Huawei BSC6900 Multimode Base Station Controller Software Security Target

Version: 1.07
Last Update: 2011-12-20
Author: Huawei Technologies Co., Ltd.

Index

Changes History

Version	Date	**Author**	Changes to previous version
V0.1	2010-12-15	Leo(Liu Jinbo)	---
V0.2	2011-3-24	Leo(Liu Jinbo)	Modify as suggestion as expert adviser
V0.3	2011-04-2	Leo(Liu Jinbo)	Modify according to Observation report
V0.50	2011-03-30	Leo(Liu Jinbo)	Modify according to Observation report
V0.51	2011-04-18	Leo(Liu Jinbo)	Modify as suggestion as expert adviser
V1.0	2011-04-29	Leo(Liu Jinbo)	Modify as suggestion as expert adviser
V1.01	2011-07-29	Leo(Liu Jinbo)	Modify as suggestion as expert adviser
V1.05	2011-08-23	Leo(Liu Jinbo)	Modify as suggestion as expert adviser
V1.06	2011-11-11	Leo(Liu Jinbo)	Modify as suggestion as expert adviser
V1.07	2011-12-20	Leo(Liu Jinbo)	Modify as suggestion as expert adviser

1 Introduction

This Security Target is for the evaluation of the product Huawei BSC6900 Multimode Base Station Controller Software Version V900R013C01SPC010.

1.1 Security Target Reference

Title: Huawei BSC6900 Multimode Base Station Controller Software Security Target

Version: 1.07

Author: Leo

Publication date: 2012-12-20

1.2 Target of Evaluation (TOE) Reference

TOE name: Huawei BSC6900 Multimode Base Station Controller Software (also, the acronym BSC6900 Software is used)

TOE version: V900R013C01SPC010

TOE Developer: Huawei

TOE release date: 2011-08-11

1.3 Target of Evaluation (TOE) Overview

The BSC6900 platform is an important Network Element (NE) of Huawei Single RAN solution. It adopts the industry-leading multiple Radio Access Technologies (RATs), IP transmission mode, and modular design. In addition, it is integrated with the functions of the Radio Network Controller (RNC) and Base Station Controller (BSC), thus efficiently maintaining the trend of multi-RAT convergence in the mobile network. The BSC6900 operates as an integrated NE to access the GSM&UMTS network and integrates the functions of the GSM BSC and the UMTS RNC.

The BSC6900 software, running in the BSC6900 platform, is compatible with GSM and UMTS technologies. Nonetheless, one unique configuration and operation mode of the TOE, the BSC6900 software, is used. This mode belongs to the one obtained from the installation process. So, the configuration of the TOE according to the security features provided is always the same, independently of the technology used in operation (GSM or UMTS).

This ST contains a description of the security objectives and the requirements, as well as the necessary functional and assurance measures provided by the TOE, the BSC6900 software. The ST provides the basis for the evaluation of the TOE according to the Common Criteria for Information Technology Security Evaluations (CC)

1.3.1 TOE usage

The BSC6900 software connects to the core networks and manages the base stations in the GSM and UMTS networks. The BSC6900 software performs functions such as radio resource management, base station management, power control, and handover control.

The BSC6900 software possesses the following functional features:

1. The BSC6900 software can work with GSM and UMTS technologies. Thus facilitating the smooth evolution from GSM to GSM&UMTS, and the evolution between GSM&UMTS and UMTS;
2. The BSC6900 software provides the highly efficient transmission resource management algorithm;
3. Industry-leading technologies, delivering excellent performance;
4. Easy maintenance through the Web LMT;
5. Flexible networking.

The major security features implemented by BSC6900 software and subject to evaluation are:

1. Authentication: Operators accessing the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords. Also, the TOE connects with the M2000 entity (external management element of the whole communication solution). The communication with the M2000 is protected connection using the SSL/TLS. Also an additional private arithmetic process common to both parties is applied before the authentication. Once the M2000 is properly connected the interaction with the TOE is made by the utilization of a special user (EMSCOMM) registered in the BSC6900 software.
2. Role-based access control: The TOE implements role-based access control, limiting access to different management functionality to different roles.
3. Auditing: Audit records are created for security-relevant events related to the use of BSC6900 software.

4. Communications security: BSC6900 software provides SSL/TLS channels (for FTP, HTTP, MML, BIN) to access the TOE.

5. Management of security functionality: The TOE offers management functionality for its security functionality.

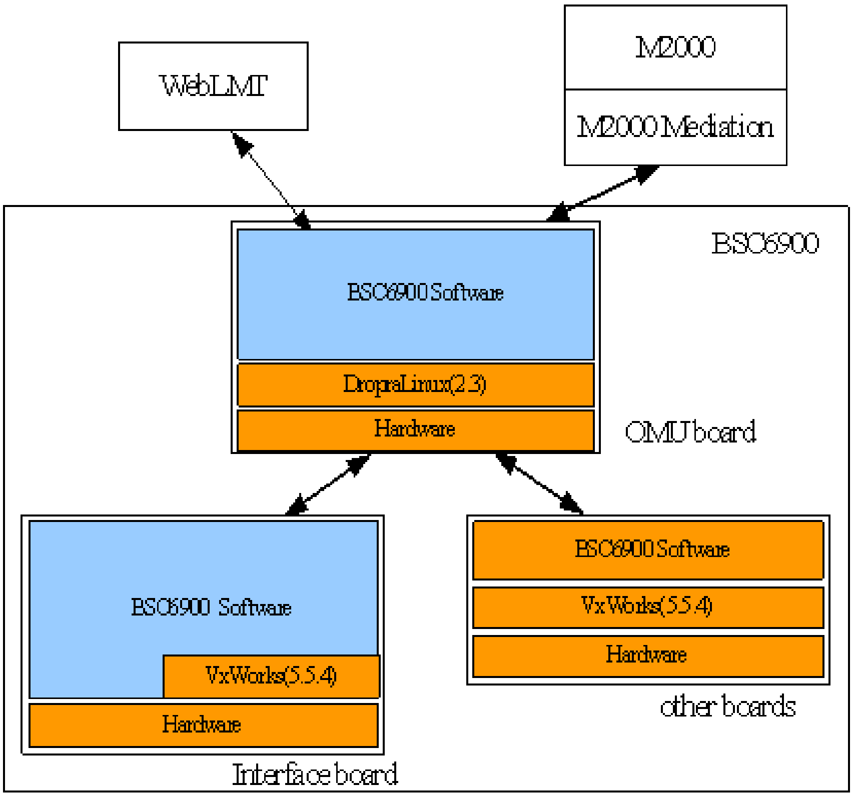
6. Digital signature: For the installation of GBTS managed element, the TOE is able to check the software integrity of the package previous to the installation of the element in order to verify its integrity.

1.3.2 TOE type

The TOE, Huawei BSC6900 Multimode Base Station Controller Software, is a BSC (Base Station Controller) Software, which provides solutions for our wireless uni RAN multi-mode controller in node function. So, the TOE consists of the software running in the OMU and Interface boards of the platform, and it must not be confused with all the software running in all the boards of the platform, neither with the whole platform.

1.3.3 Non TOE Hardware and Software

The TOE is deployed on the boards of operation and maintenance unit (OMU) and interface unit inside the whole platform where the TOE executes. Also, there are many other boards inside the same closet and other elements in the TOE environment.



Non TOE Hardware and Software environment

Application notes: In the above diagram, the light blue box area belongs in TOE while the orange box area belongs in TOE environment.

The M2000 needs a mediation software in order to communicate with the TOE. The M2000 server software consists of the main version software and mediation software. The main version software implements system functions, and the mediation software is used for the adaptation of different NE interfaces. The M2000 can manage new NEs after the corresponding mediation software is installed.

The WebLMT is accessed through Remote PCs used by administrators to connect to the TOE for access to the TOE via a secure channel SSL. It is obvious that physical networks, such as Ethernet subnets, interconnecting all the networking devices are necessary.

Looking inside the closet, for the OMU unit, it is need the corresponding hardware (OMU board) running the Dopra Linux operating system in version 2.3. In the interface board it runs a VxWorks O.S. version 5.5.4. So the physical architecture over which the TOE runs includes the following units:

- Interface process unit
- User data process unit
- Signal process unit
- MAC/ TDM switching network and control unit
- Operation and maintenance unit
- Clock process unit

As a product family, the boards that can maintain each of these units are indicated in the following table:

Board Type	**Board Name**	**Function**
OMU board	OMUa	• Handles configuration management, performance management, fault management, security management, and loading management for the BSC6900 Software. • Works as the OM agent for the LMT/M2000 to provide the BSC6900 OM interface for the LMT/M2000, thus achieving the communication between the BSC6900 Software and the LMT/M2000. • Works as the interface to provide the web-based online help.
Switching processing board	SCUa	• Provides MAC/GE switching and enables the convergence of ATM and IP networks. • Provides data switching channels. • Provides system-level or subrack-level configuration and maintenance. • Distributes clock signals for the BSC6900 Software.
TDM switching Network Unit	TNUa	• Provides 128K x 128K time slots TDM switching • Allocates the TDM network resources
Clock processing board	GCGa	Obtains the system clock source, performs the functions of phase-lock and holdover, and provides clock signals. **Differences:** Unlike the GCUa board, the GCGa board can receive and process the GPS signals.
	GCUa	
Signaling processing board	SPUb/ XPUb	Manages user plane and signaling plane resources in the subrack and processes signaling.

Board Type	Board Name	Function
Service processing board	DPUe/ DPUd/ DPUc	Processes CS services and PS services within the system.
Service identification board	NIUa	Provides the service identification function. It works with the service processing boards to schedule different types of services.
Interface processing board	AEUa	• Provides 32 channels of ATM over E1/T1. • Extracts clock signals and sends the signals to the GCUa or GCGa board.
	AOUc	• Provides four channels over the channelized optical STM-1/OC-3 ports based on ATM protocols. • Supports ATM over E1/T1 over SDH or SONET. • Provides 252 E1s or 336 T1s. • Extracts clock signals and sends the signals to the GCUa or GCGa board.
	FG2c	• Provides 12 channels over FE electrical ports or 4 channels over GE electrical ports. • Supports IP over FE/GE.
	GOUc	• Provides four channels over GE optical ports. • Supports IP over GE.
	PEUa	• Provides 32 channels of IP over E1/T1. • Extracts clock signals and sends the signals to the GCUa or GCGa board.
	EIUa	• Provides four E1/T1 electrical ports for TDM transmission • Transmits, receives, encodes, and decodes 32 E1s/T1s. The E1 transmission rate is 2.048 Mbit/s; the T1 transmission rate is 1.544 Mbit/s • Processes signals according to the LAPD protocol • Processes signals according to the SS7 MTP2 protocol

Board Type	Board Name	Function
	POUc	• Provides four channels over the channelized optical STM-1/OC-3 ports based on IP protocols, equivalent to 252 E1s or 336 T1s. • Supports IP over E1/T1 over SDH/SONET. • Extracts clock signals and sends the signals to the GCUa or GCGa board.
	UOIa	• Provides four channels over the unchannelized STM-1/OC-3c optical ports. • Supports ATM/IP over SDH/SONET. • Extracts clock signals and sends the signals to the GCUa or GCGa board.
	UOIc	• Provides eight channels over the unchannelized STM-1/OC-3c optical ports. • Supports ATM over SDH/SONET. • Extracts clock signals and sends the signals to the GCUa or GCGa board.

The green color indicates the specific board used in the configuration under evaluation and the boards where the TOE parts execute. In the rest of the boards in the closet, the software is loaded by bootp protocol from the OMU board, however, these boards are not considered as executing TOE parts.

For the boards executing parts of the TOE, the following table shows interfaces available in the BSC6900 platform hardware along with respective usage:

Boards	Supported Interfaces and Usage
OMUa	The following list shows a collection of interfaces which might be used during this evaluation for all models. • ETH interface, connector type RJ45, operation mode 10M/100M/1000M Base-TX auto-sensing, supporting half-duplex and full-duplex, compliant to IEEE 802.3-2002, used for connections initiated by users and/or administrators from a local maintenance terminal via HTTPS or SSL to perform management and maintenance operations. Management and maintenance through NMS workstation is not within the scope of this evaluation thus NMS related accounts should be disabled during the evaluation.
FG2c	• The interfaces boards are used for incoming and outgoing network

	traffic, which support VLAN, IP_based ACL, anti-DDoS attack characteristics.

1.4 TOE Description

The TOE is composed of the following two elements:

OMU

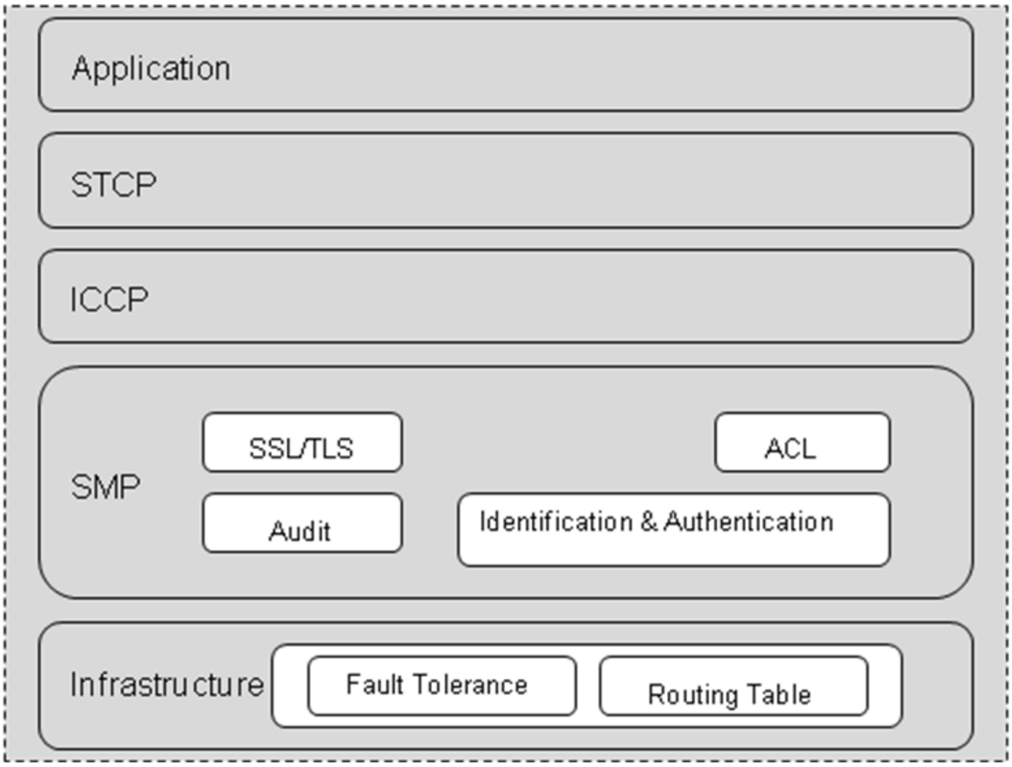
The OMU enables the management and maintenance of the BSC6900 Software in the following scenarios: routine maintenance, emergency maintenance, upgrade, and capacity expansion.

Interface Processing

The interface processing provides transmission ports and resources, processes transport network messages, and enables interaction between the BSC6900 Software internal data and external data.

1.4.1 Architectural overview

This section will introduce the Huawei's BSC6900 Software from a software architectural view.



The specific functionality detailed in the white boxes is executed in a distribute way. The modules SSL/TLS, ACL, Audit, Identification & Authentication and Fault tolerance are executed in the OMU board. The modules relating with the routing table and connection filtering out of the management network are executed on the interface board.

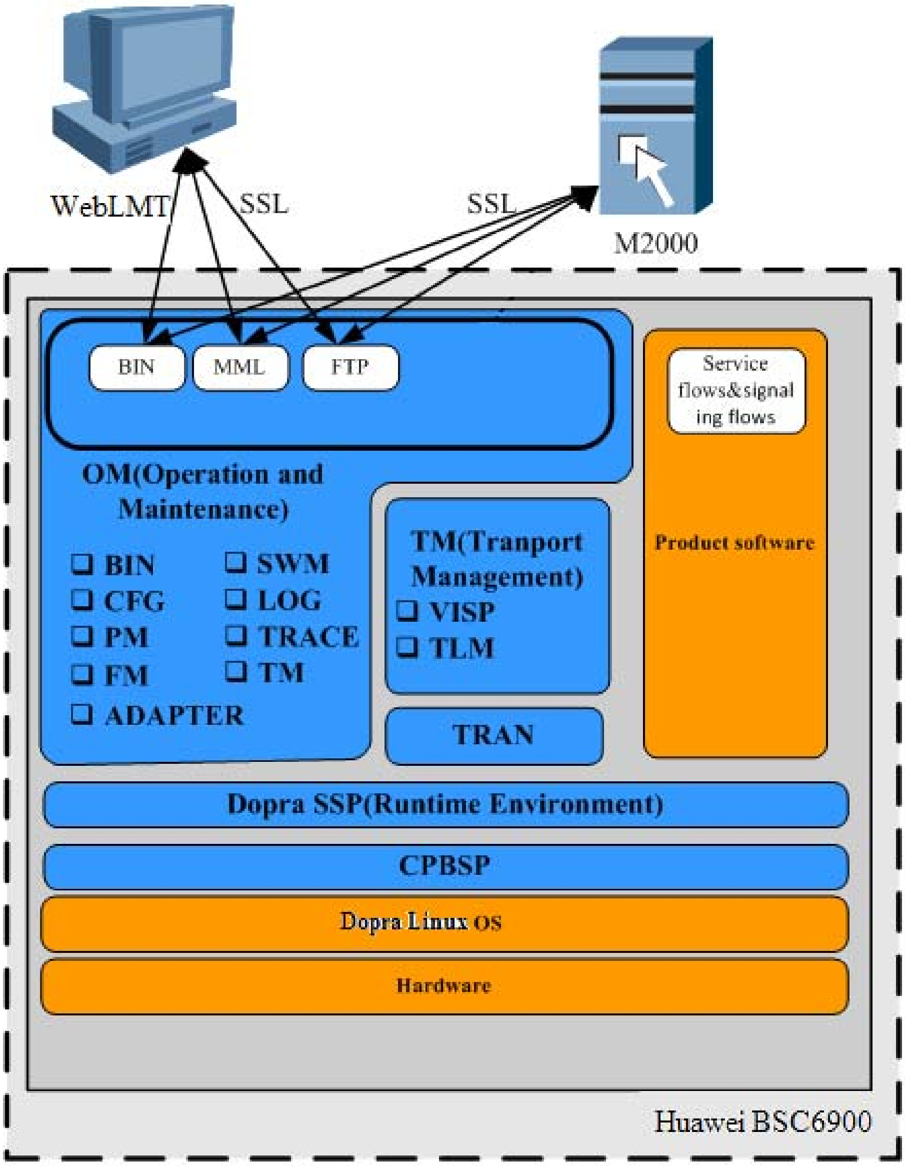
The following table shows the functions of each layer in the BSC6900 software architecture :

Layer	Functions
Infrastructure	• Provides the hardware platform and hides the lower-layer hardware implementation. • Hides the differences for operating systems, and provides enhanced and supplementary functions for the system.
Service Management Plane (SMP)	Provides the OM interface to perform the OM functions of the system.

Layer	Functions
Internal Communication Control Plane (ICCP)	• Transfers internal maintenance messages and service control messages between different processors, thus implementing efficient control over distributed communication. • Operates independent of the infrastructure layer.
Service Transport Control Plane (STCP)	• Transports the service data on the user plane and control plane at the network layer between NEs. • Separates the service transport technology from the radio access technology and makes the service transport transparent to the upper-layer service. • Provides service bearer channels.
Application	• Implements the basic functions of network element service control and controls the upper-layer service, such as call processing, mobility management, and RRM. • Hides the topology characteristics of various resources in the network and in the equipment. • Provides the resource access interface, hides the distribution of internal resources and network resources, maintains the mapping between the service control and resource instance, and controls the association between various resources. • Manages the resources and OM status, responds to the resource request from the upper layer, and hides the resource implementation from the upper layer. • Isolates the upper-layer services from the hardware platform to facilitate the hardware development.

1.4.2 Logical Scope

This section will define the scope of the TOE to be evaluated. The logical boundary is represented by the elements in blue color. These elements are the parts of the TOE, namely the BSC6900 Software.



Application notes: In the above diagram, the light blue box area belongs in TOE while the orange box area belongs in TOE environment.

The interface processing (depicted in the picture as Transport Management) is in charge of controlling the flow (datagrams) between the TOE and network elements. The network elements under the interface processing control are those like the NodeB, the GBTS and Core Network. This control is performed by matching information contained in the headers of connection-oriented or connectionless IP packets against routing table in forwarding engine. Also, a session establishment control is performed in order to accept or deny connections. In case of failure, the fault tolerance procedure will switch the active interface board with the stand-by interface board.

The OMU is in charge of the system control and security managements of the BSC6900 Software. This management is performed via a secure channel enforcing SSL/TLS. Also, it controls the flow of the connection with the M2000 and WebLMT elements. The same fault tolerance procedure is implemented in the OMU, so in case of failure, the switch with the stand-by board will remains the system operative.

1.4.3 Physical Scope

The release packages for BSC6900 Software are composed of software and documents. The BSC6900 software packages are in the form of compressed files.

The software and documents for the TOE is the following:

Software and Documents	Description
BSC6900 – OMU	Main part of the BSC6900 running in the OMU board.
BSC6900 - Interface	Interface board software package is also contained (but not executed) in the OMU board and loaded in the interface board during the start up.
(For Customer)BSC6900 GU Product Documentation (V900R013C01_Draft A)(HDX)-EN.zip and the additional guidance documentation provided	BSC6900 V900R013C01SPC010 product documentation. The product documentation covers the planning, installation, commissioning, and maintenance of the BSC6900 system.

2 CC Conformance Claim

This ST is *CC Part 2 conformant* [CC] and *CC Part 3 conformant* [CC]. The CC version of [CC] is 3.1R3. The methodology to be used for evaluation is CEM3.1 R3.

This ST is EAL3-conformant as defined in [CC] Part 3 with the augmentation of ALC_CMC.4, ALC_CMS.4. No conformance to any Protection Profile is claimed.

3 TOE Security problem definition

3.1 TOE Assets

The information assets to be protected are the information stored, processed or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information and passwords, audit records, etc.) and other information that the TOE facilitates access to (such as system software, patches) are all considered part of information assets.

The TOE consists of the following assets:

Asset	Description	Asset value
A1.Software and patches	The integrity and confidentiality of the system software and the patches when in transit across the management network should be protected from modification and disclosure.	Integrity Confidentiality
A2.Stored configuration data	The integrity and confidentiality of the stored configuration data should be protected. Configuration data includes the security related parameters under the control of the TOE (such as user account information and passwords, audit records, etc).	Integrity Confidentiality
A3. In transit configuration data	The integrity and confidentiality of the configuration data when travelling in the management network.	Integrity Confidentiality

3.2 Threats

This section of the security problem definition shows the threats to be countered by the TOE, its operational environment, or a combination of both. The threat agents can be categorized as either:

Agent	Description
Eavesdropper	An eavesdropper from the management network served by the TOE is able to intercept, and potentially modify or re-use the data that is being sent to the TOE.
Internal attacker	An unauthorized agent who is connected to the management network.
Restricted authorized user	An authorized user of the TOE who has been granted authority to access certain information and perform certain actions.

In the first and second cases, the users are assumed to be potentially hostile with a clear motivation to get access to the data. In the last case, all authorized users of the TOE are entrusted with performing certain administrative or management activities with regard to the managed device. Consequently, organizational means are expected to be in place to establish a certain amount of trust into these users. However, accidental or casual attempts to perform actions or access data outside of their authorization are expected. The assumed security threats are listed below.

3.2.1 Threats by Eavesdropper

Threat: T1. InTransitConfiguration	
Attack	An eavesdropper in the management network succeeds in accessing the content of the BSC6900 data while transferring, violating its confidentiality or integrity.
Asset	A3. In transit configuration data
Agent	Eavesdropper

Threat: T2. InTransitSoftware	
Attack	An eavesdropper in the management network succeeds in accessing the content of the BSC6900 software/patches while transferring, violating its confidentiality or integrity.
Asset	A1.Software and patches

Agent	Eavesdropper

3.2.2 Threats by Internal Attacker

Threat: T3.UnauthenticatedAccess	
Attack	An attacker in the management network gains access to the TOE disclosing or modifying the configuration data stored in the TOE in a way that is not detected.
Asset	A2.Stored configuration data
Agent	Internal Attacker

3.2.3 Threats by restricted authorized user

Threat: T4.UnauthorizedAccess	
Attack	An user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for.
Asset	A2.Stored configuration data
Agent	Restricted authorized user

3.3 Assumptions

3.3.1 Physical

- **A.PhysicalProtection**

It is assumed that the TOE is protected against unauthorized physical access.

3.3.2 Personnel

- **A.TrustworthyUsers**

It is assumed that the organization responsible for the TOE and its operational environment has measures in place to establish trust into and train users of the TOE commensurate with the extent of authorization that these users are given on the TOE. (For example, super users and users that are assigned similar privileges are assumed to be fully trustworthy and capable of operating the TOE in a secure manner abiding by the guidance provided to them).

3.3.3 Connectivity

- **A.NetworkSegregation**

It is assumed that the network interfaces that allow access to the TOE's user interfaces are in a management network that is separated from the core networks.

3.3.4 Support

- **A.Support**

The operational environment must provide the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records.

3.3.5 OperatingSystem

- **A.OperatingSystem**

It is assumed that the Operating System of the TOE' environment is secure.

3.3.6 SecurePKI

- **A.SecurePKI**

There exists a well managed protected public key infrastructure. The certificates used by the TOE and its client are managed by the PKI.

3.4 Organizational Policies

3.4.1 P.Audit

The TSF shall be able to generate an audit record of the auditable events, which associate with the identity of the user that caused the event. The TSF shall protect the stored audit records in the audit trail from unauthorized deletion. The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

3.4.2 P.RoleManagement

Different people access the TSF needs to be divided according to different roles with different permissions, as far as possible the user has the minimum required permissions.

4 Security Objectives

4.1 Objectives for the TOE

The following objectives must be met by the TOE:

- **O.SecureCommunication** The TOE shall provide a secure remote communication channel for remote administration of the TOE via SSL.
- **O.Authorization** The TOE shall implement different authorization levels that can be assigned to users in order to restrict the functionality that is available to individual users.
- **O.Authentication** The TOE must authenticate users of its user access.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant actions.
- **O.SoftwareIntegrity** The TOE must provide functionality to verify the integrity of the received software patches.
- **O.RoleManagement** The TOE shall provide role management functionality: different people access the TSF is divided according to different roles with different permissions, as far as possible the user has the minimum required permissions.

4.2 Objectives for the Operational Environment

- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as a console) shall be protected against unauthorized physical access.
- **OE.NetworkSegregation** The operational environment shall provide protection to the network in which the TOE hosts by separating it from the application (or public) network.
- **OE.OperatingSystem** The Operating System of the TOE' environment is secure.
- **OE.Support** Those responsible for the operation of the TOE and its operational environment must ensure that the operational environment provides the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records.

- **OE.TrustworthyUsers** Those responsible for the operation of the TOE and its operational environment must be trustworthy, and trained such that they are capable of securely managing the TOE and following the provided guidance.

  OE.SecurePKI There exists well managed protected public key infrastructure. The certificates used by the TOE and its client are managed by the PKI.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective is at least covered by one threat or policy.

	T1.InTransitConfiguration	T2.InTransitSoftware	T3.UnauthenticatedAccess	T4.UnauthorizedAccess	A.PhysicalProtection	A.TrustworthyUsers	A.NetworkSegregation	A.Support	A.OperatingSystem	A.SecurePKI	P1.Audit	P2.RoleManagement
O.Authentication			X	X								
O.Authorization				X								
O.SecureCommunication	X	X	X	X								
O.SoftwareIntegrity		X										
O.Audit											X	
O.RoleManagement												X
OE. Physical			X	X	X							
OE.NetworkSegregation							X					
OE.OperatingSystem									X			
OE. Support								X				
OE. TrustworthyUsers				X		X						

OE.SecurePKI										X		

Mapping Objectives to Threats

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T1.InTransitConfiguration	The threat T1.InTransitConfiguration is countered by requiring communications security via SSL for network communication between entities in the management network and the TOE (O.SecureCommunication).
T2. InTransitSoftware	The threat T2.InTransitSoftware is countered by O.SecureCommunication which establishes a secure communication channel between the TOE and external entities in the management network. This threat is also countered by O.SoftwareIntegrity: when a software package is uploaded to the BSC6900, its digital signature is verified.
T3.UnauthenticatedAccess	The threat T3.UnauthenticatedAccess is countered by the security objective for the TOE O.Authentication which requires the TOE to implement an authentication mechanism for the users in the management network. The security objective for the operational environment OE.Physical contributes to the mitigation of the threat assuring that the software and configuration files stored in the TOE, will not be modified. The security objective O.SecureCommunication counteracts the threat by preventing the reception of authentication requests from non-secure connections.

T4.UnauthorizedAccess	The threat T4.UnauthorizedAccess is countered by the security objective for the TOE O.Authentication which requires the TOE to implement an authentication mechanism for the users in the management network. It is also countered by requiring the TOE to implement an access control mechanism (O.Authorization). It is also countered by requiring the TOE to implement a trusted path between TOE and its users (O.SecureCommunication) so the user credentials cannot be captured. The security objective for the operational environment OE.TrustworthyUsers contributes to the mitigation of this threat requiring the users to be responsible with their passwords. The security objective for the operational environment OE.Physical contributes to the mitigation of the threat assuring that the software and configuration files stored in the TOE, will not be modified

Sufficiency analysis for threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, and actually contributes to the environment achieving consistency with the assumption. If all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	**Rationale for security objectives**
A.Physical	This assumption is directly implemented by the security objective for the environment OE.Physical.
A. TrustworthyUsers	This assumption is directly implemented by the security objective for the environment OE. TrustworthyUsers.
A.NetworkSegregation	This assumption is directly implemented by the security objective for the environment OE.NetworkSegregation.

A.Support	This assumption is directly implemented by the security objective for the environment OE.Support
A.OperatingSystem	This assumption is directly implemented by the security objective for the environment OE.OperatingSystem
A.SecurePKI	This assumption is directly implemented by the security objective for the environment. OE. SecurePKI

Sufficiency analysis for assumptions

The following rationale provides justification that the security objectives are suitable to counter each individual policy and that each security objective tracing back to a policy:

Policy	Rationale for security objectives
P.Audit	This policy is directly implemented by the security objective for the TOE O.Audit
P.RoleManagement	This policy is directly implemented by the security objective for the TOE O.RoleManagement

Sufficiency analysis for policies

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

FAU_GEN.1 Audit data generation

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

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

b) All auditable events for the [***selection:*** ***not specified***] level of audit; and

c) [***assignment:*** ***The following auditable events:***

i. user activity

1. login, logout

2. operation requests

ii. user management

1. add, delete, modify

2. password change

3. authorization modification

4. locking, unlocking (manual or automatic)

iii. user group management

1. add, delete, modify

iv. command group management

1. add, delete, modify

]

Application Note: The audit service is started and stopped with that of OMU service, no independent log.

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, [***assignment:*** ***workstation IP (if applicable), user (if applicable), and command name (if applicable).***]

FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [***assignment***: ***users authorized per FDP_ACF.1/Local users, FDP_ACF.1/Domain users and FDP_ACF.1/EMSCOMM user***] with the capability to read [***assignment***: ***all information***] from the audit records.

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

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [***assignment***: ***selection***] of audit data based on [***assignment***: ***log level, slot-id and parameters selection:***

- ***Source: specifies the system to which the operator to be queried logs in.***
- ***Operator: specifies the name of the user who runs the command.***
- ***Domain Name: specifies the domain name of the operator to be queried. This parameter can be set to LOCAL, EMS, or EMSOP.***
- ***Workstation IP: specifies the IP address of the terminal where the command is run.***
- ***Start Time: specifies the time when the command execution starts.***
- ***End Time: specifies the time when the command execution ends.***
- ***Final: specifies whether the command execution succeeds.***
- ***Command Name: specifies the name of the command to be executed.***

].

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion

FAU_STG.1.2 The TSF shall be able to [***selection***: ***prevent***] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall [***assignment***: ***delete the oldest files***] if the audit trail exceeds [***assignment***: ***an administrator configured value***].

6.1.2 Cryptographic Support (FCS)

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [***assignment: digital signature verification***] in accordance with a specified cryptographic algorithm [***assignment: RSA with underlying SHA-256***] and cryptographic key sizes [***assignment: 1024bits***] that meet the following: [***assignment: none***]

6.1.3 User Data Protection (FDP)

FDP_ACC.1/Local users Subset access control

FDP_ACC.1.1 The TSF shall enforce the [***assignment: BSC6900 local users access control policy***] on [***assignment: Local users as subjects and Commands as objects***].

FDP_ACF.1/Local users Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [***assignment: BSC6900 local users access control policy***] to objects based on the following: [***assignment:***

Subjects

Local Users, security attributes:

i. User name

ii. Operational rights

Objects

Commands, security attributes:

i. Command name

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***assignment***: ***the local user has execution permission of the command targeted by the request depending on the operational rights of the local user***].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***assignment: None*** **].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***assignment: None***]

FDP_ACC.1/Domain users Subset access control

FDP_ACC.1.1 The TSF shall enforce the [***assignment: BSC6900 domain users access control policy***] on [***assignment: Domain users as subjects and Commands as objects***].

FDP_ACF.1/Domain users Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [***assignment: BSC6900 domain users access control policy***] to objects based on the following: [***assignment:***

Subjects

Domain Users, security attributes:

i. User name

ii. Operational rights

Objects

Commands, security attributes:

i. Command name

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***assignment***: ***the domain user has execution permission of the command targeted by the request depending on the operational rights of the domain user***].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***assignment:* None**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***assignment:* None**]

FDP_ACC.1/EMSCOMM user Subset access control

FDP_ACC.1.1 The TSF shall enforce the [***assignment:* BSC6900 EMSCOMM user access control policy**] on [***assignment:* EMSCOMM user as subject and Commands as objects**].

FDP_ACF.1/EMSCOMM user Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [***assignment:* BSC6900 EMSCOMM user access control policy**] to objects based on the following: ***[assignment:***

Subject

EMSCOMM, security attributes:

i. User name

ii. Operational rights

Objects

Commands, security attributes:

i. Command name

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***assignment:* the EMSCOMM user has execution permission of the command targeted by the request depending on the operational rights of the EMSCOMM user**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***assignment:* None**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***assignment:*** ***None***]

6.1.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [***selection:*** ***an administrator configurable positive integer within [assignment: 1 and 255]]*** unsuccessful authentication attempts occur related to [***assignment****: authentication through the WebLMT by local users. The counter for these attempts is reset each time the user remains in the session a time frame configurable by administrator either between 1 and 60 minutes.*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***selection:*** ***surpassed***], the TSF shall [***assignment:*** ***lockout the account for an administrator configurable duration either between 1 and 65535 minutes***].

Application note: The EMSCOMM user is not considered in this requirement. The EMSCOMM user is authenticated in the TOE by automatic method and not by user and password. Domain users are authenticated in the M2000 element of the TOE environment, so they are also not considered in this requirement.

FIA_ATD.1/Local users User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***assignment:***

a) Username

b) User groups

c) Command groups

d) Password

e) Number of unsuccessful authentication attempts since last successful authentication attempt

f) Login allowed start time

g) Login allowed end time

h) Password expiration date

i) Account expiration date

j) Lock status

k) Operational rights

]

FIA_ATD.1/Domain users User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***assignment:***

a) Username

b) Password

c) Operational rights

]

FIA_ATD.1/ EMSCOMM user User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***assignment:***

a) Username

b) Operational rights

]

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet: [***assignment:***

a) an administrator configurable minimum length between 6 and 32 characters, and

b) an administrator configurable combination of the following:

i. at least one lower-case alphanumerical character,

ii. at least one upper-case alphanumerical character,

iii. at least one numerical character,

iv. at least one special character.]

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 the TSF shall allow [***assignment***:

a) Handshake command

b) ***Parameter negotiation***

c) ***Link status shake hand request***

d) ***Module shake hand***

e) ***Verification of api security***

f) ***Verification of code***

g) ***Alarm query***

h) ***Vendor network probe service]***

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.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [***assignment***: ***Authentication for:***

a) ***Local Users***

b) ***Domain Users***

c) ***EMSCOMM User***

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [***assignment***:

a) ***Local users are authenticated in BSC6900 by user and password stored in BSC6900***

b) ***Domain users authentication is delegated in the M2000 management element of the environment by user and password***

c) ***EMSCOMM user authenticates using the SSL protocol.***

].

Application Note: Also, the EMSCOMM user applies a special arithmetic procedure common to both parties, TOE and M2000 to assure the knowledge of the algorithm.

FIA_UID.1 Timing of authentication

FIA_UID.1.1 The TSF shall allow [***assignment***:

a) ***Handshake command***

b) Parameter negotiation

c) Link status shake hand request

d) Module shake hand

e) Verification of api security

f) Verification of code

g) Alarm query

h) Vendor network probe service]

on behalf of the user to be performed before the user is identified.

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

6.1.5 Security Management (FMT)

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [***assignment:*** ***BSC6900 local user, domain user and EMSCOMM user access control policies***] to restrict the ability to [***selection:*** ***query and modify***] the security attributes [***assignment:*** ***password, user group, login allowed start time and end time of local users***] to [***assignment:*** ***users with the appropriate operational rights***].

Application Note: The ability to query and modify the local users' information is provided to the users by assigning certain operational rights. The roles or user groups maintained in the system are just a mechanism to assign operational rights to the users. Then, the assignment of the requirement refers the "users with the appropriate rights". This is detailed in the TOE summary specification.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [***assignment:*** ***BSC6900 local user, domain user and EMSCOMM user access control policies***] to provide [***selection:*** ***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [***assignment:*** ***administrator defined roles with the appropriate rights***] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

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

a) local user management

b) user groups management

c) commands groups management

d) local users authorization management

e) modification of the password policy

f) Audit size limit

g) enabling/disabling SSL/TLS

h) VLAN configuration

i) IP-based access control configuration

]

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [***assignment:***

a) Guest

b) User

c) Operator

d) Administrator

e) Custom]

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

Application Note: These roles are only applicable to the local users. The domain users are not maintained in the TOE, no role neither user group is assigned to a domain user in the TOE. Also, the EMSCOMM user can not be assigned to any role. This is detailed in the TOE specification summary.

6.1.6 TOE access (FTA)

FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [***assignment:***

a) Login allowed start time

b) Login allowed end time

c) Account expiration date

d) Lock status]

6.1.7 Trusted Path/Channels (FTP)

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***selection: remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***selection: modification and disclosure***].

FTP_TRP.1.2 The TSF shall permit [***selection: remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***selection: TOE usage from users in the WebLMT***]

Application Note: Assured identification between both parties is achieved after the user authentication has been performed.

FTP_ITC.1 Inter-TSF trusted channel

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 [***selection: another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [***assignment:***

- Commands execution and data transmission with Huawei proprietary protocols

- FTP connections

].

Application Note: Assured identification between both parties is achieved thanks to the SSL server and peer bi directional authentication.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

	O.Audit	O.Authentication	O.Authorization	O.SecureCommunication	O.SoftwareIntegrity	O.RoleManagement
FAU_GEN.1	×					
FAU_GEN.2	×					
FAU_SAR.1	×					

FAU_SAR.3	×					
FAU_STG.1	×					
FAU_STG.3	×					
FCS_COP.1					×	
FDP_ACC.1/Local users			×			×
FDP_ACC.1/Domain users			×			×
FDP_ACC.1/EMSCOMM user			×			×
FDP_ACF.1/Local users			×			×
FDP_ACF.1/Domain users			×			×
FDP_ACF.1/EMSCOMM user			×			×
FIA_AFL.1		×				
FIA_ATD.1/Local users		×	×			
FIA_ATD.1/Domain users		×	×			
FIA_ATD.1/EMSCOMM user		×	×			
FIA_SOS.1		×				
FIA_UAU.1		×				
FIA_UAU.5		×				
FIA_UID.1	×	×	×			
FMT_MSA.1			×			×
FMT_MSA.3			×			

FMT_SMF.1		×	×	×		×
FMT_SMR.1			×			×
FTA_TSE.1		×				
FTP_TRP.1				×		
FTP_ITC.1				×		

Mapping SFRs to objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include user identities (FAU_GEN.2) where applicable, which are supplied by the identification mechanism (FIA_UID.1). Audit records are in a string format. Selection based on parameters values is provisioned to read and search these records (FAU_SAR.1, FAU_SAR.3). The protection of the stored audit records is implemented in FAU_STG.1. Functionality to delete the oldest audit file is provided if the size of the log files becomes larger than the

	size specified by the administrators (FAU_STG.3).
O.Authentication	User authentication is implemented by FIA_UAU.5. Also, each user must be identified and authenticated before operating with the TOE supported by FIA_UID.1 and FIA_UAU.1 (except those operations detailed in FIA_UAU.1 and FIA_UID.1). The necessary user attributes (passwords and operational rights) are spelled out in FIA_ATD.1/Local users, FIA_ATD.1/Domain users and FIA_ATD.1/EMSCOMM user. The authentication mechanism supports authentication failure handling (FIA_AFL.1), restrictions as to the validity of accounts for logon (FTA_TSE.1), and a password policy (FIA_SOS.1). Management functionality is provided in FMT_SMF.1.
O.Authorization	Access control is based on the definition of users as subject and commands as objects. The requirement for access control is spelled out in FDP_ACC.1/Local users, FDP_ACC.1/Domain users and FDP_ACC.1/EMSCOMM user. The access control policies are modeled in

	FDP_ACF.1/Local users, FDP_ACF.1/Domain users, FDP_ACF.1/EMSCOMM user. Unique user IDs are necessary for access control provisioning (FIA_UID.1), and user-related attributes are spelled out in FIA_ATD.1/Local users, FIA_ATD.1/Domain users and FIA_ATD.1/EMSCOMM user. The user roles, providing the corresponding operational rights are defined in FMT_SMR.1. Management functionality for the definition of access control policies is provided in FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1.
O.SecureCommunication	Communications security is implemented by the establishment of a trusted path for remote users in FTP_TRP.1. The communications through the ports used by the M2000 are covered by FTP_ITC.1. Management functionality to enable these mechanisms is provided in FMT_SMF.1.
O.SoftwareIntegrity	The software integrity objective is directly implemented with FCS_COP.1, so the TOE performs digital signature verification over the software of GBTS during its upload.

O.Rolemanagement	The requirements for access control on the management network are modeled in FDP_ACC.1/Local users, FDP_ACC.1/Domain users, FDP_ACC.1/EMSCOMM user, FDP_ACF.1/Local users, FDP_ACF.1/Domain users, FDP_ACF.1/EMSCOMM user. The operational rights are assigned in relation to the different roles defined in the system (FMT_SMR.1). Management functionality for access control is provided in FMT_SMF.1 and FMT_MSA.1.

SFR sufficiency analysis

6.2.3 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement. The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution

FAU_GEN.1	FPT_STM.1	Not satisfied. The time is obtained from the environment.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not satisfied. The key for the cryptographic operation is included inside the software package sent to the user. Not satisfied. The TOE does not delete keys, they are stored in the package in order to re-install the product when necessary.
FDP_ACC.1/Local users	FDP_ACF.1	FDP_ACF.1/Local users
FDP_ACC.1/Domain users	FDP_ACF.1	FDP_ACF.1/Domain users
FDP_ACC.1/EMSCOMM	FDP_ACF.1	FDP_ACF.1/EMSCOMM user

user		
FDP_ACF.1/Local users	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Local users FMT_MSA.3
FDP_ACF.1/Domain users	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Domain users FMT_MSA.3
FDP_ACF.1/EMSCOMM user	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/EMSCOMM user FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1/Local users	None	
FIA_ATD.1/Domain users	None	
FIA_ATD.1/EMSCOMM user	None	
FIA_SOS.1	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	None	
FIA_UID.1	None	
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1	FDP_ACC.1/Local users FMT_SMR.1 FMT_SMF.1

	FMT_SMF.1	
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTA_TSE.1	None	
FTP_TRP.1 FTP_ITC.1	None None	

Dependencies between TOE Security Functional Requirements

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components as specified in [CC] Part 3 with the augmentation of ALC_CMC.4 and ALC_CMS.4 components as specified in [CC] Part 3. No operations are applied to the assurance components.

Assurance class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**
Development	ADV_ARC	1
	ADV_FSP	3
	ADV_IMP	NA
	ADV_INT	NA
	ADV_SPM	NA
	ADV_TDS	2
Guidance documents	AGD_OPE	1

	AGD_PRE	1
Life-cycle support	ALC_CMC	4
	ALC_CMS	4
	ALC_DEL	1
	ALC_DVS	1
	ALC_FLR	NA
	ALC_LCD	1
	ALC_TAT	NA
Security Target evaluation	ASE_CCL	1
	ASE_ECD	1
	ASE_INT	1
	ASE_OBJ	2
	ASE_REQ	2
	ASE_SPD	1
	ASE_TSS	1
Tests	ATE_COV	2
	ATE_DPT	1
	ATE_FUN	1
	ATE_IND	2
Vulnerability assessment	AVA_VAN	2

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 Auditing

The TOE generates audit records for security-relevant events. (Please refer to FAU_GEN.1 for a list of event types, and the type of information recorded)

The auditing functionality of the TOE cannot be started or stopped independently from the operational TOE. So, the audit services start and stop together with the TOE, and the corresponding audit records for the start and shutdown of TOE, and of its individual subsystems are generated in the audit log. (FAU_GEN.1)

Where appropriate, the data recorded with each audit record includes the unique user ID associated with a subject (local, domain or emscomm users). (FAU_GEN.2)

The logs are stored in a database that is used by TOE to store configuration and other data. No user can modify or delete these logs because all the accesses to the database are limited to the BSC6900 Software. (FAU_STG.1)

If the audit records stored in the logs exceed the limit defined by the administrator, such as 5GB, the TOE will overwrite the oldest logs and continue to record. (FAU_STG.3)

Users from the M2000 and WebLMT can review the audit records available in the database. The search functionality is based on time intervals, user IDs, workstation IP and command name (please refer to the FAU_SAR.3 requirement to check the different selection parameters). (FAU_SAR.1, FAU_SAR.3)

7.1.2 Digital signature

To address security issues, digital signature mechanism to ensure the legitimacy and integrity of the software packages are provided.

1. When packaged, a hash message is calculated over the Software files and a digital signature is applied by Huawei's digital signature tool.

2. The TOE checks the software integrity using the public key of the digital signature and compares the hashes messages with the software package check code obtained after recalculation. If they are different, the signature verification fails.

The digital signature is mainly applied over the software packages of the GBTS element when it is upgraded. When the GBTS software package is uploaded to the TOE, this package is verified against its digital signature in order to check the integrity.

(FCS_COP.1)

7.1.3 Access control

The TOE controls which operations can be performed by the users on Managed Elements. The product considers three kinds of users:

- **Local users**: users that are managed by the BSC6900 and which information is stored inside the BSC6900. The local users are only enabled to access the BSC6900. Users of BSC6900 with administration operational rights can create and assign operational rights to the local users in order to allow the execution to certain commands. The assignment of the **operational rights** is as follows:
  - The users of TOE are grouped by user groups (or roles).
  - Then an administrator of TOE assigns command groups to these user groups.
  - The command groups contain the commands that can be executed.
  - Also, there is there is a special role which name is Custom. This user group allows the direct assignment of command groups to an user. So, it is possible to have different users of type Custom and with different permissions.

  Each time a local user logs in the TOE, the system gets the list of command groups and commands that the user can execute by following this assignment. Then, with the permissions information of each user, the access control mechanism is applied. (FDP_ACC.1/Local users, FDP_ACF.1/Local users, FIA_ATD.1/Local users, FMT_MSA.1)

- **Domain users**: these are users managed by the M2000 and can access different managed elements. The information about these users is stored in the M2000, so the TOE cannot manage the operational rights from these users. The creation and operational rights assignment of domain users is out of the scope of TOE. Each time a domain user logs in the TOE, this must be verified in the M2000. Then, M2000 answers with the verification result together with the command groups and commands that the domain user can execute. (FDP_ACC.1/Domain users, FIA_ATD.1/Domain users, FDP_ACF.1/Domain users)

- **EMSCOMM user**: this is a built-in user of TOE that is used by the M2000 to operate with the TOE. This user has permission to execute almost all the commands of TOE and cannot be modified neither deleted. This user is only for the communication with M2000 and cannot access the TOE through other interfaces.(FDP_ACC.1/EMSCOMM user, FIA_ATD.1/EMSCOMM user, FDP_ACF.1/EMSCOMM user)

TOE has pre-defined built-in Command Groups, such as “Alarm Management Command Group” or “Performance Query Command Group”. These commands groups are provided by default in the TOE and cannot be modified. Also, there are other command groups that can be modified by administrators in order to change the commands assignment for these command groups. (FMT_SMF.1)

TOE has 4 predefined user groups: Guest, User, Operator and Administrator. These user groups are configured by default and can not be modified. Each user group has different command groups assigned, in order to provide the operational rights to perform different commands.

In addition, there is another user group, “Custom”. This user group is used to apply a direct assignment between the users and the command groups. So, it is possible to assign both default and configured command groups to an user as required, instead of assigning only the default command groups which could be non-appropriate. (FMT_SMR.1, FMT_SMF.1)

7.1.4 Authentication

The TOE offers different kind of authentication depending on the kind of user. Every user must be authenticated before the execution of any command. The different authentication methods are:

- **Local users' authentication**: the authentication for local users is performed in the TOE and based in user and password. The TOE maintains all the security attributes for each local user in order to identify and authenticate the local users in the login. (FIA_ATD.1/Local users)

- **Domain users' authentication**: the authentication of domain users is performed in the M2000 and based in user and password. The security attributes of the domain users are stored in the M2000. The TOE asks the M2000 about the user permission to connect. Then, M2000 checks the domain user permissions about the managed elements he can connect to and communicates the result to the TOE. In affirmative case, the operational rights of the user are communicated to the TOE in order to apply the access control. (FIA_ATD.1/Domain users)

- **EMSCOMM user authentication**: this user is related with the execution of commands from the M2000 and represents a second user who is operating in the M2000 and managing configuration data of the TOE. The authentication of this user is performed each time the M2000 connects with the TOE, and each time a re-connection is necessary (power on, disconnection, network failure…). The connection is based in the SSL protocol. The M2000 public key must be contained in the TOE in order to identify and authenticate the M2000 with the corresponding private key. Also, a special arithmetic common for both parties is applied, in order to justify the knowledge of the algorithm. Once the connection is performed, the M2000 remains authenticated in the TOE until disconnection. Then, no further connections/authentications are needed each time a MML command is executed. Finally, the EMSCOMM is a built-in user of the TOE, so his information is stored within the TOE. (FIA_ATD.1/EMSCOMM user)

(FIA_UAU.5)

The TOE enforces timer-based account lockouts. Administrators can specify after how many consecutive failed authentication attempts an account will be temporarily locked, and whether the counter for failed attempts will be reset automatically after a certain amount of minutes. (FIA_AFL.1)

Authorized administrators are able to configure a system-wide password policy that is then enforced by the TOE. Besides the minimum length of the password, which can be set between 6 and 32 characters, administrators have the option to enforce the use of specific characters (numeric, alphanumeric low or capital, and special characters). (FIA_SOS.1)

The TOE can identify users in the management network by unique ID and enforces their identification before granting them access to the TSF interfaces. Warning of “error username or password” will be prompted when the user fails to provide the correct username or password. Authentication based on user name and password is enforced prior to any other interaction with the TOE for all external interfaces of the TOE, typically via the WebLMT, used by administrator. Also, a minor set of TOE functions are available previous to the user identification and authentication

- Hand shake command: Commands to check the alive status of the TOE.
- Parameter negotiation: Previous commands to the M2000 connection to the TOE (private arithmetic application).
- Link status and Module shake hand: commands belonging to operation through the BIN interface to check the status of the TOE.
- Verification of api security and code: operations performed in the WebAPI, previous to the user authentication through this interface.
- Alarm query: the access to the interface to check the alarms thrown by the TOE.
- Vendor Network Probe Service: this service is considered as independent of the rest of functionality of the TOE, and is accessed independently by the corresponding IT entity.

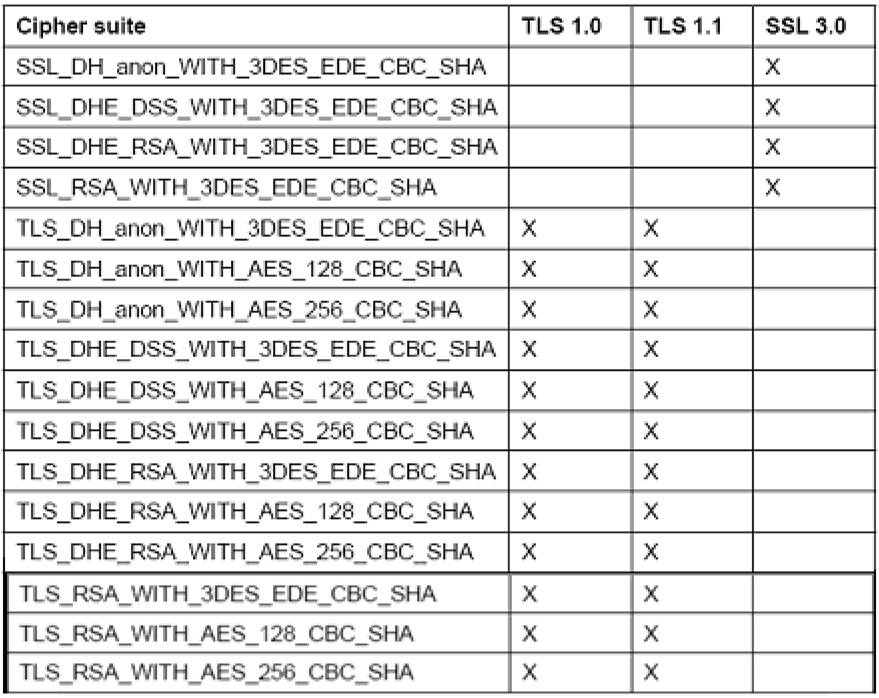
(FIA_UID.1, FIA_UAU.1).

The TOE will deny authentication depending on the timeframe of the connection. If an administrator has specified values for these parameters for a specific user, the TOE will deny authentication if the user tries to authenticate in a timeframe that lies outside of the “login start time” and “login end time” specified for the user. When the user tries to log in with an expired password, the system must request the user to modify the password. The TOE also provide login time control mechanism: each account can be configured with the login time segment, including the valid date range, time segment, and week restriction. Any login is prohibited beyond the configured time segment. (FTA_TSE.1)

7.1.5 Communications security

The TOE provides communications security for network connections to the OMU. This includes connections via the following interfaces:

1. OMU connections (include MML, BIN, FTP connections) between M2000/WebLMT and the TOE (using SSL/TLS)
2. HTTPS connections between WebLMT and the TOE (using SSL/TLS) and FTPS between the operational environment and the TOE (using SSL/TLS)
3. The SSL/TLS cipher suites supported for SSL connections are:



Cipher suite	TLS 1.0	TLS 1.1	SSL 3.0
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA			X
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA			X
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA			X
SSL_RSA_WITH_3DES_EDE_CBC_SHA			X
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DH_anon_WITH_AES_128_CBC_SHA	X	X	
TLS_DH_anon_WITH_AES_256_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	X	X	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	X	X	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	X	X	
TLS_RSA_WITH_3DES_EDE_CBC_SHA	X	X	
TLS_RSA_WITH_AES_128_CBC_SHA	X	X	
TLS_RSA_WITH_AES_256_CBC_SHA	X	X	

The certificates used for the SSL channel establishment between the elements are trusted given that they are issued by the secure PKI of the environment.

(FTP_TRP.1 and FTP_ITC.1)

7.1.6 Management of TSF

The TOE offers management functionality for its security functions, where appropriate. This is partially already addressed in more detail in the previous sections of the TSS, but includes:

1. User management, including User Group memberships, passwords, account lockout, validity periods for an account and/or password, etc.

2. Access control management, including the definition of Command Groups, and the association of users and User Groups with Managed Elements, and Command Groups in Manage Authority and Operate Authority relationships.

3. Enabling/disabling of SSL for the communication between WebLMT/M2000 and the TOE.

4. Configuration of VLAN for the different plane in the TOE environment.

5. Configuration of Role_based Access Control List for the with the TOE.

6. All of these management options are typically available both via the WebLMT GUI and the M2000 GUI.

(FMT_SMF.1)

The creation of new local users in the TOE is implemented in such a way the new user is assigned to the Guest user group as default value. This assignment can be modified during the creation by the administrator to state the appropriate assignments. (FMT_MSA.3)

8 Abbreviations, Terminology and References

8.1 Abbreviations

MSC	Mobile Switch Center
MBSC	Multimode Base Station Controller
BTS	Base transceiver station
SGSN	Serving GPRS Support Node
OSS	Operating Support System
CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
PP	Protection Profile
SFR	Security Functional Requirement
LMT	Local Maintenance Terminal
RMT	Remote Maintenance Terminal
AIU	Advanced Interface Unit
CLI	Command Line Interface
GUI	Graphical User Interface
SSL	Secure Sockets Layer
PIU	Packet Interface Unit
OMU	Operation & Maintenance Unit
RRM	Radio Resource Management

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrator: An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE's point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

Operator See User.

User: A user is a human or a product/application using the TOE.

8.3 References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. July 2009. Version 3.1 Revision 3.

[CEM] Common Methodology for Information Technology Security Evaluation. July 2009. Version 3.1 Revision 3.