



वर्गीय आवश्यकताओं के लिए मानक

टीईसी 22060:2007

(पूर्व सं: टीईसी/जीआर/ डब्ल्यूएपी-01/02.अप्रैल 2007)

STANDARD FOR GENERIC REQUIREMENTS

TEC 22060:2007

(Earlier No. TEC/GR/WAP-01/02.APRIL 2007)

वायरलेस एप्लिकेशन प्रोटोकॉल (डब्ल्यूएपी) नेटवर्क

Wireless Application Protocol (WAP) Network



ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीदलाल भवन, जनपथ, नई दिल्ली-110001, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHID LAL BHAWAN, JANPATH, NEW DELHI-110001, INDIA

www.tec.gov.in

© टीईसी, वर्ष
© TEC, YEAR

इस सर्वाधिकार सुरक्षित प्रकाशन का कोई भी हिस्सा, दूरसंचार अभियांत्रिकी केंद्र, नई दिल्ली की लिखित स्वीकृति के बिना, किसी भी रूप में या किसी भी प्रकार से जैसे -इलेक्ट्रॉनिक, मैकेनिकल, फोटोकॉपी, रिकॉर्डिंग, स्कैनिंग आदि रूप में प्रेषित, संग्रहीत या पुनरुत्पादित न किया जाए।

All rights reserved and no part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form and by any means - electronic, mechanical, photocopying, recording, scanning or otherwise, without written permission from the Telecommunication Engineering Centre, New Delhi.

Release: April, 2007

Price: Free of Cost

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document gives the requirements of Wireless Application Protocol (WAP) Network. A WAP Network has main elements like WAP Gateway/Proxy, WAP Push Proxy Gateway and WAP enabled terminals that are required for accessing applications and services based on Wireless Application Protocol (WAP). For the purpose of this document, Network complying with the requirements mentioned in this document will be referred as WAP Network. Wireless Application Protocol utilizes as few resources as possible on the WAP enabled terminal and compensate for the constraints of the device by enriching the functionality of the network. The WAP Network brings Internet contents and advanced data services to mobile phones / terminals. WAP specifies how information shall be coded and presented to mobile phone/terminal, so as to enable users of mobile phone/terminal to easily access live interactive information services and applications from the small screens of mobile phone/terminal. Services and applications include email, customer care, call management, unified messaging, weather and traffic alerts, news, sports and information services, electronic commerce transactions and banking services, online address book and directory services, as well as corporate Intranet applications. A Wireless Application Protocol (WAP) network functions with WAP enabled terminal, WAP Proxy/Gateway, WAP Push Proxy Gateway and Mobile Network.

HISTORY SHEET

Sl. No.	Standard/Document No.	Title	Remarks
1.	G/WAP- 01/01 JUN 2000	Wireless Application Protocol (WAP) Network	
2.	GR/WAP- 01/02	Wireless Application Protocol (WAP) Network	
3.	TEC 22060:2007	Standard for Generic Requirements for a Generic Requirements for Wireless Application Protocol (WAP) Network	Includes revised Numbering Scheme

Note:

1. The documents have been renumbered as per revised numbering scheme, kindly refer the Mapping-Listing Table pertaining to old and revised document number available on TEC website www.tec.gov.in/. In case of further clarification, please contact at email ID adgdoc.tec@gov.in

2. Inside the documents, General Requirements may be read as Standard for General Requirements, Interface Requirements as Standard for Interface Requirements, Several Requirements as Standard for General Requirements and Test Schedule & Test Procedure (TSTP) as TEC Test Guide.

CONTENTS

Chapter No.	Description	Page No
1.	Introduction	1
2.	WAP Enabled Terminal	3
3.	WAP Gateway/Proxy	5
4.	Push Proxy Gateway	12
5.	General Requirements	14
	Tendering Guidelines	24
	Abberivations	25

References

List of documents referred in the GR

1. Wireless Application Protocol, Version 2.0
2. ITU-T Recommendation T.50 : International Reference Alphabet (IRA).
3. ITU-T Recommendation Z.100 and subsequent addendum : Specification and Description Language (SDL).
4. ITU-T Recommendation Z.314 : The Character Set and Basic Elements.
5. ITU-T Recommendation Z.322 : Capabilities of Visual Display Terminals.
6. TEC Standard No. SD/EMI-02/02.SEP2001: Electromagnetic Compatibility Standard for Telecommunication Equipment.
7. TEC GR No. GR/TCP-01/02.AUG.2003: Generic Requirements for Routers.
8. Document No. QM 117: QA Requirement for software
9. Document No. QM 118: Quality and reliability in Product Design
10. Document No. QM 205: Guidelines for Standard of Workmanship for Printed Board.
11. Document No. QM 206: Guidelines for Standard of Workmanship for Printed Board Assemblies.
12. Document No. QM 210: Acceptability of Printed Board Assemblies containing SMDs.
13. Document No. QM 301: QA Requirement of Transmission Equipments
14. Document No. QM 324: Broad Outline of BSNL(QA) Component Approval Procedures.
15. Document No. QM 333: Specification for Environmental testing of Electronic Equipments for Transmission and Switching use.
16. Document No. QM 351: Quality Manual on QA requirements for Switching Equipment.

PART-I

Wireless Application Protocol (WAP) Network

**GENERIC REQUIREMENTS
(GR NO. GR/ WAP-01/02. APR 2007)**

Chapter - 1 Introduction

1.1.0 Introduction

This document gives the requirements of Wireless Application Protocol (WAP) Network. A WAP Network has main elements like WAP Gateway/Proxy, WAP Push Proxy Gateway and WAP enabled terminals that are required for accessing applications and services based on Wireless Application Protocol (WAP). For the purpose of this document, Network complying with the requirements mentioned in this document will be referred as WAP Network.

Wireless Application Protocol utilises as few resources as possible on the WAP enabled terminal and compensate for the constraints of the device by enriching the functionality of the network. The WAP Network brings Internet contents and advanced data services to mobile phones / terminals. WAP specifies how information shall be coded and presented to mobile phone/terminal, so as to enable users of mobile phone/terminal to easily access live interactive information services and applications from the small screens of mobile phone/terminal. Services and applications include email, customer care, call management, unified messaging, weather and traffic alerts, news, sports and information services, electronic commerce transactions and banking services, online address book and directory services, as well as corporate Intranet applications.

A Wireless Application Protocol (WAP) network functions with following elements:

- i) WAP enabled terminal
- ii) WAP Proxy/Gateway
- iii) WAP Push Proxy Gateway
- iv) Mobile Network

Each of the above elements is independently functional and interactions among them are based on a set of specifications given in the following chapters of this document. The elements are shown in Figure 1.

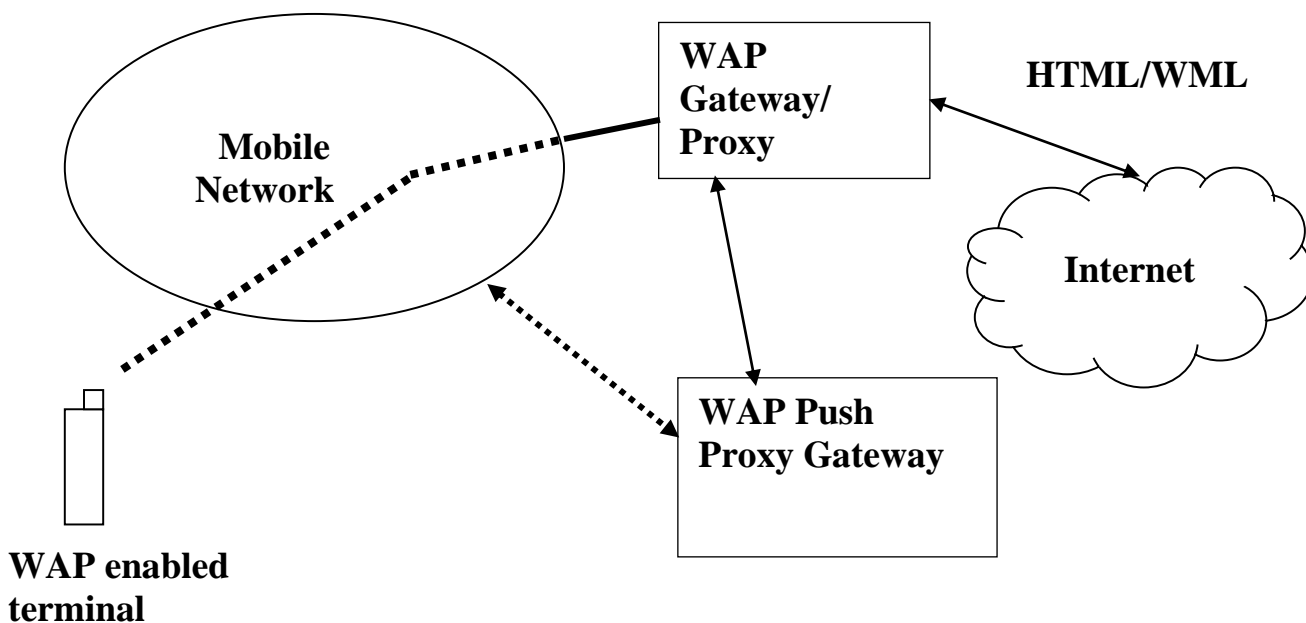


Figure 1 WAP Network

The WAP Network allows WAP enabled terminal (client) to browse the Internet or WAP Application Server contents. The WAP enabled terminal (client) connects to the WAP Proxy/Gateway through the Mobile Network over the available bearer (a list specified later) available and accesses the information from the Internet.

The WAP system shall comply to the WAP 2.0 or latest specifications for WAP access recommended by WAP forum/ Open Mobile Alliance. The WAP Proxy/Gateway contacts the Internet and fetches the information content sought by the client. If the information content is in Hypertext Markup Language (HTML) format, the WAP Proxy/Gateway translates it into Wireless Markup Language (WML) format and encodes the translated WML content into a compact binary code understood by the client based on the device capabilities. In case the information content from the Internet is in WML format, the WAP Gateway/Proxy directly encodes the WML content into the compact binary code.

WAP Push Proxy Gateway acts as an access point for content pushes from the internet to the mobile network.

The mobile network provides the bearer and interfaces required for WAP enabled terminal, WAP Gateway/Proxy, Push Proxy Gateway as indicated in the relevant chapters.

Chapter - 2

WAP Enabled Terminal

2.1.0 General

This chapter envisages common requirements of WAP enabled terminals. These requirements are only with respect to access of WAP applications and services on the terminal. The other requirements like frequency of operation, bearer, quality requirements etc. shall be as per the Generic Requirement for that terminal

WAP enabled terminal is a mobile device that incorporates a relatively simple micro browser in it, requiring limited resources. Micro browser based services and applications reside on servers and not permanently in WAP enabled terminal. The WAP enabled terminal shall comply with WAP 2.0 Specification.

2.1.1 Functional Requirements

2.1.1.1 The WAP enabled terminal shall receive and interpret the compact binary code sent to it by the WAP Proxy/Gateway. It, in turn, shall display the interpreted contents to the display screen.

2.1.1.2 The WAP enabled terminal shall be capable of storing the User Profiles, Channels, Resources like Wireless Markup Language (WML) Decks, Wireless Bit Map (WBMP) images etc.

2.1.1.3 The WAP enabled terminal shall meet the other functional requirements as per the specifications for the Global System for Mobile Communication (GSM) or Code Division Multiple Access (CDMA) mobile handsets or both.

2.1.2 Technical Requirements

2.1.2.1 Micro-Browser

The Micro-Browser of handset shall support following features:

- i. Back to previous page
- ii. Authentication on the WAP Proxy/Gateway.
- iii. Bookmarks – Minimum 10 Bookmarks with Export/Import Feature.
- iv. Access to cache
- v. Character sets: It shall support UTF8 (Default), USAASCII, Latin 1, UCS2
- vi. Homepage – For each User Profile.

- vii. Hyperlinks in Text shall be indicated.
- viii. Hyperlinks in Images shall be indicated.
- ix. Image Formats – Graphic Interchange Format(GIF), WBMP (Wireless Bitmap)
- x. WML and WML Script Support.

2.1.2.2 Repository - Capable of storing minimum three User Profiles

2.1.2.3 WAP profile setting: Minimum three different settings shall available while selecting WAP profile (Intranet, Internet, Banking Gateway etc.) i.e. minimum three WAP profiles, each with its own settings.

2.1.2.4 PPP Authentication: It shall support password authentication procedure and Challenge Handshake Authentication Protocol (CHAP).

2.1.2.5 Security issues: Shall comply with the security part as per WAP 2.0 Specification.

Chapter - 3

WAP Gateway/Proxy

3.1.0 General

The WAP Gateway/Proxy is an access point between the wireless world and the Internet/Intranet world. The WAP Gateway takes information from a Web/WAP server, process it, and sends it out over the mobile network to a WAP enabled terminal (client) and vice-versa. The WAP Gateway/Proxy connects the mobile network and the Internet by mapping the WAP protocols on the mobile side to the HTTP and TCP/IP protocols on the Internet side and vice versa. All Operation & Maintenance functions shall be available through an operation & maintenance workstation

The WAP Gateway/Proxy shall comply with WAP 2.0 specifications with backward compatibility to WAP 1.x. WAP layers of the WAP Gateway/Proxy stack shall have functionality as per WAP 2.0 specifications.

3.2.0 Functional Requirements

WAP Gateway/Proxy shall support following functions:

- i. The WAP Gateway/Proxy shall provide a gateway between the Internet/WAP Application Server and WAP enabled terminal (client) over specified bearer, by translating Hyper Text Transfer Protocol (HTTP 1.0 and HTTP 1.1 or later version) to the Wireless Session Protocol (WSP).
- ii. The implementation of Wireless Application Protocol for both connectionless and connection oriented mode according to the WAP 2.0 specifications.
- iii. Subscriber identification.
- iv. Subscriber authentication: The WAP Gateway/Proxy shall perform user authentication before allowing access to WAP application server.
- v. It shall be possible for the operator to insert subscriber's specific attributes into WAP request header before sending to the application/ content server.
- vi. Ensure Subscriber Privacy viz. protection of personal information.
- vii. Control over subscriber identifiable information (MSISDN, Client IP, etc.) in HTTP headers.
- viii. WAP Gateway/Proxy shall perform the conversion of Hyper Text Markup Language (HTML) to Wireless Markup Language (WML).

- ix. WAP Gateway/Proxy shall support negotiation capability characteristics for different WAP enabled terminals.
- x. Free Uniform Resource Locator (URL) access: The WAP Gateway/Proxy shall allow free access to a pre-defined URL for all subscribers.
- xi. User information forward: The WAP Gateway/Proxy shall be able to forward user information to application servers.
- xii. WAP Gateway/Proxy shall provide default home page.
- xiii. Cache service: It shall store commonly requested WML pages in binary format eliminating the need to fetch information from Internet.
- xiv. Cookie Service: The Gateway shall have the provision to store the Cookies on behalf of the Handset.
- xv. Script compilation: WAP Gateway/Proxy shall generate executable code from WML script present in pages sent from the WAP application server.
- xvi. WML encoding: The WAP Gateway/Proxy shall perform the encoding and decoding between WML and binary code.
- xvii. Character set transcoding: It shall perform transcoding from one character set to another if the received character set is not supported by the WAP enabled terminal (client).
- xviii. Character set support: The WAP Gateway/Proxy shall support the different character set as per WAP 2.0 specifications. Character set conversion from Utf 8 to US ASCII shall be possible.
- xix. The WAP Gateway/Proxy shall makes it possible to use ordinary WWW servers as hosts for WAP applications/services
- xx. The WAP enabled terminal (clients) shall be able to connect to the WWW/WAP server where the desired WAP application resides by using WAP enabled browser in the terminal. WAP Gateway/Proxy shall transform the user content requested into an ordinary Hyper Text Transport Protocol (HTTP) request. Content fetched from WWW server shall be returned to the WAP enabled terminal in the form of a WML deck.
- xxi. The WAP Gateway/Proxy shall support push features.
- xxii. Access Control Lists
The system shall support a comprehensive list of access controls based on the following parameters:
 - a. MSISDN
 - b. IP Address
 - c. User agent
 - d. Content type/site
 - e. Group Based
 - f. Access Point Name (APN)
 - g. IP address range
 - h. MSISDN range

- i. Permissible/ non-permissible sites
 - j. Support for URLs with or without wild- characters
- xxiii. It shall be possible to configure sites and content-types for which download status need to be maintained.

3.3.0 Subscriber provisioning and service subscriptions

WAP Gateway shall provide integrated service and subscription platform. The operator shall be able to create, delete, modify & display the subscription. In addition, it shall support interface to Billing & Customer Care System (B & CCS) and Service Delivery Platform (SDP)

It shall be possible to facilitate the following functionalities:

- a. Provisioning of the pre-paid/post-paid subscriber with details of MSISDN/ MDN.
- b. Self-provisioning by subscribers to the WAP gateway system.
- c. Operator shall be able to create the group of subscribers with one primary and many secondary numbers (multiple MSISDNs).
- d. It shall be possible to offer a variety of flexible, easily configurable services in real time.
- e. It shall be possible to suspend or resume the access of WAP service for a particular subscriber.
- f. Operator shall be able to control browsing by subscriber using the WAP service.
- g. Allow on-line self-subscription by subscribers to various services launched and to manage their subscriptions on their own.
- h. Advise the subscribers about the launched services and their charges to enable the subscriber to go for on line subscription of the services.
- i. Subscriber shall be able to check the details about the subscription on-line and via operator.
- j. Operator shall be able to create multiple internal users (administrators) with varying privileges to control the add/delete/modify operations.
- k. The operator shall be able to define various URLs to create different services.

3.4.0 Fault management

The fault management function in the WAP Gateway/Proxy shall have the following functionality:

- i) alarm collection
- ii) alarm administration
- iii) alarm reporting

Logs of all reported alarms and a list of all the currently active alarms shall be available. Provision shall be there to send alarm information to a central Network Management Centre (NMC) via the Simple Network Management Protocol

(SNMP). The system should also support delivery of alarms to an e-mail address using email and/or to mobile number(s) using SMS.

Alarms shall be raised for the following:

- a. High CPU usage
- b. High System Load
- c. High Memory Usage
- d. High Disk Usage (Disk Space Usage)
- e. High Disk I/O

3.5.0 Performance management

The purpose of Performance Management is to obtain statistical data about how the WAP Gateway/Proxy is being used. The information is used for location of congestion/fault and as a foundation for resource planning.

The following counters shall be supported by the WAP Gateway/Proxy:

- i) number of secure sessions active in the WAP Gateway/Proxy.
- ii) number of transactions at the server.
- iii) number of aborted transactions.
- iv) number of sessions.
- v) CPU Load.

3.6.0 Trend Analyser

The WAP Gateway shall forward the logs, events, statistical counters to OSS to carry out the following trend analyses:

- a. General WAP Usage (success, failure, cache hit, etc.)
- b. Report on Data usage
- c. Report on User access pattern
- d. Report on Mobile models used
- e. Report on Transaction Per Second (TPS)
- f. Report on contents accessed
- g. Reports on the web sites accessed

3.7.0 Configuration management

Configuration management provides facilities for configuring the sub-systems that make up the WAP Gateway/Proxy. Configuration management functions shall be available which can be performed from the operation and maintenance workstation connected either locally or remotely via an Intranet.

The system shall also have support for integrated configuration management in order to support configuration and management of multiple WAP Gateway servers using a single point OA&M console. The Integrated Administration Manager shall also support the following:

- a. User creation for administration and other OA & M activities.
- b. Role creation for each user (administrator) in order to provide appropriate access permission to users
- c. Analyse user request/response
- d. Statistical / graphical reports to provide current Transactions Per Second (TPS), user sessions, system's CPU load and Memory usage.
- e. Detailed reports to enable the administrator to understand the WAP usage.
- f. Shall allow the WAP gateway servers to be configured on an individual basis and on a group basis.
- g. It shall be possible to monitor WAP Service Status.

3.8.0 Charging Support

WAP Gateway shall provide interface for integration with B & CCS and IN system for charging purpose. The interface between billing unit and Gateway/Proxy shall be TCP/IP. The CDR shall have at least following information:

- i. Client address and port.
- ii. Transaction time, date and duration.
- iii. Packet size.
- iv. URI requested.
- v. Billing /service ID.
- vi. Tariff class.
- vii. MSISDN
- viii. IP address
- ix. Address of Gateway/Proxy
- x. Bearer type

3.8.1 Provision shall be there in WAP Gateway/Proxy for:

- i. Collection of CDR files from the WAP Gateway/Proxy by the external billing system/Gateway through magnetic media.

- ii. Automatic transfer as well as transfer on request of CDR files from the WAP Gateway /Proxy to the external system.

3.8.2 WAP Gateway shall support DIAMETER to interface with the service provider's pre- paid billing system.

3.9.0 Operating System

The details of Operating System for the WAP Gateway shall be provided. It shall be widely used operating system like Sun Solaris, Linux or Unix.

3.10.0 Capacity and Performance

The Gateway/Proxy shall support minimum ultimate capacity of 3,00,000 WAP customers with 10 transactions per hour per customer. The peak hour transactions can be taken as five times the average. The number of transactions per session is ten. The length of session shall be taken as 600 sec. Average size of session is 100 Kbytes towards WAP enabled terminal end. It shall be possible to dimension from 10,000 WAP customers in step of 10,000 customers.

The capacity and performance of the system and the traffic modeling shall be furnished.

3.11.0 Interface and Bearer Support

3.11.1 The physical interface shall support the following:

- i. E1 on G.703
- ii. Ethernet 2 X 10 Base T/100 Base T auto sensing as per IEEE 802.3u

3.11.2 It shall be able to provide terminations from Mobile network, Internet Gateway and WAP Push Proxy Gateway. It shall be scalable for more terminations.

3.11.3 The WAP Gateway/Proxy shall support one or more bearers mentioned below. If any interface other than the standard interface is required to be deployed at the MSC/ SMS-C end for connectivity to WAP Gateway/Proxy, it shall be supplied as a part of WAP Gateway. The implementation shall be clearly indicated. If the implementation requires additional elements like router (as per TEC GR No. GR/TCP-01/02 AUG 2003), the same shall form part of WAP Gateway /Proxy equipment.

i. GSM Network - Circuit Switched Data (CSD)

The WAP Gateway/Proxy shall support an interface (as per WAP WDP specification of WAP 2.0 Specifications) for circuit switched data access based on User Datagram Protocol (UDP)/Internet Protocol (IP).

ii. GSM Network - General Packet Radio Service (GPRS)

The WAP Gateway/Proxy shall support interface for GPRS as per WAP WDP specification of WAP 2.0 Specifications.

iii. CDMA Network - Circuit Switched Data (CSD)

The WAP Gateway/Proxy shall support an interface (as per WAP WDP specification of WAP 2.0 Specifications) for circuit switched data access based on UDP/IP

iv. CDMA Network-Packet Data.

The WAP Gateway/Proxy shall support an interface (as per WAP WDP specification of WAP 2.0 Specifications) for packet data service as bearer.

3.12.0 The WAP Gateway/Proxy shall provide firewall support between the WAP Gateway/Proxy & Internet, and WAP Gateway/Proxy & WAP server.

3.13.0 On-line documentation

The WAP Gateway/Proxy system documentation shall be available on-line and shall be presented using the same WWW browser as the subscriber provisioning interface. Access to the appropriate documentation shall be made available in a number of ways like:

- i. Navigation through the library contents list
- ii. Key-word search
- iii. Context sensitive retrieval
- iv. Help in HTML format linked with OA &M module for easy access to online help.

Chapter - 4

Push Proxy Gateway

4.1.0 General

The Push Proxy Gateway facilitates the contents to be pushed to devices by server based applications via push proxy. The push functionality is especially relevant to real-time applications that send notifications to their users such as messaging, stock price, traffic update alerts etc. A push operation in WAP is accomplished by allowing a Push Initiator (PI) to transmit push content and delivery instructions to a Push Proxy Gateway (PPG), which then delivers the push content to the WAP client according to the delivery instructions. The PI is an application that runs on the web-server. It communicates with the PPG using the Push Access Protocol (PAP). PPG uses the push Over The Air (OTA) protocol to deliver the push content to the client.

4.1.1 Services

The PPG shall conform to OMA WAP 2.0. The PPG shall support the following:

- a. PI identification and authentication; access control
- b. Parsing of and error detection in push content and control information
- c. Client discovery services (including client capabilities)
- d. Address resolution of push recipient
- e. Store & forward of push messages
- f. Protocol conversion
- g. Message Acceptance & Rejection
- h. Multicast & Broadcast services
- i. Message Handling Service
- j. WAP Push types such as confirmed / unconfirmed WSP Push, unconfirmed SMS Push, confirmed HTTP Push etc.

4.1.2 Functional Capabilities

The system shall support the following to provide reliable and controllable push message delivery platform:

- a. Retry the push message for a configurable number of times before the message is dropped.
- b. Status query of the messages that are already submitted to PPG from PI.
- c. Canceling push messages that were already submitted to PPG.
- d. Replacement of push messages that were already submitted to PPG.
- e. Capability query on particular user.

- f. Secure interface to submit push messages from Push Initiators.
- g. Content transformation of push messages.
- h. MySQL or Oracle database.
- i. Interface to generate reports and statistics based on the following:
 - Content type pushed
 - Push Initiator
 - SMSC
 - Push Type (Confirmed, unconfirmed etc.)
 - Number of Push messages (Hourly, Daily, Weekly and Monthly)
- j. Support for delivering push messages on already existing WAP session.
- k. Support to send Session Initiation Request (SIR) to users who are not in session.
- l. Capability to interface with multiple SMSCs with a feature of load balancing of push messages with multiple SMSCs.
- m. Option of fall-over to active SMSC link when connectivity to one SMSC is lost.
- n. Support Push Initiator (PI) based authentication based on the following parameters:
 - Source IP of the Push Initiator
 - Username/Password

4.1.3 The PPG shall support both GPRS and CDMA networks.

4.1.4 Capacity and Performance

The capacity and performance of the system and the traffic modeling shall be furnished.

PART-II

Chapter - 5

General Requirements

5.1.0 General Requirement

5.1.1 The Network equipment shall support multi-vendor interoperability i.e. the possibility of using multiple equipment and sub-systems like WAP enabled terminal, WAP Gateway/Proxy Server, WAP Application Server and WTA Server of different vendors without any restriction.

5.1.2 The technology used shall be in line with state of the art practice. The equipment shall be fully solid state and of proven technology. The equipment shall have the following features:

- i. Low power consumption
- ii. Minimum numbers of power supply voltages in the equipment.

5.1.3 All software updates, for a period of seven years, shall be supplied on continuing basis. These updates shall include new features & services and other maintenance updates.

5.1.4 Right of use: There shall be no imposition of any sort of precondition on the “Right of Use” of software.

5.2.0 Hardware

5.2.1 The system hardware shall be modular in design and shall permit growth in steps. The arrangement shall be such that failure/deterioration of service shall not occur when implementing the growth.

5.2.2 Design precautions shall be taken to minimise the possibility of equipment damage arising from the insertion of an electronic package into the wrong connector or the removal of any package from any connector.

5.2.3 All components shall be rated for continuous operation of the system under the normal operating conditions. The circuits shall be designed so as to prevent damage to the other equipment under any condition of operation or any conditions of fault.

5.3.0 Processors

5.3.1 The system shall have adequate redundancy of processors.

5.3.2 Adequate backup memory shall be provided. Direct memory access, with suitable safeguards, is preferred for information flow between the backup memories, the main memories and the input/output devices.

5.3.3 Provision shall be made to prevent the loss/alteration of memory contents due to power failures, improper operating procedures and the procedure for restoring the system to its normal state etc.

5.3.4 Dimensioning standards shall be furnished for the various types of memories used. This shall also include standards for provisioning of the required spare memory capacity.

5.4.0 Software

5.4.1 The software shall be modular and structured.

5.4.2 The software shall include the following characteristics:

- i. The design of the software shall be such that the system is easy to handle both during installation and normal operations as well as during extensions.
- ii. The functional modularity of the software shall permit introduction of changes, wherever necessary, with least impact on other modules.
- iii. It shall be open-ended to allow addition of new features.
- iv. Adequate flexibility shall be available to easily adopt changes in service features and facilities and technological evolution in hardware.
- v. The design shall be such that propagation of software faults is contained.
- vi. The software shall provide sufficient checks to monitor the correct functioning of the system.
- vii. The system software shall not lose complete sanity under any circumstances.
- viii. Test programs shall include fault tracing for detection and localization of system faults.
- ix. Integration of software updates shall be possible without problem to the running system.
- x. Facilities shall be in-built to ensure automatic system reconfiguration on detection of:
 - a. Software fault during access
 - b. Software fault during audits checking.

5.4.3 Availability/Redundancy

All the servers and Gateway/Proxy shall have the following features to ensure high availability and redundancy:

- i. Comprehensive hardware and software fault isolation and recovery features shall be supported and specified.

- ii. In case of fault in one of the CPUs or other sub-systems, the switch over of the function to other units/standby unit shall be automatic and shall not affect the transactions in progress.
- iii. Redundant arrays for disks (RAID 0 through RAID 5 implementation).
- iv. Multiple CPUs for increased performance and scalability.
- v. **Server health monitoring:** Ability to provide service and application redundancy by monitoring the status of another server and taking up the processes of the remote server in the eventuality of its crashing.
- vi. The controller card and network interface card shall have redundancy in WAP Application Server, WTA Server and WAP Gateway/Proxy.

5.4.4 Management and security

The server shall support the following management and security features:

- i. SNMP/RMON support for SNMP MIBs.
- ii. **Access Security:** The server shall have password protection features. Multiple management access privileges for privileged (configuration) and non-privileged (read only) tasks shall be supported.

5.5.0 Diagnostic Programs

- 5.5.1** On a faulty condition, the software shall provide for isolating the faulty sub-system and then automatically bring - in the diagnostic programs for diagnostic purposes.
- 5.5.2** It shall be possible to diagnose a fault to single card level in at least 95% of the types of cards.
- 5.5.3** The system shall provide means for tracing individual/group user transaction or activities to analyse the problem.

5.6.0 Safety of charge records

- 5.6.1** Arrangements shall exist for dumping the charging information to non-volatile backup memories automatically at periodic intervals. Facility shall be available for changing this interval by a man-machine command.
- 5.6.2** The charging information records shall be sufficiently protected against modifications by man-machine commands.

5.7.0 Operation and Maintenance Terminals

5.7.1 Input-Output devices

5.7.1.1 The communication facilities provided for exchange of information between the system and the maintenance and operating personnel shall include facilities for a system test, control and alarm indication.

5.7.1.2 Input/output terminals shall be capable of transmitting/receiving characters of a subset of the ITU-T alphabet No. 5 as per ITU-T Recommendation T.50. [2] The printing/display device shall print/display different graphic symbols for the digit zero and the capital letter O. The input/output terminal shall have the English Keyboard. Capabilities of visual display terminals shall be as per ITU-T Recommendation Z.322.[5].

5.7.1.3 Adequate number of man-machine interfaces shall be available to facilitate various types of system administration.

5.7.1.4 Provision shall be made for monitoring from a remote terminal. The reliability of the data links shall not, in any way, affect the reliability of the system. Special provision shall also be made for transmission of a failure signal even when the system is unable to transmit an output message.

5.7.1.5 A suitable alarm and display system shall be provided for a continuous indication of the system status. The alarm system shall also provide an alarm to indicate the failure of power supply to the alarm circuits. Provision shall be available to extend the alarm indications to a centralised place.

5.7.1.6 The O A&M functionality shall be accessible from any browser without the need for dedicated administration console.

5.8.0 Man-Machine Language (MML)

5.8.1 The man-machine language shall be in English. Commands shall be English based and responses shall be in English.

5.8.2 The MML shall have an open-ended structure such that any new function or requirement added will have no influence on the existing ones. The language structure shall be such that subsets can be created.

5.8.3 The character set used in the MML shall be as per ITU-T Recommendation Z.314.[4].

5.8.4 The command codes shall be function oriented. There shall be only one command per function. The codes shall be mnemonic. It is preferred if all the

command codes in a particular application consists of the same number of characters.

- 5.8.5 The output in response to input commands shall have the same format and use the same identifiers, codes and labels as the corresponding input command.
- 5.8.6 There shall be facilities for editing, canceling and stopping the completion of commands.
- 5.8.7 The MML shall provide facilities for inputting the parameters, for a command, in any sequence and the optional parameters need to be inputted only when they are required.
- 5.8.8 The system shall support Graphical User Interface (GUI) based user interface.

5.9.0 Man-machine dialogue

- 5.9.1 The MML shall offer the facility for a conversational mode of operation.
- 5.9.2 The MML shall have facility for restricting the use of certain commands or procedures to certain staff/terminals.
- 5.9.3 Where several man-machine terminals are in use on a single system, a mechanism shall be available to avoid clashes.
- 5.9.4 The execution of any command shall not result in malfunctioning and over loading of the system. It shall also be ensured that the operator is not logged out by the system.
- 5.9.5 The MML shall be implemented in such a way that errors in commands or control actions shall not cause the system to stop or unduly alter the system configuration.
- 5.9.6 Command errors detected by the system shall be indicated by the output of error messages.
- 5.9.7 Priority messages shall be able to interrupt input or output message of lower priority.

5.10.0 Checks and Safeguards

Sufficient checks and safeguards shall be built - in to the implementation of the MML so as to ensure reliable operation of the system.

5.11.0 Construction Practices

5.11.1 Equipment Practices

- 5.11.1.1** All circuits shall be mounted on plug-in PCBs of standard size to facilitate replacement. All cards of the same type and design shall be interchangeable without necessitating special adjustments.
- 5.11.1.2** All metal parts of frames, supports, etc. shall be mechanically rugged and constructed of corrosion resistant material or treated with anti-corrosive finish.
- 5.11.1.3** Suitable test access points and displays shall be provided for facilitating maintenance. All visual display devices shall be located in a position attracting immediate attention of the operating and maintenance personnel. Suitable extension boards shall be provided to facilitate access to components on a printed card.
- 5.11.1.4** The equipment shall have natural cooling arrangement that shall not involve any forced cooling such as by using fans etc. either inside or outside the equipment. However, in case this is unavoidable and the fans are to be used, these shall be DC operated.
- 5.11.1.5** It shall be indicated whether printed board connectors are of edge-type or plug-and-socket type. They shall not be easily damaged during replacements and removals. The contact particulars as well as life test performance on contact resistance for each type of connector shall be supplied.
- 5.11.1.6** All components and material used in the equipment shall be non inflammable or in absence of it, self-extinguishable. They shall be fully tropicalised.
- 5.11.1.7** Various types of cables and wires used shall be indicated. Detailed particulars of any special wires and cables like miniaturised co-axial, screened cable etc. shall be furnished with their actual usage in the system.
- 5.11.1.8** The buses, if any, shall be suitably protected against electrical and magnetic interference from neighboring systems (like electromechanical systems, fluorescent tubes, motors etc.).
- 5.11.1.9** The different plug-in cards shall have suitable mechanical safeguards to prevent damage due to accidental interchange of cards.
- 5.11.1.10** The requirement at the external interface against induced voltages and currents due to lightening, high power system etc. shall be indicated.
- 5.11.1.11** The system shall provide for isolation and protection from accidental high voltage power contact.

5.12.0 Marking

- 5.12.1** Equipment, whether fixed or plug-in type, shall be suitably marked. Identification of a type of cards in its connector shall be possible without necessitating its removal.
- 5.12.2** Connecting cables between jacks shall be marked at their extremities with identical designation as on fixed connecting flanges.
- 5.12.3** The marking on the equipment and the cables shall be the same as that used on the schematic drawings, cabling lines etc. in the documentation supplied with the equipment.
- 5.12.4** All instructions, labels, or any other marking on the equipment shall be perfectly legible and in the English language.
- 5.12.5** Colour code used for power feeding bus-bars/cables and earth shall be identical for a given voltage throughout the equipment.
- 5.12.6** Fuses shall have a suitable marking for the different ratings to enable easy identification and replacement.
- 5.12.7** Each sub assembly shall be clearly marked to show its functions and circuit reference so that its complete description can be located in the instruction manual.
- 5.12.8** The components shall be marked with their schematic references so that they are identifiable from the component layout diagram in the manual.
- 5.12.9** Marking and identification of the equipment, sub assemblies, PCBs etc. shall be as per guidelines issued by Quality Assurance Wing, BSNL vide document No. QM301.[12].

5.13.0 Components

- 5.13.1** All components used shall be of rugged construction and shall be suitably designated by a label or sign writing.
- 5.13.2** Components used in the equipment shall, in general, be de-rated as regards both voltage and power ratings, to ensure a high degree of reliability.
- 5.13.3** All components used shall be currently in large-scale production.
- 5.13.4** The failure of any component/sub-system shall not result in the failure of complete system.

5.14.0 Quality Requirements

- 5.14.1** All the equipment shall have a tropical finish and coated to protect against saline atmosphere.
- 5.14.2** Mechanical design and construction of the units /sub-assemblies shall be robust and rigid to withstand all conditions of operation, adjustment, replacement and the storage.
- 5.14.3** The equipment when packed for delivery shall be mechanically strong and be capable of withstanding vibrations and shocks during transportation etc.
- 5.14.4** The supplier/manufacturer shall conform to ISO 9001:2000 certification. A quality manual describing the quality assurance system shall be submitted by the manufacturer. Alternatively the equipment shall be manufactured as per guidelines issued by Chief General Manager, Quality Assurance Wing of BSNL vide Documents No. QM 117 [7], QM 118 [8], QM 205 [9], QM 206 [10], QM 210 [11] and QM 351 [15]. Any deviation that may seriously affect the working of the equipment shall be highlighted.
- 5.14.5** The plug-in units, whose removal or insertion endangers the reliability or performance of the equipment, shall have suitable protection.
- 5.14.6** The usage of components in the equipment either manufactured or directly imported shall comply to the guidelines issued in the Quality Assurance Wing of the BSNL document QM 324 [13] which gives broad outlines of QA component approval procedure. The source of procurement of components shall be submitted by the manufacturer. The list of all components for which second source is not available shall be provided.
- 5.14.7** The MTBF predicted and observed values shall be furnished along with calculations by the manufacturer. The equipment availability shall exceed 99.9%.
- 5.14.8** Based on the figures in clause 5.14.7, three years maintenance spares shall be specified by the supplier.
- 5.14.9** Power dissipation values (in Watts) for chassis and modules shall be provided.

5.15.0 Environmental Test Conditions

Environmental requirements for WAP Gateway/Proxy and Push/Proxy Gateway shall be as per Category A of QM-333 document of Quality Assurance Wing of BSNL.

5.16.0 Transportation and Storage Specifications

Transportation and Storage Specifications shall be as per QM-333 document of Quality Assurance Wing of BSNL.

5.17.0 Power Supply

The equipment shall operate at power supply of – 44.4 V DC to –56.4 V DC.

5.18.0 Electromagnetic Compatibility Requirement

The network equipment shall comply to electromagnetic compatibility requirements as per TEC Standard No. SD/EMI-02/02 SEP 2001.

5.18.1 The operation of the equipment shall be in the available frequency band viz. GSM 900/ 1800/ WCDMA bands for Mobile operation

5.19.0 Documentation

5.19.1 All documents to be provided shall be in English language.

5.19.2 The documents shall comprise of

- i. Equipment description documents
- ii. Equipment operation documents
- iii. Training documents
- iv. Repair related documents

5.19.3 Equipment Description Documents

The following equipment description documents wherever applicable shall be supplied along with the equipment:

- i. Over-all equipment specification and description of hardware and software.
- ii. Installation manuals and testing procedures.
- iii. Equipment layout drawings.
- iv. Cabling and wiring diagrams.
- v. Schematic drawings of all circuits in the system with timing diagram wherever necessary.
- vi. Detailed specification and description of all I/O devices.
- vii. Adjustment procedures.
- viii. Acceptance testing schedules.
- ix. Spare parts catalogue, including information on individual component values tolerances, etc., enabling procurement from alternative sources.
- x. Detailed description of software describing the principle interactions with hardware, structure of the program and data.

- xi. Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data.
- xii. Program and data listings.
- xiii. Programming language (s) manual wherever applicable.
- xiv. Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification and Description Language (SDL) as per of ITU-T Recommendations Z.100 [3] shall be provided. The description shall reflect the internal software structure in detail and the logical processes within the system.
- xv. Planning and system engineering documents.

5.19.4 Equipment Operation Documents

The following equipment operation documents shall be supplied:

- i. Operating manual of the equipment
- ii. Maintenance manual
- iii. Man-machine language manual
- iv. Operation and maintenance manual for all I/O devices and auxiliary equipments.
- v. Fault location and trouble shooting instructions including fault dictionary
- vi. Test procedures with auxiliary test equipments
- vii. Emergency action procedures and alarm dictionary

5.19.5 Training Documents

Training manuals and documents necessary for organising training in installation, operation & maintenance and repair of the system shall be made available. The structure and scope of each document shall be clearly described. The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information. All diagrams illustrations and tables shall be consistent with the relevant text.

5.19.6 Repair Related Documents

Procedure for repair giving full details of test setup shall be indicated. Test jigs and fixtures, if any, required for maintenance and repair shall also be indicated. The manufacturer shall indicate the repair philosophy.

5.20.0 WAP Application Development Toolkit

WAP Application Development Toolkit shall be provided. A developer's guide shall also be provided with the application Developer's Toolkit. The guide shall be available both as a printed manual and as online documentation. This shall allow test and verification of applications. Example applications shall also be included to show how the different Application Programming Interfaces (APIs) can be used in application development.

Tendering Guidelines

The purchaser may define the capacity/ performance of various servers in WAP network as given below taking into consideration bearer access to a number of data services such as Multi-media Messaging Services (MMS), Instant Messaging & Presence services (IMPS), Streaming, Java/ Non-Java downloads, Push based services such as Advertisements, OTA etc. at the time of procurement:

- 1. GR clause 3.10.0: Capacity and Performance (WAP Gateway/Proxy Server).**
- 2. GR Clause 3.11.1: Physical Interface** – The number & type of interfaces may be defined as per requirement.
- 3. GR Clause 4.1.4: Capacity and performance (Push Proxy Server).**

Abbreviations

API	Application Programming Interface
CDMA	Code Division Multiple Access
CGI	Common Gateway Interface
CDR	Charging Data Record
CHAP	Challenge Handshake Authentication Protocol
CSD	Circuit Switched Data
GIF	Graphic Interchange Interface
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
ITU	International Telecommunication
MAP	Mobile Application Part
MDN	Mobile Directory Number
MIB	Management Information Base
MML	Man Machine Language
MSISDN	Mobile Station International Subscriber Device Number
MTBF	Mean Time Between Failure
NMC	Network Management Centre
PAP	Push Access Protocol
PDA	Personal Digital Assistant
PDU	Protocol Data unit
PI	Push Initiator

PPG	Push Proxy Gateway
RAID	Redundant Array of Inexpensive Disk
RAS	Remote Access Server
RMON	Remote Monitoring
SDL	Specification and Description Language
SIR	Session Initiation Request
SMPP	Short Message Peer to Peer Protocol
SMS	Short Message Service
SMSC	Short Message Service Centre
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
UCS	Universal Multiple-Octet Coded Character Set
UDP/IP	User Datagram Protocol /Internet Protocol
URL	Uniform Resource Locator
USSD	Unstructured Supplementary Services Data
UTF	UCS Transformation Format
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WBMP	Wireless Bit Map
WDP	Wireless Datagram Protocol
WML	Wireless Markup Language
WSP	Wireless Session Protocol

-END of DOCUMENT-