

1 3GPP2 S.R0058
2 Version 1.0
3 Version Date: 17 April 2003



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

4
5
6
7
8
9

10 IP Multimedia Domain

11

12 *System Requirements*

13
14
15
16
17
18
19
20
21
22
23
24

COPYRIGHT NOTICE

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

25
26

1 **CURRENT EDITOR**
2 Shou Gung (Nokia) +1-972-894-4967
3 Shou.Gung@nokia.com

4
5 **REVISION HISTORY**

6

REVISION HISTORY		
Rev. 1.0	<i>Initial publication</i>	<i>17 April 2003</i>

Table of Contents

1			
2			
3	IP MULTIMEDIA DOMAIN		1
4	1 INTRODUCTION.....		6
5	1.1 REQUIREMENT NUMBERING CONVENTION.....		6
6	2 REFERENCES.....		7
7	3 DEFINITIONS AND ABBREVIATIONS.....		8
8	4 GENERAL DESCRIPTION		10
9	5 HIGH LEVEL FUNCTIONALITIES.....		11
10	5.1 ACCESS NETWORK INDEPENDENCE.....		11
11	5.2 ACCOUNTING AND AUDITING.....		12
12	5.3 ADDRESS MAPPING AND NUMBERING.....		12
13	5.4 LEGACY NETWORK PROTOCOL INTERWORKING		13
14	5.5 AUTHENTICATION		13
15	5.6 AUTHORIZATION		14
16	5.7 BEARER RESOURCES.....		15
17	5.8 EMERGENCY SERVICES SUPPORT		15
18	5.9 GEO-POSITION CAPABILITY		16
19	5.10 HANDOFF		16
20	5.11 INFORMATION STORAGE		17
21	5.11.1 <i>Storage of Network Policy</i>		18
22	5.12 IP AND SS7 TRANSPORT INTERWORKING		18
23	5.13 IP-BASED TRANSPORT.....		18
24	5.14 IPV4 / IPV6 SUPPORT		18
25	5.15 ISUP TO SIP INTERWORKING		19
26	5.16 MOBILE IP SUPPORT		19
27	5.17 OPERATIONS, ADMINISTRATION, MAINTENANCE, AND PROVISIONING.....		19
28	5.18 QUALITY OF SERVICE.....		20
29	5.19 REGISTRATION.....		21
30	5.19.1 <i>Registration for IP Connectivity</i>		21
31	5.19.2 <i>Registration for SIP-based Multimedia Services</i>		21
32	5.20 ROAMING SUPPORT.....		21
33	5.20.1 <i>Support for Subscribers of Other IP Multimedia Systems</i>		21
34	5.20.2 <i>Support for Subscribers Roaming in Other IP Multimedia Systems</i>		22
35	5.21 SECURITY.....		22
36	5.21.1 <i>Security of Signaling and Bearer Traffic</i>		22
37	5.21.2 <i>Security of Stored Information</i>		23
38	5.21.3 <i>Security of Network Topology</i>		23
39	5.22 SIP-BASED SESSION CONTROL MANAGEMENT		24

1	5.23	SESSION MOBILITY	25
2	5.23.1	<i>Add/Drop Party and/or Media</i>	25
3	5.23.2	<i>Session Redirect</i>	26
4	5.24	SUPPORT FOR PUBLIC AND PRIVATE IDENTITIES	26
5	5.25	SUPPORT FOR REGULATORY REQUIREMENTS.....	27
6			
7			

List of Tables

1		
2		
3	Table 1 - Abbreviations	8
4	Table 2 - Definitions.....	9
5		
6		

1 1 INTRODUCTION

2 This document specifies the system requirements for and operations of
3 the IP Multimedia Domain (IP-MM Domain) system. The IP Multimedia
4 Domain system encompasses the mobile station, the access network, and
5 the core network. The various major functions and capabilities of the IP-
6 MM Domain system are discussed with a focus on the broad
7 requirements that shall be met in providing those functions and
8 capabilities.

9 The requirements contained in this document apply to the complete IP
10 Multimedia Domain system. Actual development of stage 2 and stage 3
11 work is expected to be done in a phased manner, with releases of the
12 specifications containing successively more complete implementations of
13 these requirements.

14 1.1 Requirement Numbering Convention

15 The requirements in this system requirements document use a specific
16 numbering convention to assist in finding and tracing activity on
17 particular requirements. The format is <topic>-<xnnn>. The <topic>
18 field is a mnemonic that provides categorization of the requirement, such
19 as **SEC**, **AUTN**, **AUTR**, **ACCT**, or **DB**.
20

2 REFERENCES

The document references which are applicable to this specification include the following:

1. Perkins, *IPv4 Mobility*, RFC 2002, May 1995.
2. Perkins, *IP Encapsulation within IP*, RFC 2003, October 1996.
3. Perkins, *Minimal Encapsulation within IP*, RFC 2004, October 1996.
4. Solomon, *Applicability Statement for IP Mobility Support*, RFC 2005, October 1995.
5. Cong, Hamnlen, Perkins, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*, RFC 2006, October 1995.
6. Montenegro, *Reverse Tunneling for Mobile IP*, RFC 2344, May 1998.
7. Perkins, Calhoun, *Mobile IPv4 Challenge/Response Extensions*, RFC 3012, November 2000.
8. Calhoun, Perkins, *Mobile NAI Extension*, RFC 2794, March 2000.
9. 3GPP2 Specification S.R0037-0, *IP Network Architecture Model for cdma2000 Spread Spectrum Systems; Version 2.0*; May 14, 2002
10. ANSI/TIA/EIA Standard 664-000-A, *Cellular Features Description*; December 6, 2000
11. ANSI/TIA/EIA Standard 41-D, *Cellular Radiotelecommunications Intersystem Operation*; November 13, 1997
12. 3GPP2 Specification S.S0028 *OAM&P for cdma2000 (3GPP Delta Specification)*
13. Handley, Schulzrinne, Schooler, Rosenberg, *SIP: Session Initiation Protocol*, RFC 2543, March 1999.
14. 3GPP2 Specification P.S0001-B version 1.0.0 *Wireless IP Network Standard*, October 25, 2002.
15. Deering, Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 1883, December 1998

1 3 DEFINITIONS AND ABBREVIATIONS

2 The terms and abbreviations that are used within this specification are
3 defined as follows:

4 **Table 1 - Abbreviations**

AAA	Authentication, Authorization, Accounting
API	Application Programming Interface
DB	Databases
DNS	Domain Name Server
EVRC	Enhanced Variable Rate Codec
HA	Home Agent
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISUP	ISDN User Part
MGW	Media Gateway
MIP	Mobile IP
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
MS	Mobile Station
NAI	Network Access Identifier
OAM&P	Operations, Administration, Maintenance and Provisioning
PCM	Pulse Code Modulation
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAN	Radio Access Network
RFC	Request for Comments (an IETF standard)
SGW	Signaling Gateway
SIP	Session Initiation Protocol
SrvApps	Service Applications

SS7	Signaling System 7
UIM	User Identity Module
URL	Universal Resource Locator
VoIP	Voice over IP

1
2

Table 2 - Definitions

All-IP enabled RAN	An All-IP enabled RAN is an Access Network which is a network component that may support both the Multimedia and Legacy MS Domains. The access network performs mobility management functions for registering, authorizing, authenticating and paging IP based terminals, independent of circuit based terminals. The access network performs handoffs within an access network and between access networks of the same technology and may support handoffs between access networks of differing technologies.
Hard Handoff	A handoff characterized by a temporary disconnection of the Traffic Channel. Hard handoffs occur when the mobile station is transferred between disjoint Active Sets, when the CDMA Frequency Assignment changes, when the frame offset changes, or when the mobile station is directed from a CDMA Traffic Channel to an analog voice channel. See also Soft Handoff.
Soft Handoff	A handoff occurring while the mobile station is in the <i>Mobile Station Control on the Traffic Channel State</i> . This handoff is characterized by commencing communications with a new base station on the same CDMA Frequency Assignment before terminating communications with an old base station. See also Hard Handoff. Assume for soft handoff that the same carrier/frequency is used on both the serving and target BTS.
Inter-Technology Hard Handoff	Hard handoffs across access technologies, but within the same call model.

3

1 **4 GENERAL DESCRIPTION**

2 The IP Multimedia Domain system provides IP connectivity, services, and
3 features to the subscriber over a packet transport capability. The IP
4 connectivity, services, and features can be seen as being end-to-end
5 between the mobile station and other endpoints. Thus, IP connectivity
6 and addressability is supported from the mobile station into and through
7 the core network to other IP endpoints. Service applications (e.g., clients)
8 running on the mobile station communicate with other applications (e.g.,
9 servers) running in the core network or in other networks. Applications
10 on the mobile station access features based in the core network or in
11 other networks. In addition, mobile stations can use the core network
12 components to communicate with other mobile stations.

13 The IP Multimedia Domain system can be viewed at several levels and
14 from a variety of perspectives. The approach taken in this system
15 requirements specification is to view the IP Multimedia Domain system
16 from the a system perspective that examines the functions provided by
17 the system without respect to the way in which those functions are
18 provided by the system components.

19

1 **5 HIGH LEVEL FUNCTIONALITIES**

2 The following subsections provide the requirements in support of the
3 functions provided by the IP Multimedia Domain system.

4 **5.1 Access Network Independence**

5 The interface from the core network to the access network shall provide a
6 standard set of functionality, regardless of the access network
7 technology. In this way, the core network can evolve independently from
8 the access network(s), and the network operator may deploy multiple
9 access network technologies on a single core network.

10 The standard set of functions of the interface to the access network
11 includes:

- 12 ♦ support for a Mobile IPv4 Foreign Agent function,
- 13 ♦ support for a Mobile IPv6 Attendant function,
- 14 ♦ support for QoS resource authorization,,
- 15 ♦ support for a means for the mobile station to discover necessary
16 core network resources such as DNS servers, SIP servers, etc.,
- 17 ♦ support for a means for the mobile station to request Mobile IP
18 registration,
- 19 ♦ support for Simple IPv4 and Simple IPv6 connectivity between
20 the serving core network and the mobile station, and
- 21 ♦ enforcement of policy decisions made with regard to QoS
22 resources supplied to the mobile station/subscriber's activities.

23 **ANI-0001** The system SHALL connect a common core network to any
24 access network meeting these requirements.

25 **ANI-0002** The system SHALL provide the ability for a mobile station to
26 attach to any access network meeting these requirements, to
27 authenticate, to register, and to receive authorized services

28 **ANI-0003** The system SHALL provide Mobile IPv4 functionality to
29 attached mobile stations.

30 **ANI-0004** The system SHALL provide Mobile IPv6 functionality to
31 attached mobile stations.

32 **ANI-0005** The system SHALL support authorization of QoS resources,
33 and make such authorized QoS resources available to the
34 subscriber/mobile station.

35 **ANI-0006** The system SHALL provide policy enforcement functions for
36 all of its QoS resources.

1 **ANI-0007** The system SHALL provide a means for attached mobile
2 stations to discover necessary functions such as DNS
3 Servers, SIP servers, etc.

4 **ANI-0008** The system SHALL support the ability of an unauthorized
5 and unauthenticated mobile station to initiate an emergency
6 VoIP call.

7 **5.2 Accounting and Auditing**

8 Accounting and auditing functions within the core network consist of the
9 ability to gather data about resource and service utilization and forward
10 that data for analysis and billing functions. It shall be possible to gather
11 such data from all elements within the core network that are utilized in
12 providing services to the subscriber.

13 **ACCT-0001** The system SHALL support forwarding resource utilization
14 information in a consistent manner to one or more central
15 points for collection.

16 **ACCT-0002** The system SHALL provide a means for Service Applications
17 (SrvApps) to forward accounting data through a standardized
18 interface/API for collection at one or more central points.

19 **5.3 Address Mapping and Numbering**

20 Within the core network there is a need for translation between a variety
21 of address types and IP addressing. Address types include:

- 22 ♦ IP Addresses (both IPv4 and IPv6),
- 23 ♦ E.164 numbers,
- 24 ♦ URLs, and
- 25 ♦ NAIs.

26 URLs, NAIs, and E.164 numbers provide a level of abstraction from the
27 actual location of the addressed entity. In practice, the same NAI might
28 be mapped into different IP addresses depending on the location of a
29 mobile station.

30 **IP-0001** The system SHALL provide a means for translation between
31 E.164 numbers and URLs (e.g. SIP URLs).

32 **IP-0002** The system SHALL provide a means for translation of URLs
33 to IP addresses.

34 **IP-0003** The system SHALL provide a means for translation of NAIs to
35 IP addresses. This translation function shall provide a
36 standardized interface usable by all network elements as well
37 as the mobile station.

1 **IP-0004** The system SHALL provide domain name translation
2 services. This translation function shall provide a
3 standardized interface usable by all network elements as well
4 as the mobile station.

5 **5.4 Legacy Network Protocol Interworking**

6 It shall be possible to implement an IP Multimedia Domain system
7 without requiring the inclusion of Legacy MS Domain components.
8 However, any implementation of an All-IP system that includes the ability
9 to communicate with other systems using the TIA/EIA-41 protocol by
10 necessity includes elements of the Legacy MS Domain.

11 The IP Multimedia Domain system shall support voice calls between itself
12 and the PSTN. This requires ISUP interworking.

13 **IPMM-0001** It SHALL be possible to implement an IP Multimedia Domain
14 system without the inclusion of Legacy MS Domain system
15 core network components.

16 **PSTN-0001** The system SHALL provide a function that supports ISUP
17 signaling interworking with the PSTN including global title
18 translation.

19 **IP-0012** The system SHALL allow for full backward compatibility with
20 the IP-based packet services of the legacy packet system
21 <3GPP2 P.S0001>. However, this does not preclude building
22 a system without including functions unique to legacy
23 packet systems.

24 **5.5 Authentication**

25 Authentication involves the verification of the identity of an entity with
26 which communications are undertaken. Authentication capabilities
27 within the core network include the ability to verify at the transport level
28 (IP transport level) the identity of the subscriber attempting to use the
29 services of the core network. In addition, authentication at the SIP level
30 and at the Service Application level are needed.

31 <EDITOR'S NOTE: WG4 under TSG-S is dealing with security.
32 Authentication is part of security. After WG4 advances work on security
33 in the All-IP system (S.P0086-0 3GPP2 MMD Security Framework), it can
34 be determined how to best merge this section, the section below on
35 security, and the work of WG4.>

36 **AUTN-0001** The system SHALL support IP transport level authentication
37 at the time of first access, or at any subsequent time until
38 the subscriber discontinues contact with and use of the
39 operator's system.

1 **AUTN-0002**The system SHALL have the ability to cooperate with another
2 system to allow that other system to verify the identity of the
3 subscriber at the IP transport level at the time of first access,
4 or at any subsequent time until the subscriber discontinues
5 contact with and use of the operator's system.

6 **AUTN-0003**The system SHALL support SIP level authentication.

7 **AUTN-0004**The system SHALL support service level authentication.

8 **AUTN-0005**The system SHALL support a separate access level
9 authentication, for those access technologies where that
10 capability is required.

11 **AUTN-0006**The system SHALL support user identity authentication
12 independent of the mobile station. (An associated
13 requirement is given in IDEN-0003.)

14 **5.6 Authorization**

15 Authorization involves giving permission for the use of resources.
16 Authorization within the core network encompasses a policy based
17 method. Policy decisions are made at two levels: network level, and
18 subscription level. At the network level, decisions are made and enforced
19 with respect to policies that apply to all subscribers using the resources
20 of that network. At the subscription level, decisions are made and
21 enforced with respect to policies that apply to a particular subscription.

22 **DB-0001** The system SHALL have the ability to store network policy
23 rules.

24 **AUTR-0001**The system SHALL have the ability to make network policy
25 based decisions relative to individual subscriber requests.

26 **AUTR-0002**The system SHALL have the ability to enforce network policy
27 based decisions at all ingress and egress points.

28 **DB-0002** The system SHALL have the ability to store subscription
29 policy rules.

30 **AUTR-0003**The system SHALL have the ability to make subscription
31 policy based decisions relative to individual subscriber
32 requests.

33 **AUTR-0004**The system SHALL have the ability to cooperate with other
34 systems to provide subscription authorizations to such other
35 systems.

1 5.7 Bearer Resources

2 Bearer resources are functions within the core network that manipulate
3 or alter bearer IP streams. For instance, transcoders modify the bearer
4 content by converting audio information from one encoding format to
5 another – a common example is PCM encoding to/from EVRC encoding.
6 Bridges merge the content of several bearer streams and reflect that
7 merged content to the reverse components of those input streams. Tones
8 and announcements can be added to or substituted for the content of
9 bearer streams. Circuit interfaces can be used to transfer bearer content
10 to/from a packet format from/to a circuit format for transmission
11 between the core network and the PSTN. Circuit data modems convert
12 between packetized data and modulated circuit-based audio streams.

13 **BRSC-0001** The system SHALL provide the ability to configure and
14 deploy arbitrary sets of bearer resources.

15 **BRSC-0002** The system SHALL provide the ability for its bearer resources
16 to be made available both to the owning system, and to other
17 systems. An associated requirement is given in SIP-0007.

18 **BRSC-0003** The system SHALL provide the ability to discover bearer
19 resources within itself or within other core networks.

20

21 5.8 Emergency Services Support

22 Emergency services are provided by the serving network, that is, the
23 network to which the mobile station is attached. Emergency services
24 may be based on SIP sessions, or on other protocol technologies. The
25 serving core network needs to be able to provide emergency SIP-based
26 services to MSs attached to itself.

27 Individual regulatory administrations may have the need to support
28 emergency SIP-based services to all MSs, regardless of whether they are
29 registered and authenticated. These system requirements do not make
30 any decisions in this regard. However, in support of network operators
31 who shall meet regulatory mandates, the serving network shall be
32 capable of support emergency services to MSs that are not registered or
33 authenticated.

34 See SIP-0005, and ANI-0008.

1 5.9 Geo-Position Capability

2 One major aspect of a mobile network that shall be supported by the All-
3 IP network is a geographic positioning, “geo-position” capability. This
4 capability provides latitude, longitude and altitude of the mobile station
5 within defined tolerances. Note that those tolerances are not specified in
6 these system requirements and that the altitude information may not be
7 necessary for some applications.

8 The geo-position capability may be used in support of a variety of
9 network functions and services, such as emergency calls. It is also
10 useful to various value-added applications that can be accessed by the
11 subscriber.

12 **GPS-0001** The system SHALL support a geo-position capability that
13 provides latitude, longitude and optional altitude information
14 for the mobile station within tolerances specified outside of
15 these requirements.

16 **GPS-0002** It SHALL be possible for geo-position information to be
17 accessed by authorized core network entities in a standard
18 format.

19 **GPS-0003** It SHALL be possible for geo-position information to be
20 accessed by authorized and authenticated service
21 applications (SrvApps) in a standardized method.

22 **GPS-0004** The system SHALL guarantee that all access to geo-position
23 information is authorized and can be authenticated.

24 5.10 Handoff

25 The ability to support mobility within and between access networks is a
26 fundamental principle in current wireless communication technologies
27 (IS-95, GSM, TDMA, IS-2000, 802.11b, etc.). The following requirements
28 specify the different handoff scenarios that need to be supported in
29 networks based on the All IP Architecture for the IP Multimedia domain.
30 However, the method for supporting these various handoff scenarios
31 shall be detailed in stage 2 or 3 documents.

32 **HOF-0001** It SHALL be possible to do a soft handoff within a RAN and a
33 single access technology that supports soft handoff.

34 **HOF-0002** It SHALL be possible to do a hard handoff within a RAN, the
35 same Domain, and a single access technology that supports
36 hard handoff.

37 **HOF-0003** It SHALL be possible to do a soft handoff across RANs and a
38 single access technology that supports soft handoff.

- 1 **HOF-0004** It SHALL be possible to do a hard handoff across RANs
2 within the same Domain and a single access technology that
3 supports hard handoff.
- 4 **HOF-0005** It SHALL be possible to do a soft handoff between All-IP
5 enabled RANs and legacy RANs within any access technology
6 that supports soft handoff.
- 7 **HOF-0006** It SHALL be possible to do a hard handoff within the same
8 system between RANs of different technologies that support
9 inter-technology hard handoff.
- 10 **HOF-0007** It SHALL be possible to do a hard handoff between systems
11 and between RANs of different technologies that support
12 inter-technology hard handoff.

13 **5.11 Information Storage**

14 The core network elements need to access various types of information to
15 provide their individual functionalities. Some of this information is static
16 in nature, other information has a more dynamic nature. The core
17 network contains storage for such information in Databases (DBs) that
18 are accessible under proper authorization and authentication controls.
19 Privacy of the subscriber's information is of a highest priority, as is the
20 integrity of the network operator's core network itself.

- 21 **DB-0003** The system SHALL provide a means of storing both static
22 and dynamic information in the core network.
- 23 **DB-0004** The system SHALL make stored subscriber and network
24 information accessible only under proper authorization and
25 authentication controls.
- 26 **DB-0005** The system SHALL provide a means of storing dynamic
27 subscriber information in both the serving and the home
28 networks.
- 29 **DB-0006** The system SHALL provide a means of storing information
30 on the capabilities of the mobile station in use by each
31 subscriber.
- 32 **DB-0007** The system SHALL provide a means for authenticated and
33 authorized Service Applications (SrvApps) to access
34 information on the capabilities of the mobile station in use
35 by a subscriber in a standardized method.
- 36 **DB-0008** The system SHALL provide a means for authenticated and
37 authorized Service Applications (SrvApps) to access
38 information on the static subscription information, or profile,
39 for each subscription, and for each subscriber under that
40 subscription in a standardized method.

1 **5.11.1 Storage of Network Policy**

2 It is necessary for network operators to be able to set specific policies
3 about the use of their network resources. Such policies may take into
4 consideration attributes of the subscriber. The system stores such
5 policies and applies them to subscribers' requests for network resources.
6 This is also discussed in section 5.6 under the topic of authorization.

7 See requirements DB-0001 and AUTR-0001 to AUTR-0002.

8 **5.12 IP and SS7 Transport Interworking**

9 Interworking of signaling involves the conversion of the transport over
10 which such signaling is carried from one transport to another. This is
11 commonly referred to as "gatewaying" of signaling. In the All-IP network,
12 such gatewaying is done between legacy SS7 transport and IP transport.
13 The signaling that is gatewayed in a 3GPP2 All-IP network is ISUP and
14 TIA/EIA-41.

15 **SGW-0001** The system SHALL provide a function to move ISUP and
16 TIA/EIA-41 signaling between IP transport and SS7
17 transport.

18 **SGW-0002** The system SHALL be capable of maintaining correct
19 addressability for higher level signaling flows between the
20 SS7 transport and the IP transport environments.

21 **5.13 IP-based Transport**

22 A basic capability of the core network is to provide IP-based transport of
23 subscriber signaling and data, as well as core network signaling. This
24 transport is pervasive, but is of major importance as one considers the
25 Access Gateway (AGW), the Mobile IP Home Agent (MIP-HA or HA), the
26 Border Router (BR), and the Media Gateway (MGW). It is in these entities
27 that IP addressability, connectivity and QoS are supported.

28 **IP-0005** The core network SHALL provide IP-based transport for both
29 control and user planes.

30 **5.14 IPv4 / IPv6 Support**

31 The 3GPP2 ALL IP system is based on the following assumptions:

- 32 1. Use of Mobile IPv4 and/or Mobile IPv6 protocol,
- 33 2. Use, support, and interoperation of IPv4 and IPv6 in the All-IP
34 Network, and
- 35 3. Migration from IPv4 to IPv6 is supported and IPv4 and IPv6 based
36 All-IP networks shall be interoperable.

37 The following requirements shall satisfy the above mentioned
38 assumptions and architecture principle for the ALL IP Network:

- 1 **IP-0006** The system SHALL support mobile stations with IPv4
2 capabilities.
- 3 **IP-0007** The system SHALL support mobile stations with IPv6
4 capabilities.
- 5
- 6 **IP-0009** The system SHALL support IPv4 – IPv6 interoperability for
7 any features / services defined within the system (e.g., SIP).
- 8 **IP-0010** The IP addressing between RAN elements SHALL be
9 independent of the IP addressing between the mobile station
10 and the core network.
- 11 **IP-0011** The system SHALL support multiple connections (i.e.,
12 multiple concurrent media streams) to and from the mobile
13 station, each of which may have different QoS
14 characteristics.

15

16 **5.15 ISUP to SIP Interworking**

17 The core network provides session support based on the SIP protocol.
18 Session signaling within the core network is SIP based.

19 See PSTN-0001.

20 **5.16 Mobile IP Support**

21 The Mobile IP protocol [IETF RFCs 2002, 2003, and 2004] has been
22 chosen to support mobility between access networks within a single
23 network, and between networks. The Mobile IP protocol defines a Home
24 Agent (MIP-HA or HA) as an entity that can forward IP packets to the last
25 known topological location of the mobile station. See requirements ANI-
26 0003 and ANI-0004.

27

28 **5.17 Operations, Administration, Maintenance, and Provisioning**

29 Operations, Administration, Maintenance, and Provisioning (OAM&P)
30 provide the ability for the network operator to observe and control all
31 network resources. To ensure interoperability of equipment from
32 multiple manufacturers, it is important to support a common OAM&P
33 framework and set of protocols.

34 **OAM-0001** The system SHALL support standardized OAM&P interfaces
35 to all network entities.

- 1 **QoS-0006** The system SHALL support multiple QoS levels.
- 2 **QoS-0007** If the correspondent node is within the operator's network,
3 the system SHALL support end-to-end QoS levels between
4 the mobile station and the correspondent node.
- 5 **QoS-0008** If the correspondent node is outside of the operator's
6 network, the system SHALL support end-to-end QoS levels
7 between the mobile station and the egress/ingress point
8 from the operator's network.
- 9 **QoS-0009** The system SHALL make possible negotiation of QoS at
10 session setup, at handoff, and at any time during a session.
- 11 Associated requirements are given in OAM-0003 and IP-0011.

12 **5.19 Registration**

13 **5.19.1 Registration for IP Connectivity**

- 14 When a mobile station accesses a system via some access network, it
15 shall perform registration for accessing packet data services to
16 accomplish IP "reachability."
- 17 See requirement ANI-0002.

18 **5.19.2 Registration for SIP-based Multimedia Services**

- 19 Once a subscriber has established IP connectivity, other services of the
20 system can be accessed. Of these, the most prominent are SIP-based
21 services. To enable the delivery of SIP-based services to the subscriber at
22 the in-use mobile station, the subscriber shall perform SIP registration.
- 23 See requirements SIP-0001.

24 **5.20 Roaming Support**

25 **5.20.1 Support for Subscribers of Other IP Multimedia Systems**

- 26 As subscribers of other IP Multimedia Domain systems access the IP
27 Multimedia Domain in a visited network, the serving visited system shall
28 be capable of:
- 29 ◆ authenticating that subscriber via AAA-based communication
30 with the home system of the roaming subscriber,
 - 31 ◆ determining authorized service levels that can be provided to
32 the roaming subscriber under business agreements between the
33 two network operators,
 - 34 ◆ providing IP registration and connectivity to the roaming
35 subscriber,
 - 36 ◆ providing SIP registration support to the roaming subscriber,

1 ♦ supporting agreed and authorized QoS levels for the roaming
2 subscriber, and

3 ♦ storing dynamic information about that roaming subscriber.

4 With regard to authentication of the roaming subscriber, see AUTN-0002.

5 With regard to authorization of service levels, see AUTR-0004.

6 With regard to IP registration and connectivity to the roaming subscriber,
7 see IP-0004, ANI-0003, and ANI-0004.

8 With regard to providing SIP registration support to the roaming
9 subscriber, see SIP-0001.

10 With regard to supporting agreed and authorized QoS levels for the
11 roaming subscriber, see AUTR-0004.

12 **5.20.2 Support for Subscribers Roaming in Other IP Multimedia** 13 **Systems**

14 When a subscriber of a particular IP Multimedia Domain system roams
15 into another IP Multimedia Domain system and attempts to access
16 services, normal registration and authentication processes shall occur.
17 The serving (visited) system will communicate with the home system to
18 accomplish Mobile IP registration and SIP registration.

19 Requests for QoS resources by the mobile station in the visited system
20 will be processed locally in the serving system with regard to local
21 (serving) system policy rules (see AUTR-0001 and AUTR-0002). With
22 regard to subscriber policy rules, the home system may, upon MIP
23 registration, forward a complete set of subscription policy decisions to
24 the visited system to avoid repeated accesses for authorization to the
25 home system. The home system may also choose to require that each
26 QoS resource request be sent to the home system for individual analysis
27 (see AUTR-0003).

28 **5.21 Security**

29 **5.21.1 Security of Signaling and Bearer Traffic**

30 Security is an important and pervasive aspect of a system. Not only shall
31 the subscriber's profile, signaling and user traffic be kept secure, but
32 also the elements of the operator's system shall be secured.

33 In legacy systems that employ circuit based signaling and bearer paths,
34 the operator typically has a great deal of control over access to those
35 circuits, and thus to the security of the information flowing over those
36 circuits.

1 In packet based networks, signaling and user traffic from all subscribers
2 and from the network itself can be mixed on the links within the network
3 and between the network and other networks, including the Internet.
4 Entire links are not dedicated to a single user, and thus multiple users
5 have access to the packets flowing over those links. Each of those
6 packets shall be secure.

7 Methods of securing links and the traffic flowing in, through, and to a
8 network are numerous to meet the great variety of situations faced by
9 network operators. See *S.P0086-0 3GPP2 MMD Security Framework*
10 (currently being developed by TSG-S WG4), > for more detailed
11 descriptions and requirements.

12 **5.21.2 Security of Stored Information**

13 The entities of the All-IP system will contain information that is sensitive
14 to the wireless carrier and shall not be accessible to external networks or
15 to unauthorized entities within the network.

16 **SEC-0001** It shall be possible to configure the All-IP system such that
17 the system's security, manageability, and performance
18 attributes are protected from entities external to that system
19 or to untrusted entities internal to the system.

20 **SEC-0002** The All IP system SHALL at a minimum be capable of
21 securing the following types of attributes:

- 22 1. Security keys that are used
- 23 2. Node configuration parameters
- 24 3. User profile information, including user identities
- 25 4. User location information
- 26 5. Data records related to the user sessions
- 27 6. Call Data records and other billing information

28 **5.21.3 Security of Network Topology**

29 In a network scenario such as All-IP, the connection between the
30 networks of different carriers or between different regions within one
31 carrier's network can not be considered trusted. These networks are
32 therefore considered public; in the extreme case it could be the public
33 Internet.

34 Apart from the sensitive information that is carried in the payload of
35 packets flowing between such networks, there is also a risk for
36 involuntary and indirect exposure of other topology-related and sensitive
37 information. This information could possibly be extracted from the
38 headers of the packets, if means has not been taken to prevent this. This
39 topological information can be sensitive in a competitive situation.

1 **SEC-0003** It SHALL be possible to configure the All-IP system such that
2 the system's inner topology is hidden from entities external
3 to that system.

4 **SEC-0004** At a minimum the following topological information SHALL
5 be protected:

- 6 1. The numbers of nodes of a specific type;
- 7 2. Capacity of node;
- 8 3. Geographical location of the nodes;
- 9 4. The services that are provided at a node.

10 **5.22 SIP-based Session Control Management**

11 Within the IP Multimedia Domain system, session control is
12 accomplished using the SIP protocol. The functions provided include:

- 13 ♦ registration for SIP based services,
- 14 ♦ initiation and termination of sessions,
- 15 ♦ modification of existing sessions, including merging and
16 splitting sessions as needed to support services to the
17 subscriber,
- 18 ♦ management of sessions across multiple systems,
- 19 ♦ support for emergency sessions,
- 20 ♦ home system control of sessions, and
- 21 ♦ allocation, deallocation, and modification of bearer resources in
22 the home, serving and third party networks.

23 **SIP-0001** The system SHALL provide a means for registration for SIP
24 based services at the home system regardless of whether the
25 mobile station is attached to the home or a visited system.

26 **SIP-0002** The system SHALL provide the ability to initiate and
27 terminate SIP based sessions.

28 **SIP-0003** The system SHALL provide the ability to modify existing SIP
29 based sessions.

30 **SIP-0004** The system SHALL provide the ability to manage SIP based
31 sessions across multiple systems including, but not limited
32 to:

- 33 - the home IP Multimedia Domain system,
- 34 - a visited serving IP Multimedia Domain system,
- 35 - third party IP Multimedia Domain systems,

- 1 - IP Multimedia Subsystems as defined by 3GPP, and
2 - systems that are compliant with the SIP protocol as
3 defined by the IETF.

4 **SIP-0005** The system to which the mobile station is attached SHALL
5 provide emergency SIP based VoIP sessions to the mobile
6 station/subscriber.

7 **SIP-0006** The system SHALL support home system control of SIP
8 based sessions.

9 **SIP-0007** The system SHALL support the allocation, deallocation, and
10 modification of bearer resources in the home, serving, and
11 third party systems.

12 **SIP-0008** The system SHALL support multiple concurrent SIP based
13 services to the mobile subscriber.

14 **SIP-0009** The system SHALL separate call/session control from
15 mobility management.

16 **SIP-0010** The system SHALL be able to terminate SIP sessions upon
17 unintentional loss of bearer.

18 **5.23 Session Mobility**

19 The Session Mobility service maintains continuity of an established multimedia
20 session when changes in user equipment, session media, and/or underlying
21 network is required. It enables a user to move an ongoing multimedia session
22 to a different user equipment or to a different access network environment.
23 Support for this service calls for the capability of the IP MMD network to
24 maintain continuity of a multimedia session while session participants transfer
25 the session to new terminal equipment, add/drop media, and/or redirect the
26 session. In addition, this service includes a session redirect or forward service
27 for incoming calls.

28

29 **5.23.1 Add/Drop Party and/or Media**

30 **SIP-0011** It shall be possible for a participant in an ongoing
31 multimedia session to transfer the multimedia session leg to
32 a substitute party. This substitute party may be the same
33 participant using a different terminal equipment. This
34 service may be initiated by any of the parties in the session
35 while the session is in progress. Conditioned by the
36 capability of the alternative terminal equipment, this session
37 transfer may also be accompanied by an add/drop of an IP
38 bearer stream to/from the ongoing session.

39 **SIP-0012** It shall be possible for a participant in an ongoing
40 multimedia session to add a medium stream to the session.

1 **SIP-0013** It shall be possible for a participant in an ongoing session to
2 remove a medium stream from the session.

3 **SIP-0014** It shall be possible for a participant in an ongoing session to
4 suspend that session, and resume it at a later time.

5 **5.23.2 Session Redirect**

6 **SIP-0015** It shall be possible for a participant in an ongoing multimedia
7 session to transfer the session to a target MS. The target MS
8 shall negotiate session capabilities at the time of session
9 transfer.

10 **SIP-0016** It shall be possible for an IP multimedia mobile subscriber to
11 redirect session invitation to a target destination address.
12 This redirection or forwarding may include activation by any
13 combination of parameters, e.g., session initiator ID, time,
14 date, duration, location of the MS, and location of the target
15 destination address. It shall be possible for the system to ask
16 the session initiator to initiate a new session to the target
17 destination (session redirect), or for the system itself to
18 forward the incoming session (session forward). The
19 activation of this session redirect or session forward service
20 occurs prior to the establishment of the IP multimedia
21 sessions.

22 **5.24 Support for Public and Private Identities**

23 A subscriber may have several identities with which they access the
24 system, e.g., identities at work (Boss@mycompany.com and
25 President@mycompany.com”), an identity at home (“Mother@xyz.com”),
26 an identity with friends (“Mary@xyz.com”), and an identity with
27 associates (“Mrs._Smith@xyz.com”). The subscriber may wish to receive
28 services under all, any, or none of these identities at various points in
29 time. Thus there is a need to support more than one public identity per
30 subscriber. As well, there is a need to be able to uniquely identify a
31 subscriber for administration and charging purposes. A private identity
32 is assigned for that purpose.

33 It is also necessary that a subscriber’s identities are not tied to specific
34 pieces of equipment. The subscribers shall be free to make use of any of
35 a variety of devices as suits their needs.

36 **IDEN-0001** The system SHALL support the association of multiple public
37 identities and one private identity with the same subscriber.

38 **IDEN-0002** The system SHALL support the association of various sets of
39 services with each identity of a subscriber.

40 **IDEN-0003** The system SHALL support integrated and removable User
41 Identity Modules (UIM).

1 **5.25 Support for Regulatory Requirements**

2 Various regions of the world have regulatory requirements that network
3 operators shall observe. While it is not appropriate for the All-IP System
4 to mandate any particular regulatory requirements, it is important that
5 the system allow support for such requirements.

6 **REG-0001** The system SHALL allow support for all applicable network
7 regulatory mandates.

8