3GPP2 S.R0120-0
Version 1.0
Version Date: September 2007

# All-IP System – MMD Policy Enhancements

## System Requirements

## *EDITOR*

Scott Marin s.marin@motorola.com

| ***REVISION HISTORY*** | | |
|---|---|---|
| ***Revision number*** | *Content changes.* | *Date* |
| 0 v1.0 | Initial Release | September 2007 |

# Table of Contents

# List of Figures

# 1 INTRODUCTION

Multimedia Doman (MMD) specifications [3] enable an operator to apply Quality of Service (QoS) policy controls to the Internet Protocol (IP) Connectivity Access Network on session-based applications, and to provision flow-based charging rules at the Packet Data Serving Node (PDSN). These current specifications are confined to the PDSN as the sole policy enforcement point supported.

The scope of MMD policy needs to be expanded to include overall coordination of network resource usage for Session Initiation Protocol (SIP) [4] and non-SIP applications for all subscribers, enhancements to policy contexts, and incorporation of additional network elements in the policy architecture.

This document specifies the system requirements related to these MMD Policy Enhancements, which are intended to guide the associated technical specification development.

# 2 REFERENCES

## 2.1 Informative References

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

[1] 3GPP TS 23.228, *IP Multimedia Subsystem (IMS) Stage 2*.

[2] 3GPP2 S.R0079-A v1.0, *Support for End-to-End QoS Stage 1 Requirements,* July 2006.

[3] 3GPP2 X.S0013-A, *Multimedia Domain series*, November 2005.

[4] IETF RFC3261, *SIP: Session Initiation Protocol*, June 2002.

[5] IETF RFC3344, *Mobility Support for IPv4*, August 2002.

[6] IETF RFC3775, *Mobility Support for IPv6*, June 2004.

# 3 DEFINITIONS AND ABBREVIATIONS

The terms and abbreviations which are used within this specification are defined as follows:

| | |
|---|---|
| 1xRTT | 1x Radio Transmission Technology |
| AF | Application Function |
| AGW | Access Gateway |
| AN | Access Network |
| AP | Access Point |
| AT | Access Terminal |
| BREW | Binary Runtime Environment for Wireless |
| CDMA | Code Division Multiple Access |
| DSL | Data Subscriber Line |
| EVDO | Evolution Data Only (a.k.a HRPD) |
| FW | Fire Wall |
| HRPD | High Rate Packet Data |
| IMS | IP Multimedia Subsytem |
| IP | Internet Protocol |
| MMD | Multi-Media Domain |
| NAT | Network Address Translation |
| NSP | Network Service Provider |
| PCRF | Policy and Charging Rules Function |
| PDSN | Packet Data Service Node |
| QoS | Quality of Service |
| SIP | Session Initiation Protocol |
| SLA | Service-Level Agreement |
| SSOO | Single Sign-On/Off |
| TCP | Transmission Control Protocol |
| TV | Television |
| VoIP | Voice over IP |
| UDP | User Datagram Protocol |
| UE | User Equipment |
| WCDMA | Wide-band CDMA |

The following definition is used in this specification:

**IP flow:** Any identifiable (classifiable) set of IP packets from a source to one or more receivers for which a common policy treatment has been requested. For example, a stream of packets having the same source address, destination address, protocol, and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports is an IP flow.

# 4 GENERAL DESCRIPTION

Policy requirements entail QoS requirements in reference [2], which specifies an end-to-end QoS model for cdma2000®[1] networks. While reference [2] advances a number of key QoS requirements for wireless IP networks, there are other capabilities which require policy treatment which are not discussed in that document. These additional capabilities are an integral part of evolution of MMD and are summarized in the following trends:

- **Support for both SIP and non-SIP applications**. It is anticipated that MMD networks will be deployed by operators who already have deployed non-IMS applications. It is also anticipated that these operators are not likely to replace these applications with IP Multimedia Subsystem [1] (IMS)-based versions for some time, if at all. This coexistence is exhibited in Figure 1 by showing how non-IMS-based SIP services, IMS-based SIP services, non-SIP services (e.g. Binary Runtime Environment for Wireless (BREW)) and 3rd party services are expected to be provided as part of a comprehensive services architecture. As it is likely that these services will coexist for some time, policy requirements must support the coexistence of both SIP and non-SIP applications.

---

[1] cdma2000® is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

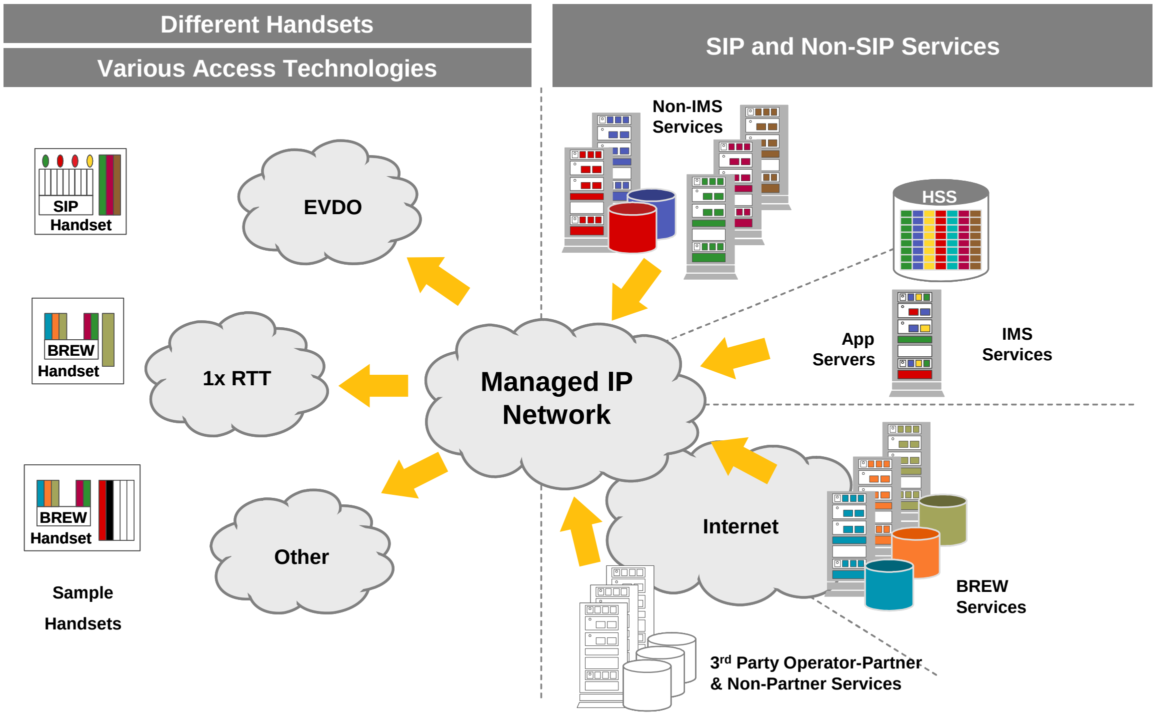

**Figure 1** A Comprehensive Services Architecture

- **Support for multiple access technologies**. The QoS requirements in reference [2] address cdma2000 access networks. However, we anticipate that network operators will incorporate access technologies other than cdma2000 (e.g.,WiFi, cable, Digital Subscriber Line (DSL), Wide-band CDMA (WCDMA), WiMAX, etc.) as they deploy network capabilities enabling seamless mobility (see Figure 1). Policy requirements must not preclude service operation over disparate access technologies and should support multiple access technologies.
- **Enhanced security**. The security policies which operators deploy serve a crucial role in the operation of their networks. Consequently, policy requirements must incorporate network security.
- **Support for 3rd party applications**. As shown in Figure 1, it is anticipated that operators, as they deploy MMD networks, will take advantage of 3rd party applications and make these applications available to their subscribers. The policies governing the access to these applications also need to be addressed in any set of policy requirements.
- **Support for ATs with multiple access technology capabilities**. The requirements should also consider the

Access Terminal’s (AT) capabilites within a given access technology and network.

- **Support for Network Address Translation traversal**. Various standards bodies are developing network-controlled, policy-driven architectures for Network Address Translation (NAT) traversal; other standards organizations have client-controlled architectures for NAT traversal. The policy requirements of this document should target an appropriate balance between these approaches.

The current MMD policy specifications primarily address policy control over IP bearer resources and per-flow accounting. Supporting the evolved MMD networks envisioned for the future necessitates enhancing the current specfications to incorporate the following items:

- **Expansion of policy contexts**. The current specifications only discuss QoS and accounting. There is a need to expand this list to include these other policy contexts:
    - **Mobility and Roaming Policy.** As part of supporting multiple access technologies, a network operator should also have the capability of controlling whether or not a roaming operation is permitted and whether or not a handoff operation is permitted.
    - **Access.** As part of providing enhanced authorization in an environment comprised of heterogeneous access technologies, a network operator should have the capability of controlling access into its network based on an AT’s security status or account status, e.g., quarantining access to a site which allows the subscriber to download required security patches, refresh their pre-paid balance or pay a delinquent account.
    - **Network Selection.** With the availability of multiple access technologies, the network operator should have the capability of defining policies used by the AT for prioritizing network access and selecting which Access Network (AN) it uses for applications.
    - **Packet Flow Optimization.** A network should have the capability of searching IP flows, within privacy limits, in order to verify that the application negotiated during session establishment is the

application actually operating. Additionally, for selected applications incapable of requesting enhanced QoS, the network should be able, by monitoring IP flows, to detect such applications and automatically employ network resources to provide the appropriate QoS.

- **Traffic Engineering.** The services architecture exhibited in Figure 1 demonstrates the need to organize and allocate network resources in the most efficient manner in order to meet customer service commitments in the most cost effective manner. A network operator should have the capability of defining policies for admission control and congestion management (e.g. identifying what resources are allocated to an application, if and how these resources can be modified by an application, how the resources are modified during network congestions, etc.).
- **Resource Selection.** When a user is in a visited network, routing traffic related to low latency applications back to the home network may result in undesireable latencies and/or network inefficiencies. A network operator should have the capability of defining policies which result in route optimization.
- **Authentication.** After a user agent provides authentication credentials within an operator-hosted session, subsequent re-entry of the same credentials associated with subsequent session hosted by the same operator should not be required. Similarly, when a user terminates a connection to an operator hosted session manager, then all sessions which were previously authenticated under that session manager should be terminated. The collection of these capabilities are commonly called Single Sign-On/Off (SSOO). A network operator should have the capability of defining policies for authentication credential management, credential sharing, and related protocol optimizations to support SSOO.
- **Content Screening.** Any content delivered by SIP and non-SIP services may be subject to a set of rules based on the subscriber/application profile and content characteristics (e.g., age-based rating).

    This alleviates each content source from implementing an independent content screening function.

    - **Parental/Enterprise Control.** One subscriber has the ability to modify policy that applies another subordinate subscriber or set of subscribers. This allows a parent/employer to manage the rights of children/employees including charging limits and content screening.
    - **User Personalities.** A subscriber has multiple sets of policy and the network selects a particular set in real time based on various conditions such as dialed digits (called party), incoming number (caller party), time of day, etc.

- **Expansion of network elements**. The current specifications define policy control interactions among a limited set of network elements. Incorporating the additional functionality discussed in this section necessitates expanding the list of network elements impacted by the policy specifications. For example, when supporting Mobile IP [5][6], the home agent may need to be aware of the mobility policy since it is involved in mobility events between different access technologies. Since different network elements may be employed for different access technologies, the home agent may become a key location for managing a network operator's mobility policies. Additionally, as MMD networks grow, allowing additional network elements to participate in policy enforcement provides a more scaleable solution.

## 4.1 Architecture Considerations

The following goals should be considered when developing the policy specifications:

- The policy architecture should not adversely affect performance (e.g., increase post-dial delay, prolong break time during hard handoff, etc.)
- The policy architecture should allow localization of policy decisions to minimize messaging between network entities for some operations. For example, the RAN may cache policy information and make local policy decisions for handoff events.
- The policy architecture should not inhibit system capacity from scaling both up and down, in terms of active subscribers & active sessions supported.

- The policy architecture should operationally scale (e.g., per-subscriber provisioning of policy data should be minimized).
- The policy architecture should provide for consistency & integrity of policy data.
- Policy-controlled packet-flow optimization should be possible, especially for latency-sensitive traffic, so as to minimize impact to traffic throughput in the packet data subsystem.

Any successfully deployed policy must accommodate multiple representations. As a policy reflects a system management objective, it must be represented in a form understood by a network operator. Since this same policy is implemented on one or more network elements, it must also be represented in a tangible form suitable for the network element. This implies that a translation must exist between a system managment objective and its realization in the network. An example of such a translation is between a Service-Level Agreement (SLA), and its objectives and metrics (Service-Level Objectives, or SLOs) which specify services that the network will provide for a given client. The SLA is usually written in high-level system management terminology and must be translated into lower-level specifications suitable for the applicable network elements.

The main control elements for policy implementation is Policy and Charging Rules Funtion (PCRF), which governs at the top-level various aspects of policy. The policy rules are disseminated to various other control elements in the network, including Access Gateways (AGW), and Access Points (AP) (e.g. to implement policy rules associated with medium access control and scheduling on the radio interface). Though most aspects of policy are expected to be implemented in the fixed network elements, some controls may be conveyed to the AT from the network, as demonstrated in the following example:

A roaming AT can contain two IP addresses, one assigned by the home network, the other by the visited network. The policy diseminated to the AT could be:

- MUST use the home network assigned address for SIP signaling to initiate VoIP session;
- MUST use the visited network assigned address for transmission of VoIP media packets, in order to optimize routing (preclude media path tromboning)

# 5 REQUIREMENTS

The requirements for MMD policy enhancements are specified in this section. Some illustrative examples are in Annex A.

## 5.1 Policy Contexts

### 5.1.1 Network-Level and User-Level Policies

User-level policies are those applied to a single user based on their subscription. MMD shall provide capabilities to define and enforce network-level and user-level policies at various states of device operation (registration, handoff, change in access technology, and other similar states) based on, but not limited to, the following:

- QoS constraints
- Accounting
- Mobility and Roaming
- Access Technology
- Authentication and Re-authentication
- Network Selection
- Traffic Engineering
- Resource Selection (e.g. routing optimization)
- Packet Flow Optimization
- Address Translation (to support NAT/Fire Wall (FW) Traversal)

## 5.2 Admission Control

### 5.2.1 IP Flow Admission

MMD shall provide support for admission control of IP flows. Admission control includes congestion related decisions at the time an application is invoked, based on, but not limited to, the following:

- Network resource allocation and service differentiation (e.g. differentiation between IP Television (TV) and Video Telephony)
- An indication from the radio access network of the mobile device availability status
- The characteristics of the mobile equipment, such as its software version, screen size, and other similar characteristics
- The subscription profile of the subscriber invoking the application (e.g. preferential access based on subscription)
- Other applications that a subscriber has simultaneously invoked (including SIP and non-SIP applications) based on service characteristics and subscriptions

- The media makeup and bearer flows associated with the application being invoked (e.g. audio, video)
- The QoS characteristics of the application (e.g. conversational, streaming, interactive and background). See reference [2].
- Time of day
- The characteristics of the content being delivered by the service.

### 5.2.2 Access Network Selection

A multi-mode User Equipment (UE) shall work in concert with the network to automatically determine which access technology (e.g., 1x Radio Transmission Technology (1xRTT), Evolution Data only (EVDO), WiFi) will be used at any given moment, based on factors such as network policy (e.g. operator preferred roaming or peering partners), RF conditions, QoS capabilities, and bandwidth capabilities. The customer may be allowed to invoke a manual override of access technology used (e.g., customer prefers WiFi).

### 5.2.3 QoS

MMD shall provide the capability for an application on an AT to request QoS with specified characteristics, and admit the application based on those characteristics.

### 5.2.4 Security Status

MMD shall provide the capability to make admission decisions at the time an application is invoked based on the security status of the mobile.

### 5.2.5 Roaming Status

MMD shall provide the capability to make admission decisions based on the roaming status of a user, including, but not limited to, the following:

- The identity of the user’s visited network
- The geographic location where the user is roaming
- The technology of the visited access network (e.g. High Rate Packet Data (HRPD), cdma2000, WiFi, DSL, etc.)

### 5.2.6 Network Status

When roaming, the visited network shall be able to make admission decisions based on, but not limited to, the following:

- The types of network resources (QoS, accounting, etc.) available to roaming users
- The amount of network resources (percentage of access bandwidth, credit balance, etc.) available to roaming users.

- Whether network resources are granted to a visited subscriber for better than best-effort service based on the identity of the home provider
- SLA in effect with the home operator
- The type of invoked application (both SIP and non-SIP)
- Any home and local security restrictions

### 5.2.7 Third Parties Applications

MMD shall provide the capability for the network to make network-resource allocation & charging decisions for applications that are provided by third party applications.

### 5.2.8 IP Address Assignment when Roaming

MMD shall be capable of assigning an IP address to the roaming UE based on permissions of its home operator’s policy settings.

### 5.2.9 Resource Admission

The MMD resource admission control decision shall be subject to policy control for both SIP and non-SIP applications.

### 5.2.10 Access to Services

MMD shall support the ability of the Network Service Provider (NSP) to use the following to control the user’s access to specific services when the user is roaming: (1) service properties, (2) operator policy specific to a roamed network, and (3) service profile data.

## 5.3 Policy Peering

### 5.3.1 Service-Level Agreement

MMD shall provide the capability to support policy peering relationships based on either SLAs between individual network operators or network operators’ mutual agreements with clearinghouses. These peering relationships shall support the exchange of policy/charging rules between the peered networks.

Note: There may be different aspects of peering, e.g.: IP-level, policy, security, and application.

### 5.3.2 Media Traffic Routing

MMD shall provide the capability of the home network to decide, on an application-by-application basis (both SIP and non-SIP) whether or not the media traffic needs to be routed through the home network. The visited network shall have the capability to override home network policy decisions related to use of visited network resources.

### 5.3.3 Roaming User Support

MMD shall enable the NSP to provide policy peering for SIP and non-SIP applications with other providers for supporting roaming users.

### 5.3.4 Home and Visited Network Control

MMD shall support policy peering to allow for both the home and the visited network to exert policy control of resources used in the visited network to meet subscriber expectations of service quality.

## 5.4 Policy Management

### 5.4.1 New Characteristics and Applications

MMD shall provide the capability to define new characteristics and add new applications over time, and to define policies based on those characteristics, along with a mechanism for managing these policies.

### 5.4.2 Policy Consistency

MMD shall provide the mechanism for distributing consistent policy and context across one or more domains to any network element that participates in policy decisions or policy enforcement.

### 5.4.3 Hierarchical Policy Rules

MMD shall allow for a hierarchical set of policy rules. The policy rules shall explicitly specify their precedence. The policy enforcement point shall act in accordance with precedence of rules, so that any conflict between them can be resolved.

### 5.4.4 Subscription Information

MMD shall provide the capability to base policy decisions upon subscription information. The Policy and Charging architecture should avoid duplication of subscription information relevant for policy decisions.

### 5.4.5 Policy Change

The policy data repository function shall provide a mechanism which allows relevant network elements to be informed about policy changes.

### 5.4.6 New Services and Features

Changes to the policy peering interface between roaming partners shall not be required when new services or features are introduced in the home network.

### 5.4.7 Parental and Enterprise Control

MMD shall support parental/enterprise control by providing the capability of an authorized entity (parent, corporate administrator, etc.) to update the policy of a particular subscriber or set of subscribers.

### 5.4.8 User Personalities

MMD shall support User Personalities by allowing a subscriber to have multiple sets of policy and selecting a particular set in real time based on various conditions such as signaling message parameters and time of day.

### 5.4.9 Dynamic Policy Changes

MMD shall have the capability to change policy decisions after an application has been invoked, based on changes in access technology, time of day, location, & application-specific behaviors.

### 5.4.10 Emergency Services and Priority

MMD shall be capable of providing emergency services with QoS, and priority treatment over existing calls, based on NSP policy.

## 5.5 Authentication

### 5.5.1 Trust Hierarchies and Horizontal Relationships

MMD shall provide the capability to define policies associated with trust hierarchies and horizontal relationships between trust domains. A trust domain is a collection of network elements subject to a common set of security policies.

### 5.5.2 Credential Distribution

MMD shall provide the capability to define policies which govern the distribution of security credentials across network elements.

### 5.5.3 Credential Expiration

MMD shall provide the capability to define policies that govern expiration and refresh of security credentials.

### 5.5.4 Credential Information Exchange

MMD shall provide the capability to define policies that enable and disable credential information exchange which support optional authentication procedures.

## 5.6 Privacy

### 5.6.1 Asserted User Identities

In roaming and peering contexts, MMD shall be able to define and manage the policy as to which asserted user identities may be communicated between certain network entities in the same network and exported from the home network to external networks.

# Annex A Requirement Examples (Informative)

This annex contains illustrative examples. The examples are not exhaustive. Each example is linked to the corresponding requirement by means of the associated paragraph number and title. The paragraph numbers in the annex correspond to the associated requirement in the body of the document.

## A.1 5.2.1 IP Flow Admission

- An indication from the radio access network of the mobile device availability status

  Example: If a mobile device presence status is “not available”, a Voice over IP (VoIP) attempt to that device may be directed to a Voice Mail Server before resources are committed to establish a VoIP session.
- The subscription profile of the subscriber invoking the application (e.g. preferential access based on subscription)

  Example: A VoIP session attempted by a priority user may be admitted, while ordinary users’ attempted sessions may be blocked.
- Other applications that a subscriber has simultaneously invoked (including SIP and non-SIP applications) based on service characteristics and subscriptions

  Example: If a subscriber is in a VoIP session, adding a multimedia streaming session may be disallowed while congestions persists.
- The media makeup and bearer flows associated with the application being invoked (e.g. audio, video)

  Example: In cases of severe congestion, attempted PSVT sessions may be curtailed to audio only.
- The QoS characteristics of the application (e.g. conversational, streaming, interactive and background). See reference [2].

  Example: An application that is more delay tolerant has lesser probability of being admitted, or visa-versa, an application that is not delay tolerance has lesser probability of being admitted. The operator can decide to implement the policy either way.
- Time of day

  Example: Admission regime may change depending on the time of day. For example, a proportion of traffic “reserved” for VoIP may be increased during the traditional peak usage hours important for business users.

- The characteristics of the content being delivered by the service.

  Example: Admission for users attempting to access business-related content may be different than if the content is of entertainment nature.

## A.2 5.2.6 Network Status

- The amount of network resources (percentage of access bandwidth, number of charging counters, etc.) available to roaming users

  Example: The visited network may impose admission related policies to the roaming subscriber similar to those enumerated in 5.2.1.
- SLA in effect with the home operator

  Example: Based the identity of the home provider, network resources granted to a visited subscriber may be restricted to best-effort services only.

## A.3 5.4.1 New Characteristics and Applications

Example: Introducing multimedia priority service for a certain class of users may require new policies, such as preferential admission. These new policies may require new mechanisms for the policy implementation, such as priority treatment in SIP-aware network elements.

## A.4 5.4.3 Hierarchical Policy Rules

Example: Policy rule #1: In case of congestion, admission for high latency applications (e.g. web browsing) shall be curtailed first, and admission for real-time application last. Policy rule #2: Users subscribed to multimedia priority services shall have preferential admission. Let us assume that congestion occurs in the network, so that high latency applications are not being admitted, e.g. all but VoIP are being curtailed. If a multimedia priority service is invoked for a high latency application, such as web browsing, the priority subscriber is nevertheless admitted, i.e. rule #2 has precedence over the rule #1.

## A.5 5.4.4 Subscription Information

Example: Duplication of information that affects policy in PCRF and HSS should be avoided. For example, if the PCRF contains information that affects admission policy, any analogous information should not be duplicated in the subscription profile in the HSS.

## A.6 5.6.1 Asserted User Identities

Example: A roaming subscriber’s account with an adult content channel is not revealed to the visited network by specific reference to that subscriber’s explicit public identity, though the fact that special charging rules apply is revealed.