Huawei WCDMA NodeB Software Security Target

Version: 1.19

Last Update: 2011-11-11

Author: Huawei Technologies Co., Ltd.

Table of Contents

List of tables

Changes control

Version	Date	**Author**	Changes to previous version
V 1.13	2011-04-28	**ZhangLing**	---
V 1.14	2011-05-24	**ZhangLing**	Modifications to include M2000 access into the access control policy.
V 1.18	2011-09-01	**ZhangLing**	Modifications of the CC test problem.
V 1.19	2011-11-11	**ZhangLing**	Modifications of the CC test problem.

1. Introduction

1 This Security Target is for the CC evaluation of Huawei WCDMA (Wideband Code Division Multiple Access) NodeB Software, the TOE Version is V200R013C01SPC010 and is based on HERT BBU (Huawei Enhanced Radio Technology-Base Band Unit) version HERTBBU V200R007C01SPC040B811.

1.1. ST Reference

Title	Huawei WCDMA NodeB Software Security Target
Version	1.19
Author	Zhang Ling
Publication Date	2011-11-11

1.2. TOE Reference

TOE Name	Huawei WCDMA NodeB Software
TOE Version	V200R013C01SPC010
TOE Developer	Huawei
TOE Release Date	2011-08-12

2 In addition to the TOE Name indicated at the table above, the following reference is used, for the sake of simplicity, along the whole product documentation:

- ✓ NodeB

1.3. TOE Overview

3 Huawei WCDMA NodeB (the equipment) use the advanced wideband, multi-mode system, and modular design, and have features such as the compact size, high integration, low power consumption, and easy and quick deployment. The innovative design and flexible combinations of the function modules and auxiliary devices encourage Huawei to diversify multi-mode NodeB products.

4 The 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 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

5 Huawei WCDMA NodeB (the equipment) has a cutting-edge modular design, thus compatible with functional modules of different network systems. With simply three types of units, the 3900 series NodeBs

feature small size, high integration, low power consumption, easy and fast deployment.

6 The innovative design and flexible combinations of the functional modules and auxiliary devices lead to the diversity of NodeB. The operators can install boards of different network systems in one cabinet to form a NodeB that applies to different scenarios. This accelerates the introduction of new radio network technologies and complies with the development trend of the mobile network towards integration of different network systems.

7 The 3900 series NodeBs are based on IP switch and multi-carrier technologies and support the bandwidth of over 100 Mbit/s. This ensures a high data transmission rate for users during mobile data service expansion. The Huawei WCDMA NodeB (the equipment) networking supports various access modes, including the FE, GE, optical fiber, microwave access, and satellite.

8 The major security features implemented by NodeB and subject to evaluation are:

A. Authentication

9 Operators using local and remote access to the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.

B. Access control

10 Huawei WCDMA NodeB Software implements role-based access control for LMT and M2000. NodeB supports various kinds of users: Local users through LMT (“admin”, “guest”), Domain users through LMT and “EMSCOMM” user through M2000. Depending on the kind of user and its certain privileges, a concrete user will be able to perform its applicable set of actions into the TOE.

C. Auditing

11 Audit records are created for security-relevant events related to the use of NodeB.

D. Communications security

12 NodeB offers SSL/TLS channels for FTP, MML (man-machine language, which is a kind of Command Line Interface), and BIN (Huawei’s private binary message protocol) access to the TOE.

13 VLAN (Virtual Local Area Network) are implemented to separate the traffic from different flow planes, which reduce traffic storms and avoid resource overhead.

14 ACL (Access Control List) implements Packet filtering features to restrict resource use via IP address, ports, etc. Those features protect NodeB against various unauthorized access from unauthorized NEs.

15 The communication between the Network Elements and NodeB uses SSL, and certificates for this purpose are deployed.

E. Security function management

16 The TOE offers management functionality for its security functionality.

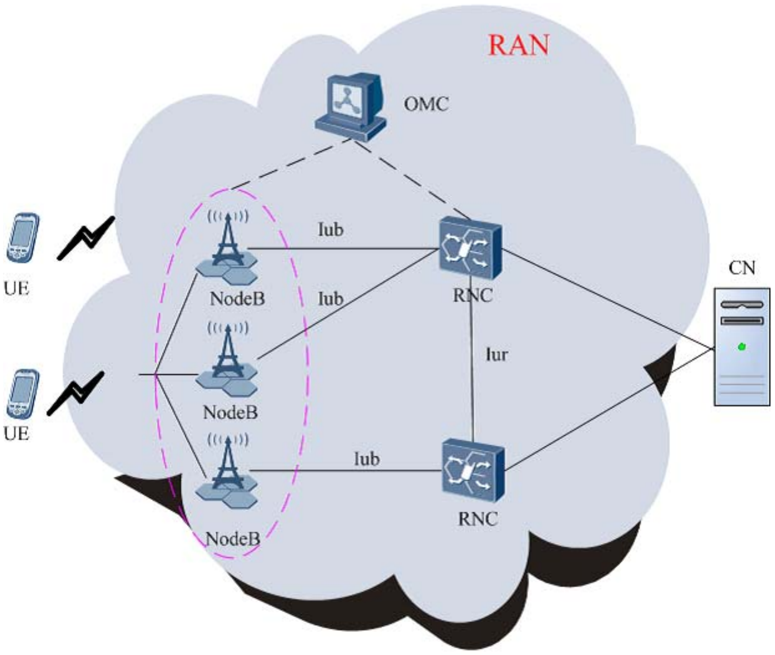
F. Digital signature

17 In the production and distribution phases, the digital signature scheme, protect the software package by message digest and signature. The TOE verifies the software digital signature’s validity.

1.3.2. TOE type

18 The TOE comprises management and control software that is deployed into a NodeB. That software includes identification and authentication, system access control, audit management, enforcement of network transmission against data peeking, management functionality to manage the security functions of NodeB, and digital signature validation to guarantee the confidentiality and integrity of the software packages that are deployed.

19 The following figure shows the position of the NodeB in the network.



NodeB network

1.3.3. Non TOE Hardware and Software

20 The physical structure of Huawei WCDMA NodeB Software can be:

- DBS3900: Distributed base station. The DBS3900 typifies the compact design, easy installation, and low power consumption. In addition, it can reside in the spare space of an existing 2G site. The RRU also has a compact design and light weight. It can be installed close to the antenna to decrease feeder loss and improve system coverage. All the previously mentioned features of the distributed NodeB facilitate the site selection, network planning and optimization. This enables the operators to efficiently deploy a high-performance 3G network with a low TCO because less manpower, electric power, and space are required during network construction.

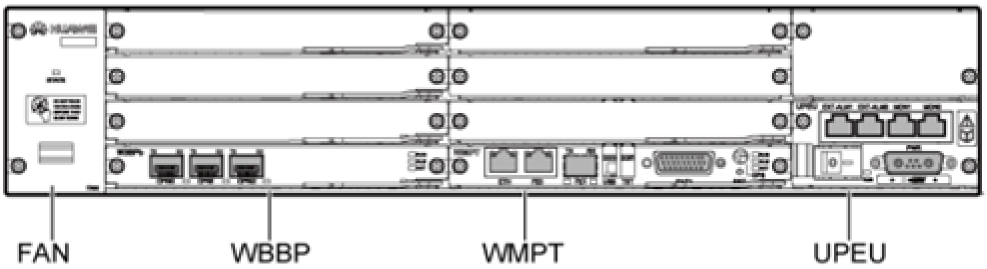
- BTS3900: Indoor cabinet macro base station. The BTS3900, as one of the most compact indoor macro NodeBs in the telecommunication industry, boasts large and expandable capacity. It is light, and supportive of the GSM-WCDMA dual-mode application.

- BTS3900A: Outdoor cabinet macro base station. The BTS3900A, one of the most compact outdoor cabinet macro NodeBs in the telecom industry, boasts light weight and easy transportation due to its stackable design.

- BTS3900L: Large indoor cabinet macro base station. This type of NodeB is just like BTS3900.But it can provide more cabinet space, In order to facilitate the evolution to a multi-mode base station.

21 The TOE can be deployed in all these physical configurations with no changes in the functionality, or in the installation procedures to be followed.

22 The TOE runs into the BBU3900 subrack and in the RFU. The structure of BBU3900 is shown in the following figure:



BBU3900 subrack

23 The BBU3900 contains, at least, the following mandatory boards:

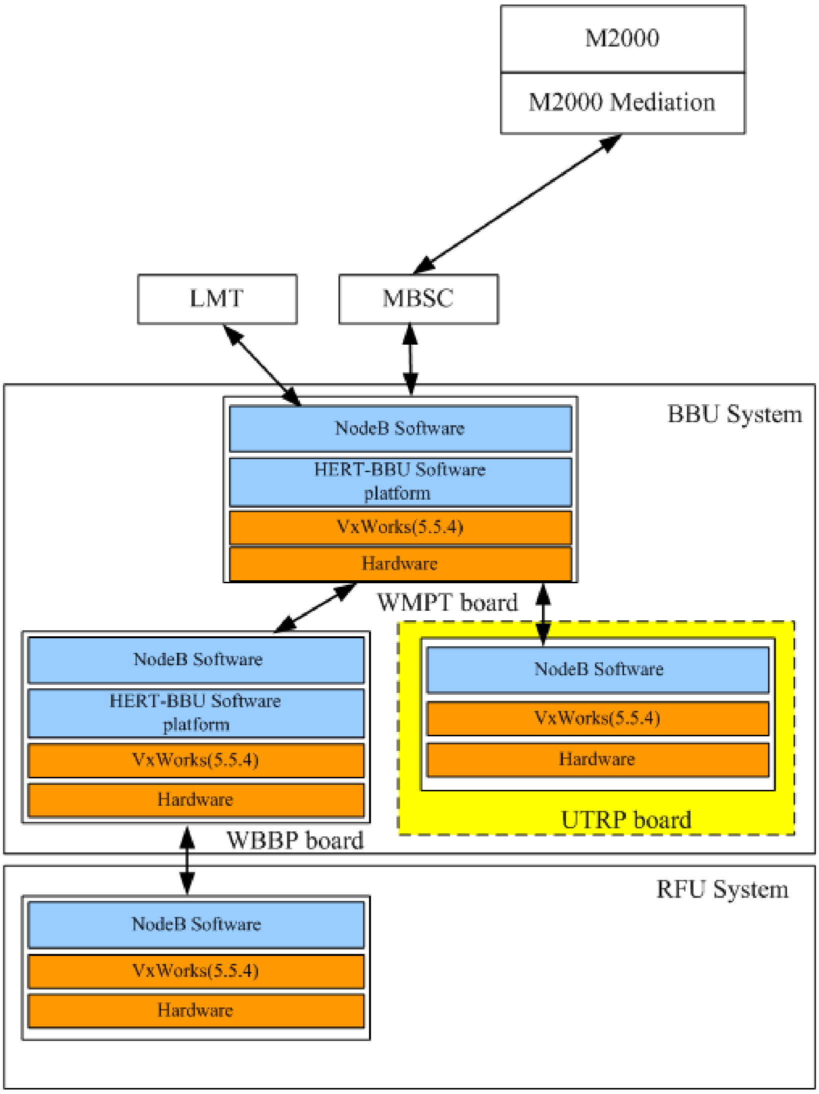
- The WCDMA Baseband Process Unit (WBBP), whose purpose is to provide an interface between BBU3900 and Radio Remote Unit (RRU) or Radio Frequency Unit (RFU)
- The WCDMA Main Processes and Transmission unit (WMPT), which is the main board of BBU3900.
- The Universal Power and Environment Interface Unit (UPEU), whose purpose is providing power to the whole BBU3900 subrack.
- The FAN unit of the BBU3900 controls the fan speed, monitors the temperature of the FAN unit, and dissipates the heat from the BBU.

24 In addition to these boards, another one can be added to incorporate some certain capabilities to the whole equipment, whose name is Universal Transmission Processing unit (UTRP). In this board, some TOE functionality can be deployed once connected to the equipment.

25 Given this circumstance, two different configurations belong to the scope of the evaluation:

- A configuration where BBU3900 does not have an UTRP board connected, and where the entire TOE functionality is deployed in the WMPT, WBBP and RFU.
- A configuration where BBU3900 has an UTRP board connected, and where the TOE is deployed in WMPT, UTRP, WBBP and RFU.

26 The TOE is Huawei WCDMA NodeB Software packages. It is deployed on the boards of base band unit (BBU) and Radio Frequency unit (RFU). These hardware boards are TOE environment. The OS and part of BS software which is provided by Huawei’s particular products is also TOE environment.



Non TOE hardware and software environment

27 In the above diagram, the light blue box area belongs to the TOE while the orange box area belongs to the TOE environment.

28 The yellow box where the UTRP board is contained indicates that it is an optional board, which is not always included.

29 The components of the TOE environment are the following:

- Physical networks, such as Ethernet subnets, interconnecting various networking devices.
- NodeB Operating System: Vxworks, version 5.5.4.
- An M2000 server providing access to the management functions of the TOE via SSL. M2000 version can be V200R011C01SPC130 (which is the evaluated one).

- MBSC (Multi Base Station Controller) and NodeB together complete WCDMA wireless communication access. The MBSC version is V900R013C01SPC010.

- LMT to connect to the TOE for accessing the command line interface through WMPT's ETH and FE interface via a secure channel enforcing SSL. LMT is in turn defined by the version of NodeB.

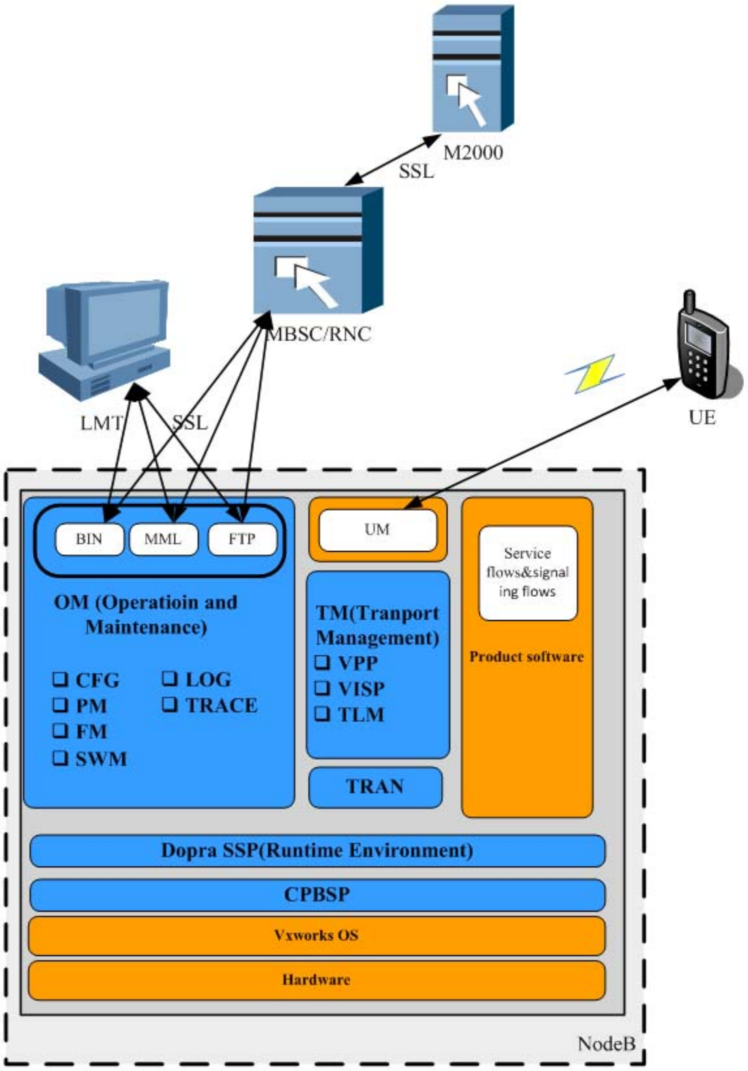
- M2000 Mediation: The M2000 server software consists of the main version software and mediation software. The main version software implements system functions, and the mediation software is used for the adaptation of different NE interfaces. The M2000 can manage new NEs after the corresponding mediation software is installed.

- The physical structure of NodeB includes BBU3900 and RFU. BBU3900 is based on HERT hardware platform. HERT BBU is a common platform for wireless multiple products, different boards can be configured according to each product. Beside the hardware support platform subsystem, in most cases only need to configure the WCDMA Main Process and Transfer board (WMPT), WCDMA base-band process unit (WBBP). HERT BBU Version is V200R007C01SPC040B811.

1.4. TOE Description

1.4.1. Logical Scope

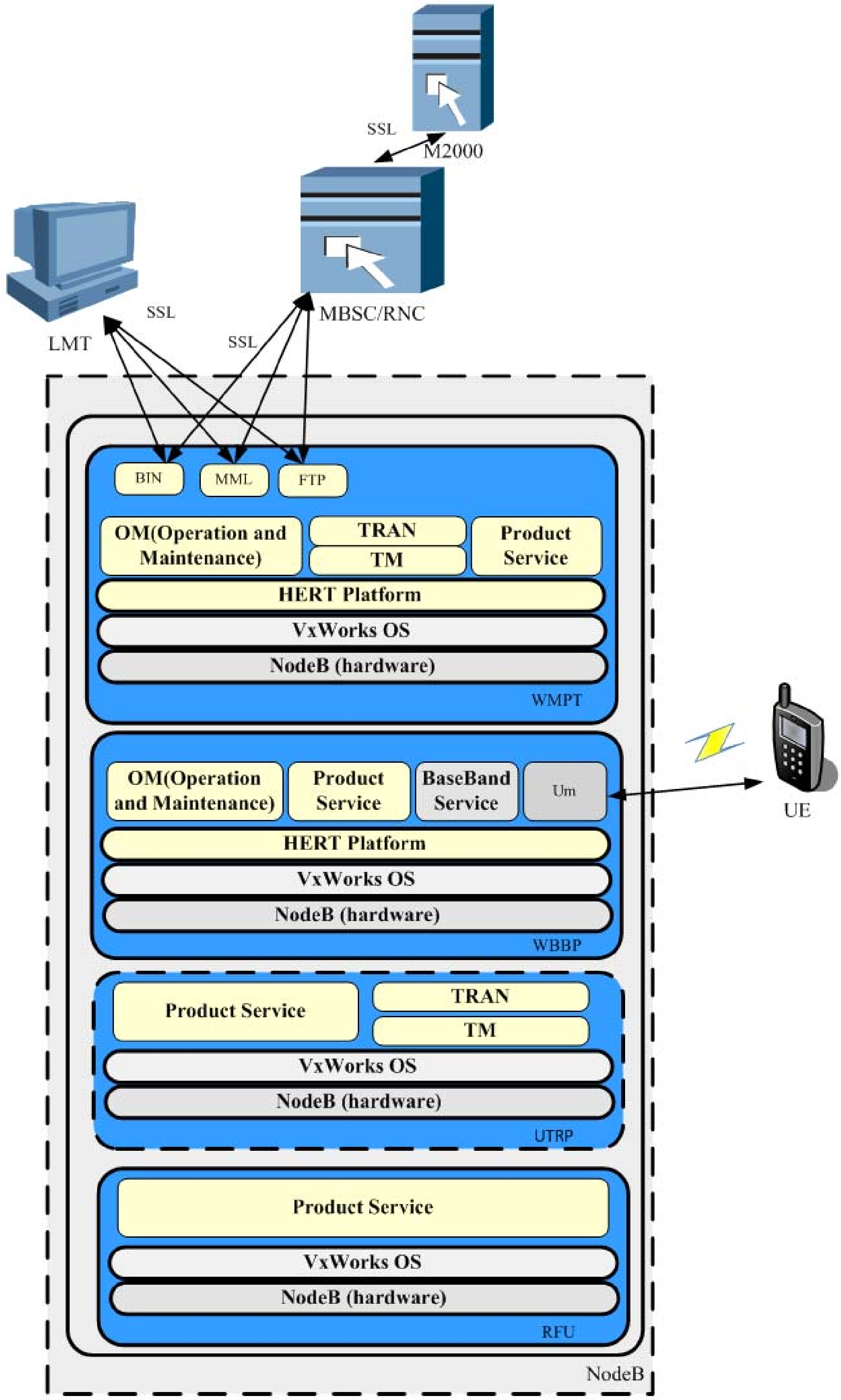
30 This section will define the logical scope of Huawei WCDMA NodeB Software V200R013C01SPC010. The software architecture of the TOE is indicated in the following figure:



Software architecture

31 An explanation of each identified part is described below.

32 From the Logical point of view, the following figure includes the TOE Logical Scope, where all the connections to the TOE are indicated, and also the way the TOE is deployed in the different boards of the product.



TOE Logical Scope

33 The TOE is pure software. OS and other software provided by particular products is TOE environment. In the above diagram, the blue areas are parts of the TOE. NodeB includes Operation and Maintenance (OM), Baseband Service, and HERT platform.

34 Both figures include an UE access trough UM which is not under the scope of the evaluation, but is included for better understanding.

35 The TOE security functionality, as stated in the section **1.3 TOE Overview** is:

- Authentication.
- Access control.
- Auditing.
- Communications security.
- Security functionality management.
- Digital signature.

36 As shown in the figure *Software Architecture*, the TOE is entirely composed by software. The Operating System, and other software provided by particular products belong to the TOE environment. The TOE itself includes OM, TM, TRAN, CPBSP and Dopra SSP.

37 For each of the identified parts of the TOE, a correspondence between them and the TOE security functionality can be achieved. That way, for each part, the appropriate security associated functionality is indicated in the following table:

Element	Part	Associated security functionality
Operation and Maintenance (OM)	Communications through the protocols: BIN: Huawei's private binary message protocol. MML: Man-Machine Language. FTP	Communications security
	CFG: Configuration Management, responsible for the managed elements configuration.	Security functionality management
	PM: Performance management, responsible for the calculation of performance data and the storage of it.	NA
	FM: Fault management, which include fault and alarm monitoring.	NA
	SWM: Software management, responsible for software upgrade and rollback.	Digital signature

	LOG: Responsible for the audit and storage of security log and operational log.	Auditing
	TRACE: Responsible for the trace messages which show the state of the BS (Base Station).	NA
Transport Management (TM)	VPP: Voice Protocol Platform, which is composed of voice and signal processing component, such as XML Parser, Stream Control Transmission Protocol (SCTP) and Signalling ATM Adaptation Layer (SAAL).	NA
	VISP: Versatile IP and Security Platform, which provides TCP / IP protocol stack management interface.	Communication Security
	TLM: Transport layer management. The functions include control and supervision of the transport bearer (data forwarding) functions, maintaining the transport resource assignment to product services.	Security functionality management
TRAN	Huawei's wireless transmission platform, which provide hardware driver management interface.	Communication Security
Dopra SSP (Runtime Environment)	Provide Operating System mid-ware layer. It function includes: Operation System Adapter, Memory management, Timer management, etc.	NA
CPBSP	Provide a standard API interface for the hardware.	NA

38 All the identified elements and parts run in the WMPT board. When an UTRP board is also connected to NodeB, the software associated to TRAN and TM run in both, WMPT and UTRP boards. Dopra SSP and CPBSP are also deployed in the WBBP board and also in RFU.

39 System control and security management are performed on WMPT board via a secure channel enforcing SSL. The management of the functionality of the TOE can be done through different interfaces, which belong to the TOE environment:

- An M2000 server providing management functions to the TOE.
- LMT to connect to the TOE for access through WMPT or UTRP’s ETH or FE interface via a secure channel enforcing SSL.

- Remote communications between LMT (Local Maintenance Terminal which can run on PCs for remote management of the device.) and the WMPT of NodeB are based on TCP/IP.

1.4.2. Physical Scope

40 The release packages for NodeB are composed of software and documents. The NodeB software packages are in the form of binary compressed files.

41 The NodeB software packages can be downloaded and stored in the WMPT board, and then, they will be checked up, unpacked, and then distributed to each board module, such as WMPT, WBBP and UTRP.

42 The list of the files and documents required for the products is the following:

Software and Documents	**Description**	**Remark**
Software.csp	Board software package (In the form of binary compressed files)	The software packages which are the TOE will be digitally signed to ensure their legitimacy and integrity.
vercfg.xml	Version description file	
Software.sgn	Board software package signature file	These signature files are generated by Huawei digital signature tool
vercfg.sgn	Version description signature file	
NodeB documents	Release notes, MML command reference, and alarm reference.	The guidance documents of NodeB are part of the TOE.

Table 1 *Physical Scope*

2. CC conformance claim

43 This ST is CC Part 2 conformant [CC] and CC Part 3 conformant [CC]. The CC version of [CC] is 3.1R3.

44 This ST is EAL3 conformant as defined in [CC] Part 3, with the assurance level of EAL3 Augmented with ALC_CMC.4, ALC_CMS.4.

45 The methodology to be used for evaluation is CEM3.1 R3

46 No conformance to a Protection Profile is claimed.

3. Security Problem Definition

3.1. TOE Assets

47 The following table includes the assets that have been considered for the TOE:

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
A4.Service	Recoverability in terms of the capacity of recovery in case of denial of service.	Recoverability

Table 2 *TOE assets*

3.2. Threats

48 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 in the management network who has been granted authority to access certain information and perform certain actions.

Table 3 *Threats agents*

49 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 BS file 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 BS software/patches while transferring, violating its confidentiality or integrity.
Asset	A1.Software and patches;
Agent	Eavesdropper

3.2.2. Threats by Interactive Network Attacker

Threat: T3.UnwantedNetworkTraffic	
Attack	Unwanted network traffic sent to the TOE will cause the TOE's processing capacity for incoming network traffic to be consumed thus failing to process legitimate traffic. This may further causes the TOE fails to respond to system control and security management operations. The TOE will be able to recover from this kind of situations.
Asset	A4.Service
Agent	Internal Attacker

Threat: T4.UnauthenticatedAccess	
Attack	An attacker in the management network gains access to the TOE disclosing or modifying the configuration date 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: T5.UnauthorizedAccess	
Attack	A 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. Organizational Policies

3.3.1. P1.Audit

50 The TOE shall provide audit functionality:

- Generation of audit information.
- Storage of audit log.
- Review of audit records.

3.4. Assumptions

3.4.1. Physical

A.PhysicalProtection

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

3.4.2. Personnel

A.TrustworthyUsers

52 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).

3.4.3. Connectivity

A.NetworkSegregation

53 It is assumed that the network interfaces that allow access to the TOE's user interfaces are in a management network that is separate from the management flows, service flows and signaling flows the application (or, public) networks that the network device hosting the TOE serves.

3.4.4. Support

A.Support

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

3.4.5. SecurePKI

A.SecurePKI

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

4. Security Objectives

4.1. Security Objectives for the TOE

56 The following objectives must be met by the TOE:

O.Authentication

57 The TOE must authenticate users and control the session establishment.

O.Authorization

58 The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual users.

O.SecureCommunication

59 The TOE shall provide a secure remote communication channel for remote administration of the TOE via SSL.

O. SoftwareIntegrity

60 The TOE must provide functionality to verify the integrity of the received software patches.

O.Resources

61 The TOE must implement VLAN separation and IP based ACLs to avoid resource overhead.

O.Audit

62 The TOE shall provide audit functionality:

- Generation of audit information.
- Storage of audit log.
- Review of audit records.

4.2. Security Objectives for the Operational Environment

OE. PhysicalProtection

63 The TOE (i.e., the complete system including attached interfaces) shall be protected against unauthorized physical access.

OE.NetworkSegregation

64 The TOE environment shall assure that the network interfaces that allow access to the TOE’s user interfaces are in a management network that is separated from the networks that the TOE serves over the management flows, signaling flows and service flows.

OE. TrustworthyUsers

65 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.Support

66 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.SecurePKI

67 There exists a 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

68 The following tables provide a mapping of security objectives to the environment defined by the threats, policies and assumptions, illustrating that each security objective covers at least one threat and that each threat is countered by at least one objective, assumption or policy.

	T1.InTransitConfiguration	T2.InTransitSoftware	T3.UnwantedNetworkTraffic	T4.UnauthenticatedAccess	T5.UnauthorizedAccess	A.PhysicalProtection	A.TrustworthyUsers	A.NetworkSegregation	A.Support	A.SecurePKI	P1.Audit
O.Authentication				X	X						
O.Authorization					X						
O.SecureCommunication	X	X			X						
O.SoftwareIntegrity		X									
O.Resources			X								

O.Audit											X
OE.PhysicalProtection				X	X	X					
OE.TrustworthyUsers					X		X				
OE.NetworkSegregation								X			
OE.Support									X		
OE.SecurePKI	X	X			X					X	

Table 4 *Mapping of security objectives*

4.3.2. Sufficiency

69 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). The SSL communication between the entities and the TOE make use of certificates that belongs to a secure PKI. (OE.SecurePKI).
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. The SSL communication between the entities and the TOE make use of certificates that belongs to a secure PKI. (OE.SecurePKI).This threat is also countered by O.SoftwareIntegrity: when a software package is loaded, its message digest and signature are verified.
T3.UnwantedNetworkTraffic	The threat T3.UnwantedNetworkTraffic is directly counteracted by the security objective for the TOE O.Resources.
T4.UnauthenticatedAccess	The threat T4.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.PhysicalAccess contributes to the mitigation of the threat assuring that the software and configuration files stored in the TOE, will not be modified.
T5.UnauthorizedAccess	The threat T5.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 SSL communication between the entities and the TOE make use of certificates that belongs to a secure PKI. (OE.SecurePKI). 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.PhysicalAccess contributes to the mitigation of the threat assuring that the software and configuration files stored in the TOE, will not be modified

Table 5 *Sufficiency analysis for threats*

Assumption	Rationale for security objectives
A.PhysicalProtection	This assumption is directly implemented by the security objective for the environment OE.PhysicalProtection.
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.SecurePKI	This assumption is directly implemented by the security objective for the environment. OE. SecurePKI

Table 6 *Sufficiency analysis for assumptions*

Policy	Rationale for security objectives
P1.Audit	This policy is directly implemented by the security objective for the TOE O.Audit

Table 7 *Sufficiency analysis for organizational security policy*

5. Security Requirements for the TOE

5.1. Security Requirements

5.1.1. Security Audit (FAU)

5.1.1.1. 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 (SEC)

2. operation requests (OPE)

ii. user management

*1. password change (OPE)***]**

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).*****]**

Application note: There are two kinds of log files, security log file and operation log file.

5.1.1.2. 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.

5.1.1.3. FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [assignment: ***all users*****] 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.

5.1.1.4. 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:** ***date and time range, user name, terminal type, and/or result.*****].**

5.1.1.5. FAU_STG.1 Protected audit trail storage

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

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

5.1.1.6. 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:** ***the pre-defined limited size of 1Mbyte*****].**

Application note: There are two audit files, when the new file is full, the old one is deleted.

5.1.2. Cryptographic Support (FCS)

5.1.2.1. FCS_COP.1/Sign 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*****]**

Application note: This requirement addresses the digital signature verification of the new remote loaded software packages.

5.1.2.2. FCS_COP.1/SSL Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: ***channels encryption and decryption*****] in accordance with a specified cryptographic algorithm [assignment:** ***all SSL supported encryption algorithms*****] and cryptographic key sizes [assignment:** ***all SSL supported key sizes*****] that meet the following: [assignment:** ***none*****]**

Application note: This requirement addresses the communication encryption using SSL between the TOE and M2000, the TOE and FTPServer, and the TOE and LMT.

5.1.2.3. FCS_CKM.1/SSL Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: ***cryptographic key generation methods supported by SSL/TLS*****] and specified cryptographic key sizes [assignment:** ***all key sizes supported by SSL/TLS*****] that meet the following: [assignment:** ***none*****].**

5.1.3. User Data Protection (FDP)

5.1.3.1. FDP_ACC.1/Local Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: ***Local access control policy*****] on [assignment:** ***local users as subjects, commands as objects, and execution of commands by local users*****].**

Application Note: The only applicable users for this access control policy are the "admin" and "guest" users, which can access to the TOE via LMT.

5.1.3.2. FDP_ACF.1/Local Security attribute based access control

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

[assignment:

a) users and their following security attributes: user ID and Role

b) operations and their following security attributes: 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: ***if the user is "admin", and the command belongs to the "admin" accessible commands, the access is granted. If the user is "guest", and the command belongs to the "guest" accessible commands, the access is granted.*****].**

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*****]**

Application Note: NodeB has two Local users for the access through LMT: "admin" and "guest".

5.1.3.3. FDP_ACC.1/Domain Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *Domain access control policy*] on [assignment: *domain users as subjects, commands as objects, and execution of commands by domain users*].

5.1.3.4. FDP_ACF.1/Domain Security attribute based access control

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

[assignment:

a) *users and their following security attributes:*

   i. *user name*

b) *commands and their following security attributes:*

   ii. *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: *if the user is assigned to the requested commands, then access is granted.*]

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*]

Application note: This requirement implements the domain users' access control policy. The users will login to the TOE through the LMT but the authentication is performed by an external entity which will send the operational rights to the TOE so it can exercise the access control policy.

5.1.3.5. FDP_ACC.1/EMSCOMM Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *EMSCOMM access control policy*] on [assignment: "*EMSCOMM" user as subject, commands as objects, and execution of commands by the "EMSCOMM" user*].

5.1.3.6. FDP_ACF.1/EMSCOMM Security attribute based access control

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

[assignment:

a) *"EMSCOMM" user and its following security attributes:*

   i. *user name*

b) *commands and their following security attributes:*

   ii. *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: ***If the command is accessible through M2000, the "EMSCOMM" user will always have execution permission of the targeted command.*****]**

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*****]**

Application note: This requirement implements the M2000 access control policy.

5.1.4. Identification and Authentication (FIA)

5.1.4.1. 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 LMT since the last successful authentication of the user and before the counter for these attempts is reset after a configurable time frame 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 a 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 not considered in this requirement neither by the TOE authentication functionality.

5.1.4.2. FIA_ATD.1 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) *Number of unsuccessful authentication attempts since last successful authentication attempt*
d) *Lock status*]

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 neither by the TOE authentication functionality.

5.1.4.3. FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 the TSF shall allow [assignment:

a) Handshake command;

b) Parameter negotiation;

c) Link status handshake;

] 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.

5.1.4.4. FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [assignment: *The following authentication mechanisms:*

a) Authentication for Local Users

b) Authentication for Domain Users

c) Authentication for “EMSCOMM” user

] to support user authentication.

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

a) Local Users are authenticated in the TOE by user and password stored in the TOE.

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

c) “EMSCOMM” user is authenticated in the TOE by a special arithmetic procedure common to both parties, the TOE and the M2000.

].

5.1.4.5. FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment:

a) Handshake command;

b) Parameter negotiation;

c) Link status handshake;

] 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.

5.1.4.6. FIA_SOS.1 Verification of secrets

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

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

b) a 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.

c) that they are different from a configurable number between 1 to 10 previous used passwords **]**

Application Note: The unique secret contemplated is the password of the “admin” and “guest” users that access to the TOE through LMT.

5.1.5. Security Management (FMT)

5.1.5.1. FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: *Local access control policy*\] **to restrict the ability to [selection:** *query and modify*\] **the security attributes [assignment:** *none*\] **to [assignment:** *none*\]**.**

5.1.5.2. FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [assignment: *Local access control policy*\] **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: *none*\] **to specify alternative initial values to override the default values when an object or information is created.**

5.1.5.3. FMT_SMF.1 Specification of Management Functions

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

a) Configuration of password policy

b) Modify the “admin” and “guest” passwords

c) Unlock the “admin” and “guest” accounts

d) Configuration of SSL (Certificates and authentication mode)

e) Configuration of ACL

f) *Configuration of VLAN*

g) *Enable/Disable software digital signature*

h) *FIA_AFL.1.1 configurable values*]

Application Note: The “admin” and “guest” user accounts can be only unlocked using the “EMSCOMM” user, Domain users, or the “admin” user account.

5.1.5.4. FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [assignment: ***ADMIN_ROLE, GUEST_ROLE, EMSCOMM_ROLE*****]**

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

Application note: The TSF maintain three users: “admin”, ”guest” and “EMSCOMM”. Each of them is traced to a security role. This way, “admin” is traced to the role ADMIN_ROLE, “guest” is traced to GUEST_ROLE, and “EMSCOMM” is traced to EMSCOMM_ROLE. The domain users permissions are not maintained in the TOE, no role is assigned to a domain user.

5.1.6. TOE access (FTA)

5.1.6.1. FTA_TSE.1/SEP TOE session establishment

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

a) *Protocol type (IP, ICMP, TCP, UDP or SCTP)*

b) *Source IP address and mask*

c) *Source port range*

d) *Destination IP address and mask*

e) *Destination port range*

f) *DSCP value*

g) *VLAN id*]

Application note: This requirement addresses the VLAN separation and IP based ACLs to avoid resource overhead, through the FE physical interface.

5.1.6.2. FTA_TSE.1/Local TOE session establishment

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

a) *Lock status.*]

Application Note: That requirement applies only to the access to the TOE through LMT using the “admin” or “guest” user.

5.1.7. Trusted Path/Channels (FTP)

5.1.7.1. 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: *accessing the FMT_SMF.1 related functionality*].

Application note: This requirement is exercised when accessing the TOE through M2000.

5.2. Security Functional Requirements Rationale

5.2.1. Coverage

70 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.Resources	O.SoftwareIntegrity
FAU_GEN.1	×					
FAU_GEN.2	×					
FAU_SAR.1	×					
FAU_SAR.3	×					
FAU_STG.1	×					
FAU_STG.3	×					
FCS_COP.1/Sign						×
FCS_COP.1/SSL				×		
FCS_CKM.1/SSL				×		
FDP_ACC.1/Local			×			
FDP_ACF.1/Local			×			
FDP_ACC.1/Domain			×			
FDP_ACF.1/Domain			×			
FDP_ACC.1/EMSCOMM			×			

FDP_ACF.1/EMSCOMM			×			
FIA_AFL.1		×				
FIA_ATD.1		×				
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/Local		×				
FTA_TSE.1/SEP					×	
FTP_ITC.1				×		

Table 8 *Mapping SFRs to objectives*

5.2.2. Sufficiency

71 The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable.

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 authentication mechanism (FIA_UID.1). Functionality 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 prevent audit data loss is provided by FAU_STG.3
O.Authentication	User authentication is implemented by FIA_UAU.1 and FIA_UAU.5, and supported by individual user identification in FIA_UID.1. The necessary user attributes are spelled out in FIA_ATD.1. The authentication mechanism supports authentication failure handling (FIA_AFL.1), and a password policy (FIA_SOS.1), restrictions as to the validity of accounts for logon (FTA_TSE.1/Local). Management functionality is provided in FMT_SMF.1.
O.Authorization	User authentication is implemented by FIA_UAU.1 and FIA_UAU.5 and supported by individual user identification in FIA_UID.1. The requirements for the local users' access control policy are modelled in FDP_ACC.1/Local, FDP_ACF.1/Local, FMT_MSA.1 and FMT_MSA.3. This access control is based on the definition of roles (FMT_SMR.1). Management functionality for this access control policy is provided in FMT_SMF.1.

	The domain users' access control policy is modelled in FDP_ACC.1/Domain and FDP_ACF.1/Domain. The EMSCOMM access control policy is modelled in FDP_ACC.1/EMSCOMM and FDP_ACF.1/ EMSCOMM.
O.SecureCommunication	Communications security is implemented using encryption for the communication with LMT users, with the M2000 through the integration port interface and in the communication with the FTP servers. The keys used for the channels are generated as part of the SSL connection establishment process. (FCS_COP.1/SSL, FCS_CKM.1/SSL) In addition, the communication between the TOE and M2000 is performed through a trusted channel which maintains confidentiality, integrity and assured identification of its ends points. (FTP_ITC.1) Management functionality to enable these mechanisms is provided in FMT_SMF.1.
O.Resource	FTA_TSE.1/SEP implements the separation of traffic based on VLANs and the IP based ACL to avoid resource overhead. Management functionality to configure the ACL and the VLANs is provided in FMT_SMF.1.
O.SoftwareIntegrity	The software integrity objective is directly implemented with FCS_COP.1/Sign so the TOE performs digital signature verification over the software patches.

Table 9 *SFR sufficiency analysis*

5.2.3. Security Requirements Dependency Rationale

72 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.

73 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 resolved. The audit time is depended on the reliable time stamp. Reliable time stamp is depended on external time sources.
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.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/Sign	[FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1]	Not resolved. The digital certificate used for signature verification is loaded as part of the manufacture process.
	FCS_CKM.4	Not resolved. The digital certificate used for signature verification is loaded as part of the manufacture process and are never destructed.
FDP_ACC.1/Local	FDP_ACF.1	FDP_ACF.1/Domain
FDP_ACF.1/Local	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 /Domain FMT_MSA.3
FDP_ACC.1/Domain	FDP_ACF.1	FDP_ACF.1/Domain
FDP_ACF.1/Domain	FDP_ACC.1	FDP_ACC.1/Domain
	FMT_MSA.3	Not resolved. The dependency with FMT_MSA.3 is not resolved because the attributes of the access control policy are not under the control of the TOE.
FDP_ACC.1/EMSCOMM	FDP_ACF.1	FDP_ACF.1/ EMSCOMM
FDP_ACF.1/EMSCOMM	FDP_ACC.1	FDP_ACC.1/ EMSCOMM
	FMT_MSA.3	Not resolved. The dependency with FMT_MSA.3 is not resolved because the attributes of the access control policy are not under the control of the TOE.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	
FIA_SOS.1	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	none	
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTA_TSE.1/SEP	None	
FTA_TSE.1/Local	None	
FCS_COP.1/SSL	[FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1]	FCS_CKM.1/SSL
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not need to be securely removed.

FCS_CKM.1/SSL	[FCS_CKM.2 | FCS_COP.1]	FCS_COP.1/SSL
	FCS_CKM.4	Not resolved. The generated keys are not externally accessible so they do not need to be securely removed.
FTP_ITC.1	None	

Table 10 *Dependencies between TOE Security Functional Requirements*

5.3. Security Assurance Requirements

74 The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components as specified in [CC] Part 3, augmented with ALC_CMC.4 and ALC_CMS.4. 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

Table 11 Security Assurance Requirements

5.4. Security Assurance Requirements Rationale

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

6. TOE Summary Specification

6.1. TOE Security Functionality

6.1.1. Authentication

76 The TOE offers the enforcement of timer-based account lockouts: users 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). The TOE will deny access to local users based on their lock status. (FTA_TSE.1/Local)

77 The TOE authenticates the local users based on individual user IDs and passwords. User IDs are unique within the TOE and stored together with associated passwords and other security attributes in the TOE's configuration database. Those attributes can be configured by users with the appropriate rights. (FIA_ATD.1, FMT_SMF.1)

78 The TOE can identify users in the management network by a unique ID and enforces their authentication before granting them access to the TSF management interfaces. Warning of "error username or password" will be prompted when the user fails to provide a correct username or password. Some not security related actions can be performed before identification and authentication. (FIA_UID.1, FIA_UAU.1)

79 Several authentication mechanisms are provided for the different available users below. This functionality implements (FIA_UAU.5).

a) Local users

b) Domain users

c) EMSCOMM

6.1.2. Access control

80 The TOE implements an identification and authentication mechanism before the access control. Three different access control policies are contemplated for the TOE:

a) Local access control policy.

b) Domain access control policy.

c) EMSCOMM access control policy.

81 The Local access control policy is exercised when accessing to the TOE by using the "admin" or "guest" user through LMT. Depending on the rights of the certain user, a different set of commands will be available for him. (FDP_ACC.1/Local, FDP_ACF.1/Local, FMT_MSA.1, FMT_MSA.3).

82 The domain access control policy allows users managed by the M2000 to execute commands in the TOE. The management of the security attributes of this access control policy is out of the scope of the TOE. Each time a domain user logs in the TOE (through the integration port or through the LMT), the TOE send the used user and password to the M2000 which performs user authentication and return to the user the commands that the user can execute. (FDP_ACC.1/Domain, FDP_ACF.1/Domain)

83 The “EMSCOMM” user is a built-in user that is used by the M2000 to operate the TOE. This user has permission to execute all the commands of the TOE and cannot be modified neither deleted. This user can only be implicitly accessed through the integration port. (FDP_ACC.1/EMSCOMM, FDP_ACF.1/EMSCOMM)

84 TOE supports three roles: ADMIN_ROLE, GUEST_ROLE and EMSCOMM_ROLE. The Domain users do not belong to any role, given that their authentication is out of the scope of the TOE, and their permissions are stored and maintained in M2000. (FMT_SMR.1)

6.1.3. Auditing

85 The auditing functionality of the TOE cannot be started or stopped independently from the operational TOE. However, the TOE generates audit records for the start and shutdown of base station, and for several auditable events, storing the audit data in the appropriate file. (FAU_GEN.1)

86 Where appropriate, the data recorded with each audit record includes the unique user ID associated with a subject during authentication. (FAU_GEN.2)

87 The logs are recorded in the files which stored in the flash. No user is available to modify or delete these logs because there is no way for any user to do that. The files are in the operational environment in order to keep the database from overflowing. (FAU_STG.1)

88 There exist two kinds of audit files, the operation log and the security log.

1. Security log: Records user operations related to the system security, including user behavior and configuration commands, for example, account locking due to consecutive login failure and updating the security policy.

2. Operation log: Records all MML commands run by users.

89 For each of these kinds there exist two files that are rotated in the following way: if one exceeds 1MB the oldest file is deleted and a new one is created. (FAU_STG.3)

90 The audit records are stored with user information (when it is applicable). The user information is given by the system, when implementing the identification and authentication mechanism. (FIA_UID.1).

91 All users can send MML commands to the TOE to obtain the whole set of audit records (FAU_SAR.1). The TOE offers search functionality based on time intervals, user IDs, interface, and/or result. (FAU_SAR.3).

6.1.4. Communications security

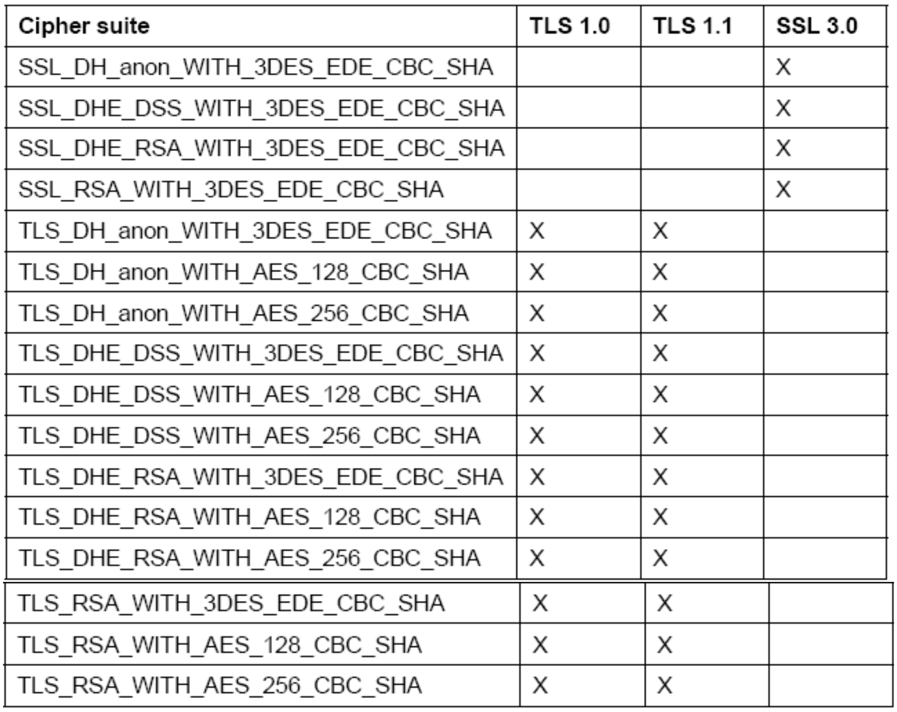
92 The TOE provides communications security for network connections to the WMPT. This includes connections via the following interfaces:

1. The TOE includes a FTP client which can connect and authenticate with a FTP server. The authentication parameters include the username and password and the IP address of the FTP server, which can be configured. SSL/TLS is used in this connection.

2. The connection with the LMT also uses SSL/TLS and authentication based on user id and password.

3. The connection between the TOE and M2000 is performed using a SSL trusted channel. This access provides management functionality. (FTP_ITC.1)

93 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	

94 This functionality is implemented through FCS_COP.1/SSL and FCS_CKM.1/SSL.

95 This functionality is configurable. (FMT_SMF.1).

96 The TOE provides VLAN to separate the traffic from different flow planes, which reduce traffic storms and avoid resource overhead.

97 The TOE support VLAN division based on flows such as signalling flows, media flows, or management flows. In other words, different VLAN tags are marked on the three types of flows passing the BS and they are separate from each other. (FTA_TSE.1/SEP)

98 The TOE supports IP-based Access Control List (ACL) to filter traffic destined to TOE which might cause system overload and service interruption.

99 The ACL provides a simple security policy that controls the incoming and outgoing data of unauthorized users. The ACL determines what data is allowed to enter the transmission port and what data is not allowed to enter the transmission port. In this way, the ACL filters the illegitimate data.

100 The ACL controls the network access, preventing the network attacks. In addition, the ACL filters out illegitimate data flows, improving the network performance.

101 The ACL consists of multiple rules. Each rule contains the following filtering conditions:

1. Protocol type (IP, ICMP, TCP, UDP, and GRE)
2. Source IP address and mask
3. Source port range
4. Destination IP address and mask
5. Destination port range
6. Differentiated Services Code Point (DSCP) value
7. ACL Action (Deny, Permit)

102 The ACL rules can be preset in the IUB Signaling network interface, and the ACL Action can be designated in advance. In this way, the different types of communication flows can be permitted or denied, and the illegitimate data can be filtered. This method effectively prevents illegitimate intrusions and malicious packet attacks, ensuring the security of network devices. (FMT_SMF.1, FTA_TSE.1/SEP)

6.1.5. Security function management

103 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:

- Configuration of SSL for the communication between LMT/M2000 and the base station.
- Configuration of ACL for the communication between the TOE environment and the base station.
- Configuration of VLAN for the different plane between the TOE environment and the base station.
- 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 to be between 6 and 32 characters, administrator has the option to enforce the use of specific characters (numeric, alphanumeric low or capital, and special characters). (FIA_SOS.1)
- Enable or disable the software digital signature check while updating the TOE software.
- Configure the number of authentication attempts before locking an user account, and he time the account will be locked.

104 Not all the management functionality is available for all the users. That way, some management functionality is accessible for a user depending on its role.

- Reset the password of the “admin” user to a password specified by the “EMSCOMM” user. → Only available for “EMSCOMM” user.
- Unlock the accounts of the “admin” and “guest” users → Only available for “admin” user, “EMSCOMM” user and Domain users.

105 The ADMIN_ROLE and GUEST_ROLE role are the unique capable to perform the following actions:

- Modify the “admin” and “guest” password.

106 All of these management options are available via the LMT or M2000 (FMT_SMF.1)

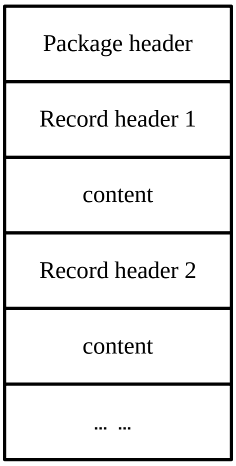
6.1.6. Digital Signature

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

108 The TOE automatically checks the digital signature of the software when the user runs the DLD SOFTWARE command to download the software.

109 The CSP files will be the files downloaded from the FTP server to update the TOE software and this way exercise the digital signature mechanism implemented in the TOE.

110 In the following image the CSP structure is depicted:



111 This way, a directory structure is stored in the CSP file. This structure is expected to contain some important files:

112 VERDES.SGN contains the signature of the VERDES.XML file. This way, the TOE will verify the hash and CRC value of each of the files using the VERDES.XML file, and will also verify that the file VERDES.XML has not been tampered using the VERDES.SGN stored signature (FCS_COP.1/Sign).

113 This way, the integrity chain is guaranteed.

7. Abbreviations, Terminology and References

7.1. Abbreviations

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
NE	NetEngine
CLI	Command Line Interface
GUI	Graphical User Interface
SRU	
MPU	Main Process Unit
LPU	Line Process Unit
SFU	Switching Fabric Unit
WCDMA	Wideband Code Division Multiple Access
MBSC	Multi Base Station Controller

7.2. Terminology

114 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.

115 **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.

116 **Operator:** See User.

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

7.3. References

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

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