Resolved
	ASE_ECD.1	Resolved
	ASE_REQ.1	Resolved by hierarchical component ASE_REQ.2
ASE_ECD.1	--	--
ASE_INT.1	--	--
ASE_OBJ.2	ASE_SPD.1	Resolved
ASE_REQ.2	ASE_ECD.1	Resolved
	ASE_OBJ.2	Resolved
ASE_SPD.1	--	--
ASE_TSS.1	ASE_INT.1	Resolved
	ASE_REQ.1	Resolved by hierarchical component

		ASE_REQ.2
	ADV_FSP.1	Resolved by hierarchical component ADV_FSP.2
ATE_IND.1	ADV_FSP.1	Resolved by hierarchical component ADV_FSP.2
	AGD_OPE.1	Resolved
	AGD_PRE.1	Resolved
AVA_VAN.1	ADV_FSP.1	Resolved by hierarchical component ADV_FSP.2
	AGD_OPE.1	Resolved
	AGD_PRE.1	Resolved

As demonstrated, all dependencies are resolved or not necessary for this particular evaluation/certification.

6 TOE Summary Specification

6.1 Coverage of the Security Functional Requirements

Authentication and access restrictions

All human users have to authenticate before using restricted functions of the TOE. This is implemented by Username/Password mechanisms at the server side (for administrators) and by a non-replayable PIN mechanism at the phone side (for phone users). The identification of the user at the phone side is by "his" phone number of the phone. If the user wants to use another phone, he has to "move" his phone number to this phone. Subsequently, authentication is mandatory. The "move" of the phone number is an unrestricted feature of the system.

The management functions of the servers are restricted to the appropriate administrator roles. These roles are enforced by the TOE server applications itself. If a remote administrator wants to access the TOE server components, he has (1) to pass the SSG. Here, the customer-admin manages the access restrictions and the permissions of the remote administrators on network level. Simply spoken, SSG works as type of packet filter which controls whether an administrator is allowed to access a special network device at a special time. (2) He has to log into the respective server by performing an Identification & Authentication process.

This covers FIA_UAU.2 (AdminServer), FIA_UID.2 (AdminServer), FIA_UAU.1 (UserServer), FIA_UID.1 (UserServer), FIA_UAU.3 (UserServer), FMT_SMF.1 (Server), FMT_SMF.1 (SSG), FMT_MTD.1 (Server), FMT_MTD.1 (SSG) and FMT_SMR.1 (Com) (partly).

Securing the confidentiality and integrity of communication data

Signaling data as well as media streams will be protected regarding confidentiality and integrity as long as they are inside the TSC defined as the network where the TOE components are connected to. The Internet and the SIP trunk are explicitly not part of the TSC. At first, this objective will be achieved by implementing a dependable mediation algorithm. Only intended participants are allowed to attend a call, which is implemented by an identification & authentication of the human users against the servers prior to the assignment of a phone number to a phone. Replay attacks against this authentication process are prevented by using unique additional identification values per authentication procedure. The rules and parameters, according to which this mediation algorithm works, can be configured by the administrators. The TOE servers (e.g. the G650) implement a strict separation of each call. So, no unintended information flow between calls is possible. Additionally, all signaling data and media streams are encrypted as long as they are inside the TSC. Only the intended participants and the TOE servers (e.g. the G650) have the respective cryptographic keys. If e.g. the G650 performs the encryption for some phones which are not compatible regarding the cryptography, the G650 does ensure that no key information can be determined. The G650 does not provide an appropriate interface and deallocate the memory area where all key information is stored after end of usage (usually end of the call). The cryptographic algorithms used are state-of-the-art (e.g. AES 128). External calls (incoming and outgoing) using the SIP-Trunk are not encrypted, neither the signaling nor the media stream. No confidential information of media streams or

cryptographic material will be logged. The log files will only be stored on a trustworthy platform.
This covers FIA_UAU.1 (UserServer), FIA_UID.1 (UserServer), FIA_UAU.3 (UserServer), FDP_ITT.2 (Conf), FDP_ETC.2 (Conf), FDP_ITC.2 (Conf), FTP_ITC.1 (Conf), FPT_TDC.1 (Conf), FDP_RIP.2 (Conf), FDP_ETC.1 (Export), FDP_IFC.1 (Export), FDP_IFF.1 (Export), FMT_MSA.3 (Export), FMT_MSA.1 (Export), FMT_SMF.1 (Export), FDP_IFC.1 (Mediation), FDP_IFF.1 (Mediation), FMT_MSA.3 (Mediation), FMT_MSA.1 (Mediation), FMT_SMF.1 (Mediation) and FMT_SMR.1 (Com) (partly).

Self-protection of the telephones and servers

The phones store its basic application (a firmware) on an internal storage. An upgrade of this firmware is possible and restricted to authorized issuer of the firmware (Avaya). In order to prevent an unauthorized firmware to be used for an upgrade, the phone checks a digital signature of the new firmware. If the digital signature does not match to the software or if the certificate of this digital signature is not owned by one of the authorized issuer or the digital signature does not exist, the phone does not upgrade its firmware. For building/checking the digital signature, the cryptographic algorithm SHA-1 (hash) and DSA-1024 (signature algorithm) will be used.
Furthermore, the phone provides some (local) configuration options beside the firmware. The security relevant options at the phone are protected by a secret key combination so that only administrators are allowed to use them. The key combination can also be configured by the administrator.
The major configuration of the phones will be performed by editing a special configuration file located at a configuration server. The phones load and use this file right after start-up. The access permissions of this configuration server (on OS level) and the physical protection by the room where the server is located ensure that only administrators can edit the files. The phones want to establish a HTTPS tunnel to the configuration server to download the file. HTTP will not be accepted by the phones (which is configurable; an appropriate hint in the admin guidance is given). For HTTPS the phones require a strong authentication of the configuration server based on a digital certificate. The digital certificate of the server must be signed by an Avaya root certificate, which is also stored in the firmware of the phones. If the phones could successfully verify the digital certificate of the configuration server, they establish the HTTPS connection and download the configuration file. Otherwise, they do not establish the connection and use their already stored configuration.
The servers do not need any further self-protection because they are sufficiently protected by physical means and the underlying operating system.
This covers FDP_IFC.1 (DigSig), FDP_IFF.1 (DigSig), FMT_MSA.3 (DigSig) and FMT_MTD.1 (Phone), FMT_SMR.1 (Phone), FMT_SMF.1 (Phone), FIA_UAU.2 (ServerPhone), FIA_UID.2 (ServerPhone) and FTP_ITC.1 (ServerPhone).

Logging of security relevant events

Logging is implemented in the server components of the TOE. They recognize the respective events, add date/time, users identity (if available and applicable) and some more information and build an audit record. These audit records will be stored on the hard disk of the underlying hardware. The file is protected by means of the underlying operating system. The TOE ensures that the audit information will be written to the correct file at

the correct place. File and Place can be configured by the administrator.
This covers FDP_ETC.1 (Export), FDP_IFC.1 (Export), FDP_IFF.1 (Export), FMT_MSA.3 (Export), FMT_MSA.1 (Export), FMT_SMF.1 (Export) and FAU_GEN.1 (Com)

Managing of User Access Restrictions

The user access to certain phone numbers may be restricted by the administrators. For this purpose, the administrators can manage white- and blacklists of numbers, which can be applied on corporate level, for a group of people and/or for single persons (identified by their personnel phone number). The Communication Manager checks the appropriate lists prior to mediation of the call. If the called party's phone number is not allowed, the call will not be established.
This covers FDP_ACC.1 (Restriction), FDP_ACF.1 (Restriction), FMT_MSA.3 (Restriction), FMT_MSA.1 (Restriction), FMT_SMF.1 (Restriction) and FMT_SMR.1 (Com) (partly).

7 Abbreviations

AAA Server	Authentication, Authorization, Accounting Server
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
CC	Common Criteria
DoS	Denial of Service
EAL	Evaluation Assurance Level
H.235.5	Framework for secure authentication in RAS using weak shared secrets http://ftp3.itu.ch/av-arch/avc-site/2005-2008/0507_Gen/H2355_for_consent.zip
H.323	Packet-based multimedia communications systems http://ftp3.itu.int/av-arch/avc-site/2005-2008/0604_Gen/H.323v6.zip
IP	Internet Protocol
OS	Operating System
OSP	Organizational Security Policy
PAM	Plugable Authentication Module
PBX	Private branch exchange
PSTN	Public Switched Telephone Network
SAR	Security Assurance Requirement
SDK	Software Development Kit
SES	SIP enable services
SFP	Security Function Policy
SFR	Security Functional Requirement
SIP	Session Initiation Protocol
SRTP	Secure Real-Time Transport Protocol
SSG	Secure Service Gateway
ST	Security Target
TDM	Time Divison Multiplex
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
VoIP	Voice over IP
VPN	Virtual Private Network

8 References

[CC]	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 1, CCMB-2006-09-001, • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 2, CCMB-2007-09-002, • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 2, CCMB-2007-09-003
[SecureConfigG]	Security Configuration Guidelines of the certified system based on the Communication Manager 5.1 Version 1.3 (17.02.2009)