Mobile Wireless Internet Forum

ARCHITECTURE REQUIREMENTS

Technical Report MTR-002

Release 1.7

Contribution Reference Number: MWIF 2001.011.7

NOTICE: Please review this Draft Technical Report for any undisclosed intellectual property (including but not limited to trademarks, copyrights, patents or any similar, registered or other allowable intellectual property rights, published or unpublished, anticipated or actual, presently existing or potentially arising in the future, in any country). If you have any undisclosed intellectual property that either will or may be infringed by the implementation of this Draft Technical Report, you must disclose this fact to the Board of Directors of MWIF immediately. If you fail to make such a disclosure, and the Draft Standard is adopted, you must grant all Members of MWIF a nonexclusive worldwide license to use this intellectual property on fair, reasonable and nondiscriminatory terms. Please direct any questions to the Board of Directors.

Mobile Wireless Internet Forum

Contribution Reference Number: **MWIF 2001.011.7**

Last Saved: **28th February 2001**

Title: **Architecture Requirements**

Working Group: **Operator Requirements Working Group**

Editor **Martin Harris**

Status: **Version 1 of this document has been approved by the Technical Committee of MWIF and has been endorsed for publication by the Board of Directors of MWIF. This is Version 2 of this document and it has been endorsed for publication by the Board of Directors of MWIF.**

IPR Acknowledgement: **Attention is called to the possibility that use or implementation of this MWIF Technical Report may require use of subject matter covered by intellectual property rights owned by parties who have not authorized such use. By publication of this Technical Report, no position is taken by MWIF or its Members with respect to the infringement, enforceability, existence or validity of any intellectual property rights in connection therewith, nor does any warranty, express or implied, arise by reason of the publication by MWIF of this Technical Report. Moreover, the MWIF shall not have any responsibility whatsoever for determining the existence of IPR for which a license may be required for the use or implementation of an MWIF Technical Report, or for conducting inquiries into the legal validity or scope of such IPR that is brought to its attention. This Technical Report is offered on an "as is" basis. MWIF and its members specifically disclaim all express warranties and implied warranties, including warranties of merchantability, fitness for a particular purpose and non-infringement.**

For additional information contact:

Mobile Wireless Internet Forum
39355 California Street, Suite 307, Fremont, CA 94538
+1 (510) 608-5930
+1 (510) 608-5917 (fax)
info@mwif.org
www.mwif.org

Abstract:

This document expands on the MWIF Principles to produce specific architectural requirements. These requirements reflect the wishes of the network operators and service providers within MWIF. Compliance with these requirements is considered to be essential in the production of the MWIF Architecture.

TABLE OF CONTENTS

1 INTRODUCTION

This Technical Report (MTR-002) provides the Architecture Requirements for the work of the Mobile Wireless Internet Forum (MWIF). The Operator Requirements Working Group produced the report at the request of the MWIF Technical Committee.

1.1 Objectives

The objective of this Mobile Wireless Internet Forum Technical Report is to detail the requirements that are derived from the MWIF Architecture Principles [1]. These requirements are intended to form the basis for the development of the MWIF Architecture.

The MWIF Architecture Principles Technical Report was produced in order to support the following business goals:

- Significant cost reduction
    - Data communications cost curve
    - Multi-vendor procurement
    - Modular & incremental infrastructure growth
- Accelerated Time to market
    - End user services
    - Infrastructure
- Variety of services with open service creation environment
    - Faster services & applications development
    - New business development opportunities
    - Alignment of data services and the Internet
- Grow Internet services business
    - Take advantage of wireline Investment in Internet, VoIP, IP-based services and applications

This report builds on these already defined principles and produces specific requirements.

1.2 Definitions

This document employs the following terminology:

- Must, Shall, or Mandatory — the item is an absolute requirement of the Technical Report.
- Should — the item is highly desirable.
- May or Optional — the item is not compulsory, and may be followed or ignored according to the needs of the implementers.

1.3 Overview of the Technical Report

The Architecture Principles were developed as part of the founding of MWIF to outline the objectives of MWIF. The intent of this report is to expand on these principles to define the base requirements for the MWIF architecture.

1.4 Release plan

It is the objective of the MWIF to provide timely industry direction for mobile wireless internet. In order to accomplish this, the MWIF will periodically release Technical Reports. The period in which Technical Reports will be released will be frequent enough to meet the objective of timely industry direction.

This Technical Report is one of a series intended to specify the MWIF architecture. At the time of release of this report, the following MWIF Technical Reports are scheduled:

MTR-001	MWIF Architecture Principles
MTR-002	MWIF Architecture Requirements
MTR-003	MWIF Layered Functional Architecture
MTR-004	MWIF Network Reference Architecture
MTR-005	MWIF Gap Analysis
MTR-006	MWIF IP Transport in the RAN
MTR-007	MWIF Open RAN Architecture

This document is the second release of MTR-002 that has been produced to specify the MWIF Architecture Requirements, based on the Architecture Principles defined in MTR-001. Where it has not been possible to fully identify requirements, these areas are marked for further study and will be addressed in subsequent versions of the technical report.

The Architecture Requirements document is a living document. MWIF will periodically review this document and update it as necessary (in line with the MWIF approval process) to meet the objective of "Timely Industry Direction For Mobile Wireless Internet". The Architecture Requirements outlined herein allow flexibility and room for improvement in the MWIF Architecture over time.

2 REFERENCES

[1] MTR-001: MWIF Architecture Principles

[2] ITU-R M.1079: Performance and quality of service requirements for international mobile telecommunications-2000 (IMT-2000); Revision 1 to Document 8/116-E 19 November 1999

[3] IETF RFC 2700; Internet Official Protocol Standards

[4] ITU-T Recommendation E.164 (05/97), "The international public telecommunication numbering plan".

[5] MTR-007: Open RAN Architecture

3 ABBREVIATIONS AND GLOSSARY OF TERMS

3.1 Abbreviations

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
AMR	Adaptive Multi-Rate (codec)
API	Applications Programming Interface
BSC	Base Station Controller
BTS	Base Transceiver Station
CAMEL	Customised Application of Mobile network Enhanced Logic
CDR	Call Detail Records
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
DSL	Digital Subscriber Line
GPS	Global Positioning System
EVRC	Enhanced Variable Rate Codec
HLR	Home Location Register
HSS	Home Subscriber Server
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU	International Telecommunications Union
LAN	Local Area Network
LI	Legal Interception or Lawful Interception (both terms are used)
MAP	Mobile Application Part
MExE	Mobile Equipment Execution Environment

MGW	Media Gateway
MSF	Multiservice Switching Forum
NAI	Network Address Identifiers
NAT	Network Address Translation
OAM&P	Operations, Administration, Maintenance and Provisioning
OSA	Open Services Architecture
OTAPA	Over The Air Parameter Administration
OTASP	Over The Air Service Provisioning
OTDOA	Observed Time Difference of Arrival
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAN	Radio Access Network
RFC	Request for Comments
RNC	Radio Network Controller
SAT	SIM Application Toolkit
SDR	Software Defined Radio
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Messaging Service
SMV	Selectable Mode Vocoder
SNMP	Simple Network Management Protocol
SP	Service Provider
TIPHON	Telecommunications and Internet Protocol Harmonisation Over Networks
UTRAN	UMTS Terrestrial Radio Access Network
VHE	Virtual Home Environment
WIN	Wireless Intelligent Network
XML	Extensible Mark-up Language

3.2 Glossary of terms

Accounting: Accounting answers the question “what did you do and when did you do it?”.

Applications: Applications are service enablers—deployed by operators, services providers, manufacturers or users. Applications are invisible to the user. They do not appear on a user’s bill.

Authentication: Authentication answers the question “prove that you are who you say you are?” An exchange happens between the entity to be authenticated and the authentication function, in which the entity offers proof of its identity, and the authentication function determines whether the authentication credentials are valid.

Authorization: Authorization answers the question “what may you do?” Authorization is the act of certifying or providing permission for provision of one or more services to a subscriber.

Billing (or charging): The process by which accounting information is used by the network operator to bill or charge the relevant subscriber.

Inter-administrative Domain Terminal Mobility: This level of terminal mobility refers to the ability of the terminal to move across administrative domain boundaries. The terminal may be within any wireless or fixed network.

Legacy terminals (networks): Legacy terminals (or legacy networks) are those terminals (or networks) that employ GSM MAP or ANSI 41 call signalling or location management.

Macro Terminal Mobility: This level of terminal mobility refers to the ability of the terminal to move across subnet boundaries within the same administrative domain.

Micro Terminal Mobility: This level of terminal mobility refers to the ability of the terminal to move across internal boundaries of an access network.

Node B: BTS in the 3GPP UMTS architecture.

Plug and play: This is the requirement for easy installation and configuration of a network entity, especially Node B/BTS or other Base Station/Access Point Functional Entity.

Services: Services are the portfolio of choices offered by services providers to a user. Services are entities that services providers may choose to charge for separately.

4 ARCHITECTURE REQUIREMENTS

This section provides detailed requirements for the principles described in the MWIF Architecture Principles – MWIF Technical Report (MTR-001) [1] in addition to other operator requirements. These requirements are to be used for development of the Layered Functional Architecture (MTR-003) and Network Reference Architecture (MTR-004).

4.1 Embrace Internet Technologies and Infrastructure Services

The MWIF Architecture shall adopt[1] existing or evolving Internet (IETF) protocols to extend wireless support services, inter-operate with other next generation fixed or mobile networks (commonly known as Next Generation Networks), and inter-operate with media gateways (legacy and PSTN).

4.1.1 Adoption of Internet Technologies

In order to meet the intent of this principle, the MWIF architecture shall consider the following:

- Extension of Internet technology across IP (layer 3) in access networks and core networks for both transport & control. Layer 3 is considered to be IP and should be agnostic to layer 2. Applications should not run directly on layer 2.
- Preferential adoption of suitable Internet protocols (e.g. RFC2700 [3]) where they either meet or can be enhanced to meet the functional requirements.
- Recognition that MWIF will adapt, extend, and/or promote necessary changes to relevant specifications and protocols (e.g. 3GPP, 3GPP2, IETF) to meet MWIF requirements.
- Extension of IP based signalling and transport, where appropriate, beyond the core network into the Radio Access Network, while respecting the need for spectrum efficiency in radio access networks.
- Support for connectivity from IP-based mobile subscriber to any other hosts, subscribers, web-sites, etc. on the Internet

[1] This adoption of IETF protocols is not intended to be exclusionary of other standard or protocols.

- Recognition that Network Address Translation (NAT) is not a fundamental part of the MWIF Architecture.
- Recognition that IPv6 will become the dominant protocol and that the MWIF Architecture should exclusively support IPv6, although the MWIF architecture must be capable of interworking with IPv4 networks and devices.
- Recognition that it is necessary to take measures to ensure spectral efficiency over the radio interface and that ways of reducing IP overhead, for example by introducing robust header compression, should be employed.

4.1.2 Adoption of Internet Infrastructure Services

The inclusion of the following capabilities and services are a minimum to meet the MWIF principle of embracing Internet technologies.

4.1.2.1 Mobility Management

The Mobility Management functionality shall be hierarchical and independent of other functions within the architecture. The various aspects of mobility that shall be supported are:

- Terminal Mobility

  The MWIF architecture shall support the ability of a terminal to move within and across network domains while continuing to receive access to telecommunication services. Terminal mobility shall be of three types: inter-administrative domain terminal mobility, macro terminal mobility, and micro terminal mobility.

- Session Mobility

  The MWIF architecture shall support the ability of the user to maintain sessions, including continuity of Internet sessions (e.g., http, ssl, tcp, telnet, ftp), during any discontinuity in the access network and while changing between terminal devices and/or access technologies. For example,

  1. the user of a mobile terminal shall be able to transfer a session to a laptop with DSL connection without losing a specific session;
  2. as a session transfers from an IS-2000 RAN to an 802.11 LAN via handover from one access network to another, the MWIF Architecture shall support session continuity both within the core and in interfaces to other networks.

- Personal Mobility

  The MWIF architecture shall support the ability of a subscriber to obtain services in a transparent manner within any network and on any terminal (subject to the limitations of the network and terminal) on the basis of personal identification, and the capability of the network to provide those services according to the subscriber's service profile. This mobility includes the ability of the home service provider to control the services it provides to the subscriber in a serving network. (Also known as Subscriber Mobility, SIM Roaming or Subscriber Service Mobility.)

4.1.2.2 Authentication

The MWIF Architecture shall support:

- independent authentication of both a user’s identity and a terminal’s identity
- authentication algorithms from GSM/UMTS/ANSI-41 networks
- the capability to allow un-authenticated calls (e.g. to emergency services)

- the capability for authentication, including access to user/terminal authentication processes, for e-commerce and other services must be supported at application layer (including 3rd party applications).
- separate authentication for access network and core network
- authentication with entities in other administrative domains (inter administrative domain authentication).

4.1.2.3 Authorization

Authorization for service access within the network shall be supported independently of authentication. The capabilities are required to support authorization at application level and to support separate authorization for services in home and visited networks.

Authorization shall be supported to control use of other access networks, i.e. once authenticated and authorized on one access network, additional authorization is required to move to alternative access networks.

4.1.2.4 Accounting

Accounting is the process, within the MWIF Architecture, by which use of network resources is recorded. Accounting shall record network resources used (e.g. packet count), QoS provided (e.g. bandwidth, bearer capabilities) and time and duration of provision of network resources.

The MWIF Architecture shall provide an accounting function that allows operators to perform billing and auditing functions on individual sessions. The capability shall exist for a multi-tiered, flexible accounting process (recording of resources used by packet/octet/byte count, content, session length, level of QoS provided) that is capable of handling intra-domain and inter-domain accounting. For example, the operator may adopt multi-tiered billing which may be used to provide revenue sharing among network (or multiple network) providers, content providers, ISPs, etc., and it is necessary that the accounting records provide sufficient capability for this to be undertaken.

Information shall be provided via an open interface to the network and service management functions.

4.1.2.4.1 Accounting information

It is not possible to identify charging models that network operators will use for services as part of 3G and beyond – indeed such information is likely to be commercially confidential. It can, however, be readily acknowledged that network operators will wish to adapt charging systems as the market evolves, being free to introduce innovative schemes to reflect the deployment of new services. Equally well, while traditional interconnect charges continue to exist for calls connected over the PSTN or legacy networks, it will be necessary to support destination and time dependent charging.

Network operators require flexibility in the generation of accounting information to:

- account
    - on the basis of usage of network resources e.g. QoS, packet count (in both directions), duration of connection,
    - on a non-usage basis (e.g. subscription for a given time)
    - on the basis of call or session duration and destination
    - on a fixed charge basis, e.g. fixed charge for an SMS message
    - on the basis of access to the end service or content (e.g. microcharging)
    - on a combination of the above.
- account for both mobile originated and mobile terminated calls or sessions;

- separately account for certain sessions for which a pre-paid user may have a contract subscription (e.g. WAP services);
- take into account changes in quality of service that may occur during a call or session;
- allow mobile terminated calls or sessions where there is no charge to the called party;
- allow mobile originated calls or sessions where there is no charge to the calling party;
- allow calls or sessions to certain destinations e.g. emergency services irrespective of the status of the subscriber subscription level;
- allow a change in the accounting rate after a given resource usage (e.g. first 50 minutes per day free, after which there is a charge, or first 20 Mbytes at 0.05€ / Mbyte, after which it is 0.03€ / Mbyte);
- allow collection of accounting information as the subscriber roams between network domains.

4.1.2.4.2 Support of pre-paid services

Given that the support of pre-paid subscribers is a significant part of most mobile network operators business, it is essential that the MWIF architecture supports pre-paid subscribers (in additional to post-paid contract or subscription charging). That is, the MWIF architecture shall provide the capability for real-time control of subscriber access to network resources dependent on the current level of the individual subscriber's subscription.

The MWIF architecture shall support pre-paid usage in both home and visited networks, allowing control by the home network of access to network resources in both the home and visited networks based on the current subscription level.

Accounting information shall be available such that the user can access account balance at any time.

4.1.2.4.3 Prevention of fraud

The generation of accounting information shall be such as to prevent fraudulent abuse of the accounting system by users, hackers or any other party. The architecture shall support the capability to always accurately assign accounting information against the relevant subscriber and a particular QoS, irrespective of any attempts that the subscriber might make to:

- hide the identity of the source or destination;
- pass off the packets as being from another source;
- disguise the assigned QoS; or
- otherwise attempt to defraud the network operator.

4.1.2.4.4 Accuracy, reliability and resilience

In all accounting and charging entities, especially in usage-dependent charging, it is essential that the records are accurate, are reliably produced and stored, and that the accounting system is resilient to network failures.

Traditionally, great emphasis has been placed on the accuracy of packet counting, especially in handover / handoff / re-location situations where "duplicate packet counts" have been deducted from the total packet count. Additionally, packet loss is a fact of life on the Internet and accounting systems need to ensure that the performance of accounting systems with respect to packet loss is clearly understood. The specific packet count accuracy required within an MWIF architecture is FFS.

4.1.2.4.5 Support of advice of charge

The provision of accounting information, in near real-time, detailing all network resources used, is necessary for the support of advice of charge services.

4.1.2.5 Naming, Numbering & Addressing

The MWIF Architecture shall provide the capability to separate an IP address from a subscriber name, number or device.

The name or number is used to uniquely identify the call parties whereas addresses are used to determine routing of the call or session.

Addressing will remain the link between different network technologies while naming and numbering may evolve towards higher level common identification mechanisms covering all communication systems (IP, mobile, fixed). The MWIF Architecture should support such evolution.

Although a called party may be addressable via different means, the MWIF Architecture should allow the user to be reachable through a given name, independent of his location.

The MWIF Architecture shall support:

- static and dynamic IP addresses for mobile terminals
- associating public IP addresses with mobile terminals
- associating private IP addresses with mobile terminals
- mapping Network Access Identifiers (NAI) to mobile terminals
- connection of subscribers to private IP networks
- mapping between subscriber number (e.g. E.164) and IP addresses or URLs.

4.1.2.6 Quality-of-Service - Support in the Infrastructure for QoS

The MWIF Architecture shall allow Service Providers to select QoS support and implementations.

See section 4.7, Quality and Reliability, for more detail on QoS.

4.1.2.7 Session Management

The MWIF Architecture shall support the function of Session Management including the ability to provide:

- call state for isochronous (real-time) communication association between two or more entities;
- call state for non-isochronous (non-real-time) communication association between two or more entities;
- The MWIF Architecture shall support mobility management, security management, resource management and service control functions in support of a call or session.

4.1.2.8 Policy and Profile Services

4.1.2.8.1 Network Policy

The MWIF Architecture shall support the capability to implement business, network and service policy in accordance with specified policy rules. As such, the MWIF architecture shall support the storage and provisioning of the data necessary for the implementation of these, policies, together with capability to implement the specified network policies. The scope of the network policies includes, but is not limited to:

- Provision and support of QoS
- Interconnection with other networks
- Provision of, and access to, services
- Provision of service under varying network load conditions.

4.1.2.8.2 Profile Services

The MWIF architecture shall support the capability to store and manage subscriber/user profile information. Such profile information may include, but is not limited to:

- Subscriber identity (e.g. names, addresses)
- Subscriber service preferences (e.g. call presentation, diversions, barring)
- Subscriber preferences (e.g. language, call alerts)
- Subscriber terminal capabilities (e.g. display capabilities, access capabilities)
- Authorised services
- Authorised bearer and access capabilities (including QoS)
- Authorised roaming capabilities

4.1.2.9 Resource Management

The Resource Management function manages status, tracking, allocation and de-allocation of network or other resources required for the subscriber’s service to be implemented according to business and subscription policy.

Resource Management for roaming users shall comply with the following:

- Network resources in networks supporting roaming (visiting) users shall not be controlled by the user's home network;
- Resources in the visited network should be managed by that visited network;
- Network operators should not be required to reveal internal network structure to other networks; and
- Networks should not need to identify explicit IP addresses of nodes within their networks except for gateways and firewalls.

4.1.2.10 Service Control

In the MWIF Architecture, all service logic (e.g., providing value-added voice and data services and classical supplementary services) shall be separated from the Session Management function. Interaction between Service Layer functional entities (service logic, service creation and service management) and Control Layer functional entities shall be supported by open interfaces.

4.1.2.11 Directories/Databases

Any implementation of the MWIF Architecture will use several parameters including user and device identity, service authorization, inter-administration business profiles, service profile, location information and policy data. These data shall operate on database systems which are scaleable to network and subscriber growth and operate with open interfaces to other MWIF Architecture Service and Control Layer functional entities that interact with such data.

4.2 Separation of Services, Control and Transport

The MWIF Architecture shall support a layered logical architecture to include the following layers (note that this requirement is the basis for the Layered Functional Architecture in MTR-003):

- Transport (Access and Core) Layer
- Control Layer
- Service Layer

- Application Layer

4.2.1 Logical Separation of User Transport and Control

The purpose of logical separation of user transport (bearer) and user control (signalling) is to allow the network operator to scale the transport and control functions of the network independently of each other. Scalability of a compliant network is considered essential since user bearer traffic may increase at a different rate from the signalling associated with control of that traffic. That is, it is impossible to accurately predict whether the dominant traffic in the future will be short duration sessions, with a high signalling overhead, or whether there will be long, high bit rate, sessions with minimal signalling overhead.

4.2.1.1 Media Gateways And Control

The separation of media gateway functions and media gateway control functions is necessary to support multi-vendor equipment deployment, alignment with the work of other bodies (e.g. MSF and TIPHON) and both wireline and wireless legacy network interoperability.

This is to ensure that separation of bearer from signalling (control) traffic is maintained in the interfaces to other networks including wireline legacy and wireless legacy (ANSI-41 and GSM-MAP) networks. This will allow flexibility in the use of media gateway resources within the network.

4.2.2 Separation and Independence of Logical Functions

The MWIF Architecture, based on this requirements document, will be populated with many entities within the layers. The operators believe that separation of these functions will allow for an implementation of the MWIF Architecture that maintains the most flexibility and scalability of network entities. To the maximum extent possible the MWIF Architecture shall require that the following functions be logically separate and independent, both within a logi cal layer and across logical layers:

- Session management
- Mobility management
- Service control
- Gateway control
- Gateways (access, media and signalling)
- Authorization, Authentication and Accounting – i.e., the objective is that the traditional AAA function should be separated into its component parts and distributed across the logical layers as appropriate
- Database system(s) or Unified Directory System
- Policy management
- Resource manager
- Address management

For example, Session Management should be independent of mobility specific information. This allows communication sessions to be transparently maintained irrespective of the movement and/or location and network connectivity of the terminal or user.

The implementation of Mobility Management within the MWIF archi tecture shall not prevent the service provider or network operator providing a set of common features across the various access networks.

4.2.2.1 Independence (Floating) of Vocoder and Transcoder Functions

The MWIF Architecture shall support flexible vocoder (coded speech, e.g. EVRC, SMV, AMR) and transcoder (ability to translate between vocoder types) placement in order to allow operators to place these functions in the most practical, cost-effective part of the network. The MWIF Architecture shall support tandem-free and transcoder free operation (i.e., to avoid unnecessary conversion to-and-from 64Kbps for a voice session that originates and terminates on mobile terminals with the same vocoder technology).

4.3 Open Interface Requirements

The MWIF Architecture shall use open interfaces between any network entities that may be implemented by operators/ISPs and manufacturers as separate systems, sub-systems, or network entities. This includes RAN Internal/external interfaces and Core Network Interfaces.

4.3.1 Access Networks

The MWIF Architecture shall support open interfaces between the core network and the access network and open interfaces for network and service management.

To ensure compatibility with existing mobile networks, the architecture shall provide direct support for open A and Abis interfaces within the 3GPP2 RAN and Iu, Iur and Iub interfaces within the 3GPP UTRAN and GERAN.

4.3.2 Core

The MWIF Architecture shall support the following:

- Open interfaces between the functional entities
  - Session management
  - Mobility management
  - Service control
  - Gateway control
  - Gateways (access, media and signalling)
  - Authorization, Authentication and Accounting
  - Database system(s) or Unified Directory System
  - Policy management
  - Resource manager
  - Address management
- Open interfaces for network and service management

The MWIF Architecture should be designed to minimize the number of signalling interfaces between administrative domains.

4.4 MWIF Core Network Independence of Access Technology

The MWIF Architecture shall be designed to ensure that a common core network can be used with various wireless access technologies (cdma2000, W-CDMA, Wireless LAN, etc.) and wireline access technologies (xDSL, Cable, Digital Broadcast, etc.). The Core Network is required to be independent of access technology. Access technology specific entities in the Core Network should be discouraged.

The MWIF Architecture shall support:

- A unified, IP-based access and core network that can serve as a single, common network architecture for all 3G and IMT-2000 air interface technologies;
- An access-independent core network subsystem (identical to the "core network" portion of the above integrated access/core network) that can serve different access network technologies, both wireline and wireless.

Independence allows harmonisation of core network equipment throughout various networks. This is a key design goal as operators' networks expand within and across regional boundaries.

4.4.1 Independent Evolution of Core Network And Access Networks

The MWIF Architecture shall support transport independence. That is, layer 3 shall be independent of the underlying transport mechanism (layer 1 and layer2). Furthermore the MWIF Architecture shall be such that network operators shall have the freedom to utilise any combination of layer 1 and layer 2 transport technologies.

4.4.2 Common Core Network Mobility Management Function Independence of Access Technology

The MWIF Architecture shall support a core network mobility management function that enables mobility across all access technologies. The mobility management function must be flexible; supporting deployment of new access technologies and upgrading of access networks independent of core network enhancements.

4.4.3 Common Core Network Mobility Management Function Which Supports Session Mobility between Access Networks

The MWIF Architecture shall support a core network mobility management function that supports session mobility across different access technologies. That is, mobility shall be supported across heterogeneous networks in addition to homogeneous networks,

4.4.4 Independence of Media and Access Gateways from Core Network

The MWIF Architecture shall be designed such that it shall be possible for any server to request resources of any media gateway (MGW) within the same administrative domain. It shall be possible, within an administrative domain, for any access gateway to provide signalling connectivity to any server and bearer connectivity to any media gateway.

4.4.5 Support Of Independent Wireline Or Radio Access Networks

It has been considered whether the MWIF architecture should support the capability for network operators to implement either wireline or radio access networks independently of a core network, such that core network provision is under the control of third parties.

The MWIF architecture shall, where feasible, support the capability for both wireline and radio access networks to be deployed independently of core networks, allowing for the session control and service provision to be provided by third parties.

4.5 Global Alignment

4.5.1 Eliminate Regional/Country Differences In Key Interfaces

The objective of the MWIF Core Network Architecture (control and services) shall be to eliminate regional or country differences in any open interface between the functional entities identified within the MWIF Layered Functional Architecture (MTR-003). Therefore, the MWIF Architecture is required to meet this objective.

4.5.2 Global Access to Services

The MWIF Architecture shall support global access to services when roaming regardless of access type.

In order to ensure the widest level of services for subscribers, the MWIF Architecture should support globally accessible services within the capabilities of the terminal, access technology and the serving network, via:

- the support of common protocols and open APIs
- the support of concepts such as VHE
- a common representation of user service profiles (i.e., XML)
- access to services from any network or server utilising service brokering (i.e. the user can negotiate access to services from servers or 3 rd party networks that are neither in the home nor visited network)

4.5.2.1 Service Provision For Roaming Users

Network operators wish to provide roaming users with services from the home network (that are identical to those available in the home network) as an alternative to the provision of services by the visited network.

- The capability should exist within the MWIF architecture to provide services from the home and visited networks
- The decision as to the source of service provision should reside with the home network
- The visited network should provide access to services provisioned from the home network
- The visited network must provide emergency service support
- The MWIF Architecture should support the capability for the visited network to provide local services (e.g. local information services)

4.5.3 Interoperability With Legacy (2G/3G) And Non-IP Networks And Services

The MWIF Architecture shall provide the capability to receive calls from, and terminate calls to, circuit switched networks that include PSTN, ISDN and PLMN (MAP, ANSI-41).

4.5.3.1 Interoperability With Legacy (2G/3G) Networks

The MWIF Architecture shall provide support for roaming users and roaming terminals (with appropriate multi-mode and multi-band functions). This shall include roaming between IP based and non-IP based networks.

In this respect, the MWIF Architecture shall support interworking with both MAP signalling (GSM MAP and ANSI-41) of legacy (2G/3G) networks.

4.5.3.2 Support For Legacy (2G/3G) Mobile Terminals

The MWIF Architecture shall support mobile terminals designed to operate in the packet switched domains of the 3GPP and 3GPP2 architecture.

It is recognised that:

- there are a large number of legacy terminals currently in existence that are designed to operate with circuit switched (MAP/ANSI-41) networks;
- that many operators have a significant deployment of, and investment in, circuit switched (MAP/ANSI-41) networks;

- that circuit switched (MAP/ANSI-41) networks are likely to exist in parallel with packet (IP) based networks;
- that as 3G networks are deployed, terminals are likely to support dual modes of operation, including MAP/ANSI-41 and IP (SIP) call/session control;
- that most users change their terminals frequently (within 2-3 years);
- network operators wish, in the long term, for a single, packet (IP) based, core network that will eventually supersede the existing circuit switched (MAP/ANSI-41) networks;
- network operators may, over time, migrate their users from their existing circuit switched (MAP/ANSI-41) networks to packet (IP) based networks as service capabilities evolve;
- that operators will have to control their own migration from circuit switched (MAP/ANSI-41) to packet (IP) based and that these migration strategies may be operator dependent.

As a result, it is not a requirement to support legacy terminals within the MWIF architecture since the capability will exist to migrate users from legacy networks to packet (IP) based networks aligned with the MWIF architecture, although the precise migration strategy is outside the scope of MWIF.

NOTE: Consideration has been given to the requirement to hando ver calls in progress between circuit switched (MAP/ANSI-41) networks and packet (IP) based networks[2]. This may be needed, for example, either to maintain a voice call if a user moves out of packet (IP) coverage while legacy circuit switched (MAP/ANSI-41) coverage exists, or if a user, having initiated a call on the legacy circuit switched (MAP/ANSI-41), wishes to invoke multimedia services only available on the packet (IP) network. The technical complexity of seamlessly implementing such a handover is, however, recognised, given that such handovers would only be necessary during the migration period between circuit switched (MAP/ANSI-41) networks and packet (IP) based networks. As such, there is no requirement for such handovers.

4.5.3.3 Legacy Services

The MWIF Ar chitecture shall allow operators to implement a set of 2G compatible services that meet their business needs. That is, the Architecture shall provide the capabilities for the network operator to implement a set of services that are compatible with 2G servi ces and that may appear to the user as identical to the 2G services; however these services may be implemented in a different manner within the network.

4.5.3.4 Handoff (Handover)

The MWIF Architecture shall support handoff (handover) of IP based services and bearers both to and from the packet switched domains of legacy 2G and 3G networks for legacy 2G and 3G mobile stations.

4.5.3.5 Interoperability with PSTN

The MWIF Architecture shall support interworking with the PSTN signalling and bearer capabilities.

4.6 Scaleable, Distributed Architecture

4.6.1 Scaleable Architecture

The MWIF Architecture shall provide network operators the ability to expand specific functions within the network without unnecessary expansion in other functions. As such, all functional entities

[2] This has been an ongoing topic of discussion within 3GPP SA1 and SA2, however the capability for this is not supported within 3GPP release 5.

defined within the MWIF Layered Functional Architecture should be capable of expansion independently of other entities. The architecture should support the capability for this expansion to occur on distributed platforms rather than within a single platform.

In addition, the MWIF Architecture shall be defined such that it allows network operators to gradually deploy network entities and to migrate existing networks towards the MWIF Architecture.

4.6.2 Promote Distributed Functional Entities

The MWIF Architecture shall, by virtue of a distributed design, support the decomposition of monolithic functionality into a distributed IP based system, thus enabling a far more scaleable, open network, with open, standardised interfaces.

To achieve this, each functional entity defined within the MWIF Layered Functional Architecture should be capable of being deployed on a stand-alone platform, connecting to other entities through the open interface. In addition, each functional entity should in itself be capable of being deployed across multiple platforms, to aid scalability and resilience.

4.7 Quality and Reliability

4.7.1 End-To-End Quality-Of-Service Mechanism For Any Given Service

The MWIF Architecture should support management and control of QoS for a wide variety of services at the appropriate places within the architecture - recognising that QoS is implemented in many places within both the Core Network and Access Networks.

- The MWIF Architecture shall support QoS bearer capabilities for the following classes
  - Conversational class
  - Streaming class
  - Interactive class
  - Background class

as defined in draft revision to Recommendation ITU-R M.1079 [2].

- The MWIF Architecture shall be capable of simultaneously providing multiple QoS levels to different applications within the same terminal.
- The MWIF Architecture shall provide the means to support end-to-end[3] QoS. That is, it shall support protocols for the control and negotiation of QoS when operating with a third party provided service platform (the Operator and 3rd Party are both required to ensure that the network entities under their respective control provide the necessary component of QoS). QoS across administrative boundaries is enforced by both network techniques and business policy enforcement between companies.
- The MWIF Architecture shall provide a scaleable QoS. That is, the process used to implement QoS within the MWIF Architecture shall be capable of the flexible support of additional QoS bearer attributes and the assignment of specific (preferred) values to these attributes in order to address evolving capabilities within the core and access networks.
- The MWIF Architecture should be capable of supporting multiple levels of static QoS (negotiation of parameters before the session setup) as well as dynamic QoS (negotiation of parameters while the session is in progress).

[3] end to end in this context means from terminal to the termination point of the call or session

4.7.2 Reliability

Platform, element and system (or sub-system) reliability is driven by a combination of Operator, subscriber, and regulatory needs (e.g., emergency services). The MWIF Architecture should support the necessary functionality to ensure that the necessary reliability can be achieved. That is, the MWIF Architecture shall provide the capabilities to support a deployment of network entities such that in the event of the failure of a single entity, the performance of the network is not seriously degraded.

Specification of precise reliability figures is outside the scope of this Technical Report.

4.8 Security

NOTE: The architecture of a network plays only a part in ensuring the integrity and security of a network. Other aspects such as physical security of buildings and network resources, personnel management, password management and an operator's security policy all contribute to the security of a network. These aspects are, however, outside the scope of the work of MWIF.

4.8.1 Adopt Internet Trust (Security) Models

The MWIF Architecture shall employ multi-layered security, dependent on requirements of the application. That is, the MWIF Architecture shall support Internet Authentication and Authorization protocols. In the case of roaming subscribers, this shall include implementation of Authentication and Authorization in the visited, as well as the home, network.

4.8.2 Support Authentication, Confidentiality, Integrity, Non-Repudiation

The MWIF Architecture shall support:

- Mutual authentication (subscribers, 3rd party services, etc.)
- Confidentiality
- Integrity
- Non-repudiation
- Encryption
  - This should be sufficiently flexible to support different algorithms at an appropriate level to satisfy customer and 3rd party needs
- Data protection (rights of access, privacy)
- Fraud information gathering system

4.8.2.1 Security Log

The MWIF architecture shall support the capability to generate a security log containing information sufficient for after-the-fact investigation of loss or impropriety. The security log should, as a minimum, be capable of recording events such as:

- all sessions established,
- invalid user authentication attempts,
- unauthorized attempts to access resources (including data and transactions),
- changes in users' security profiles and attributes,
- changes in access rights to resources,
- changes in the network element security configuration,

- modification of network element software.

For each such event, the record should, as a minimum, include date and time of event, initiator of the event such as: user-ID, terminal, port, network address, etc., names of resources accessed, and success or failure of the event.

4.8.3 Objectives And Security Features

The following sections identify the security objectives and security features to be supported within the MWIF architecture.

4.8.3.1 Objectives

The MWIF architecture shall be designed to meet the following objectives:

- ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation;
- ensure that the resources and services provided by serving networks and home environments are adequately protected against misuse or misappropriation;
- ensure that the security features standardised are compatible with world-wide availability. (There shall be at least one ciphering algorithm that can be exported on a world-wide basis (in accordance with the Wassenaar agreement));
- ensure that the security features are adequately formulated and standardised to ensure effective world-wide interoperability and roaming between different serving networks, as well as preventing misuse or misappropriation of network resources by roaming subscribers;
- ensure that the level of protection afforded to users and providers of services is better than that provided in contemporary fixed and mobile networks;
- ensure that the implementation of current security features and mechanisms can be extended and enhanced as required by new threats and services.

4.8.3.2 Security Features To Be Supported In The MWIF Architecture

The following security features shall be supported within the MWIF architecture.

- subscriber identity (IMSI) confidentiality;
- subscriber identity (IMSI) authentication;
- user data confidentiality on physical connections;
- connectionless user data confidentiality;
- signalling information element confidentiality
- user location confidentiality (unless authorised by the user).

Use of these security features is at the discretion of the operator for its own subscribers while on the home network. For roaming subscribers, use of these security features is mandatory unless otherwise agreed by all the affected PLMN operators

4.8.3.3 Security Threats To Be Countered By The MWIF Architecture

The MWIF Architecture shall support functionality intended to counter:

- Unauthorised access to sensitive data (violation of confidentiality)
    - Eavesdropping: An intruder intercepts messages without detection.
    - Masquerading: An intruder hoaxes an authorised user into believing that they are the legitimate system to obtain confidential information from the user; or an intruder hoaxes a

legitimate system into believing that they are an authorised user to obtain system service or confidential information.

- Traffic analysis: An intruder observes the time, rate, length, source, and destination of messages to determine a user's location or to learn whether an important business transaction is taking place.
- Browsing: An intruder searches data storage for sensitive information.
- Leakage: An intruder obtains sensitive information by exploiting processes with legitimate access to the data.
- Inference: An intruder observes a reaction from a system by sending a query or signal to the system. For example, an intruder may actively initiate communications sessions and then obtain access to information through observation of the time, rate, length, sources or destinations of associated messages on the radio interface.

- Unauthorised manipulation of sensitive data (Violation of integrity)
  - Manipulation of messages: Messages may be deliberately modified, inserted, replayed, or deleted by an intruder
  - Manipulation of databases: Databases may be deliberately modified, or records deleted by an intruder
- Disturbing or misusing network services (leading to denial of service or reduced availability)
  - Intervention: An intruder may prevent an authorised user from using a service by jamming the user's traffic, signalling, or control data.
  - Resource exhaustion: An intruder may prevent an authorised user from using a service by overloading the service.
  - Misuse of privileges: A user or a serving network may exploit their privileges to obtain unauthorised services or information.
  - Abuse of services: An intruder may abuse some special service or facility to gain an advantage or to cause disruption to the network.
  - Repudiation: A user or a network denies actions that have taken place.
- Unauthorised access to services
  - Intruders can access services by masquerading as users or network entities.
  - Users or network entities can get unauthorised access to services by misusing their access rights
- Defrauding of accounting system
  - Users can pass themselves off as someone else, or hide their identity, in order to avoid billing charges to their account (and pass charges on to other accounts)
  - Users can make the accounting system believe that they are using a quality of service different from the actual one they are using.
- Use of stolen SIMs or terminals
  - SIMs or terminals may be stolen and used by unauthorised persons

4.8.4 Legal Interception

Legal (lawful) intercept is, in many cases throughout the world, a mandatory requirement included in the licences of network operators. As such, the operators cannot ignore this requirement and hence the capability for supporting legal intercept shall be implemented in the MWIF architecture. It is recognised, however that the precise mandatory requirements will differ depending on the jurisdictions throughout the world.

The MWIF architecture shall provide one, or more reference points within the architecture that allows for the interception of information (packets). These reference points shall allow for the:

- reception and authentication of interception authorisations from the applicable interception authority and initiate interceptions;
- transparent interception of communications such that the target is unaware of the interception;
- provision of different levels of interception, e.g.
    - call / session information only, i.e. source, destination, time of call or session;
    - call / session information and content;
    - terminal location;

NOTE: It is recognised that the user may encrypt the content of the session. In many cases it may be beyond the capability of the network operator to decrypt the session content, however the requirement may still exist to provide content of the intercepted communication.

- identification of the target (e.g. IP addresses and/or number, accounts, aliases) and attachment status;
- management and interception of all calls / sessions of the target, including simultaneous sessions, that are within the scope of the authorised intercept;
- verification of the intercepted material as stated on the authorisation, discarding any material not within the scope of the authorised intercept;
- maintenance of a secure record of interception activities and the transmission of this to the appropriate authority;
- running and management of multiple simultaneous intercepts on different targets;
- routeing of the intercepted material to the appropriate destination identified by the interception authority;
- ensure security and privacy of the intercepted information such that only specifically identified information is available to the interception authorities.

4.9 Network and Service Management[4]

4.9.1 Requirements for a Mobile Wireless Internet Network and Service Management

In principle, the high level requirements for the network and service management of a mobile wireless Internet are that it should:

- provide the means by which the behaviour and or status of the network or its services can be known at an acceptable practical level;
- be capable of realising network-wide management policies through appropriate translation of policies into device-level abstractions and vice-versa,

[4] MWIF has taken the decision to consider the topics of OAM&P under the heading of network and service management. The issues of security and accounting/charging, frequently considered under the heading of OAM&P are discussed in detail elsewhere in this report.

- be highly automated network and service management platform with well defined human interfaces, processes, functions, data, and necessary flow through for automation,
- be secure and provide means of protecting the network and subscriber resources, and data against unauthorized modification by customers or unauthorized personnel, i.e., it should provide
    - means of secure communications with and among management entities, and
    - means of access control to management system objects, etc.,
- provide a comprehensive network and service management platform for supporting necessary configuration, performance, fault, security, and accounting/billing management functions over multiple temporal scales (e.g., real-time response, long term maintenance) in accordance with the business practices of operators and/or providers,
- strive to remain as “technology independent” as possible,
- utilize a common information model for defining the objects, modules, etc., across different management functions as well as different technology platforms, and maintain common databases for managed objects,
- be scaleable and allow that the growth of network and service management parallels the expansion of the underlying network and service infrastructure as necessary with minimal disruption in current subscribers’ services,
- be built upon relevant IETF network management protocols (e.g., SNMP, COPS, etc.) within both the core and access networks, and re-use relevant ongoing work in other forums to the extent possible,

NOTE: In practice, operators may continue to use their existing network and service management systems in a mobile wireless Internet for some time, especially in those areas specific to wireless access. However, this requirement is consistent with the spirit and letter of MWIF architectural principles [1] as well as the precedent in MWIF’s decision to use IETF protocol as the basis of its signalling architecture.

- take into account ongoing work in other fora, e.g. TMF, 3GPP TSG-SA WG5 and 3GPP2 TSG-S WG2,
- be interoperable with the network and service management of wireline Internet as well as those of the PSTN, and
- support legal intercept, i.e., allow authorized surveillance to be carried out and ensure that only those with absolute need to know and with proper clearance know what surveillance is actually carried out.

4.9.2 Functions of a Mobile Internet network and service management

The functions of a network and service management system can be broadly divided into five specific categories; these are:

- Fault Management
    - Including fault detection, reporting and recovery procedures
- Configuration Management
    - Including remote configuration capabilities
- Billing Management / Accounting Management

  - Accounting is the process, within the MWIF Architecture, by which use of network resources is recorded (see section 4.1.2.4) and the applicable call detail records (CDRs)[5] passed to the billing system. The process of charging and billing for use of these network resources is under the control of individual operators and is outside the scope of MWIF.

- Performance Management
  - Including traffic measurement, congestion detection and reporting
- Security Management
  - While security is important within the context of network and service management, security is not specific to this area and is relevant to many areas within the MWIF architecture. Security, pertinent to the whole of the network architecture, is considered elsewhere in this report (see section 4.8).

An important issue that relates to all these tasks is that the MWIF architecture should support means of service and network management over multiple temporal scales. In principle, a network and service management should support dynamic real-time actions such as reconfiguration through protection switching), quasi-dynamic actions (e.g., several hour time span) such as updating the subscription profiles, and "static" actions such as periodic preparation of subscribers' bills. In general, multiple time scales are supported through different applications (i.e., policies) using different subsets of the available information/data. These applications are operator-specific (probably proprietary too) and are not subject to standardization, though the network and service management data should contain sufficient information for supporting such applications.

4.9.2.1 Fault Management

Fault management is responsible for detection, isolation and recovery of the network from failures. It also collects information about and manages the errors/faults occurred in and alarms raised by the network and/or its elements. More specifically, the fault management tasks include

- Service, network , and element outage reporting;
- Alarm surveillance, namely, status monitoring, fault detection, correlation and reporting;
- Fault isolation or localization through alarm analysis, and their correlation with reported outages and performance degradations;
- Fault recovery through either
  - requesting the configuration management to reconfigure the network (e.g., re-routing around the point of failure) or one of its elements (e.g. activating a standby); or
  - scheduling and dispatching of the repair force;
- Testing, e.g., performing periodic audits;
- Trouble administration, i.e. reception of trouble reports from subscribers, and responding to them appropriately.

4.9.2.2 Configuration Management

Configuration Management is responsible for network provisioning, subscriber profile management, and configuration of network elements (e.g., routers, network servers) as well as the relations among them. In a mobile wireless Internet, this module should perform network as well as subscriber configuration management tasks.

The network configuration management supports:

[5] The IPDR forum is investigating data records for IP operational support.

- Reconfiguration and update of network transport, control and service layer elements (e.g., servers, gateways, routers, etc.) in the network as necessary,
- Management of the address space and IP address manager,
- Provision, translation, and enforcement of network wide configuration management policies in coordination with other network and service management modules
- Network provisioning, including
    - Radio network planning including frequency allocation, cell configurations, "optimal" placement of BTS for maximum coverage, power control, etc.,
    - Forecasting the traffic growth, and planning and network sizing for growth and upgrading of the radio access network and as well as the CORE,
    - Reconfiguration of the RAN or CORE network topology in response to events and triggers from other network and service management (e.g., fault management, and performance management) modules.
- Auto-discovery and inventory of network elements in detail,
- Auto-mapping of the network topology,
- Automatic configuration and initialization of the network and its services including the configuration and initialization of transport, control, and service layer elements,

The subscriber configuration management tasks include but not necessarily limited to

- Configuration of subscriber terminals upon subscription, including assignment of the terminal ID, subscriber ID, IP address, etc.,
- Preparing the subscriber profile and storing it in the profile server,
- Auto-configuration of subscriber terminal as necessary,
- Updating the subscriber profile by the authorized personnel or subscriber as necessary.

4.9.2.2.1 Over-the-Air Service Provisioning (OTASP)

The MWIF Architecture shall support over the air activation and provisioning of services, such as terminal code download of preferred roaming lists, configuration of software defined radio (SDR), MExE, SAT upgrades.

4.9.2.2.2 Over-the-Air Parameter Administration (OTAPA)

The MWIF Architecture shall support over the air parameter administration (e.g. mobile identity).

4.9.2.2.3 Profile Management

The MWIF architecture shall support open interfaces to the various Directories and Databases, including the Policy Data Repository, contained within the architecture, in order to allow:

- management by the network operator of:
    - the subscriber/user/service profiles;
- management by the subscriber/user of:
    - the subscriber and service profile (subject to the necessary authentication and authorisation).

4.9.2.3 Billing Management / Accounting Management

Billing Management is responsible for collection, storage, and processing of all necessary data for billing network services according to the value chain. Specifically billing management performs the following tasks:

- Retrieves (or receives), stores, and processes the accounting records from the Accounting Server to sort, determine and consolidate each customer's usage of each subscribed service,
- Prepares subscribers' bills, and collects them,
- Sets the operator or providers' pricing and charging policies taking into account laws, regulations, operator's investments and market place conditions, etc.,
- Handles delinquent accounts through periodic reminders or requesting the configuration manager to suspend subscriptions,
- Analyzes accounting records to forecast future demand for services as well as adapts the operator's service portfolio, pricing policies, and marketing practices to enhance the operator's competitiveness and profitability.

Billing management, beyond the potential definition of the interface between the accounting server and the billing management system is outside the scope of the work of MWIF.

It must be recognised that charging and billing information is currently transferred between roaming partner's using the GSM Association's TAP3, allowing access to in excess of 120 roaming partners. TAP3 can be run over IP transport but is not an IETF protocol. Protocols relating to the exchange of charging and billing information between roaming partners are outside the scope of MWIF.

4.9.2.4 Performance Management

Performance Management is comprises of all functions - data collection, analysis, comparison and reporting - necessary to ensure QoS and efficient use of resources in the network. The performance management module provides means of:

- Performance quality assurance to set and assess the network QoS policies,
- Performance monitoring for event correlation and filtering, and threshold crossing alerts,
- Setting, assessing, and updating of the network traffic management policies, and
- Performance analysis to
  - make recommendations on performance improvement, traffic demand forecasting for network expansion,
  - obtain subscriber's service and traffic summary, and
  - traffic exception and capacity analysis, and network performance characterization.
- Setting network wide quality assurance policies;
- Translating the quality assurance policies into end-to-end reliability, availability and survivability (RAS) criteria for the network, as well as RAS criteria for network elements;

4.9.2.5 Security Management

Security Management is responsible for maintaining the network security infrastructure (e.g., passwords, security credentials). The functions of the security management module include but not limited to

- Setting network-wide security policies and data
- Preventing security breaches through restricting access of unauthorized users to management information and capabilities,

- Detecting security breaches such as unauthorized access, corruption of data, customer fraud, and unauthorized actions through security alarm surveillance, traffic monitoring, and monitoring of subscribers usage patterns,
- Containing the damage to the network and users through isolating viruses that corrupt the data as well as revoking unruly subscribers' privileges to prevent them from performing certain activities,
- Managing, establishing, and updating security infrastructure, credentials and privileges, e.g., key management, frequent password updates, and maintaining password files,
- Performing regular audits to detect breaches, contain them, restore the services and re-instate integrity of the network.

For more detailed requirements on security see section 4.8.

4.9.3 Secure Network and Service Management Interconnection

MWIF network elements shall provide means for remote management, maintenance and communication with network and service management systems (e.g. the billing system). Often an operator's corporate computer network is used for this purpose; while this may considerably lower infrastructure costs, it poses significant security threats for MWIF network entities. As a principle, the MWIF shall support the logical separation of network entities from any operator's corporate computer network that may be used for network and service management purposes. All network and service management input ports of the MWIF architecture (including direct, dial-up and network access) should support authentication of a session requester, without any provision for a bypass mechanism.

4.10 Services

4.10.1 Services And Service Types

The MWIF Architecture shall support the capability for a wide range of services, including real-time, non-real-time, multi-media services. The MWIF Architecture shall support:

- Real-time speech of a quality no worse than 2G networks (e.g. GSM EFR codec). (While speech quality in circuit switched networks is generally dependent on vocoder capability, rather than network capabilities, this may not be the case in packet based networks where the QoS provided by the network may have a significant impact on speech quality)
- Point-to-Multipoint Services
    - IP Broadcast, IP Multicast
- Multiple concurrent bearer services to the mobile subscriber as well as fixed subscriber
- Basic SMS services compatible with legacy (2G/3G) networks i.e. point-to-point and cell broadcast
- Enhanced SMS, supporting simple text formatting, user defined pictures, predefined and user defined sounds and animation
- Capabilities to provide support for legacy services (see 4.5.3.3)
- Location services (geographic position information)
    - Acquisition of geographical position information via a variety of techniques, e.g. network position determination equipment, Cell-ID, OTDOA, GPS assisted, depending on the positional accuracy required and the capabilities of the mobile terminal
    - The transfer of geographical position information to applications to enable provision by the network operator and/or service provider of location-based services
    - The transfer of geographical position information to emergency services

- Personalised Services based on Network Provided Identity
  - The provision of the network authenticated identity to applications to enable support of personalised services
- Calling Line Identification (CLI) services
  - Including CLIP, CLIR
- Support external service platforms
  - The MWIF architecture shall support separate service platforms for the provision of services such as voice-mail, messaging services, personal assistant services
- Support of CAMEL and WIN
  - The explicit support of CAMEL and WIN in the MWIF architecture is not recommended since they are not considered to be access network independent and the supported capabilities can be implemented by other, more access independent, methods.
  - The support of CAMEL and WIN may, however, be needed by certain networks on a transitional basis as network operators migrate from their existing networks to MWIF based architectures. Details of these migration paths are, however, outside the current scope of the work of MWIF.

This is not an exhaustive list of services, rather an indicative list illustrating the types of services that the MWIF architecture shall be capable of supporting.

4.10.2 Service Provision by the Home and Visited Network

4.10.2.1 Home network

Given that the objective of the MWIF architecture is to support service provision to roaming subscribers from the home network, it shall be possible for the home network to:

- Control access to services depending on the location of the user, and serving network;
- Control access to services on a per user basis e.g. subject to subscription;
- Control access to services depending on available service capabilities both in the serving network and in the terminals;
- Manage service delivery based on for example end to end capabilities and/or user preferences;
- Request version of specific services supported in serving network and terminal;
- Request details (e.g. protocol versions and API versions) of available service capabilities supported in the serving network, and terminals;
- Define the scope for management of services by the user, for services provided by the HE;
- Inform the serving network of the type of charging (i.e. prepaid or/and postpaid) for any required service;
- Inform the serving network of the threshold set for a given service required by the user and charged on a prepaid account;
- Inform the serving network how to manage a service for which the threshold has been reached;
- Manage the prepaid accounts (e.g. increase, decrease the credit, or pass the information to any application which manages the credit);
- Deploy services to users or groups of users;
- Manage provision of services to users or groups of users.

4.10.2.2 Visited network

In supporting service provision via the home network, it shall be possible for the visited network to perform the following:

- Provide the necessary service capabilities to support the services from the home environment as far as possible;
- Dynamically provide information on the available service capabilities in the visited network;
- Provide transparent communication between clients and servers in terminals and networks;
- Request the charging information (type of charging, threshold for prepaid services and behaviour if the threshold is reached) for any service possibly required by the user;
- Handle the call according to the instructions received by the home environment regarding charging activities;
- Inform the home environment of the chargeable events (e.g. send CDRs).

4.10.3 Service Provision through Open Interfaces

The MWIF architecture shall support the development and provision of services at the application layer, e.g. in a service execution environment, through the support of open interfaces, e.g. APIs, to network resources and databases.

4.10.3.1 Service Execution Environment

The MWIF architecture shall support a service execution environment that will allow applications to be run on a service platform provided by the network operator. The architecture shall allow, at the operator's discretion, for applets or other code to be executed on network elements.

NOTE: Development of the applications can be undertaken independently of the service execution environment.

4.10.3.2 Service interfaces

The requirements of the service interface are:

a) To provide a common interface between the applications and the underlying network that:

  - is independent of the core network and access network technology;
  - is independent of the specific network configuration;
  - is agnostic to changes in the network configuration;
  - is independent of specific protocols used within the network
  - is readily extensible by the network operator to meet specific requirements;

b) To provide controlled and/or restricted access (via authentication and authorisation) to network resources in line with policies defined by the network operator;

c) To support the transfer of accounting and billing records between the network and the application in respect of network resources used by that application;

d) To allow applications to be ported across different networks and to operate consistently across those networks;

e) To support service registration and discovery procedures, so that an application determine the service interfaces that are available;

f) To provide a standard, widely understood, interface that encourages the provision of services by different parties.

In practice there may be several levels or types of service interfaces supported by the network to allow various types of service to be developed.

The MWIF architecture shall support open interfaces from between the services and transport layers as well as between the control and transport.

4.10.3.3 Database interfaces

The MWIF architecture shall support open interfaces from the applications layer to allow applications controlled read and write access to network directories or databases (e.g. subscriber identities, service preferences, terminal capabilities, authorised services and capabilities) subject to appropriate authorization and authentication in line with network operator policies.

4.10.3.4 Event notification

The MWIF architecture shall be able to support notifications of events, such as incoming call, or call abandoned, being sent to applications via the service interface.

4.10.4 Rapid Service Creation

The MWIF Architecture shall support the capability for rapid service creation by network operators, service providers and third party service providers independently of the equipment manufacturer. Rapid service creation is one of the drivers for the MWIF Architecture and therefore should be a capability resulting from the design requirements stated in this document. The operators believe that the implementation of the MWIF Architecture will facilitate rapid service creation. Rapid is considered from real-time to weeks rather than many months to years.

In addition to rapid service creation by the above parties, the following business scenarios should be supported:

- Development by third party but provided by the operator
- Service offered by third party - the operator can broker this third party service

4.10.4.1 New Service/Business Model

The MWIF Architecture shall support the separation of service provider from netwo rk provider (the dot.com model). This will enable different means of revenue generation for both service and network providers (e.g., billing service, micro-payments).

A model illustrating the relationship between network operators, service providers and third-party service providers is provided in Annex A.

4.10.5 Support Software Re-Use/Re-Usability

The MWIF Architecture shall enable:

- Maximum use of API's or other standard interfaces; and
- The capability to re-arrange network functional blocks to support a service provider's needs.

In order to ensure scalability and expansion of service provision it is necessary that the software API’s be sufficiently well designed to ensure portability of applications (layer 3 and above) across infrastructure supporting diverse networks.

4.10.6 User Customisation Of Services

The MWIF Architecture shall enable the subscriber and/or user to change the behaviour of their service to suit their requirements - both dynamically (real-time) and semi-permanently as required. That is, the MWIF Architecture shall support the capability for the subscriber and/or user to modify their service profile (within the limits of the subscription); modification of the profile should be possible through any access.

Specifically, the MWIF architecture shall support the capabilities for the user to:

- Personalise services;
- Personalise User Interface settings (within the capabilities of terminals);
- Modify a user profile (for example to include new services) from any location;
- Activate or deactivate user services;
- Access new services in the home network;
- Discover and access services provided in a visited network
- Access services from any network or terminal subject to network capabilities, terminal capabilities and any restrictions imposed by the home environment;
- Use services in a consistent manner irrespective of serving network and terminal, within the technical limitations;
- Select a particular user profile;
- Indicate (on a session basis if necessary) to which subscription charges are to be applied
- Recovery of user profile information normally resident in the user terminal to protect against loss or damage of user equipment

4.11 Regulatory Requirements

The MWIF Architecture shall provide the capability to support various regional, national, state or local regulatory requirements including, for example:

- Emergency Services
    - Including requirements for provision of geographical location
- Legal intercept
    - Legal intercept shall be possible on all media components (e.g. speech, data, video)
    - Invoking of legal intercept shall not be noticeable in any way to the user
- Number Portability
    - E.164 [4] number portability
- Malicious call trace
- Identity restriction (e.g., calling number/name presentation restriction)
- Support for facilities for hard of hearing (e.g. TTY/TDD)

5 OPEN RAN ARCHITECTURE REQUIREMENTS

The Open RAN Architecture Requirements are specified in MTR-007 [5]

6 OTHER ACCESS NETWORK REQUIREMENTS

Precise requirements for other access network (beyond radio access networks) are for further study.

ANNEX A: INDICATIVE BUSINESS MODEL

An indicative business model for MWIF has been included here in order to illustrate the inter-relationships between the various business entities in a typical network environment.

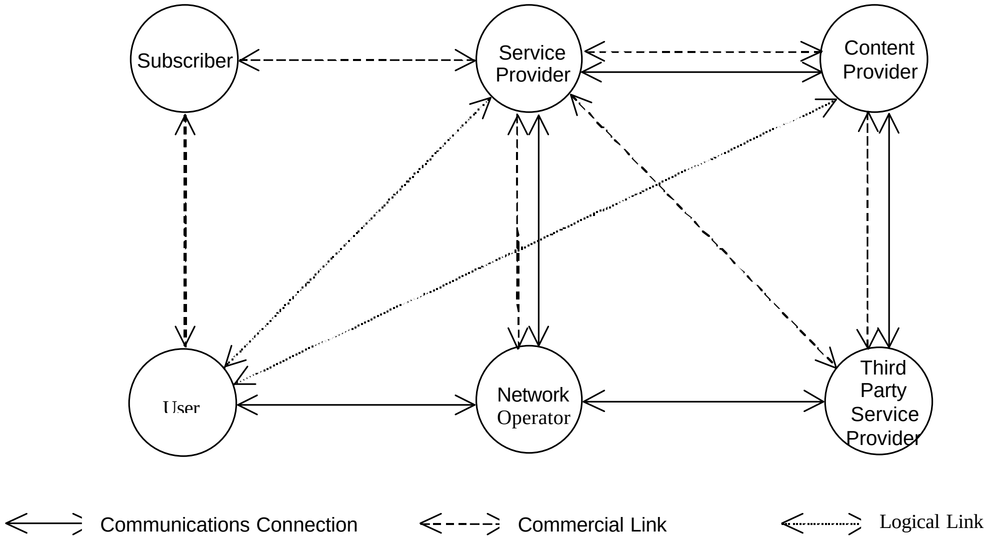

Figure 1: Assumed Business Model

In this business model the Subscriber is a customer of the Service Provider (SP). Commercial agreements are set up and maintained between them for the provision of services from the SP to the User via the Network Operator. The Subscriber may have contracts with multiple SPs and maintains these on behalf of one or more users. There is no commercial relationship between the User and the SP that prevents Users directly requesting additional or modified services. Approval must be gained from the Subscriber who subsequently authorises the SP to provide the service.

The Subscriber informs the SP which services each user should have access to and may choose to set limits on how much a User can use a particular service. For instance the Subscriber may authorise $x a day of video calls with a high QoS and unlimited video calls with a lower QoS.

The SP must enter into contract(s) with one or more Network Operators in order to deliver services to Users. Other companies may wish to sell services without having a contract with a Network Operator. This can be achieved by adopting the role of Third Party Service Provider and selling service via the SP. Other Companies may wish to sell just content. This is made possible by developing a commercial relationship with either a SP or a Third Party Service Provider.

It is important to note that Users, Subscribers, etc are roles, and that one entity may adopt more than one role. For instance an individual may adopt the roles of both User and Subscriber. A company may adopt the roles of Network Operator, SP and Content Provider.

A user initiates a service by requesting it from the Service Provider, not the Network Operator. On receipt of a service request the Service Provider uses Network Operators and Third Party Service Providers to service the request in the best way possible. In the example of the video call the Service Provider may choose to use different Network Operators for high and low QoS calls.

DOCUMENT HISTORY

Date	Version	Comment
8th June 2000	0.1	Version with Charles Lo comments Converted into MWIF MTR format
20th July 2000	0.3	Revised prior to MWIF Toronto meeting
27th July 2000	0.4	Update at MWIF TC#6 Submitted for TC review
30th August 2000	0.5	Incorporation of agreed comments following TC review
6th September 2000	0.6	For submission for TC approval
10th October 2000	1.0	Endorsed by the Board of Directors for Publication
11th October 2000	Draft 1.1	Draft version for discussion in WG-1 expanding on issues for further comment. Deleting service portability requirement (4.1.2.1) Security (4.8) Adding profile management requirement (4.9.5) Secure OAM&P interfaces (4.9.6) Service provision in home and visited networks (4.10.2) Service provision by third parties (4.10.3) New section on Open RAN requirements
21st December 2000	Draft 1.2	Expansion of OAM&P requirements (4.9) Additional information on accounting (4.1.2.4) Network policy and user profiles (4.1.2.8)
10th January 2001	Draft 1.3	Inclusion of text on "plug and play" Additional text on support of pre-pay Inclusion of text on legal intercept Inclusion of text on support of legacy terminals Replacement of term OAM&P with network and service management Inclusion of text on support of independent wireline and radio access networks
11th January 2001	Draft 1.4	Updated following WG-1 meeting, distributed for WG-1 comment.
19th January 2001	Draft 1.5	Updated with comments received during WG-1 review: Reference to GSMA TAP3 for exchanging billing information; Existing non-IP network management may be in place for some time; Need for adequate security & authentication when roaming.

5th February 2001	Draft 1.6	Editorial changes to draft 1.5 Version for TC review
28th February 2001	Draft 1.7	Changes following TC Review For TC ballot
27th April 2001	Draft 1.7	Approved by the membership via ballot.
15th May 2001	Draft 1.7	Ratified by the MWIF Board of Directors.