ATIS EXPLORATORY GROUP ON CONVERGENCE (EGC) REPORT AND RECOMMENDATIONS

September 2007

ATIS (Alliance for Telecommunication Industry Solutions) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 22 industry committees and its Incubator Solutions Program.
< http://www.atis.org/ >

ATIS Exploratory Group on Convergence

This is an ***ATIS Report*** developed by the **Exploratory Group on Convergence** for the **TOPS COUNCIL**.

This document is a *work in progress* and subject to change.

Published by
Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright © 2007 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < http://www.atis.org >.

Printed in the United States of America.

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 1

2 INTRODUCTION 4

3 DEFINITIONS AND ASPECTS OF CONVERGENCE 7

3.1. SERVICE CONVERGENCE 7
3.2. NETWORK CONVERGENCE 8
3.3. OPERATIONAL CONVERGENCE 8
3.4. SERVICE CONTINUITY AND SERVICE TRANSFER 8
3.5. QUALITY OF EXPERIENCE (QOE) 9
3.6. SERVICE INTEGRATION 9
3.7. SERVICE CONCURRENCE 9
3.8. SERVICE PROVIDER 10
3.9. ACCESS TECHNOLOGY 10
3.10. USER INTERFACE 10
3.11. SECURITY 11
3.12. USER PROFILE 11
3.13. DEVICE PROFILES 11
3.14. QUALITY OF SERVICE & SERVICE LEVEL AGREEMENTS (QOS/SLA) 11
3.15. POLICY-BASED RESOURCE CONTROL AND MANAGEMENT 12
3.16. NETWORK ATTACHMENT 14
3.17. SERVICE SUBSCRIPTION 15
3.18. SERVICE PROVISIONING AND MONITORING 15
3.19. SERVICE INSTANCE (TUPLE CONCEPT) 15
3.20. INFORMATION MODELS 16
3.21. SERVICE INTERACTION MANAGEMENT 16

4 USE CASES 17

4.1. APPLICATION TO NETWORK INTEGRATION 18
4.2. UNIFIED USER PROFILE 18
4.3. CONSISTENT FEATURE INTERACTION 19
4.4. MEETING FINDER 20
4.5. SECURITY RELATIONSHIPS FOR CONVERGED DEVICES 20
4.6. SERVICE TRANSFER 21
4.7. QOS/SLA 21
4.8. QUALITY OF EXPERIENCE (QOE) 22
4.9. MULTI-PROVIDER SERVICE BUNDLES 22
4.10. WEB/IMS HYBRID SERVICE 22
4.11. FLEXIBLE POLICY USE CASE 23
4.12. BILLING CONVERGENCE 23
4.13. UNIFIED PRESENCE 23
4.14. MACHINE-TO-MACHINE & MONITORING 24
4.15. SERVICE CONTINUITY BETWEEN ACCESS NETWORKS 24
4.16. SERVICE INTERACTION MANAGEMENT USE CASES 25

5 CONVERGENCE REQUIREMENTS 26

5.1. SERVICE CONVERGENCE 27
5.2. SERVICE CONTINUITY/ SERVICE TRANSFER 27
5.3. ACCESS AND CORE TECHNOLOGY 29
5.4. SECURITY 30
5.5. USER PROFILE 31
5.6. QOS/SLA 32

5.7. SERVICE PROVISIONING AND MONITORING 34
5.8. POLICY 34
5.9. SERVICE INTERACTION MANAGEMENT REQUIREMENTS 34

6 ARCHITECTURE ASSESSMENT 35

6.1. OAM&P 38
6.2. APPLICATION & SERVICE CAPABILITY 39
6.3. SESSION & TRANSPORT CONTROL 40
6.4. NETWORK INFRASTRUCTURE 40
6.5. ASSESSMENT SUMMARY 41

7 CONVERGENCE ISSUES 42

7.1. OAM&P ISSUES 43
7.2. APPLICATION & SERVICE CAPABILITIES 44
7.3. SESSION & TRANSPORT CONTROL 44
7.4. NETWORK INFRASTRUCTURE 45
7.5. CONCLUSIONS 46

8 RECOMMENDATIONS 47

APPENDIX A: ATIS BOOT STRAP PROCESS 49

APPENDIX B: STANDARDS INITIATIVES 51

APPENDIX C: EXAMPLE ARCHITECTURE MODELS 55

APPENDIX D: FRAMEWORK REFERENCE POINTS 71

APPENDIX E: FRAMEWORK-USE CASE MAPPING 73

APPENDIX F: TUPLE CONCEPT EXPLANTATION 80

APPENDIX G: SERVICE INTERACTION MANAGEMENT 83

APPENDIX H: ACRONYMS & ABBREVIATIONS 87

APPENDIX I: EGC MEMBERS 91

1 EXECUTIVE SUMMARY

Convergence from a telecommunications point of view often promises the ability to deliver any-service, anytime, anywhere, via any-access technology. The need for and value of realizing such convergence across both wireline and wireless service offerings has been contemplated for the last decade but has recently taken on a sense of urgency within the industry. Today's market conditions and subscriber demands continue to drive the introduction of non-standard "convergence-like" applications, while in parallel, specific steps required to achieve full convergence and deliver innovative new services with a quality user experience need to be assessed.

Recognizing the sense of urgency to deliver full convergence in a consistent and standardized manner, the ATIS Technical and Operations (TOPS) Council formed an Exploratory Group on Convergence (EGC) in August 2006. The EGC was chartered with the purpose of recommending steps to better address the standards and business needs of the telecommunications industry based on aspects of convergence within the context of a Next Generation Network (NGN).

In this report, the EGC documents its findings, provides its conclusions and offers its recommendations towards addressing convergence. More precisely, the EGC defines the meaning and scope of convergence and its various aspects, delineates "use cases" and the network requirements needed to enable converged services, and provides an assessment of the current architectural frameworks standardized today to ascertain the level and types of support currently enabled versus those needed longer term to enable network-based converged services.

As service providers continue their deployment of the NGN towards a common consolidated Internet Protocol (IP) core network, it is of paramount importance that the delivery of services be sufficiently similar across different providers, through different end-devices and across multiple access technologies. In addition, while not necessarily vital to the delivery of converged services, efficiencies gained in CAPEX and OPEX as a result of network convergence is also a driving factor. Accordingly, delivery of true network-based convergence --while anticipated to be incrementally deployed over time -- will require the identification, standardization and implementation of: (1) consistent application and service capabilities (eventually offered from a centralized service-platform), and (2) deployment of common network functions and interfaces supportive of a consolidated IP core network.

From this study, the EGC concludes that realizing the full potential of convergence will require a fundamental shift in the industry's approach to traditional wireless, wireline, and service silos. To support and enable the development of standards to achieve full convergence, the EGC also concludes that standardization programs must broaden their efforts from a technology or service specific (vertical) approach to that of a comprehensive holistic end-to-end (horizontal) standpoint that considers the entire telecom ecosystem (e.g., device, access networks, core networks, services and applications). As the industry takes steps to consolidate offerings to enable convergence, so too should its standardization efforts.

Other observations and conclusions of the EGC, which are more fully detailed in Section 7 of this report, are as follows:

- Security and subscriber profiles are often access specific while user and network attachment concepts are almost never clearly separated.

- Today, there is no clear mechanism to ensure that service interaction can be effectively managed across service types or service domains (e.g., a combined Multimedia Sub-system (IMS) + Web Services architecture).

- It is not clear how service interaction can be avoided between service logic in the Application Servers/User Equipment (UE) and the service enablers in the network. In particular, there is a need to avoid having service enablers be affected by evolving functionality in the UE, while still allowing applications to take advantage of network provided service enablers.

- Today there is no generic service ordering interface, especially between different commercial entities.

To assist the industry's movement towards convergence by addressing the issues summarized above and further enumerated in this report, the EGC fundamentally recommends that initiatives be undertaken to attain a consistent approach to convergence whereby development of necessary standards is across technology and/or service domains (i.e., silos). More specifically, the EGC offers its recommendations as stated below. The extent to which these recommendations are incorporated and enacted is deferred to ATIS, given their procedural and organizational impacts.

A. Adopt the EGC framework as the basis for the coordination of ATIS' convergence efforts.

B. Establish an initiative for the coordination and development/evolution of a common NGN architecture that enables full convergence.

C. Adopt the "enhanced Telecom Operations Map" (eTOM) model developed by the Tele-Management Forum and endorsed by ATIS Telecom Management and Operations Committee (TMOC), as the basis for Operations, Administration, Maintenance and Provisioning (OAM&P) and support standardization across all aspects of convergence services and Network Infrastructure.

D. Establish an initiative for the coordination and standardization of Service Capabilities enabling convergence applications and services. The initial focus should include, but not be limited to:

    - User Data such as Identity Management and User/Subscriber Profiles
    - Service Brokering (interaction management) including NGN and Service Oriented Architecture (SOA) technologies
    - Content Functions such as content preparation, content sourcing, and rights management

- Coordination of other relevant standards/specification efforts

E. Adopt a common model for Transport Control, such as ITU-Telecommunications Standardization Sector (ITU-T) model for the standardization of the Network Attachment and Control functions and Resource and Admission Control functions.

F. Establish an initiative for the coordination and standardization of consistent interfaces between a converged IP Infrastructure and any access supporting features such as end-to-end security and Quality of Service (QoS).

G. Establish an initiative for the coordination and standardization of methods, objects, and corresponding metadata definitions to promote convergence services and applications. Initially, these include:

- Access independence for security and QoS
- Network Service Provider to Application/Content Service Provider interactions
- Transport Control Framework
- User Profile and Identity Management
- Service continuity, beyond voice to include multimedia, video, and data

H. Establish an initiative for further study on Premises Equipment frames (residential, Small Office/Home Office (SOHO), Server Message Block protocol (SMB), and Enterprise), as appropriate.

I. Establish an initiative for further study on inter-provider interworking, as appropriate.

2 INTRODUCTION

A number of ATIS committees, such as ATIS Packet Technologies & Systems Committee (PTSC), Wireless Technologies & Systems Committee (WTSC), Internet Protocol Television (IPTV) Interoperability Forum (IIF), and ATIS Telecom Management and Operations Committee (TMOC), are working in the area of convergence, all having recently launched efforts to address specific convergence-related issues. However, as the full scope of convergence will involve many technology and service aspects, the ATIS Technology and Operations Committee (TOPS) Council anticipated that issues in the telecommunication's industry standards will only become apparent when analyzed from an access independent, Next Generation Network (NGN) perspective. For this reason, among others, the ATIS TOPS Council NGN Focus Group identified convergence topics in their 2006 Gap Analysis; stating that additional work in terms of the scope and impact of convergence needs to be studied.

This document identifies findings including definitions, requirements summary, architecture view and issues identified for convergence, provides conclusions and offers recommendations towards addressing convergence.

What is Convergence?

As NGNs are deployed and evolve, there will be an increasing need to provide continuity of service between the various types of access networks from a user perspective. To support the needed equipment interworking, standards that specify core service requirements and a fundamental architecture are needed. Convergence in this context includes Service Convergence and Core Network Convergence. Service Convergence means the ability of all services to be sufficiently similar from the user's perspective as he or she accesses those services from different providers, through different end devices and access technologies. Network Convergence means the ability to enable Service Convergence from a single consolidated core.

The requirements to satisfy all forms of broadband access technologies should be considered including wired, wireless; fixed, nomadic, and mobile; and all forms of real-time and non-realtime services including voice, audio, video and data. The requirements to support a range of services, including those from third party service providers, should also be considered. The end goal is any-service, anytime, anywhere on any access technology. Acknowledging this goal, the initial standards focus may be constrained to satisfy pressing market needs.

Areas considered in the development of convergence include the following aspects of service convergence and network convergence:

- Standards to link a variety of user devices, across various access technologies, to a user profile. This includes the ability to have all the user's devices simultaneously associated with a user profile, even if not all the devices are active.

- Standards to allow services from different service providers to be linked to a user profile, and to be coordinated in an appropriate fashion.

- Seamless service continuity between different access networks (e.g., Circuit Switched, Global System for Mobile communications (GSM) and Internet Protocol (IP) Wireless Local Area Network (WLAN), and WiMax, etc.) and associated call/session control interworking (e.g., Public Land Mobile Network (PLMN)/Public Switched Telephone Network (PSTN) and IMS).

- Standards to enable service control from a single consolidated core network with a single common and consistent service environment.

- Interoperability between multiple NGN business entities and legacy operations.

- Delivery of services, independent of access technology.

- Coordination of service data in and between user equipment, access networks, and core networks for a consistent user experience.

- Flexible subscriber addressing, including multiple directory numbers (e.g., two or more E.164 numbers) and new means of identification.

- Network/Domain selection for originating and terminating calls.

- Consistent Supplementary Services support (e.g., Call Forwarding, Call Waiting, Call Hold, etc.)

- Consistent Security.

- Quality of Experience.

- Full Multimedia support (e.g., Voice, Video, Data) based on access method.

- Emergency Services support.

- Digital Rights Management support.

This list provides some of the issues that need to be addressed to achieve a compelling degree of convergence in tomorrow's networks.

The telecommunications industry is undergoing transformation to a more dynamic mobile and Internet influenced service model reflecting 21st-century market conditions and user expectations. As service providers migrate to NGNs and deploy a mix of access network technologies such as shown in Figure 2-1, there will be an increasing need to provide service continuity between access networks, and provide a consistent user experience (to the degree possible) for the provided services.

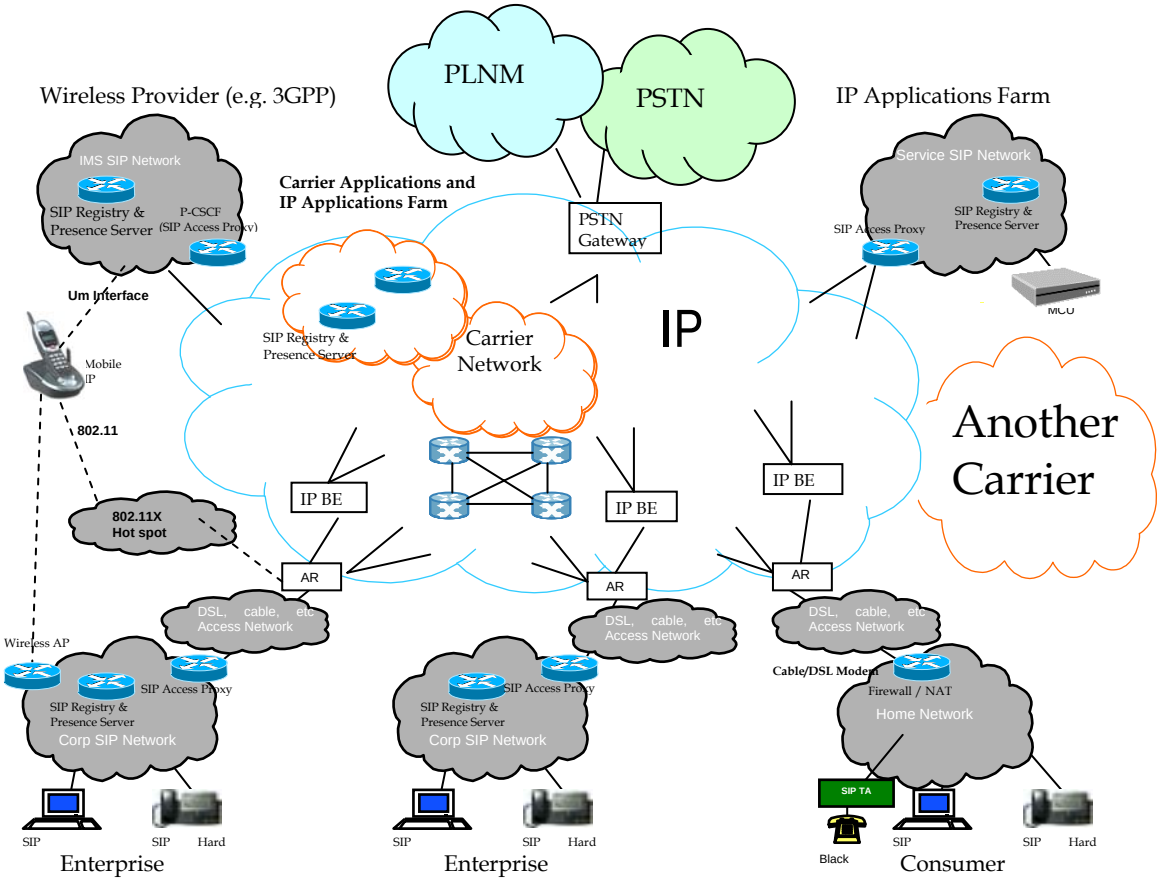


Figure 2-1 Various Access Networks

Driven by IP technologies, the first steps of network convergence are already well underway in many service providers. In this context, wireline-wireless convergence can be seen as the unification of any (or many) access method(s) via a shared IP core. New service applications such as IPTV and IMS sessions can be added to existing Internet and Enterprise applications given a capable IP network. Business processes and operations can be extended to interwork across multiple providers to support "full" convergence. Yet, from a user viewpoint, networks and operations are typically less important than the communication of content and media.

A pressing need for service continuity between types of networks (wireline and wireless) is the ability to provide voice communication between WLAN products that are based on IEEE 802.11x standards (WiFi)-enabled Digital Subscriber Line (DSL) and GSM access. A subscriber may have a Voice over IP (VoIP) call established on a dual-mode (WiFi/GSM) user equipment, move out of coverage of the WLAN access but be within GSM coverage, and need the call to continue seamlessly. Conversely, a subscriber may move from GSM coverage into WLAN coverage, and desire the call to seamlessly transfer from GSM to WiFi. These are specific examples of convergence that should be covered by the more generic convergence standards. Further use case examples may be found in Section 4.

The initial realizations of convergence may focus on voice-service continuity between wireline and wireless networks; however, other services such as multimedia and video offers must be taken into consideration. A key aspect of convergence in this context is consistency of service definitions across a range of access networks, or suitable mapping between access networks. This broader view is also in scope for the EGC.

Following consensus on the scope of "Convergence" as stated above and further defined in Section 3, Figure 2-2 indicates the EGC process leading to the recommendations found in Section 8. The process to identify the Convergence Issues (Section 7) and the resulting Recommendations (Section 8) built from the use case descriptions (Section 4) and Convergence Requirements (Section 5) and the "boot-strap" process indicated in the gray shading and further discussed in Section 6 Architecture Assessment. Supplementary material can be found in the Appendices.

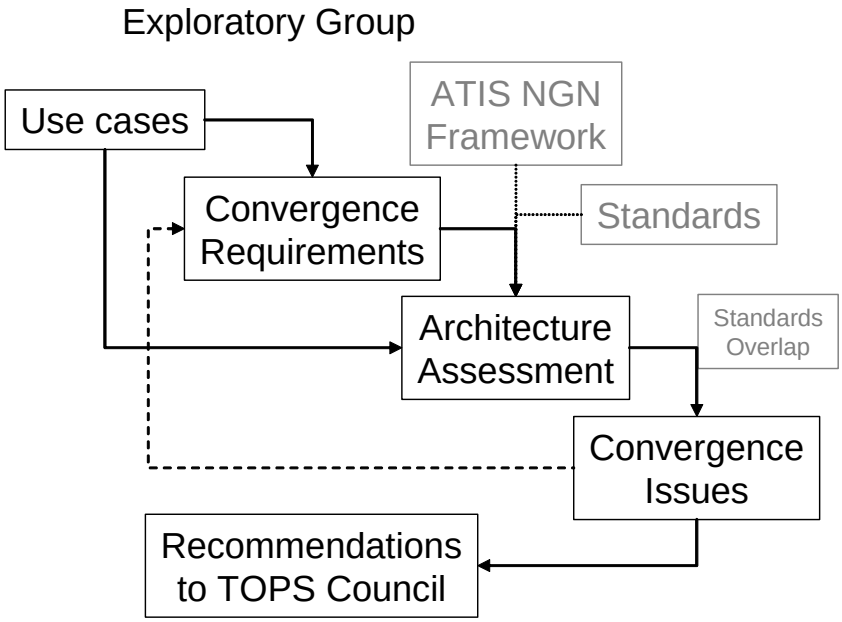


Figure 2-2 - ATIS EGC Process

3 DEFINITIONS AND ASPECTS OF CONVERGENCE

The end goal of convergence, to provide users with any-service, anytime, anywhere via any access technology, implies capabilities such as service continuity, service transfer, network security, user profile management and service provisioning and monitoring. These are examples of the capabilities necessary for "service convergence." To characterize convergence and its aspects, we specifically define:

3.1. Service convergence

Service convergence is a sufficiently similar service experience from the user's perspective provided across different provider networks, access technologies, and end devices, recognizing limitations of different devices and technologies. Converged services can leverage shared application functions, across different

access media, terminal types, and service providers. An example of service convergence would be the same service delivered to a mobile terminal, a television, or a computer with a sufficiently similar experience. These devices could be connected, for example, over a wireless data link, over a wireless voice link, over a co-axial cable plant, over a fiber plant, or over twisted pair.

3.2. Network Convergence

Network convergence enables service providers to deliver consistent services from an IP infrastructure across a diversity of access networks. The IP infrastructure also supports session and policy control, applications and service capability, and Operations, Administration, Maintenance and Provisioning (OAM&P). While network convergence is not necessary for service convergence it can simplify its implementation. A key driver for network convergence is reducing Capital Expenditures (CAPEX) and Operational Expenditures (OPEX).

3.3. Operational Convergence

Operational convergence provides maximum functional commonality or interworking of Business Support System (BSS), Operations Support System (OSS), network management, service provisioning, billing, et cetera across all service types (data, voice, video and any combination thereof) within the context of a Service Delivery Environment (SDE). The TeleManagement Forum (TMF), for example, has defined a Next Generation Operation Support System (NGOSS) architecture that is applicable.

3.4. Service Continuity and Service Transfer

Service continuity is the continuation of active service from the user's point of view, across devices or access networks or both. For example, service continuity can apply to single services such as voice, or to composite services such as voice and video along with associated data exchange such as web browsing or instant messaging. Service continuity may be seamless and performed automatically. Alternatively, service continuity may involve some degree of interruption or service modification; it may be governed by user preferences or may be user-initiated or user-approved. Regardless, technical limitations of devices, access networks or the service provider will influence the characteristics of service continuity.

Service continuity includes all aspects of the service:

- media flow (e.g., voice video or data, singly or in combination)
- features and applications (e.g., presence or call waiting or program guide)
- context and association information (e.g., application state, or audio/video bookmark, or history, favorites or cookies)

Service transfer refers to the means whereby service continuity is supported from the network point of view.

3.5. Quality of Experience (QoE)

An important aspect of service is Quality of Experience (QoE). QoE requirements define the overall, subjective performance at the services level from the perspective of the end user. The establishment of consistent, baseline QoE for end users and the corresponding objective engineering targets is critical to the market success of many service offerings. When the user experience is within defined bounds, the service is deemed to be operating as expected within its QoE profile. A key direct measure of QoE is the Mean Opinion Score (MoS). Many objective measures, such as the duration of periods of degraded service (e.g., Degraded Seconds, Errored Seconds, Unavailable Seconds), may provide easily-measured parameters that can provide inferences to QoE, but may not measure all aspects of a given user experience of the service. QoE is also studied and formally defined in several places, including the ITU Telecommunications Standardization Sector (ITU-T) Study Group 12 (Q.13/12), in the ATIS IIF, Quality of Service (QoS) Metrics Task Force, and in the DSL Forum Technical Report TR-126.

Since consistent QoE is recognized as a critical factor in providing a successful service, it is important to quantify the relationship between QoE and QoS. The reason that this relationship is important is twofold: it allows measurement of QoS to predict an expected QoE; and, given a target QoE, it allows the derivation of required service layer performance. This relationship is actively being explored in several standards forums, and the ATIS IIF (Issue IIF-2006-020) aims to create a concise and effective set of QoS measurements that would allow prediction of QoE for IPTV. The relationship between QoS and QoE may be expressed by means of one or more models and computations for video, audio, multimedia, and transactions.

3.6. Service Integration

Service integration imparts to the user the experience of one seamless, composite service instead of separate services, by way of *additional functionality* that binds them together. For example, IPTV and VoIP service where the viewer's IPTV screen displays "Mom" over the current program and the sound mutes while the incoming call from Mom is delivered to the target device (e.g., house phone). Or as another example, a caller's yellow pages web query for nearby Thai restaurants leads to a reservation confirmed with the chosen restaurant with caller preferences (e.g., no smoking), and the reservation and directions downloaded to the caller's Personal Digital Assistant (PDA)/calendar.

3.7. Service Concurrence

Service concurrence is a sharing of an active service among devices or networks. This can include various manipulations to share, extend, or prune membership

in a multi-party service or multi-network connectivity that supports it. The concept of concurrence applies not only to a service, but also to sessions, application associations and to context.

Session concurrence
Session concurrence is the simultaneous participation of a plurality of devices or networks in supporting a session as well as merging two or more existing sessions into a single session. Typical manipulations include adding or dropping devices from a session. Like the transfer case, session concurrence may involve pausing or making a session quiescent before manipulation, or it may not. For example, it is reasonable to expect a session to be concurrent on two different access networks in order to support a dual-mode device moving among different access types. However, it may also be reasonable to expect to pause a video session before extending it to additional devices.

Context/Association concurrence
Context/Association concurrence is the sharing or synchronization of other information associated with a service, such as application state or security context. Examples of this include: history, favorites and cookies associated with web browsing – or the point in a video where playback is happening, the playback state, as well as Digital Rights Management (DRM) information and traffic encryption keys.

3.8. Service Provider
Service provider convergence allows continuity of service across multiple service providers. This is intended to include services incorporating mobility and nomadicity, which includes roaming between providers. For example, service providers may provide access, network connectivity, applications or content.

3.9. Access Technology
Access technology convergence covers a full range of access technologies encompassing mobility, nomadicity, and roaming between networks. Example access technologies include broadband wireline Ethernet via DSL, Cable, and Fiber, broadband wireless such as Universal Mobile Telecommunications System (UMTS), EV-DOrA, WiMax, and WiFi, and narrow band access including wireline analog and wireless GSM and Code Division Multiple Access (CDMA) circuit switched voice, as well as General Packet Radio Service (GPRS)/Enhanced Date rate for GSM Evolution (EDGE) and Single Carrier Radio Transmission Technology (1xRTT) for Short Message Service (SMS) and other low bandwidth data applications.

3.10. User Interface
User interface convergence covers a full range of user interface types, including fixed terminals, mobile handsets or other user devices and interfaces.

3.11. Security

Security covers all aspects of security, including network access, media access, media distribution, software upgrades, billing exchange, and application authorization. In addition, security must consider how all these individual security mechanisms can be combined to achieve end-to-end security.

To be successful, effective security policies must be developed and implemented in a systematic, consistent, and rigorous manner for services and networks. Developing effective security policies is best achieved by using a comprehensive security model such as the International Telecommunication Union (ITU) X.805 Security Architecture. The X.805 Security Architecture allows for a structured approach to developing security policies and determining what security services need to be deployed.[1]

3.12. User Profile

User Profile is user specific information related to communications, multimedia services (e.g., Home Subscriber Server (HSS), User Profile Server Function (UPSF)) and applications (e.g., Universal Description Discovery and Integration (UDDI)). User Profile also includes user policies applicable to multiple access media, different service providers, and different presence personalities. The User Profile can be accessed securely with its subsets able to be exchanged securely as required, including for billing and management purposes.

3.13. Device Profiles

Device profile is device specific information which identifies the capabilities of a device. This can include information on embedded applications and firmware as well as device configuration and ideally contains information on upgrades, updates and version numbers to applications or physical device accessory attachments. The device profile is used in the context of service convergence to define the parameters which affect QoE, transfer/concurrence and security posture.

3.14. Quality of Service & Service Level Agreements (QoS/SLA)

QoS/SLA is the application of Quality of Service management mechanisms and any applicable corresponding Service Level Agreements, to a given service, irrespective of the access media, terminal type or service provider. QoS encompasses the cumulative effect of numerous factors affecting service and network performance such as application availability and network transport characteristics. Typical QoS management in the IP domain involves the delivery of services within defined parameters for delay/latency, dropped packets, mis-ordered packets, jitter and error. QoS has end-to-end considerations across single or multiple providers.

[1] ATIS Next Generation Network (NGN) Framework, Part I: NGN Definitions, Requirements and Architecture, Issue 1.0, November 2004, Section 2.5.2.

3.15. Policy-based Resource Control and Management

Policy-based Resource and Control Management refers to a set of logical functions and physical components that enable the optimal operation and management of network resources. Policy Management provides policy control, resource allocation and management, and admission control functions based on pre-defined policy rules that can be associated with the access transport, session control, applications, peering, core transport and routing. Policy is a critical enabler for convergence since it allows consistent behavior for a variety of services, across a range of access technologies based on an individual customer's requirements.

Policy Management Framework

The Policy Management framework spans the organizational control of the access network, including the User-to-Network Interface (UNI), the core transport and session control, the Application-to-Network Interface (ANI) and the Network-to-Network Interface (NNI). The Policy Management framework includes the following functions:

- Policy Engine and Repository: describes and stores the business policy rules provisioned by an organization.

- Policy Decision Point (PDP): also known as a policy server, the PDP makes policy decisions based on the business policy rules and all other relevant static or dynamic network resource information.

- Policy Enforcement Point (PEPs): typically network resources that enforce and deploy policy decisions.

- Application Functions: typically network or client services that request certain QoE/SLA's.

- Resource Management (RM) function: enables the allocation of a pool of resources (e.g., media servers) to a specific service/service group, for load balancing, monitoring and control of such resources. It is important to track resource usage information on a per session basis to serve as input to the Resource Management function for decision-making and enforcement to ensure compliance with the required SLAs with end users and/or other networks.

Policy Domain Independence

Domain independence is defined as the ability of the Policy Engine to specify the behavior of the converged network by high-level policy rules in a declarative way and not by explicit configuration of individual system elements as in traditional networks. Policies are the links between a high-level business specification of desired services and low-level network element (NE) configurations that provide those services. An example of this would be a high-level business specification that only "Gold Users" may use video telephony during peak traffic hours. Independence between QoS signaling and Application

Session Control signaling becomes critical in order to achieve a converged, domain independent, service-based policy framework.

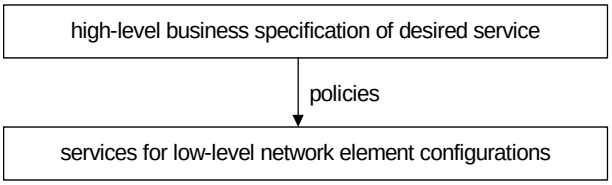


Figure 3-1: Policy Domain Independence

In the "Policy Domain Independence" model, requests for specific QoE/SLA are typically triggered from Application Functions (AF) to independent PDP elements. The PDP's use the policy rules along with runtime network resource information to make decisions and authorizing the corresponding domain-specific QoS resources. It is also possible to federate policy decisions between distributed PDP's.

Policy domain independence is especially important in the provisioning of end-to-end QoS between network boundaries. In this case, a special SLA must describe the QoS requirements for the traffic passing between different domains (e.g., guaranteed bit-rates, delay, jitter, etc), and network elements must be capable of mapping QoS signaling in order to police and condition the traffic at the network border.

The inclusion of a well-defined policy layer below the application and session control layers and above the network transport layer enables the separation into horizontal planes and abstraction of vertical control interfaces. The policy layer provides an adaptation layer between application-specific bandwidth needs and the network-specific controls needed to allocate resources in the access or core network. Thus, generic QoS requests can be translated into specific network commands. This frees the applications from needing to know the topology or details of the underlying networks.

Policy Controlled Resources

In a global single converged network architecture, PDP's interact with PEP to actually allocate and control QoS resources. Based on the type of physical resource requested and entities involved, the following grouping of resources and corresponding QoS capabilities can be identified:

- Access transport resources: entails policy management (admission control) of QoS resources that must be provided to a single or combined set of IP flows or the bearer associated with those flows in the access network or UNI. These types of rules can also prevent theft of service and/or denial of service.

- Core transport and routing resources: entails policy management of QoS resources to manage bandwidth control, routing and prioritization of

services within core network elements. In these types of resources, policy information is typically provided in advance, for example, when the NE is turned on or adjusted to different operation modes based on the time of day.

- Peering resources: implies multi-domain QoS Policy Management rules in order to support end-to-end QoS services across service provider's network boundaries or NNI, either in a peer-to-peer relationship or in a hierarchical multi-domain architecture.

- Application resources: entails the governance of application resources or service capability functions related to application service logic and media processing in the ANI. Policy rules enable flexible selection and tuning of the application resources and participate of the overall orchestration of converged services, e.g., through policy-based triggering rules such as load balancing or parental controls. In this regard, it is important to track resource usage information on a per session basis for admission control and managing resources to ensure compliance with the required SLAs with end users and other networks.

- Session control resources: implies the allocation of session control resources based on network-based rules e.g., based on utility computing requirements.

3.16. Network Attachment

The Network Attachment Control Functions (NACF) manages the functionality provided to the user by the access network. The specific functions provided by the NACF include:

- Network Access Configuration: allocates an IP address, assigns an access network identifier and provides network configuration data.

- Transport Authentication and Authorization: authenticates and authorizes the user equipment, or the user, for a given access network.

- Transport User Profile: stores user profile information applicable to the access network, and provides controlled access to this information to ensure the user receives the level of performance they are entitled to.

- Transport Location Management: registers the association between IP address, network location and geographic location.

- Access Management: acts as the control interface between the User Equipment and the access network, translating network access requests received from the User Equipment (UE).

3.17. Service Subscription

Admission and control may occur at multiple layers of the system: network, call and session control and application layers. Network registrations enable a device to attach and originate, or terminate IP packet flows. Call control registration enables the ability to send and receive session requests. In the case of some applications, such as video and gaming, a subscription may be needed to gain admission or access to content services.

Each of these layers involves a type of registration service and may require authentication and authorization. Such an authorization may be accompanied by encryption keys to enable packet and message exchanges associated with a registration, session, or subscription to be continuously protected by authentication, integrity and confidentiality services. It is important to note that the time scales for each layer may be different. Network access may change every few minutes. Session registrations could last for hours or days. Subscriptions could last for months.

Having long-lived keys for subscriptions may enable the underlying multicast and broadcast services to be relieved of the need at session setup time to establish security between the terminal and the network and thus reducing setup time and enhancing the speed at which service continuity may be achieved during terminal movement. For example, a video terminal may need to simply download the broadcast guide, tune it and deliver content with little per-terminal state maintained by the network.

3.18. Service Provisioning and Monitoring

Service provisioning and monitoring is the provisioning to establish and revoke service, and the monitoring of service availability in order to maintain service levels. Maintaining service quality requires the providers to communicate network characteristics and cooperate in delivering the service, be it for prevention, provisioning, growth, customer issue management or other purposes. The diagnostics can isolate the area of the fault in an end-to-end service, and possibly across multiple service providers.

3.19. Service Instance (Tuple Concept)

The Tuple Concept purpose is to provide flexibility through identification of atomic components that can be derived separately, but taken together, compose a coherent composite Profile. To support the concept of a Flexible User Profile, it is recognized that what once was a single monolithic object making assertions by one service provider about one service type for one device connected to one network and used by one user, needs to evolve to a composite object that can make multiple assertions from multiples of each dimension. In database terms, a given instance of a record has several attributes, each of which may take various values. In telecommunications terms, an assertion of a service instance is composed of a combination of various assertions about the nature of that service

instance. A tuple is simply a reference to a combination of components, for example:

ServiceInstance = (User, Device, AccessNetwork, CoreNetwork, ServiceType, Account)

That is, a collection of discrete assertions are aggregated into a composite description of the authorizations currently in effect that determine what services may be provided by the system as a whole. Actual service usage may then result in certain profile data being recorded in detail records.

It is also useful to differentiate between Authentication and Authorization. Authentication involves validating an assertion of Identity. Authorization involves an assertion that a user (authenticated or not) may use a service, in effect binding the Identity of the user to the Identity of the service. One may infer that asserting an association between a User/Device to a Network type also infers basic (Best Effort) data transport service over that network.

The set of identities and associations among identities will depend on the degree of granularity required in the architecture. The preceding example merely shows that when multiple players are involved, discrete assertions should be collectible into a unified expression that is referred to here as the Tuple. Defining those elements should be the focus of a standardization effort so that different players can contribute their part across administrative domains. For an expanded discussion of the Tuple Concept, see Appendix F.

3.20. Information Models

An information model is an abstract but formal representation of entities including their properties, relationships and the operations that can be performed on them. The entities can be either real or intangible.

3.21. Service Interaction Management

Service Interaction Management is the core of the distributed NGN service stratum architecture. It is a function that controls application interaction for the presentation of a service or services. The terms are defined as follows.

Application

Application software is a subclass of computer software that employs the capabilities of a physical computing platform directly to a task being performed. This should be contrasted with system software which provides an underlying set of tools and resources, but typically does not directly apply them in the performance of tasks that are the primary purpose of the computer. In this context the term "application" refers to both the application software and its implementation.

Application Server
An application server is a physical computer that supports a runtime environment for applications. The system software is an intrinsic part of the application server. Application servers ease application development by providing a suite of system software building blocks provided by the application server.

Service
A service refers to a discretely defined set of contiguous and autonomous business or technical functionalities. A service is comprised of a single application or multiple applications working in conjunction with one or more service interaction managers.

4 USE CASES

The EGC is exploring a level of convergence beyond that which is available in the marketplace today. With limited network-based service convergence,[2] consumer equipment and applications are emerging to support other forms of convergence-like services. This section begins with examples that are available in consumer devices today. These concrete examples provide a baseline for the more complex use cases that follow. The intent is to firmly ground "the concepts of convergence" by beginning with services and functionality that most readers will readily recognize or relate to. This section then builds a more complete picture of the functionality that network-based service convergence can provide.

Baseline Examples

Example 1: Service Convergence on a Single Device
Many people use their personal computer (PC) or PDA as the focal point for all their online activities and have a wide range of applications installed on it. These can include work email, personal email, several instant messaging platforms, online banking, and VoIP among others. The individual applications are separate, but the credential manager on the PC can provide easy access to any and all of these applications without having to remember the individual user names and passwords. It is also possible to share contact lists between different applications, or to find Instant Messaging (IM) applications that link together several other IM platforms to provide a crude form of service convergence.

Analysis: Convergence of credentials and exchanging contact lists between applications does provide value to users, and is becoming more popular. However, in general, any convergence beyond this level must be performed by specialized applications, or by the user. This creates a very "brittle" form of convergence. It is also limited to convergence on a specific device. If the user moves to a different device the convergence capabilities cannot follow.

[2] Current noteworthy examples of network-based service convergence are unified messaging, call forwarding, web-based call control such as incoming call screening or click2dial; and, arguably, common supplementary services on voice and switched digital calls facilitated by the ISDN/AIN architecture.

Example 2: Access, Location and Time Independence.
Television (TV) Subscribers (e.g., cable TV) can use their computer hard drives or other devices to record shows in order to watch them later. Other consumer electronics devices allow users to access their local TV channels from any location, over the Internet. Sophisticated users can even combine the two devices to watch recorded shows from remote locations. Up to a point, the combination of these two devices effectively makes a user's TV channels available "anywhere and anytime."

Analysis: In this case, a range of video services are "converged" by the combination of two consumer electronic devices. However, there are many limitations with this approach, such as computer storage capacity, or power failures that may make the service unavailable. In addition, to make this configuration work, the computer must accept remote commands that control the playback functions, creating a security vulnerability that could be exploited by hackers.

4.1. Application to network integration

Thomas subscribes to an enhanced Voice Call Continuity service (e-VCC) that supports seamless handover of calls between different access networks. This application supports handover of his mobile calls to his WLAN connection when he is in his home. When he enters his home, the e-VCC application coordinates securely with his home WiFi network to determine the Wired Equivalent Privacy (WEP) key, and downloads this securely to the phone, which then performs the transfer. The e-VCC application can also coordinate with "free" public WiFi networks to negotiate priority QoS for a small fee. The fee is added to Thomas' monthly e-VCC bill. If Thomas dials 9-1-1 when he is using the WiFi capability, the e-VCC application determines the phone location using the wireless network-based location capability, and communicates this to the Public Safety Answering Point (PSAP).

4.2. Unified User Profile

Bernard subscribes to Internet access from the telco that also provides his home phone. The Internet access includes email and a VoIP service. The phone company has integrated the various applications so that his home phone and VoIP client share the same phone number, and both ring when someone calls that number. The home phone also rings when the VoIP client is called using the Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) assigned to it. When there is no answer, a voice mail is left on the home phone and sent as an attachment to the email account. In addition, contact lists are automatically synchronized between email, VoIP and the home phone network-based speed dial capability. The email and VoIP also share the same userid and password, which can be changed from either account and automatically synchronized.

Analysis: To achieve this scenario, it is necessary to converge the concept of a user and their attributes across multiple environments, including multiple service providers. This may require a broad federation model, similar to the model for Identity used by the Liberty Alliance. It would eventually need to address issues related to schema, but in practice it may need to be a federation

model rather than a single unified schema, since the latter may not be practical anytime soon. These principles must apply to content as well as services and embrace IMS, Web Services and even Internet services.

4.3. Consistent Feature Interaction

Meghan has a number of friends who travel the world in search of adventure. On more than one occasion, she has called someone in the afternoon, only to discover that it is in the earliest morning hours in their current location. She now subscribes to a service that determines where the person is before completing the call, and prompts her to confirm she really wants to complete the call if it is between midnight and 6:00 AM at the called location. For this service to work properly, it must do the following steps in a predefined order:

1. IMS queries Infrastructure ENUM (I-ENUM) to determine if the number is ported, and if so, to which service provider.
2. Query the service provider to determine the location. (For a fixed line it determines the city. For a mobile phone it determines if it is turned on, and current location.)
3. Pass this information to a web services application to look up the time zone for the current phone location. The web services application then passes this information to Meghan's email application.
4. The email application then checks if it is between midnight and 6:00 AM at the called number location. If it is, then her email application prompts Meghan to confirm that she really wants to complete the call.
5. If Meghan confirms that she does want to complete the call, then the email application passes the target number to IMS to set up the call.

Meghan has a "friend" list in IMS, and also uses a web services based "click to call" service from within her email. She wants to ensure that this service behaves in a consistent fashion whether it is initiated from her IMS friend list, or from her email "click to call." Specifically, the processing logic must begin at step 1, even if the call is initiated from within her email application. For example, if the email application checked the time (step 4) before checking for number porting, it might use the wrong time zone.

Analysis: This use case requires that service logic must always be executed in the same order. If the Web Services application checked the time zone before checking for number portability, then it would get the time at the original location, rather than the time at the ported location. When fixed numbers can be ported to mobile numbers, this would make the problem more complex, since it would identify the original number location rather than the current mobile location. The Service Capability Interaction Manager (SCIM) uses filter criteria to provide consistent service execution order for IMS, but does not cover Web Services. A similar situation applies for the Service Broker function within Web Services. To ensure consistent service execution it isn't necessary to have a "Super Service Broker" that applies to IMS, Web Services, and other environments. However, it does require some mechanism, potentially at the provisioning level, that ensures service logic is applied in a consistent order

across environments. For example, in this case the email application would have to be provisioned to pass a "click to call" to IMS to initiate the service, and then let IMS pass it back to Web Services to check time zones. The key here is that Service Brokering is a concept, not a single entity in the network. It is possible, even preferable, to have separate instances deployed in and optimized for each service environment. This works as long as there is some mechanism that can consistently provision rules that span both domains.

4.4. Meeting Finder

Tim travels to a different city every week, meeting with several clients on each trip. To help keep him organized, Tim has now subscribed to a new "Meeting Finder" service that combines his calendar, a location based service, and a map service into a converged application. As Tim is finishing his first meeting of the day, he calls his assistant, Lisa and asks for directions to his next meeting. Lisa initiates a calendar application which determines the address of the next meeting, and passes this to a map application. A location service determines Tim's current location (based on the GPS in his mobile phone), and passes that to the map application. With the start and end locations, the map service calculates the directions to get from current location to the next meeting. The map application then pushes the directions to Tim's PDA. This works even though the call was initiated from a mobile phone. It could even work if Tim had initiated the process by calling Lisa from a conference room phone, sending an SMS or even an email.

Analysis: This scenario shows convergence of services, but also shows how different aspects of an individual must be linked. For example, the call is initiated on mobile phone, but the PDA has a better screen and GPS, so directions are downloaded to it and not the mobile phone. The user profile must link the user's various devices so that the mobile phone links to the email application, which in turn knows which device to download to.

4.5. Security relationships for converged devices

Phil has a new device – a PDA with cellular, WiFi and Bluetooth network capabilities. This device is used primarily by Phil – however he is interested in reducing the amount of clutter on his belt, and is interested in having both his business as well as his personal cell phone services converged on this device. The same is true for his e-mail and web access. The PDA is completely capable of providing all these services to Phil at the same time.

The problem is that Phil's employer does not want their corporate calling list or e-mail directory to be exposed to applications that are associated with Phil's personal phone or web access. Similarly, Phil is interested in keeping his personal contacts personal. There is a need to be able to coordinate the access to the supporting data and profile information for these services so that they can all work on his phone without gaining access to each other. Similarly, the accounting for calls and the history list for website visits should be kept separate, and when Phil is using the web browser in the corporate context he should be

given access to corporate intranet websites, whereas when he uses the browser in the Internet context, he should not. Management of and support for the applications should be capable with multiple service and access providers for these services.

4.6. Service Transfer

Jim has basic Secure Digital (SD) television service from Service Provider A but orders the HD pay-per-view fight from a Graphical User Interface (GUI) on his PC for his buddies and him to view later that night. On the way home that evening Jim and the gang stop by a convenience store to grab refreshments for the fight. Unfortunately, the lines are much longer than expected and the fight is about to start. Jim borrows Tom's PDA (from Service Provider B) and pulls up the confirmation email where he recalls seeing a mobile option for viewing. Since Jim already logged into his email, he quickly downloads the mobile viewer client to Tom's PDA and starts the fight.

As they turn onto Jim's street, he uses the mobile remote-control function to turn-on his TV and select the pay-per-view event form his personal channel line-up. Upon arrival, Jim finds a notification on the TV that the pay-per-view event has started but is currently being viewed on another device. He selects the option to move the view to the TV. The fight pops onto the screen and a notification is sent to the PDA on which Tom was viewing the fight from the car.

4.7. QoS/SLA

Tom has a new PDA device that includes a SIP/IMS telephony application as well as several radio technologies. Tom uses this client in several contexts, and it is his primary telephony communications tool at work, home, and on the go.

The device registers with two IMS-enabled soft-switches – one that is owned and managed by his corporate Information Technology (IT) department and that is responsible for his business communications, and a second that is owned and managed by the public carrier and that provides Tom's personal voice communications.

The device is able to connect to these two soft-switches using one of three methods: Cellular, 802.11g or Bluetooth, and these network types have varied coverage in Tom's home, office and everywhere else. Notably, Tom's office has 802.11g access points with excellent coverage, and Tom's PC at home has Bluetooth and broadband access. For whatever reason, Tom never got around to installing a WiFi Access Point (AP) at his home.

The telephony requirements also differ between Tom's business and personal services. Tom's business is interested in maintaining a high-quality experience for Tom's clients and is interested in making sure that the experience includes their telephone conversations with Tom. Tom, however, is not as interested in that high-quality experience for his personal calls and would rather pay less for basic communications.

To support this, the behavior of the telephony application in the business context is to request resources from a supporting network so that call quality is ensured. This includes picking from the different networking technologies to provide the best quality available. This also includes an optional extra feature that allows business calls to seamlessly hand-off among different network providers to maintain a high QoE. At the same time, the telephony application that supports Tom's personal communications is making similar choices that minimize cost by selecting free access hotspots and avoiding the expense of hand-offs among networks by providing subtle signals to Tom that the signal is degrading, prompting him to either select a manual hand-off to a better network or to move back to a stronger signal location.

4.8. Quality of Experience (QoE)

Rebecca transfers the TV show she is watching from her WiFi / Third Generation (3G) enabled PDA to her Ethernet capable widescreen TV. The QoE profile associated to each device specifies a codec bit rate range, a list of supported codecs, a packet error rate max, a viewing resolution and a service access authorization for that device. These and other parameters, possibly allowable rate plans, define the acceptable QoE for the given service. As the TV show is transferred to the new device, it is likely a new QoE profile is part of the continuity or transfer process, for example, the transfer to the widescreen TV includes an increase in minimum codec bit rates and a new codec type.

4.9. Multi-provider service bundles

Joe subscribes to home phone service from one company, mobile phone service from a second company, Internet access from a third company and IPTV from a fourth company. The providers coordinate their offerings so that Joe receives a single bill, and integration of the various services. He can access video services and the Internet from his mobile phone based on authentication of the Subscriber Identity Module (SIM) card. He can also access video services from his Internet connection, using his Internet userid and password. The Quad-play service bundle performs exactly as it would if he were receiving all the services from the same provider.

4.10. WEB/IMS hybrid service

Mark subscribes to "Color Ring" service, where he can dial a special code and IMS will connect him to an application server. After completing authorization, he specifies a ring tone, an optional picture and a target phone. Then the application server downloads the selected ring tone and picture to the target phone. When Mark calls the specified number (within time limits) the called phone uses the requested ring tone and displays the provided picture for alerting the recipient of Mark's call.

Analysis: This shows a service that integrates web services capabilities into a "pure IMS" call. Some variations on this would also illustrate the need to ensure consistent order of executing service logic.

4.11. Flexible Policy Use Case

Joe subscribes to high speed Internet and voice service from his local service provider. He also subscribes to a third party application package that includes online video games, Karaoke on Demand, and an electronic newspaper service. Joe wants to receive consistent QoS across the various applications except for the electronic newspaper, which is best effort. He also has a number of policies that he wants applied to his services. He is competing in the international Karaoke championships, so he has defined a policy that ensures he is not disturbed when he is practicing his Karaoke. This policy automatically diverts all calls to voice mail while he is using the Karaoke on Demand, except for calls from Lisa, his Karaoke coach.

Analysis: It must be possible to apply flexible policy, so that the service provided will depend on defined criteria, such as the location, user preferences, specific network or application involved. From a standards perspective, it must be possible for this policy to be set by any of a number of entities (user, service provider, application provider, etc.) The standards must allow for this flexibility, but the decision as to how policy is controlled in a given situation is out of scope for standards.

4.12. Billing Convergence

Martha joins an international conference call from her home phone at 6:30 AM, using the company pre-paid calling card. She needs to be in the office for another appointment later that morning, so after an hour she "transfers" the call to her personal mobile phone and listens to the call while she commutes. The charges should continue to be covered by the prepaid account, transferring credentials, authorization and limits, etc., without the need to re-authorize or re-dial into the conference call. In addition, since Martha pays for minutes of her mobile use after 8:00 AM, the airtime charges should also be applied to the pre-paid card. However, she has unlimited local minutes from 8:00 PM to 8:00 AM, so there should not be any airtime charges until 8:00 AM.

4.13. Unified Presence

Larry subscribes to a "Unified Presence" service which combines presence from a number of sources and allows him to control which aspects of this unified presence are shared with different subscribers to this presence information. Larry has set up the policy in his profile to provide a composite presence based on the following factors:

- Whether or not his company mobile phone is turned on, and if it is on, whether or not it is in use.

- His email calendar.
- Instant Messaging service.
- Whether or not his office phone is in use.
- IPTV (He has specified that some programs indicate he is unavailable to anyone, while others show him as available to family. Football shows him as busy to anyone but his football friends list.)

Larry wants the ability to specify what is included in his presence, what each device means, and what the resulting presence status should be for each category of presence watcher, and who should be able to see this information.

Analysis: This requires a flexible presence system that can tie together a wide range of systems for input. It also requires the ability to apply a wide range of policies to this presence information, including what each presence input means in an absolute sense, what it means for the presence that will be displayed to each category of presence watcher and whether or not a given watcher will receive any information at all.

4.14. Machine-to-Machine & Monitoring

Curly has a fully automated home, linked to his IMS subscription. This service allows him to monitor the temperature in each room of his house, and automatically adjust it based on policies that he has predefined. (For example, when he is approaching home, as detected by his location service, the system automatically adjusts the temperatures to his preferences.) These policies include things like time of day, season and detected presence of someone in the room. He also has a number of unusual plants that require very precise environmental conditions. Curly likes to move these around his house, so each of these plants has a Radio Frequency Identification (RFID) tag affixed to allow the system to detect which plants are in a room and ensure the required environmental conditions are maintained. The system also alerts Curly if his predefined temperature control policies cannot be maintained because he has moved two plants with incompatible policies into the same room.

Analysis: Requires flexible policy and introduces machine-to-machine communication and RFID. Opening the network to allow control also introduces stringent security requirements.

4.15. Service Continuity between Access Networks

Fred has a mobile device that supports multiple access technologies, and wishes to ensure that he can have service continuity as he moves between the different access methods.

Analysis: Service continuity between specific access networks is already being dealt with in various SDOs. Generic service continuity is being considered, but has not yet been completed. An objective analysis of which access technologies would be the most important to consider has not yet been undertaken.

4.16. Service Interaction Management Use Cases

These service interaction management types can be used at multiple levels within a single service and/or between services to control the interaction of discrete but coordinated services. Here are examples of each.

Example 1

A single service presented to the user is a call logs service. Three layers of service interaction are used:

1. The user endpoint is registered to a Call Session Control Function (CSCF). That CSCF is a service interaction manager that controls the interaction between the users Class V application server and a call log event application server.
2. The call log event application server is connected to a service orchestration function. The service orchestration function publishes the call log events to the call log storage application and the call event popup application.
3. The call log storage application controls the interaction with the call log database.

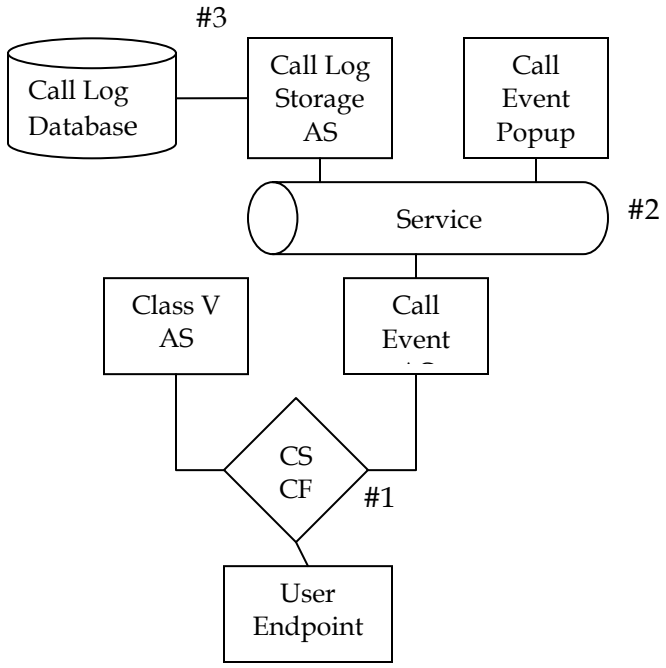


Figure 4-1

Example 2
In the second example, three applications are controlled by a single service interaction manager. In this example, the interaction of three discrete services is controlled by a CSCF. The services are as follows:

1. Call Routing Application
2. Conferencing Application
3. Directory Service Application

Note that the Conferencing Application is the application that is not the conferencing media resource but is the application that controls the service.

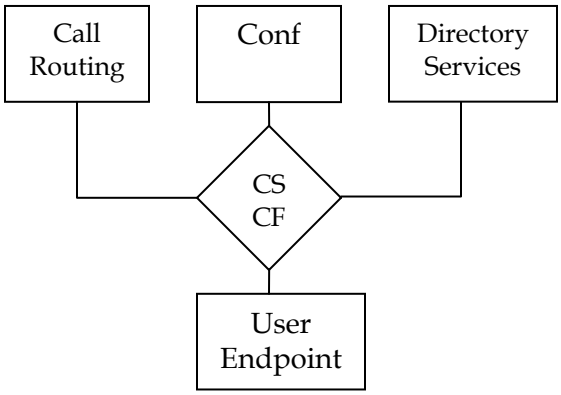


Figure 4-2

Example 3
The interaction of the discrete services is handled by the CSCF in this example. The initial filter criteria is used to determine which applications server to invoke and in what order. This interaction can differ depending on the specific SIP invite. For example, the Director Services Application would only be invoked if 0, 00, or other appropriate key sequence was dialed.

5 CONVERGENCE REQUIREMENTS

From the user's perspective, service convergence enables an enhanced, more ubiquitous user experience than might otherwise be provided. Connectivity is provided over a greater diversity of access networks and the service set available behaves consistently, even with the addition of new services (e.g., IMS based services) as the network evolves. Services may be constrained due to the limitations of the differing access networks used.

For service providers, a key attraction is that convergence supports the development of a single consolidated core network with one service environment rather than several service environments. From this perspective, a key requirement is to minimize infrastructure impacts (e.g., little or no impacts to the existing Circuit-Switched (CS) infrastructure, and minimal impacts to the IMS infrastructure).

Based on the use cases previously outlined in this document, the following requirements have been identified.

5.1. *Service Convergence*

5.1.1. Service Consistency

- Subscribers shall have a consistent user experience regardless of the access network used, subject to the constraints of the UE and access network.
    - A reduced set of services may be offered subject to constraints of the UE and access network.
- Mandated services (e.g., Emergency calls, lawful intercept, accessibility and priority services such as Emergency Telecommunications Service (ETS)) shall be provided in accordance with applicable regulations.
- With respect to providing support for devices while roaming (provision of services outside of the home network), if the roaming partner does not or cannot support converged (e.g., IMS centralized) services, for example, due to architectural or technical limitations, then the service offering may be limited or may not be possible to those roaming subscribers. In such cases, either:
    - The subscriber does not receive converged services. The roaming subscriber may still be able to originate and terminate basic services, (e.g., bi-directional speech calls).
    - The subscriber receives a subset of converged services (based on roaming agreements).
    - The subscriber is barred from roaming in those networks.
- Call independent service management shall be supported. This is intended to address issues that may arise when supplementary services are modified independently of an active call. For example, activation of call forwarding or changing the forwarded-to number.

5.1.2. Existing Infrastructure Impacts

- Where applicable, converged services should be accessible from existing CS infrastructure within the constraints of the device and network.
- Converged services should not require significant changes to existing CS and Internet infrastructure.

5.2. *Service Continuity/ Service Transfer*

As is defined in Section 3, service continuity refers to the user experience and service transfer refers to the means whereby it is accomplished. Therefore, requirements about them can be phrased either way. In this set, the requirements

are expressed as transfer requirements with the corresponding continuity requirements being implied.

- It shall be possible to transfer service from device D1 to a targeted device D2 across the same or different access networks, where service is from the same service provider. Note that D1 and D2 may be different network interfaces on the same device (e.g., a cellular/wi-fi hybrid device moving across access network types).

- It shall be possible to transfer all aspects of the active service including:

  - media
  - application/feature support
  - context/association

- It shall be possible to transfer user A's service from user A's device D1 to a targeted user B's device D2.

  - Transfer may require registration of device D2 with the network/service provider. It may also require user B permissions or involve user B policies. (Note that a distinction between users is from a network perspective and in practice the users could be the same or different persons.)

- It shall be possible for transfer to occur through the following options that may be employed in any given situation and are determined as part of product offering descriptions and/or user preferences:

  - End user initiated and controlled service transfer of an active session.
  - Network initiated and controlled service transfer. In this case, it shall be possible to notify the user that the transfer has occurred.
  - Network initiated, but end user controlled service transfer. In this case the network initiates the transfer, but the end user has the option to accept or reject the transfer. The end user control could be explicit (e.g., push a button) or implicit (e.g., set up preferences).

- When a service is transferred, an additional session is established between the service and the client. The network shall perform policy decisions in the same way that policy decisions were performed when the initial session was established. Depending on a variety of factors (user profile, device, access network, network state, etc.) this may result in the transferred service being identical to the service on the original device, or it may result in a modification of the service characteristics.

- It shall be possible to indicate to the user which aspects of the service have changed (e.g., QoS, features, association/context info, charging).

- For user-initiated transfer, it shall be possible to invoke the transfer and receive status information with any of the following options:
    - At the current device D1.
    - At the targeted device D2.
    - At a third user device D3 that is different from the transfer-from/-to devices D1 and D2.

Service Transfer across service providers is not considered in the above requirements. While it may be desirable from the consumer point of view and therefore should be considered by standards, the business model(s) needs to be better understood, which may in turn influence technical/standards solutions.

5.3. Access and Core Technology

The Access and Core Transport networks must be capable of interconnecting and interoperating through support of a set of compatible capabilities, as follows:

5.3.1. Identity and Authentication

It must be possible for the access network to identify and authenticate itself to the core network. It must be possible for the terminal devices attached to a visited network to identify and authenticate to that network. It must be possible for subscribers to identify and authenticate themselves through the access network to the services in the home network.

5.3.2. Security

It must be possible for the access network to establish secure connections between devices in the access and core network at multiple protocol layers. At transport levels, this may be Virtual Private Network (VPNs) secured with Internet Protocol Sec (IPSEC) to provide tunnels for user, signaling and control, and management protocols in the service layer. Higher layer service protocols may require their own end-to-end confidentiality and other capabilities, which should not be impeded. (Section 5.4 addresses security aspects further.)

5.3.3. Transport Control

It must be possible for policy-based mechanisms in both the access and core networks to translate a multitude of services into defined sets of QoS and QoE categories and to interoperate such that equivalent capabilities are delivered end-to-end.

5.3.4. Inter-Provider

Interconnection interoperability and underlying mechanisms (e.g., policy, control, security, etc.) must be able to span multiple provider environments, (i.e., it is possible for access and core networks to be owned/operated by different companies or divisions within a company.)

5.3.5. Migration

Service convergence must be maintained as the core and access networks continue to evolve.

5.4. Security

5.4.1. Federation of User Identities

It should be possible to federate user identities from one service provider to another or from one security domain to another, including single sign-on authentication, and anonymity/pseudonymity services (e.g., third parties can provide authorized user information or provide services to a given user with no knowledge of the user's real identity).

5.4.2. User profile and Policy Information Sharing

It should be possible to support sharing of user profiles and policy information among service providers. Where such information is shared, it must be possible to do so selectively and confidentially. (End users can provision their data once and let applications from different service providers access it: "enter once, share everywhere," with appropriate confidentiality. For example, user identity information may be selectively withheld from other service providers to maintain anonymity.)

5.4.3. Harmonization of Security Standards

There is a requirement for an industry security methodology that harmonizes existing security related standards by which information and communications security in evolving networks can be systematically addressed. Efforts are underway to align current telecom and enterprise standards such as ITU-T and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards. The PTSC Security Subcommittee (PTSC-SEC) Issue PTSC-SEC-2006-048, Network Performance Reliability and Quality of service Committee (PRQC) Issue PRQC-2006-127, and TMOC Issue TMOC-2006-067 contain initial technical contributions.

5.4.4. Security Relationships for Converged Devices

In the Security relationships use case, the example put forward is one where multiple service providers are supporting services on a single device, and where there is some security concern that the information concerning one set of services should not be shared with the services from the other provider. The resulting requirements from this use case are:

- Services shall be provided using an information model that supports the establishment of policy in sharing entities, properties, relationships and operations.

- Service information models shall be created including the necessary aspects that both allow convergence and blending with other services, as well as provide controls and safeguards to control access. Furthermore, sufficient information must be collected to allow for accounting, settlements and non-repudiation of the operation of the information model.

- NGN infrastructure as well as other infrastructure shall be provided in a way that sharing of information models can be established as well as controlled. This controlled sharing shall be established both among cooperating infrastructure as well as between supporting infrastructure and client applications.

- Infrastructure shall support multiple application and service environments in a way that provides virtualization of networks as well as devices.

- Devices should support service containers that allow private application execution and provide reasonable security from other service containers.

- Infrastructure aspects of information models shall be constructed to support policies that control the interaction between virtualized devices.

5.5. User Profile

The key requirements related to user profile are:

- It shall be possible for multiple entities to create, retrieve, modify and delete user profiles that include all information for all services of the respective user. The ability to perform these actions against the user profile shall be subject to appropriate permissions.

- It shall be possible for the user profile to span multiple service and application providers.

- It shall be possible to establish rules so the profile content required for any service or any service provider shall not impact the profile content of any other service or service provider that does not directly use the information.

- It shall be possible to establish rules so "cross editing checks" are performed in order to prevent a contradiction of profile data across services, service providers or entities.

- It shall be possible to establish a "governing model" that defines and facilitates ownership of respective attributes, and provides the respective entity (owner) the ability to assign or delegate permissions to the respective attributes.

- It shall be possible for entities to establish access to the user attributes via “agreed upon” key(s) which does not force the same key structure across the converged domains or converged entities.

- It shall be possible to federate user profile service logic (such as HSS (initial Filter Criteria (iFC) logic) in ways that guarantee an isolation of services from entities or applications that have no benefit for interacting.

- It shall be possible to federate user profile service logic (such as HSS iFC logic) in ways that guarantee services from authorized entities or applications are able to interact.

- It shall be possible for the user profile implementation to guarantee response times in accordance with agreed upon service level agreements between entities.

- It shall be possible to create a new service that makes use of the profile for existing services, and adds additional parameters to expand the service offering, without negatively impacting existing subsystems and services. The new service may be dependent on the existing profile, but must not impact the existing services.

5.6. QoS/SLA

5.6.1. Network Infrastructure Capabilities

Next generation applications may require the support of specific capabilities of network infrastructure, and convergence will drive the need to support a set of compatible capabilities across different network and access types to support a range of applications. Furthermore, since all the possible supporting networks cannot be known by an application in advance, applications must be able to interrogate and negotiate the capabilities of a new network that they may encounter.

In some cases, the matching of application needs to network capabilities may be contracted and enforced through a SLA. In these cases it may also be necessary to provide the means for the network to prove it met the SLA, or for the application to prove the network did not.

To meet these requirements, various aspects of QoS must be supported and coordinated across different infrastructure technologies and multiple service providers. The offered QoS will be constrained by the capabilities of the specific technologies and agreements between service providers – both Applications Sever Providers (ASP) and Next Generation Network Service Providers (NGNSP). A NGNSP may require connectivity from other providers that do not provide QOS. In these cases, the services requiring QOS may not be available end-to-end or may operate in a degraded manner.[3]

It should be possible to discover the available QoS capabilities of a network, and to select QoS classes or to request or reserve resources if they can be allocated on

[3] ATIS NGN Framework, Part I, Section 2.4.1

a per-application basis. These interactions may vary according to a given service, as well as with the access media type, terminal type, or service provider.

5.6.2. QoS, SLA and Bandwidth Attributes

Availability of a network resource, such as bandwidth, at various points within a network or within disparate networks is an important aspect of end-to-end QoS. When the availability of these resources is governed by a SLA then it is also necessary to provide mechanisms that can determine the conformance to the network characteristics specified by the SLA. These are especially important when the underlying IP-centric converged networks are responsible for providing transport for a number of applications that require different network characteristics in terms of maximum and minimum bandwidth, bandwidth variability, delay, jitter, packet loss and packet re-ordering. No less important in a converged NGN are characteristics surrounding the performance of establishing access, transitioning between disparate network access types and providers, and even discerning network capabilities. It is therefore necessary to properly extend existing mechanisms or define new mechanisms to create, reserve and admit into (or not) network resources statically or dynamically, as required. The ability to potentially report on the availability, variability and performance of these characteristics is also required.

In the QoS/SLA use case the same application (telephony) is shown in two contexts, business and personal. High-level policies are established to maximize the QoE in the business context and to minimize cost in the personal context. The following requirements can be derived from this use case:

- Infrastructure shall be able to provide information about its capabilities to client applications, including QoS and bandwidth capabilities for networks.

- Infrastructure shall be able to provide network information needed to determine, either directly or indirectly the ability of the infrastructure to support the application.

- Infrastructure shall be able to provide information to applications or other infrastructure so that price sensitive applications and policies can be supported.

- Access technologies and their resulting network access service shall be standardized in a way that supports QoS for IP networks.

- Access technologies and their resulting network access service should be standardized so that QoS and bandwidth management for IP networks can be supported. This is not a requirement for guaranteed bandwidth although that could be one implementation.

5.7. Service Provisioning and Monitoring

The key requirements related to service provisioning and monitoring are:

- Service providers should support roaming where the user is connected to the home network for services. Note that some level of service, e.g., e-911, may be provided locally.
- Service providers should support roaming where the user is provided services in the visited network.
- The end user should be able to access services from multiple service providers.

5.8. Policy

The key requirements related to policy are:

- It must be possible to apply policy at various levels in the network, coordinated across all applications.
- It must be possible for the policy to apply to the services received by a user, independent of the access method or even the application provider.
- It must be possible to apply policy to user profile information, so that the accessible information depends on factors such as who is asking, location, and presence status.
- It may be possible to apply policy to billing, enabling capabilities such as limiting the amount that can be spent on a given service.
- It must be possible for aspects of policy to be set by various parties, including content providers, application providers, Service Providers, Network Providers and the end user.
- It must be possible to apply strict security and authorization capabilities to ensure that policies are only created and modified by the parties authorized to do so.

5.9. Service Interaction Management Requirements

Additional description of service interaction management and detail on each aspect below may be found in Appendix H.

5.9.1. General

Service interaction management shall reside in the application layer and in the user equipment. The transport stratum enables applications through a series of standardized interfaces.

5.9.2. *Interaction Manager Type Specific*

The requirements of an individual service interaction management type are specified by the checked columns in the table. For example, an IMS CSCF shall support linear service invocation. It shall support multiple services. The interaction shall be tightly coupled. It shall support interfaces as specified in IMS.

It also follows that a system supporting all of the above functions but also supporting web services interfaces is not a CSCF. It is a service broker.

These requirements define the required characteristics of service interaction managers, but they can also be used to classify existing systems. The intent is to refine a previously ambiguous topic so that individual functions can be specified.

Function	Linear Invoke	Dynamic Invoke	Single Service	Multiple Service	Loose Couple	Tight Couple	IMS	Web Services	NGN
IMS S-CSCF	X			X		X	X		
Application Server		X	X			X	(X)	(X)	X
IMS SCIM		X		X		X	X		
Service Orchestration		X		X	X			X	
Service Broker		X		X		X	(X)	(X)	X

Figure 5-1- Service Capability Interaction Management Requirements

6 ARCHITECTURE ASSESSMENT

The ATIS EGC looked to extend the view of the NGN framework as documented in the NGN-FG's reports and to assess the state-of-the-industry regarding an NGN architecture for convergence. Understanding that any NGN framework represents somewhat arbitrary groupings of functions to organize complex concepts, this exercise was not intended to produce an exhaustive architectural model, but rather an assessment of various architectural views based on a common framework. The EGC architectural assessment and identification of convergence issues was undertaken per the process depicted below, recognizing on-going and equally important efforts on various aspects of convergence from other standards initiatives.

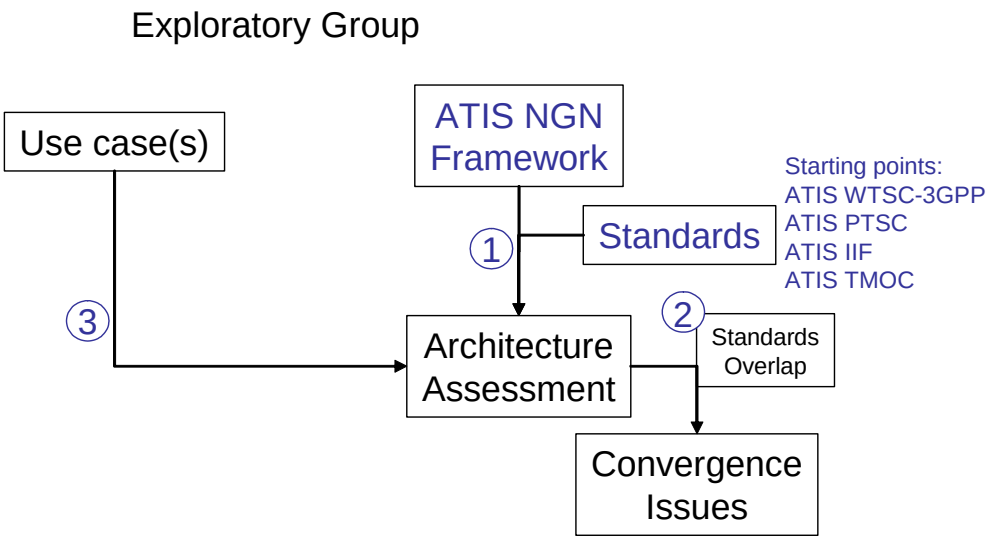


Figure 6-1 – EGC "Framework" process

Underpinned by the ATIS NGN framework, for a converged architecture selected ATIS efforts and supporting standards were reviewed. The resulting view within each "frame" of the framework established the base EGC framework.

Figure 6-2 shows, at a high-level, the features of the EGC framework discussed in subsequent subsections. Starting from the foundation of a network infrastructure, a shared IP core provides signaling and media connectivity for any access type. While physical connectivity is realized at the network level, logical connectivity is indicated at every frame between different providers (i.e., inter-providers). Shared transport control supports major service control types. These service control types have complimentary application servers in the application layer but share common service capabilities such as user profile and content functions. Finally, though shown as a separate frame, the OAM&P is seen as an integral wrapper to all elements of a convergence architecture.

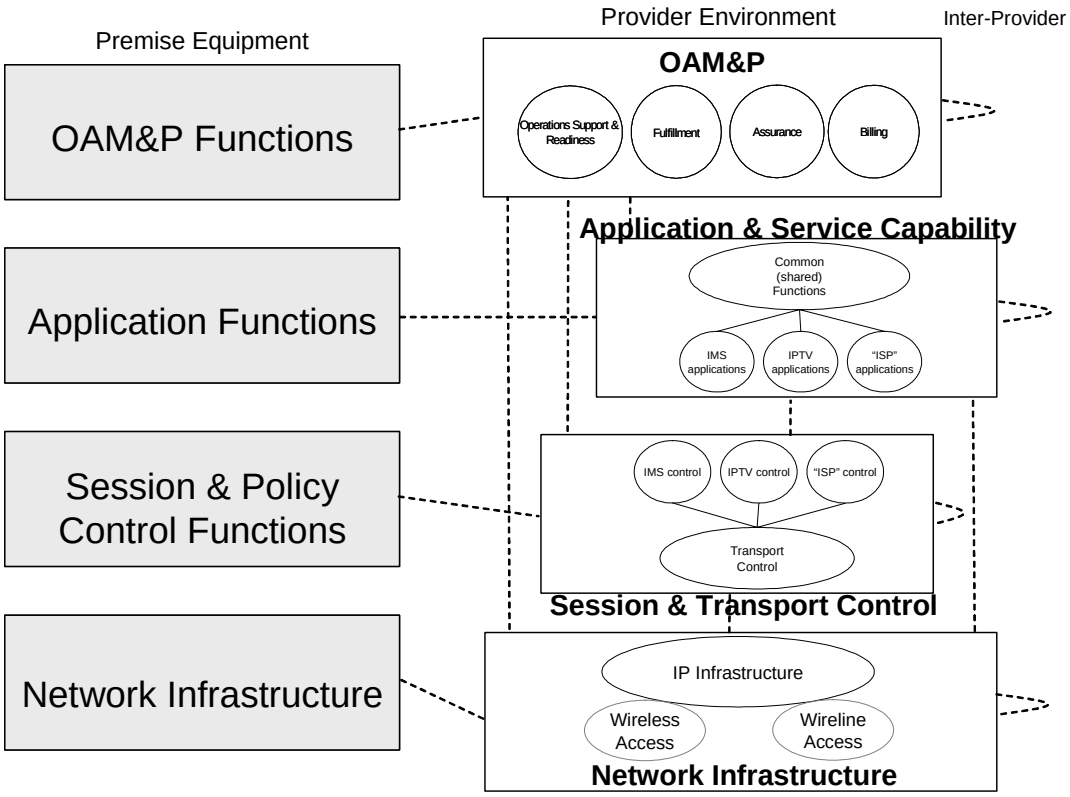


Figure 6-2 - High-Level View of the EGC Framework

Further perspective on each frame of the Provider Environment can be found in the following subsections: 6.1 OAM&P; 6.2 Applications & Service Capabilities; 6.3 Session & Transport Control; 6.4, Network Infrastructure; and a summary of salient points in Section 6.5, Assessment Summary. Premise Equipment frames, though identified as part of the EGC framework, are not covered in this report.

Comparison of architectural reference points within and between frames of the EGC framework assured a method of consistency in applying various architectures to the framework and indicated a variety of issues in the present state of convergence. Overlaps and inconsistencies between standards as identified in the construct of the EGC framework are documented in Section 7, Convergence Issues. Background work on the architectural assessment can be found in Appendix A and C. In addition, Appendix D provides an example exercise applying a use case from Section 4 to the framework.

6.1. OAM&P

The following figure provides a comprehensive mapping of the highest-level OAM&P functions into Level 2 function sets according to management domains of Customer Relationship Management, Service Operations & Management, Resource Operations & Management, and Supplier/Partner Relationship Management found in eTOM Release 7.0, 2007.

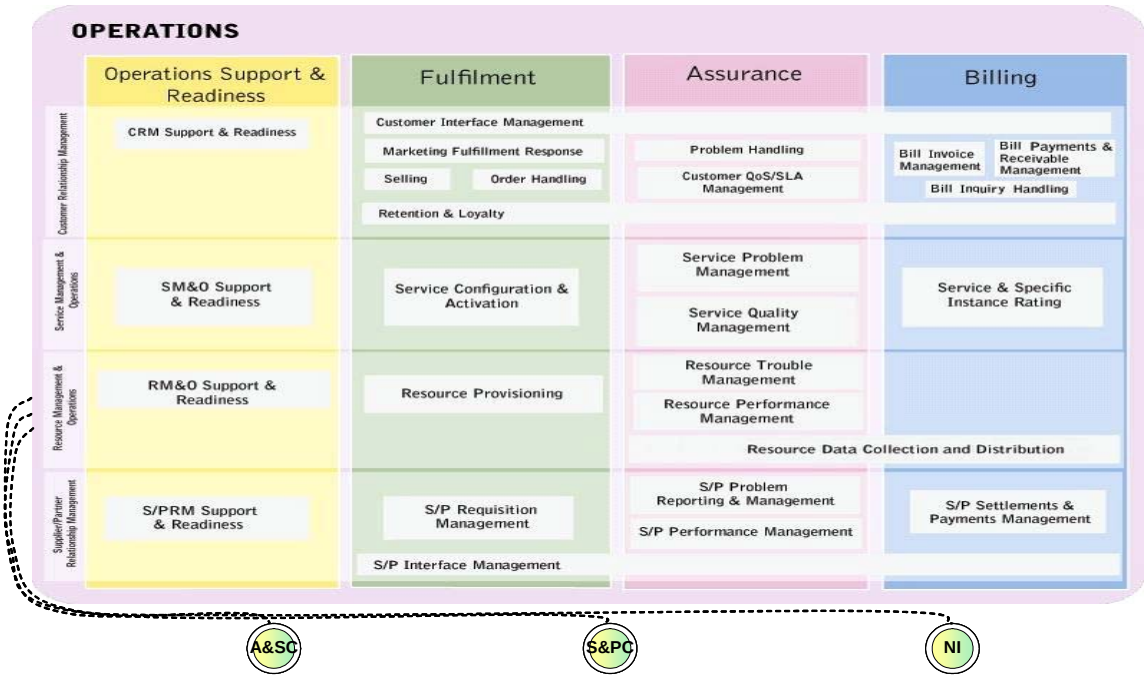


Figure 6-3 - OAM&P Process Model – Level 2 and Interface Categories

Resource Management & Operations (RM&O) addresses the OAM&P aspects for all resources found in network infrastructure, session policy and control functions, and application functions within the converged network.[4] Without any known exception, these standards emanate from the RM&O Layer of the eTOM model. There are nearly 1400 such standards that comprise the touch points for OAM&P to the NGN strata.[5]

Customer Relationship Management (CRM) considers the fundamental knowledge of customers needs and includes all functions necessary for the acquisition enhancement and retention of a relationship with a customer. When an enterprise sells its products to a partner these transactions are handled through CRM.

[4] See ETSI TR 102 647 V1.2.1 (2006-10) Annex A for a more comprehensive listing of standards concerning OAM&P reference interfaces and protocols for NGN management.

[5] Around 500 of these standards deal with "generic" management capabilities that may apply to various technologies, applications, or control mechanisms and/or span fulfillment, assurance, billing, or support and readiness functionality. Additional sets of specific standards deal with the NGN strata and are for applications and service capabilities functionality (~280), for session and policy control functionality (~120), and for management of network transport stratum (~480) of the NGN. The latter set also includes standards dealing with any allowed remote management aspects of User equipment.

Supplier/Partner Relationship Management (S/PRM) covers all aspects of the buying of S/P products for the enterprise including processes of ordering, order management, quality, and settlements. All inter-provider OAM&P interactions are covered by S/PRM.

Service Management & Operations (SM&O) addresses service management layer concerns within a Service Provider domain and interact internally with RO&M and S/PRM in order to support customer services. It focuses on the knowledge of services (Access, Connectivity and Content) and includes all functions necessary to support service proposals to the customer.

A globally consistent view based on a unified and consistent understanding of functionality and reference points will allow network owners and service providers to procure NGN OSSs that address these OAM&P functions independent of the specific mechanisms used for session and policy control (IMS, Web Services, or other) or application function details within the NGN framework. A unified NGN OAM&P framework should lead to simplified and consistent operations for voice, video, data and other services whether provided over wireless or wireline access.

6.2. *Application & Service Capability*

The ATIS convergence model for the Applications & Service Capability frame of the EGC Framework focuses on commonality or shared functions as shown in Figure 6-4. Following the ATIS IIF work on IPTV, content functions are recognized as a key grouping within the common functions which also includes user data, shared service features, charging collection, and service-capability registry. This view also recognizes the application specific aspects of three service types paralleling the Session and Transport Control frame. Real-time service applications for IP Multimedia and IPTV compliment best-effort, non-realtime Internet or "Internet Service Provider (ISP)" applications and associated clients in the premise equipment. Service Interaction Management can be used in and across these areas to broker the service types.

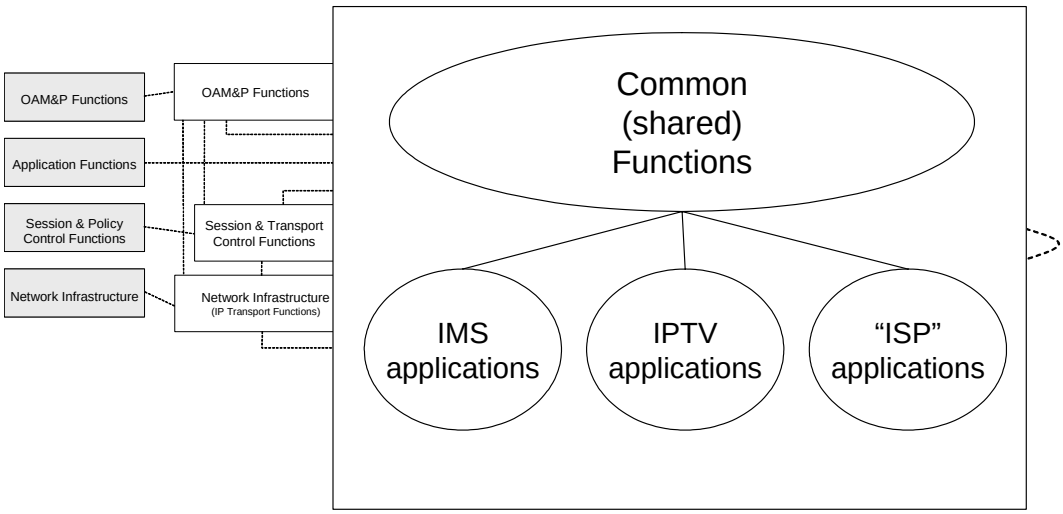


Figure 6-4 - Application & Service Capability Frame

6.3. Session & Transport Control

The ATIS EGC view of the Session and Transport Control frame is shown in the figure below. Multiple interworking functional-groups are shown for Session Control of IP multimedia, IPTV, and ISP (Internet control) services. Enterprise and peer-to-peer control of service types are also recognized as equally valid approaches but details reside in the premise frames. Transport Control in the form of network attachment and resource admission control is used by each of the service control elements consistent with agreed policy for internally and externally exposed provider functionality.

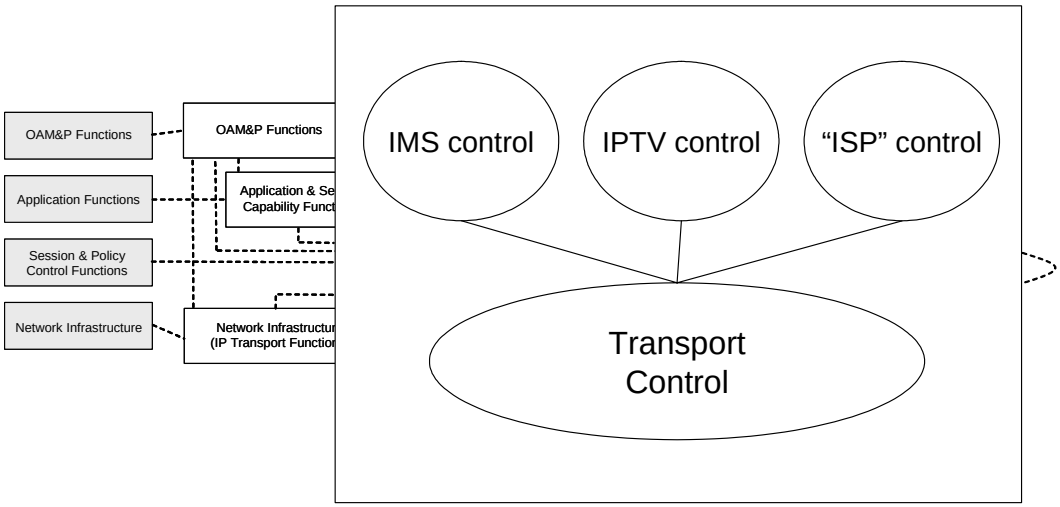


Figure 6-5 - Session and Transport Control Frame

6.4. Network Infrastructure

The ATIS convergence model for the Network Infrastructure frame of the EGC Framework is shown in the figure below. In support of mobile roaming and nomadic scenarios, network elements for home and visited core networks are understood as part of the IP Infrastructure. Network elements for access-specific infrastructure, whether for home or visited use, are grouped broadly under wireless and wireline access for visual simplicity; however, the specific accesses listed under each group are recognized to have separate elements and separate issues regarding convergence. From a services view, this also implies some unique device-client functionality to support specific accesses.

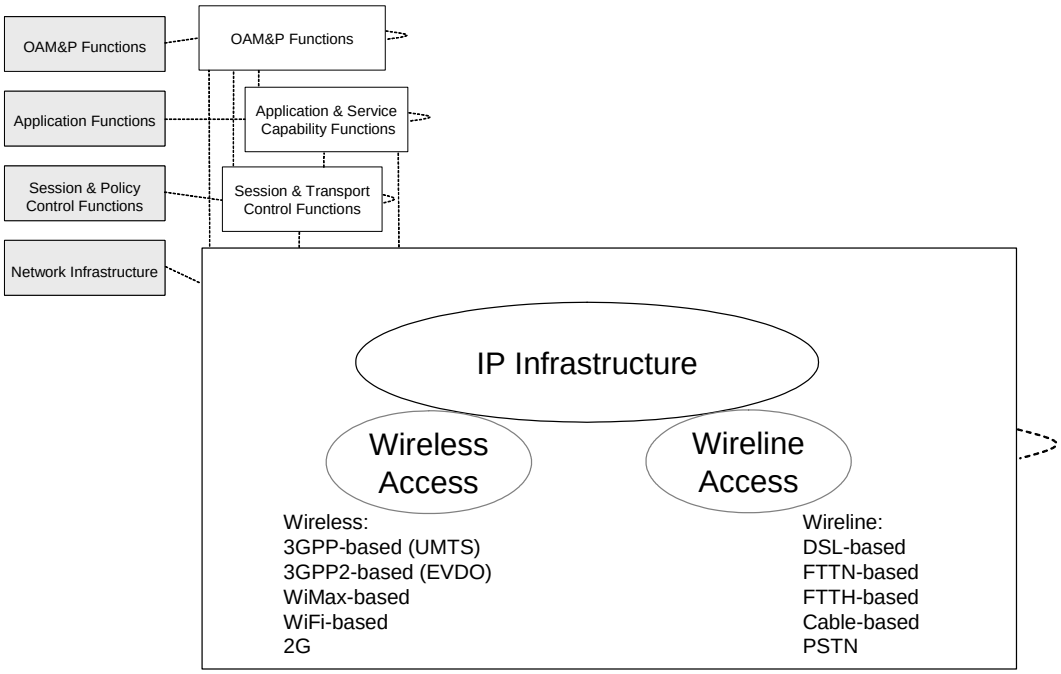


Figure 6-6 - Network Infrastructure Frame

6.5. *Assessment Summary*

While important work is on-going in several fora on various aspects of convergence, from an architectural perspective, significant work remains. The following highlights the key points of this assessment for each of the frames of the EGC framework.

- OAM&P: ATIS TMOC endorses the TMF's enhanced Telecom Operations Map® (eTOM) business process model. This work is important to support operations across all converged service providers.

- Application and Service Capabilities (A&SC): While applications should not be limited by standards, ATIS IIF and others have begun work on the identification of shared Service Capabilities. This work is important to support faster development of new and converged applications by building on underlying service enablers.

- Session & Transport Control (S&TC): ATIS PTSC supports the ITU-T view of NACF and Resource and Administration Control Functions (RACF) work by serving as the conduit to provide contributions from North America. On the other hand, ATIS WTSC endorses Third Generation Partnership Project (3GPP) PCRF work addressing their mobile-wireless perspective. Coordination and alignment of common Transport Control functions is important to support the different session control functions for data, voice, video or other service types.

- Network Infrastructure: Each of the ATIS bodies and other organizations that the ATIS EGC studied support an IP infrastructure; however, separate

terminology and details of different accesses are recognized. Coordination and alignment of a shared IP infrastructure is important to support any access as part of a converged Network Infrastructure.

- Premise Equipment: Whether a single mobile device or a campus Local Area Network (LAN)/WLAN and all associated terminals, premises are seen as an analogous construct to the Provider Environment. Therefore, a richer understanding of the premise from connectivity to control to clients and applications to operations including subscriber self-service and provider initiated upgrades is important to address the full breadth of convergence.

7 CONVERGENCE ISSUES

While the information and findings gathered during the EGC's exploration of the various aspects of convergence are by no means exhaustive, the EGC is able to provide the following essential observations. Issues that affect convergence from a broader view (i.e., across multiple frames of the convergence framework) are discussed below, followed by issues associated within specific frames.

Network migration may be complicated by the fact that different access technologies today often have different security architectures. Existing networks also often fail to clearly differentiate between "device attachment" and "user authentication." These issues point to the need for a common security architecture that clearly separates concepts such as subscriber, user device, and network. Identity management including coordination of subscriber preferences, presence, authorization, and authentication for a user on different devices, for different users (or multiple user-personas of a single user) on the same device and for single devices supporting multiple access technologies is also needed. In this context, the concept of a user identity separate from the device subscription is as important to full convergence as is the mobility concept of a visited network-access being separate from the home service-provider.

A number of security issues have been identified in this report, especially related to inter-provider security. It should be noted that this area is being addressed by ATIS committees (PTSC-SEC, PRQC and TMOC).

Service Interaction is done in many places, including the UE. There is a need to define how the interaction in various places is coordinated to provide consistent behavior. The service interaction functionality in the UE must only interact with the service interaction functionality in the "service." It must not interact with the capability in the network. This means that the "network domain service enablers" in the network will not generally be dependent on service interaction functionality in the UE (or, for that matter, in the service). This essentially mirrors the client-server internet model. The network is not quite "hollow", but it is largely independent of the services. This does not mean that new network domain service enablers cannot be deployed, but it does mean they will be deployed sparingly.

Standards in support of inter-provider interfaces are generally not mature enough to support the level of roaming anticipated in a converged NGN. This issue applies to inter-provider interfaces for business, operations and service aspects between both network and application providers.

Numerous SDOs have developed distinct, yet similar architectures along with functional elements, references points, and protocol choices that have significant overlap. The current state of architecture evolution is such that, for a given network or service capability, the interfaces and functions lack coherence in both scope and substance. A similar interface may use the same or different protocols, and a given protocol may be augmented by different access-specific options. A predictable result will be that roaming and handoff won't work (e.g., GSM over WiFi or Femto-cells) and services will be degraded or break depending on what combination of domains is encountered. Convergence in both services and network capabilities will demand alignment of NGN Architecture across multiple access technologies (and their SDO champions). Setting this consistency as a goal for both ATIS internal and external activities will enable achievement of convergence long-term.

7.1. OAM&P Issues

Currently there is no standard for billing and settlements between IP NGN services providers, although some preliminary work has been done in the Internet Protocol Detail Record (IPDR) organization with acceptance of the IPDR framework within ATIS for usage data recording. It is usual that billing settlements agreements between partners are based on an abstraction of usage data record aggregation. The framework includes Extensible Markup Language (XML) description of business data elements, External Data Representation (XDR)-encoding and use of a specialized (new) streaming protocol. Detailed schema and standards for voice, video or data services settlements are yet to be determined. A complication involves an existing (competing) 3GPP IMS charging architecture involving Abstract Syntax Notation (ASN).1 encoding and File Transfer Protocol (FTP) file transfer of usage data records. Although 3GPP has approved the IPDR framework as an optional approach, no implementation has used it yet.

There is a growing need in the industry for the management of customer (user) network equipment. This situation is leading to a proliferation of disparate end user and customer identity modeling and equipment management schemes, which may be in conflict with other frameworks or standards. Harmonization of these initiatives will benefit all providers of service and network facilities.

Existing supplier/partner relationships often require months for negotiation of pair-wise implementation agreements even when there is a standard interface to use as the basis for negotiation. When service contents are provided by a third party (i.e., Content Provider role) and there are many such individual content providers, this inefficiency will have adverse business implications. Consequently, it is desirable to construct a framework for mechanization of these implementation agreements including standardization of content description,

unique identification of the content provider and (if appropriate) identification of billing settlements arrangements.

As noted previously, less than 10% of standards deal with touch points to CRM and SM&O standards. In particular, there is specific interest in development of an Ordering Application Programming Interface (API) (CRM-F) for IPTV Services. Fixed and wireless operators have started the introduction of IPTV service in their networks based on an NGN roll-out. There is a need for definition of generic Ordering Framework and APIs to improve efficiency of IPTV support systems & operations and encourage vendors to introduce standard solutions. IPTV service is to be viewed as a new Media type that needs to be provisioned, rated, billed and supported in the back-office systems. In defining the framework, consideration should be given to Content Provider context, IPTV OSS/BSS High Level Architecture and Digital Rights Management.

One of the most challenging aspects of NGN operations will be troubleshooting arising from customer complaints and network build out when service content and service flow control is based on a highly distributed application server environment. The routine maintenance of server hardware and software release upgrades alone poses significant difficulties. There is a paucity of effective standards dealing with inventory management (other than configuration data synchronization), remote software upgrade and activity scheduling and tracking. Standards in these subject areas would improve the management of so many application servers as network resources. In order to begin to address customer complaint troubleshooting, a framework for meaningful event correlation, including alarm correlation with other types of events, will be necessary. Only client-server trail correlation techniques documented in some network technology standards are available today.

7.2. Application & Service Capabilities

Current regulatory service requirements are generally tied to specific networks, which often implies access type. The whole point of convergence is to decouple services from access types. This creates a real issue which will cause all sorts of ambiguities about how or if current regulatory requirements (e.g., NG E9-1-1, CALEA, USF, equal access) apply. This will be a problem in some contexts, and an opportunity in other contexts, which will further complicate the issue.

There is a need for "unified" user profile that encompasses a full range of services (i.e., IMS and Web Services). The IIF has started some work in this area, but this needs to be expanded and brought into other ATIS groups.

7.3. Session & Transport Control

Current standards provide mechanisms to request and/or negotiate capabilities at session initiation. However, they do not generally support capability discovery mechanisms. Without such a mechanism, when you use a new access network, you will not know if something is possible until you try it. This could be very frustrating and potentially expensive if you are paying for access use and

could effectively make "convergence" less meaningful for the end user. (This may need to also include some mechanism to easily discover if a given access network can provide connectivity to your service provider home network.)

Service continuity has been defined for voice with VCC. Other services such as licensed video delivery have additional requirements. A generic continuity mechanism needs to be defined. For example, licensed video requires the use of DRM and the license introduces additional complexity to the handoff. Other applications might include text/instant messaging and web portals. This can also include the coordinated transfer by a generic continuity mechanism of separate, but linked services (e.g., voice + web interaction.)

For service continuity, policies applied to the transferred call or session may be different from that of a brand new one. For example, in a situation of tight resource constraints it may be desirable to give preference to admission of transferred sessions over new sessions, or it may be desirable to provide an inferior QoS rather than not have the session transfer at all. Therefore there may need to be some kind of mechanism to distinguish transferred sessions from new sessions, along with some indication of how it should be handled.

7.4. Network Infrastructure

There is a need for consistency across all network types. Authentication, security and policy etc., are today generally applied to users. We have identified requirements for this to be applied to access networks as well, e.g., an access network authenticating itself to the core. This appears to be a standards gap.

There is a need for a consistent, abstracted interface for QoS between applications and the network, and between networks (not necessarily the same interface).

The border gateway functions connecting different accesses as defined today are not sufficient to support a common IP infrastructure for all access types. With network convergence, a common IP network can support multiple access types. In order to identify the service capabilities of the access network, there is a need for a mechanism to identify the access capabilities in signaling (in-band or out-of-band). The current signaling standards may not be adequate to identify this. Finally, there are a plethora of protocols used for authentication and any mismatch between the clients from one network type to an access network of a different type can disrupt the service.

The handling of Authentication, Authorization and Accounting (AAA) and policy control when roaming occurs requires the coordination of the security, policy and accounting planes to work between visited and home networks. There needs to be consistent and efficient methods to control content access and admission regardless of service access types such as provider maintained or "over-the-top." Additionally, methods utilized to assign IP addresses to mobile devices (e.g., Client Mobile IP, CMIP vs Proxy Mobile IP, Proxy Mobile IP (PMIP)) needs to be common across access network types as inconsistencies will

lead to inter-working problems between clients and access network, and between access networks and core networks

7.5. Conclusions

As an overarching conclusion, the EGC finds that realizing the full potential of convergence will require a fundamental shift in the industry's approach to traditional wireless, wireline and service silos. Moreover, in order to support and enable the development of standards to achieve the entirety of convergence, the EGC also finds that standardization programs should broaden their efforts from an access, technology or service specific (vertical) approach to that of a comprehensive holistic end-to-end (horizontal) standpoint that considers the entire telecom ecosystem (e.g., device, access networks, core networks, services and applications). More precisely, as the industry takes steps to consolidate offerings to enable convergence so too should its standardization efforts. The EGC concludes that ATIS is well positioned to demonstrate solid leadership in this respect.

From the findings presented in this document, the EGC provides the following observations and conclusions:

- Security and subscriber profile are often access specific. In addition, user and network attachment concepts are almost never clearly separated. Aspects of this problem are being addressed in various forums; PTSC Service Access Code (SAC) and SEC are addressing portions of this, as is the ITU-T Identity Management Focus Group. However no forum is currently providing overall coordination.

- Today, there is no clear mechanism to ensure that service interaction can be effectively managed across service types or service domains (e.g., combined IMS + Web Services architecture).

- It is not clear how service interaction can be avoided between service logic in the Application Servers/UE and the service enablers in the network. In particular, there is a need to avoid having service enablers be affected by evolving functionality in the UE, while still allowing applications to take advantage of network provided service enablers.

- Today there is no generic service ordering interface, especially between different commercial entities. This is being considered by the ATIS Ordering and Billing Forum (OBF), but the work is complicated by the lack of objective requirements for the functionality of such a generic interface, and by the absence of an industry model for "generic future services."

A number of standards topics critical for meeting business drivers for convergence, based on the high-level architecture and requirements assessment

of the exploratory group, do not appear to be fully addressed within the context of current ATIS standards.

8 RECOMMENDATIONS

To address the findings and conclusions and to better enable the telecommunications industry's movement forward to convergence these deficiencies, the following recommendations are provided to ATIS and its committees. The extent to which these recommendations are incorporated and enacted is deferred to ATIS, given potential procedural and organizational impacts.

A. Adopt the EGC framework as the basis for the coordination of ATIS' convergence efforts.

B. Establish an initiative for the coordination and development/evolution of a common NGN architecture that enables full convergence.

C. Adopt the eTOM model, as endorsed by ATIS TMOC, as the basis for OAM&P and support standardization across all aspects of convergence services and Network Infrastructure.

D. Establish an initiative for the coordination and standardization of Service Capabilities enabling convergence applications and services. The initial focus should include, but not be limited to:

- User Data such as Identity Management and User/Subscriber Profiles
- Service Brokering (interaction management) including NGN and Service Oriented Architecture (SOA) technologies
- Content Functions such as content preparation, content sourcing, and rights management
- Coordination of other relevant standards/specification efforts (i.e., Organization for the Advancement of Structured Information Standards (OASIS), Parlay, Liberty Alliance)

E. Adopt a common model for Transport Control, such as ITU-T model for the standardization of the Network Attachment and Control functions and Resource and Admission Control functions. As part of this work, establish an initiative for the coordination and standardization of a network policy framework that enables common Transport Control for the converged Network Infrastructure (any access, shared IP infrastructure).

F. Establish an initiative for the coordination and standardization of consistent interfaces between a converged IP Infrastructure and any access supporting features such as end-to-end security and QoS.

G. Establish an initiative for the coordination and standardization of methods, objects, and corresponding metadata definitions to promote convergence services and applications. Initially, these include:

- Access independence for security and QoS
- Network Service Provider to Application/Content Service Provider interactions
- Transport Control Framework
- User Profile and Identity Management
- Service continuity, beyond voice to include multimedia, video, and data

H. Establish an initiative for further study on Premises Equipment frames (residential, Small Office/Home Office (SOHO), Server Message Block protocol (SMB), and Enterprise), as appropriate.

I. Establish an initiative for further study on inter-provider interworking, as appropriate.

APPENDIX A: ATIS BOOT STRAP PROCESS

As a starting point to the EGC boot-strap process to the architecture assessment, several ATIS work groups were identified with existing or on-going architecture documentation. Specifically, the architecture work of ATIS PTSC, ATIS WTSC, ATIS IIF, and ATIS TMOC were used to organize the next level of detail of the ATIS NGN framework. A mapping of these key ATIS work groups to the NGN framework is shown below. A description of the ATIS committees used in this mapping also follows.

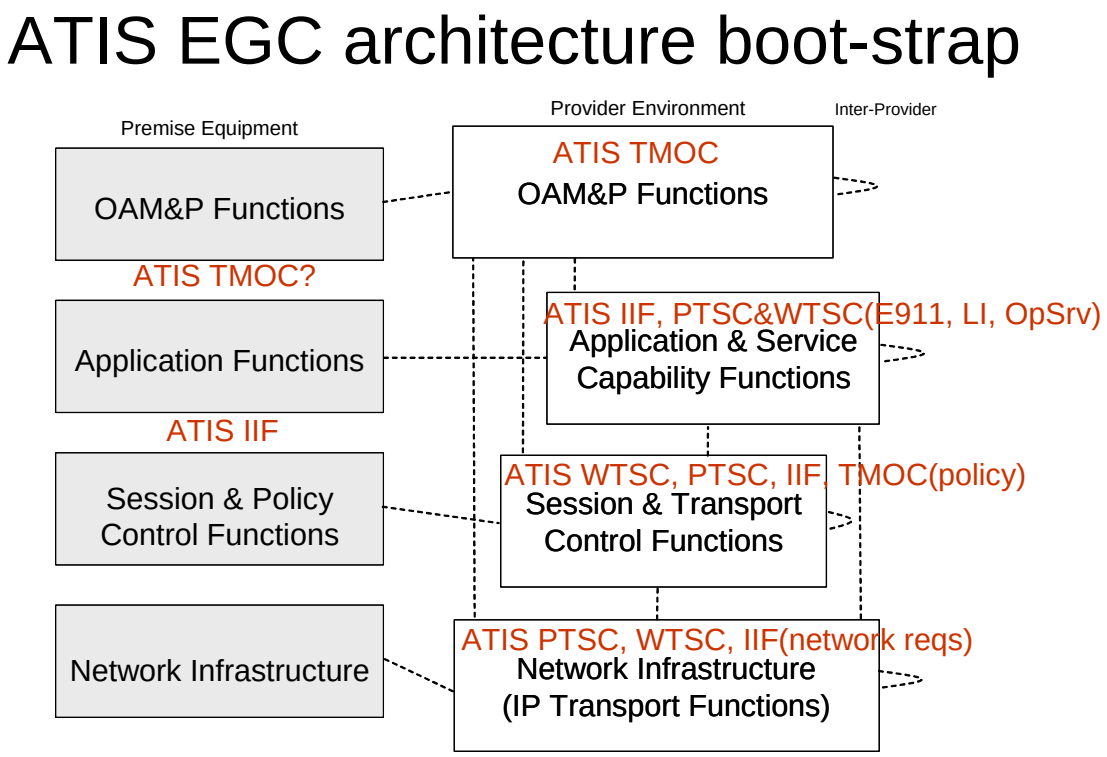


Figure A-1-ATIS Committee mapping to NGN Framework

ATIS IPTV Interoperability Forum (www.atis.org/IIF)

The **IIF** focuses on the creation of an industry overall reference architecture for IPTV; content delivery (quality of experience); DRM; interoperability standards and testing requirements for components; reliability and robustness of service components; and the establishing user expectations. The IIF enables the interoperability, interconnection, and implementation of IPTV systems/services by developing ATIS standards and facilitating related technical activities. This forum will place an emphasis on North American and ATIS Member Company needs in coordination with other regional and international standards development organization.

ATIS Packet Technology and Systems Committee (www.atis.org/PTSC)

The **PTSC** develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. It also reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations.

ATIS Telecom Management and Operations Committee (www.atis.org/TMOC)
TMOC develops operations, administration, maintenance and provisioning standards, and other documentation related to OSS and Network Element (NE) functions and interfaces for communications networks - with an emphasis on standards development related to U.S.A. communication networks in coordination with the development of international standards.

ATIS Wireless Technology and Systems Committee (www.atis.org/WTSC)
WTSC develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies and reviews and prepares contributions on such matters for submission to the appropriate U.S. preparatory body for consideration as ITU contributions or for submission to other domestic and regional standards organizations. WTSC coordinates closely with other standards developing organizations (e.g., Telecommunications Industry Association (TIA), IEEE, European Telecommunications Standards Institute (ETSI), etc) on wireless issues to ensure that the work programs are complementary.

APPENDIX B: STANDARDS INITIATIVES

This appendix contains a description of the other organizations and activities that may be applied to or may affect convergence. This list is illustrative of the breadth of convergence related work and organizations and is not intended as a comprehensive resource.

Recognizing that the ATIS committees do not cover all aspects of convergence, various international standards bodies are also important to aspects of convergence within their expertise. For example, the ATIS WTSC endorses the architecture work of 3GPP while the ATIS PTSC strongly aligns with ITU-T NGN architecture and ATIS TMOC follows the TMF eTOM process model.

3GPP has defined a Generic Authentication Architecture (GAA) that enables 3G networks to provide the bootstrapping of application security (authentication between the user and the application), using the trust relationship between a user's device equipped with an UMTS Integrated Circuit Card (UICC) or SIM and the 3G service provider. Independently, the Liberty Alliance Project (LAP) has created an open network identity infrastructure for web services that supports single sign-on and a decentralized authentication and authorization for multiple providers. 3GPP Rel7 is developing a technical report (TR 33.390) that provides guidelines on the interworking of GAA and LAP architecture, specifically, details of possible interworking methods between the Liberty Alliance Identity Federation Framework (ID-FF), the Identity Web Services Framework (ID-WSF) and a component of GAA called the Generic Bootstrapping Architecture (GBA). This document only applies if Liberty Alliance and GBA are used in combination.

3rd Generation Partnership Project (www.3gpp.org)
The **3GPP** is a collaborative Agreement between Standards Development Organizations (SDOs) and other related bodies for the production of a complete set of globally applicable Technical Specifications and Reports for a 3G System. The original scope of 3GPP was to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA) both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes). The scope was subsequently amended to include the maintenance and development of the Global System for Mobile communication (GSM) Technical Specifications and Technical Reports including evolved radio access technologies (e.g., General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)). The Operational Partners of 3GPP are ATIS, ARIB, CCSA, TTA, TTC, and ETSI.

3rd Generation Partnership Project 2 (www.3gpp2.org)
3GPP2 was born out of the ITU "IMT-2000" initiative, covering high speed, broadband, and Internet Protocol (IP)-based mobile systems featuring network-to-network interconnection, feature/service transparency, global roaming and seamless services independent of location. 3GPP2 is a collaborative effort between ARIB, CCSA, TIA, TTA, and TTC. 3GPP2' scope includes developing a collaborative 3G telecommunications specifications-setting project comprising North American and Asian interests

developing global specifications for ANSI/TIA/EIA-41, Cellular Radiotelecommunication Intersystem Operations network evolution to 3G, global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41.

CableLabs® (www.cablelabs.com)
CableLabs is a non-profit research and development consortium that is pursues new cable telecommunications technologies and to helping its cable operator members integrate those technical advancements into their business objectives.

Consumer Electronics Association (www.ce.org)
The **CEA** is a trade association promoting growth in the consumer technology industry. CEA members are involved in the design, development, manufacturing, distribution and integration of audio, video, mobile electronics, wireless and landline communications, information technology, digital imaging, home networking, multimedia and accessory products, as well as related services that are sold through consumer channels. CEA develops ANSI standards through 70 committees in the above areas.

Digital Living Network Alliance (www.dlna.org)
DLNA is a cross-industry organization of leading consumer electronics, computing industry and mobile device companies. DLNA has publishes the DLNA Networked Device Interoperability Guidelines. The DLNA Networked Device Interoperability Guidelines cover Architecture & Protocols, Media Format Profiles and Link Protection for interoperable networked platforms and devices for the digital home. The digital home vision integrates the Internet, mobile, and broadcast networks through a seamless, interoperable network. The guidelines also focus on interoperability between the devices for personal media uses involving imaging, audio and video.

DSL Forum (www.dslforum.org)
DSL Forum is an international industry consortium covering telecommunications, equipment, computing, networking and service provider companies. The DSLF engages in developing the global standardization of Asymmetric Digital Subscriber Line (ADSL), SHDSL, Very high rate Digital Subscriber Line (VDSL), ADSL2plus, and VDSL2. The outcome of their Technical Working groups is published via Technical Reports.

European Telecommunications Standards Institute, Telecoms & Internet converged Services & Protocols for Advanced Networks (www.etsi.org/tispan)
ETSI TISPAN is the core competence group under ETSI for fixed networks and for migration from switched circuit networks to packet-based networks, and architecture that can serve in both. TISPAN is responsible for all aspects of standardization for converged networks including the NGN (Next Generation Network) and including, service aspects, architectural aspects, protocol aspects, QoS studies, security related studies, mobility aspects within fixed networks, using existing and emerging technologies.

Institute of Electrical and Electronics Engineers "802" (www.ieee802.org)
The **IEEE** promotes the engineering process of creating, developing, integrating, sharing, and applying knowledge about electro and information technologies and sciences. The

IEEE LAN/MAN Standards Committee (LMSC) and its deliverable family of standards deals with local area networks and metropolitan area networks. More specifically, the IEEE 802 standards are restricted to networks carrying variable-size packets. The Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs are the most widely used of these standards.

Internet Engineering Task Force (www.ietf.org)
The **IETF** is an open international community, consisting of thousands of individuals who are network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF is organized into approximately eight functional areas, under which over 100 working groups are organized. The scope of the IETF has traditionally been "above the wire and below the application" but as access technologies and use of internet protocols evolve a clear boundary of the IETF scope is harder to define. IETF standards are not created in the traditional sense (no members, no voting) nor are they formally recognized by any certifying process or legal mandate (no submission to other bodies.)

International Telecommunications Union (www.itu.int)
ITU is an international organization within the United Nations System where governments and the private sector coordinate global telecom networks and services. ITU membership represents a cross-section of the telecommunications and information technology industry, from the world's largest manufacturers and carriers to small, innovative new players working in new fields like IP networking. It is estimated that the membership includes over 190 countries, 650 sector members, and 90 associate members. The three Sectors of the Union – Radio-communication (ITU-R), Telecommunication Standardization (ITU-T), and Telecommunication Development (ITU-D) - work today to build and shape tomorrow's networks and services. Their activities cover all aspects of telecommunication, from setting standards that facilitate seamless interworking of equipment and systems on a global basis to adopting operational procedures for the vast and growing array of wireless services and designing programs to improve telecommunication infrastructure in the developing world. ATIS is a sector member of the ITU-T and ITU-R.

MultiService Forum (www.msforum.org)
MSF is a open membership global association of service providers, system suppliers and test equipment vendors committed to developing and promoting open-architecture, multiservice Next Generation Networks. Founded in 1998, MSF's activities include developing Implementation Agreements, promoting worldwide compatibility and interoperability of network elements, and encouraging input to appropriate national and international standards bodies.

Open Mobile Alliance (www.openmobilealliance.org)
The mission of the **OMA** is to facilitate global user adoption of mobile data services by specifying market driven mobile service enablers that ensure service interoperability across devices, geographies, service providers, operators, and networks, while allowing businesses to compete through innovation and differentiation. The OMA seeks to deliver high quality, open technical specifications based upon market requirements that drive modularity, extensibility, and consistency amongst enablers to reduce industry implementation efforts.

Society of Cable Telecommunications Engineers (www.scte.org)
SCTE is a non-profit professional association that provides standards that cover a wide range of industry needs from "F" connectors to protocols for high-speed data access over cable. SCTE is accredited by the American National Standards Institute (ANSI), recognized by the ITU.

Telecommunications Industry Association (www.tiaonline.org)
TIA is a trade association for the information, communications and entertainment technology industry. TIA represents the communications sector of the Electronic Industries Alliance (EIA). TIA was formed in April 1988 after a merger of USTSA and the Information and Telecommunications Technologies Group of EIA. EIA began as the Radio Manufacturers Association in 1924. In the fall of 2000, the Multimedia Telecommunications Association (MMTA) was integrated into TIA.

TeleManagement Forum (www.tmforum.org)
The **TMF** takes a generic approach to network management (meaning the OSS/BSS area) across business processes, telecommunications applications, information modeling, and interfaces, in order to emphasize commonality and facilitate re-use across services. Distinctions among services are driven to the lowest level possible. Current working groups in the TMF are the multi-Technology OSS Program (mTOP), OSS/J group (recently incorporated into the TMF) IPDR group (which is the incorporation of the former IPDR.org into the TMF), SLA Management team Service Delivery Framework group (recent consolidation of the Next Generation Network Management (NGN-M) group and the Landscape team).

WiMAX Forum (www.wimaxforum.org)
The **WiMAX Forum** was formed to certify and promote the compatibility and interoperability of broadband wireless products based upon the harmonized IEEE 802.16/ETSI HiperMAN standard. A WiMAX Forum goal is to accelerate the introduction of these systems into the marketplace. The WiMax Forum works through six technical working groups, as well as three working groups to address marketing, regulatory, and service provider specific issues.

World Wide Web Consortium (www.w3.org)
W3C is an international consortium that works to develop Web standards and guidelines. W3C operations are jointly administered by the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) in the USA, the European Research Consortium for Informatics and Mathematics (ERCIM) headquartered in France and Keio University in Japan.

APPENDIX C: EXAMPLE ARCHITECTURE MODELS

This appendix provides a more detailed look at architectural aspects of the EGC framework as a learning exercise to uncover convergence related issues. The effort is not exhaustive and does not represent a precise or final architecture; rather, it draws on multiple architectures to assess and identify discrepancies but in no way intends to provide the "grand unified theory" on convergence. With that understanding, it is hoped the examples prove useful beyond this report for other groups following up on the EGC's recommendations.

Reference points and interfaces between all frames and sub-frames are coded per the legend below. Appendix D provides a single, consolidated table for reference-point information.

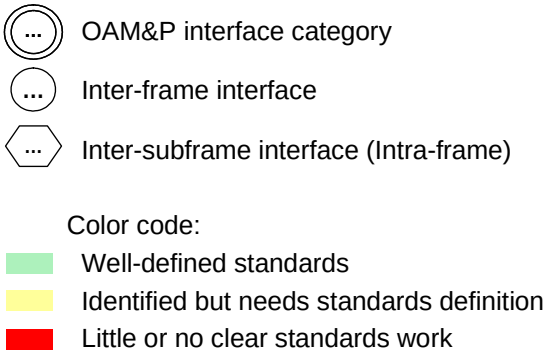


Figure C-1 - Reference Point Legend

C.1 Application & Service Capabilities Architecture Model

Further details of the A&SC model provide examples of the required functionality and standards needed for convergence. These are discussed in two groups; the application service functions and the common service-capability functions.

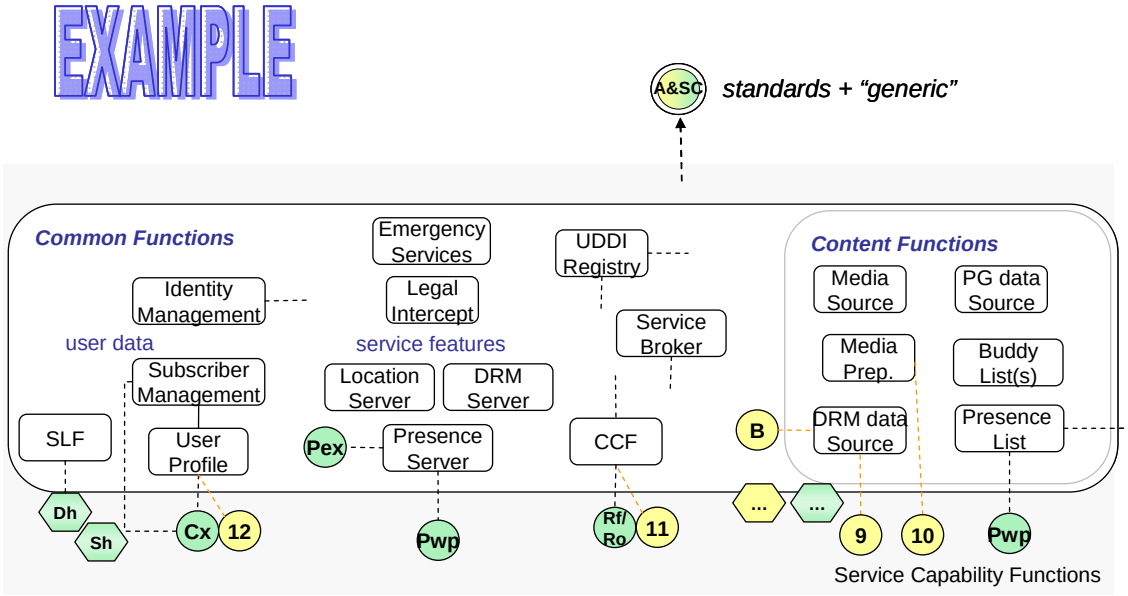


Figure C-2 - Common (shared) Functions

A complete figure of the Common Service-Capability Functions is beyond definition at this time. Figure C-2 showing common functions is provided to indicate many of the shared capabilities needed to realize service convergence. Within this large grouping, several concepts are promoted from different standards bodies.

For example, the 3GPP IMS HSS concept of a single subscriber profile is promoted to support not only IMS, but all user data including aspects of identity management as is being discussed by W3C. Content functions are shown as a key group promoting the work of the ATIS IIF, but extended to show shared content regardless of service or access type. Service features, not generally offered as applications on their own, are grouped in support of any service application. Aggregate presence should be considered as a feature of Instant Messaging and VoIP applications (or emergency services supporting VoIP), as well as video conferencing.

Some functions stand on their own, such as the 3GPP Charging Collector Function (CCF), which is applicable for any IP based service. Other functions needing more definition in the context of convergence include the UDDI Registry and Service Broker. The UDDI registry is a SOA concept as promoted by OASIS while the Service Broker function is a promotion of the 3GPP IMS SCIM concept.

While the common functions represent conceptually higher aspects of the AS&C model, the application server functions can be more important from a user viewpoint. Application sub-frames group functions consistent with service control types identified in the Network Infrastructure frame. However, for convergence, user expectations require that service-specific applications must interwork to allow a richer user experience. Converged application servers that support multiple, service-specific interfaces are also a way forward.

Figure C-3 provides examples of the service-specific application functions but a complete figure is beyond the scope of the EGC work.

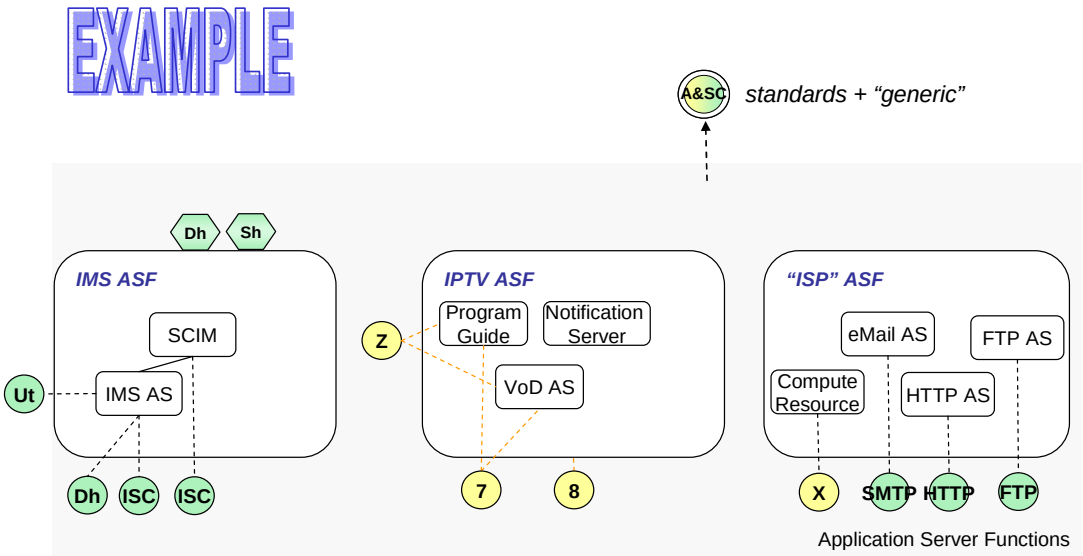


Figure C-3 - Application Server Functions

Information on the AS&C reference points and interfaces can be found in Appendix F.

C.2 Session & Transport Control Architecture Model

Figure C-4 provides a view of IMS, ISP and IPTV session control functions. IMS Control includes both the IMS core and the functions used to interwork with the PSTN, PLMN, and other IP networks (providers) at the control layer Internet Border Control Function (IBCF), Interworking Function (IWF) and Signaling Gateway Function (SGF)). ISP control includes those functions needed to control Internet service. IPTV Control as defined by ATIS IIF includes the Media Delivery control function for Broadcast and VoD and the IPTV Service Control Function (SCF). ATIS IIF provides the option for the IPTV SCF to be IMS based or be an independent function of IPTV.

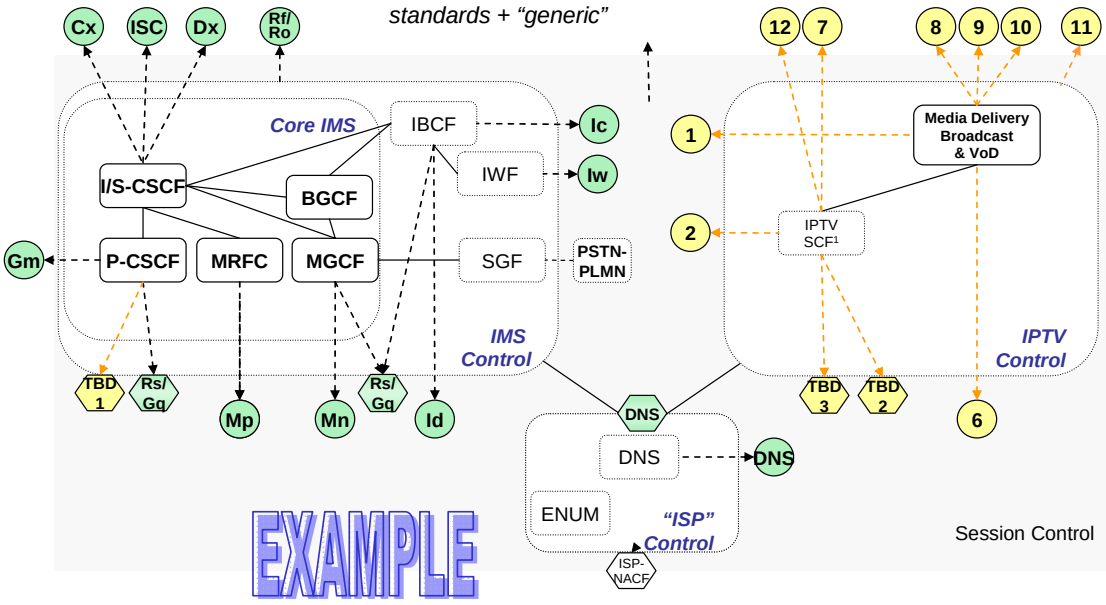


Figure C-4 Session Control Functions

Transport control functions RACF and NACF exist within the transport stratum to provide IP connectivity services to NGN users.

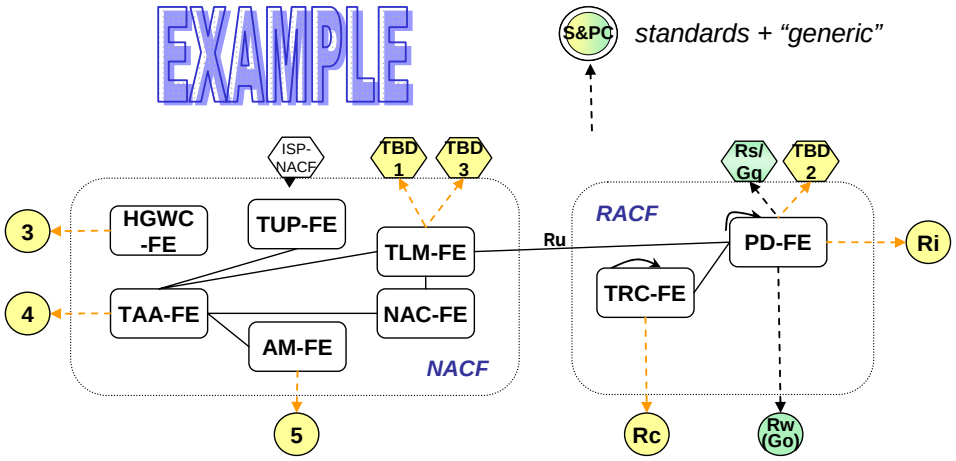


Figure C-5 Transport Control Functions

The RACF interacts with service control and transport equipment making policy decisions based on service agreements, subscription information, policy rules, service priority and the current utilization of network resources. The RACF also distributes control information to transport functions to enforce these decisions. The RACF are made up of the Policy Decision Functional Entity (PD-FE) and the Transport Resource Control Functional Entity (TRC-FE).

The NACF are responsible for the dynamic provision of IP address (e.g., using Dynamic Host Configuration Protocol (DHCP)), user authentication and authorization of network access, access network configuration and location management. The NACF interacts with Service Control, RACF, Transport and Customer Premises Equipment (CPE). The NACF has the following functions:

- Network Attachment Control Functional Entity (NAC-FE).
- Access Management Functional Entity (AM-FE).
- Transport Location Management Functional Entity (TLM-FE).
- Transport Authentication and Authorization Functional Entity (TAA-FE).
- Transport User Profile Functional Entity (TUP-FE).
- Home GateWay Configuration Functional Entity (HGWC-FE).

Information on the S&TC reference points and interfaces can be found in Appendix F.

C.3 Network Infrastructure Architecture Model

The following sections provide some representative architectures from the wireline forums (PTSC and ITU-T) and wireless forums (3GPP System Architecture Evolution (SAE), 3GPP2 NAE, and WiMAX). Because of network convergence, it is possible that a wireless terminal could connect to either wireline or wireless network types. For example, a DSL, Fiber Optic or Cable-based system could have dual-mode WiFi-based handsets terminating within the customer network with the possibility to roam or handoff onto a 3GPP, 3GPP2 or WiMAX-based network. For this reason, the architecture diagrams in the following subsections are organized along the same generic structure.

Network Infrastructure comprises *access-agnostic* and *access-aware* network elements. This first distinction is represented by the grey and white shaded areas, respectively, in the figures that follow.

In general, what makes elements access-aware is the relative involvement in the final interface between the network and the user equipment, also called the UNI interface. Access-aware infrastructure may fall into two categories: Wireless Broadband Access and Wireline Broadband Access. In the wireless cases, the spectrum used and the air interface specifications have been evolving from

narrowband to broadband capabilities. Wireline cases are analogous except for the fact that the electro-magnetic transmission is guided by a wire. The trend is toward pushing IP-based protocols all the way to the network edge so that network infrastructure requires minimal changes as access interface technology evolves and is replaced. It would also enable the same network to be used to support multiple access interface technologies.

Wireless Broadband Access includes the following types:

- 3GPP-based (UMTS): This is the GSM-based systems that are following a path toward an IP-based architecture called SAE.

- 3GPP2-based Evolution Data Optimized (EVDO): This is the CDMA-based systems that are following a path toward an IP-based architecture referenced as a Long Term Evolution (LTE). Both GSM and CDMA utilize spectrum allocated to cellular and Personal Communications Services (PCS).

- WiMAX-based: This is the emerging Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.16d/e systems that were designed as IP-based architecture from the beginning.

- WiFi-based: This is the existing IEEE 802.11a/b/g systems that were IP-based architecture from the beginning. Various letters of the alphabet represent extensions for security, mobility and other mechanisms.

Wireline Broadband Access includes the following types:

- DSL-based: This is the architecture that extended use of twisted-pair copper to the home by using higher frequency DSL modems and aggregation devices to bypass the voice switches and support IP-based connectivity to the Internet.

- Fiber to the Node (FTTN)-based: This is the fiber-to-the-node architecture that brings high bandwidth infrastructure closer to the home.

- Fiber to the Home (FTTH)-based: This is the fiber-to-the-home architecture that brings high bandwidth connections all the way to the home.

- Cable-based: This is the architecture that uses hybrid fiber and coaxial-cable to the homes, initially deployed for TV, but extended to support IP-based data connections.

Access-aware infrastructure functional elements may include:

- Security Control: This includes elements that participate in protocols such as Extensible Authentication Protocol (EAP) to do device and subscriber authentication before admission to the network.

- Address Control: This includes elements that participate in protocols such as DHCP and (Proxy) Mobile IP to manage IP address assignment in the network.

- Policy Enforcement: This includes elements that implement resource and policy enforcement. They may further be sources of accounting information.

- Handover Control: This includes elements that participate in handover decisions (e.g., mobile cell-to-cell handover) and managing per-mobile context or state in the network to ensure that bearer connections reach a mobile terminal.

- Network Address Translation (NAT) Traversal: This may be needed in cases where the terminal sits behind NATs and firewalls in the customer premise network to enable terminal discovery of NAT capabilities and ensure the incoming communications succeed.

- Location Register: This may include functions that enable the terminal to register its civil or geographic location or the network to determine and report location to a mobile terminal.

- Radio Control: This may include functions for radio resource management to direct handovers and paging to locate mobiles in an idle or sleep state.

- Other elements, such as Timing and Synchronization Control may exist as well.

Access-agnostic infrastructure may fall into two categories: Home Network Infrastructure and Visited Network Infrastructure. The core network elements may be similar, but the nature of the functions used corresponds to the roles that are played. For home networks, the focus is on subscriber authentication and service authorization. For visited networks, the focus may be on device authentication and access network resource utilization. Services may be provided in both, but the nature may differ due to location awareness.

Home Network Infrastructure elements include:

- Security Control: Same as above, but may focus more on subscriber services.

- Address Control: Same as above, but may focus on management of IP addresses owned by the home network. Typically provide Home Agent (HA) functionality.

- Policy Enforcement: Same as above, but the focus is on bearer paths through the home network.

- Handoff Control: The focus here may be on application, e.g., SIP, level service interactions such as VCC or on inter-technology handoffs using mobile IP.

Visited Network Infrastructure elements include:

- Security Control: This may involve support of protocols that extend between access and home networks.

- Address Control: Same as above, but the Home Agent can be dynamically provided and utilize IP addresses managed in the visited core infrastructure.

- Policy Enforcement: Supports the policy and resource control in the visited network. The focus is more on local network policy decisions and enforcement.

- Handoff Control: This involves support of handoffs from one access network domain to another access domain, e.g., from one access Gateway (GW) (and supported base stations) span of control to another access GW. That could also include inter-technology handoffs across access technology types.

It should be noted that the home core, visited core and access network domains may be operated by the same service provider or different ones. When more than one operator is involved, additional requirements are placed on inter-provider or NNI interfaces and related border elements.

The following figures use connector bubbles at the top to depict the vertical interfaces to the Session & Policy Control, Application & Service Capability, and OAM&P Functional layers of the architecture. The connectors to the side represent horizontal interfaces between elements of the same general type. For example, base station to base station, or access GW to access GW of various flavors. In some cases, those interfaces are boundaries between technology types requiring interworking.

When comparing the network infrastructure diagrams in the following subsections, the following observations are made with respect to the customer, UNI and NNI interfaces:

- Intra-Customer Network: Most groups recognize that the device that connects to the access network may not be a single device but a gateway device that supports the access of multiple hosts on a customer premises network. This R interface may have common properties independent of architecture and may have an impact on the air or wireline interface to the service provider network. For example, the ability to assign multiple IP addresses is an issue. Whether due to shortage of IPv4 addresses, security, or business choices, this has often resulted in the use of NATs instead of just firewalls by the customer at the edge. NATs have created a host of problems in the network and thus must be dealt with.

- Terminal to Access Network (UNI): Whether called Airborne Internet (AI), UMB_AI, Uu or R1 there are variations on this interface to the access network. While physical and link layer characteristics may be distinct, it may be worth investigation whether the Layer 3 aspects are truly unique. A degree of convergence may be possible if the same Internet Engineering Task Force (IETF) protocols are used in all these architectures.

- Access Network to Visited Core Network (NNI): This interface (U1, Iu, S1, S5, R3) represents one of the points where two service providers may be involved. It could be challenged to see if those interfaces really are unique. In the WiMAX architecture, this is planned to be an external network interface, where others tend to keep this internal. It should also be noted that while the Access GW connecting to the base stations is considered access-specific, there is no reason that a generic access GW could not support multiple Base Stations (BS) of different types.

- Visited to Home Core Networks (NNI): This interface (U16, Gn, Gp, S8b, S2a, S2b, R5) represents the interface between the visited and home core networks. It may be worth investigating whether those designations are just small variations of the same interface. Harmonization across architectures could be useful.

Network infrastructure issues that need to be addressed are in the areas of Policy Decision Function (PDF) or Policy and Charging Rules Function (PCRF) that is part of Policy and Charging Control (PCC) currently in development in 3GPP, 3GPP2 and WiMAX. Traditionalists would have the control pass horizontally between visited and home networks through the SIP plane, but there is no guarantee that the visited network even supports a SIP proxy. A ubiquitous policy control plane would solve this and support more than just IMS, it could support any application, present and yet to be created.

In the following subsections the wireline and wireless broadband access types are further discussed via standards architectures to include a Wireline NGN, 3GPP, 3GPP2, and WiMAX.

C.3.1 Wireline Network Infrastructure

The following figure depicts the wireline-based architecture drawing upon the ITU-T SG13 architecture and the ATIS PTSC NGN architecture. With this, and the subsequent figures, the focus will be on the parallels and differences in functional elements and interfaces that exist, have been identified and are being developed or may be omitted.

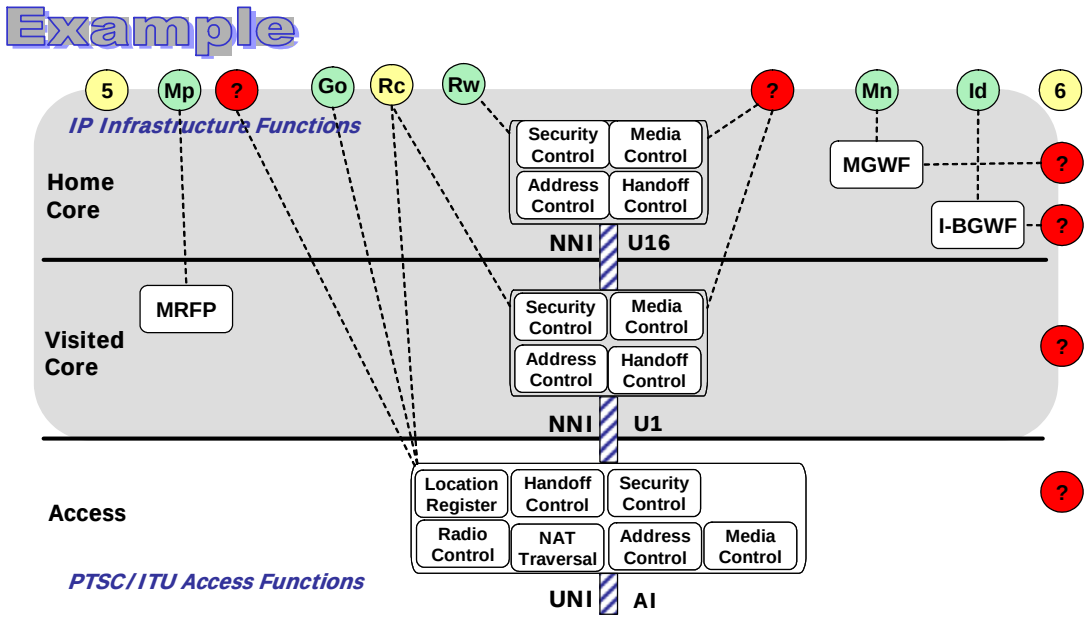


Figure C-6- Wireline Network Infrastructure

The following observations may be made with respect to vertical interfaces in the Wireline Network Infrastructure architecture:

- Content: This interface to the Application & Service Capability Frame has been identified as an area for further study.

- NACF: This interface from the Session & Policy Control Frame is currently being addressed by standardization within the ITU-T with input from various SDOs.

- Media Resource Functions Platform (MRFP): This interface is being defined in ITU-T and IETF for media resource (i.e. media server) control. The media server is shown in the visited network, but could equally likely be done in the home network. Further work is needed as to where to best place the MRFP.

- Equipment Identity Registers (EIR): The EIR is not defined and this interface does not exist. However, its value in the architecture should be evaluated.

- Policy and Charging Resource Functions (PCRF): This function and associated interfaces (Go, Rc, Rw) are in various stages of development in

ITU-T. ATIS expects to use the ITU-T specifications. The other network architectures call out additional reference points as will be shown in later figures. This is an area where the interfaces and protocols used should be identical across architectures.

- AAA: The need for these functions is common across all architectures. Comparison of wireline, which does not identify a direct connection to the network frame, with usage in the wireless network frames is needed.

- Media Gateway Function (MGWF): The Mn reference point is well defined in ITU-T and ATIS PTSC and protocols here are widely used in all architectures.

- Border Gateway Function (BGWF): The Id reference point is identified but not that well defined. It is considered a closed interface in ATIS PTSC, but could be the subject of future investigation should centralized signaling control but distributed policy enforcement be desired.

The following observations may be made with respect to horizontal interfaces in the Wireline Network Infrastructure architecture:

- PSTN: This interface is not usually identified, but is commonly understood to be SS7 and Time Division Multiplex (TDM) interconnection.

- Internet: This interface is not usually identified, but is commonly understood to be an IP interconnect point established through bilateral agreements. There is some work in some forums to address QoS and SLA concerns.

- Home to Home Network: See PSTN or Internet.

- Visited to Visited Network: None identified.

- Access to Access Network: None identified.

C.3.2 Wireless 3GPP Network Infrastructure

The following figure depicts the 3GPP-based wireless architecture.

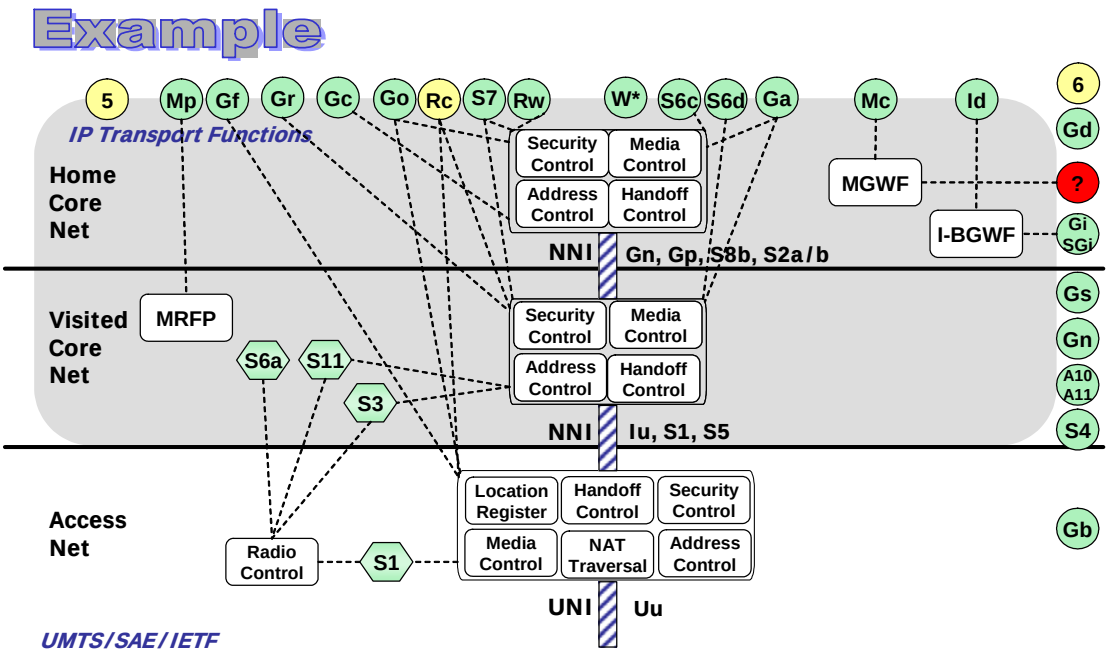


Figure C-7 - 3GPP-based Network Infrastructure

The following observations may be made with respect to vertical interfaces in the 3GPP Wireless Network Infrastructure architecture:

- Content: This interface to the Application & Service Capability Frame has been identified as an area for further study.

- NACF: This interface from the Session & Policy Control Frame is currently being addressed by standardization within the ITU-T with input from various SDOs.

- MRFP: This interface is not included in the architecture, but could easily be included.

- Equipment Identity Registers (EIR): The EIR is defined along with the Gf interface. However, its value in other architectures should be evaluated.

- Policy and Charging Resource Functions (PCRF): The SAE architecture identifies an additional S7 interface. 3GPP also identified a Changing Gateway Function (CGF) with a Ga reference point separately.

- AAA: The 3GPP architecture identifies the S6c interface to the home core network and S6d to the visited core network. Various W interfaces connect to other non-trusted components in other architectures. In addition, there are HSS and Home Location Register (HLR) functions with Gc, Gr, and S6a reference points to home core, visited core and access radio control functions respectively. These HSS/HLR seem to overlap the functions assigned to AAA for other architecture types.

- MGWF: The Mn reference point is well defined in ITU-T and ATIS PTSC and protocols here are widely used in all architectures.

- BGWF: The Id reference point is identified but not that well defined. It could be the subject of future investigation should centralized signaling control but distributed policy enforcement be desired.

The following observations may be made with respect to horizontal interfaces in the 3GPP-based Network Infrastructure architecture:

- PSTN: This interface is not usually identified, but is commonly understood to be SS7 and TDM interconnection.

- Internet: This interface is not usually identified, but is commonly understood to be an IP interconnect point established through bilateral agreements. 3GPP does identify Gi and SGi interfaces.

- Home to Home Network: In addition to PSTN and Internet connections, 3GPP identifies the Gd reference point between GMSCs.

- Visited to Visited Network: 3GPP also identifies several interfaces to visited network elements:

    - Gs to Media Server Control (MSC)/Visitors Location Register (VLR)
    - Gn to Serving GPRS Support Node (SGSN)
    - A10/A11 to Packet Data Servicing Node (PDSN)
    - S4 to SAE-GW

  The issue here generally is whether all architecture types should enable signaling or bearer paths directly between visited core networks (e.g., SGSN) of different architecture types to enhance handover across architectures. To the extent that architectures can be converged on common IP infrastructure down to interfaces to the access GW level, such features could become possible.

- Access to Access Network: 3GPP identifies a Gb reference point for backward compatibility to BSS. Note also the Um interface between mobile terminal and BSS. The issue here generally is whether all architecture types should enable signaling or bearer paths directly between BS or access GW of different architecture types to enable features like Fast Handoff. To the extent that architectures can be converged on common IP infrastructure down to the Access GW or BS level, such features could become possible.

- Radio Resource Control: The 3GPP identified the following reference points with respect to radio resource control (i.e. MME):

- S1: MME (Mobility Management Element) to BS
- S3: MME to SGSN
- S10: MME to MME
- S11: MME to SAE GW

These interfaces tend to be highly proprietary and access-specific. Similar interfaces exist in other architectures and could be investigated for convergence.

C.3.3 3GPP2 Network Infrastructure

The following figure depicts the 3GPP2-based wireless architecture.

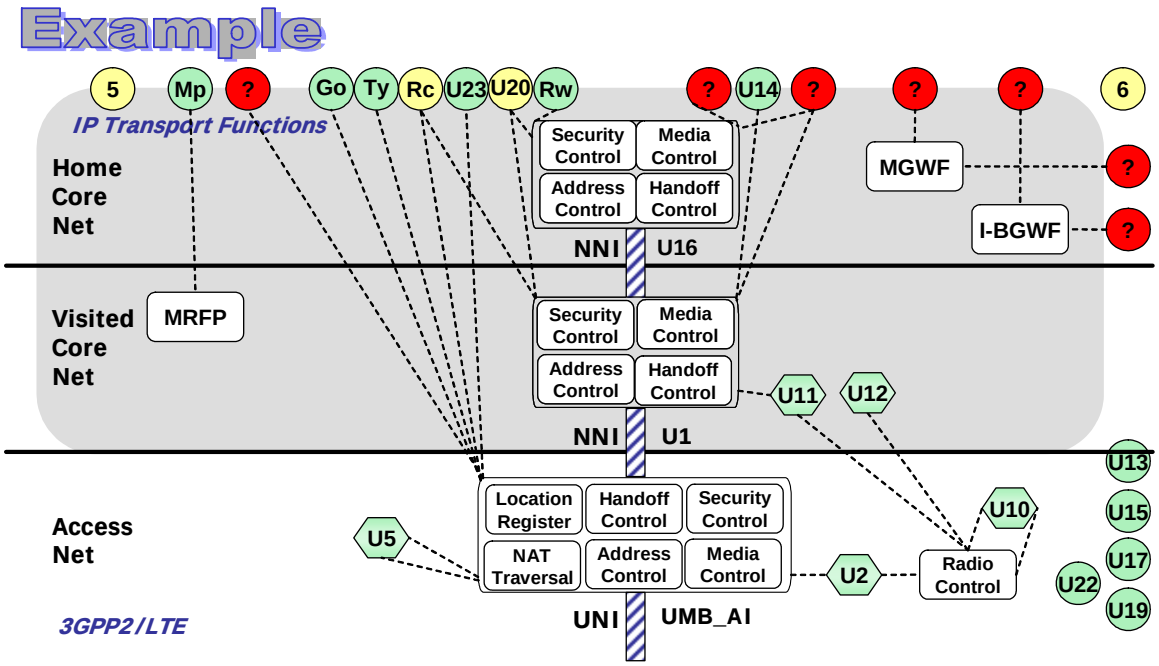


Figure C-8 - 3GPP2-based Network Infrastructure

The following observations may be made with respect to vertical interfaces in the 3GPP2-based Network Infrastructure architecture:

- Content: This interface to the Application & Service Capability Frame has been identified as an area for further study.

- NACF: This interface from the Session & Policy Control Frame is currently being addressed by standardization within the ITU-T with input from various SDOs.

- MRFP: This interface is not included in the architecture, but could easily be included.

- Equipment Identity Registers (EIR): The EIR is not defined and this interface does not exist. However, its value in the architecture should be evaluated.

- Policy and Charging Resource Functions (PCRF): The 3GPP2 architecture variants identify additional Ty, U23, and U20 reference points.

- AAA: 3GPP2 identifies the U14 interface to the visited core network, but does not name the reference point to the home core network node.

- MGWF: The Mn reference point is well defined in ITU-T and ATIS PTSC and protocols here are widely used in all architectures.

- BGWF: This reference point is not identified. It could be the subject of future investigation should centralized signaling control, but distributed policy enforcement, be desired.

The following observations may be made with respect to horizontal interfaces in the 3GPP2-based Network Infrastructure architecture:

- PSTN: This interface is not usually identified, but is commonly understood to be SS7 and TDM interconnection.

- Internet: This interface is not usually identified, but is commonly understood to be an IP interconnect point established through bilateral agreements.

- Home to Home Network: See PSTN or Internet.

- Visited to Visited Network: None identified.

- Access to Access Network: 3GPP2 also identifies several interfaces to visited network elements (Access Gateway (AGW)/Multicast & Anycast Group (MAG) or FA/Link Management Agent (LMA)/MAG):

    - U13 to High Rate Packet Data (HRPD)-AN
    - U15 to AGW
    - U17 to ePDIF
    - U19 to PDSN
    - U22 between ePDIF and PDSN

- Radio Resource Control: The 3GPP2 identified the following reference points with respect to radio resource control:

    - U2: Signaling Radio Control (SRNC) to BS
    - U10: SRNC to SRNC
    - U11: SRNC to AGW
    - U12: SRNC to VAAA (3GPP2)
    - U13: SRNC to HRPD-AN

These interfaces tend to be highly proprietary and access-specific. Similar interfaces exist in other architectures and could be investigated for convergence.

C.3.4 WiMAX Network Infrastructure

The following figure depicts the WiMAX-based network architecture.

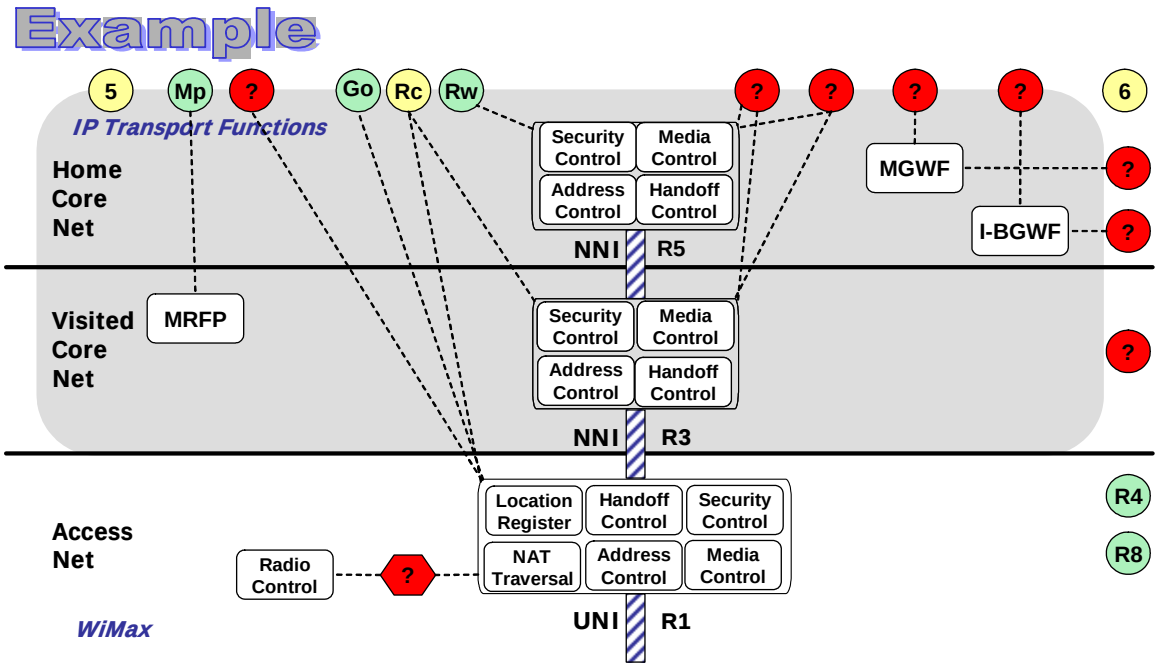


Figure C-9 - WiMAX-based Network Infrastructure

The following observations may be made with respect to vertical interfaces in the WiMAX-based Network Infrastructure architecture:

- Content: This interface to the Application & Service Capability Frame has been identified as an area for further study.

- NACF: This interface from the Session & Policy Control Frame is currently being addressed by standardization within the ITU-T with input from various SDOs.

- MRFP: This interface is not included in the architecture, but could easily be included.

- Equipment Identity Registers (EIR): The EIR is not defined and this interface does not exist. However, its value in the architecture should be evaluated.

- Policy and Charging Resource Functions (PCRF): The WiMAX Forum Networking Group (NWG) is currently addressing the PCC architecture as part of Release 1.5, but will likely try to adopt 3GPP work in this space.

Additional WiMAX-specific attributes may be needed. Currently, the issue is about mobility aspects missing from Release 7 specifications.

- AAA:

- MGWF: The Mn reference point is well defined in ITU-T and ATIS PTSC and protocols here are widely used in all architectures.

- BGWF: This reference point is not identified. It could be the subject of future investigation should centralized signaling control, but distributed policy enforcement, be desired.

The following observations may be made with respect to horizontal interfaces in the WiMAX-based Network Infrastructure architecture:

- PSTN: This interface is not usually identified, but is commonly understood to be SS7 and TDM interconnection.

- Internet: This interface is not usually identified, but is commonly understood to be an IP interconnect point established through bilateral agreements.

- Home to Home Network: See PSTN or Internet.

- Visited to Visited Network: When HA is located in visited network, then access to the Internet occurs here rather than through the home network.

- Access to Access Network: WiMAX identifies the R4 interface between ASN GWs and the R8 interface between BS.

The WiMAX Forum does not identify reference points between the radio resource control and the base station or ASN GW. These interfaces tend to be highly proprietary and access-specific. Similar interfaces exist in other architectures and could be investigated for convergence.

APPENDIX D: FRAMEWORK REFERENCE POINTS

The example architectural context for the reference points and interfaces can be found in Appendix C.

D.1 Network-Control

Ref Pt	From - To	Standards Ref(s)	Comments
• Mp	• MRFC to MRFP	• PTSC-SAC-2007-067 • 3GPP TS 23.002 v7.1.0	• PTSC –Closed • H.248
• Mn	• MGCF to T-MGF	• PTSC-SAC-2007-067 • 3GPP TS 23.002 v7.1.0	• PTSC -Closed • H.248
• Id	• IBCF to IBGF	• PTSC-SAC-2007-067	
• Rc • (Rn?) • U23 • Ty	• TRC-FE to Transport functions • TRC-FE to TRE-FE • PCRF to AGW • V-PCRF to AGW	• ITU-T Y.2111-09/06 • ITU-T Y.2012-09/06 • 3GPP TS 23.402 v0.4.0 • ??	
• Rw (Go) (S7, S8b) U20	• PD-FE (PDF) to Access Border Gateway Function (A-BGF), GGSN • • • • PCRF to HA	• ITU-T Y.2111-09/06 • ITU-T Y.2012-09/06 • PTSC-SAC-2007-067 • 3GPP TS 23.002 v7.1.0 • 3GPP TS 23.402 v0.4.0 • 3GPP2 –X50-20070326-030r2 & X.R0046	• PTSC –Closed • COPS
• 6[6]	• Media DeliveryBroadcast & VoD to Transport	• ATIS-0800007	• Media Stream
• 5 • W* • S6c • S6d • U12 • U14	• AM-FE to A-BGF • to AAA? • PDN SAE Gwy to 3GPP AAA svr • Serving SAE Gwy to 3GPP AAA Proxy • SRNC to AAA • AGW to AAA	• ITU-T Y.2111-09/06 • • 3GPP TS 23.402 v0.4.0? • 3GPP TS 23.402 v0.4.0 • 3GPP2 –X50-20070326-030r2 & X.R0046	(AAA?) UMTS.. Home PLMN Visited PLMN 3GPP2

D.2 Control-Applications

Ref Pt	From - To	Standards Ref(s)	Comments
• Cx	• S-CSCF to HSS/UPSF	• PTSC-SAC-2007-067	• Diameter
• ISC	• S-CSCF to AS, SCIM (SSF, OSA CS)	• PTSC-SAC-2007-067	• SIP
• Dx	• S-CSCF to SLF	• PTSC-SAC-2007-067	• Diameter
• Rf/Ro	• IMS Core to Charging Function	• PTSC-SAC-2007-067	• Diameter
• Pi	• S-CSCF to Presence Network Agent	• 3GPP TS 123 141	• ISC/SIP
• 7	• IPTV-SCF to IPTV Applications	• ATIS-0800007	• Optional[7]

[6] Place Holder – No reference point identifier assigned.
[7] The use of IPTV SCF and/or Core IMS are optional within ATIS IIF

Ref Pt	From - To	Standards Ref(s)	Comments
• 8	• Media Delivery Broadcast and VoD to IPTV application	• ATIS-0800007	
• 9	• Media Delivery Broadcast and VoD to IPTV DRM server	• ATIS-0800007	
• 10	• Media Delivery Broadcast and VoD to IPTV Content Function	• ATIS-0800007	
• 11	• IPTV to Charging Function (Offline/Online)	• ATIS-0800007	
• 12	• IPTV SCF to Service User Profile Functions	• ATIS-0800007	Optional

D.3 Control-User Equipment Premise

Ref Pt	From - To	Standards Ref(s)	Comments
• Gm	• P-CSCF to UE	• PTSC-SAC-2007-067	• SIP
• 1	• Media Delivery Broadcast and VoD to ITF (Control)	• ATIS-0800007	•
• 2	• IPTV SCF to ITF[1]	• ATIS-0800007	•

D.4 Control-Control

Ref Pt	From - To	Standards Ref(s)	Comments
• Ic	• IWF to Other Network	• PTSC-SAC-2007-067	• H.323 or Non-compatible SIP
• Iw	• IBCF to Other Network	• PTSC-SAC-2007-067	• SIP
• Ri • U18	• PD-FE to PD-FE • PCRF to PCRF?	• ITU-T Y.2111-09/06 • 3GPP2 –X50-20070326-030r2 & X.R0046	•

D.5 Intra- and Inter-OAM&P Interfaces

Again referring to Annex A of ETSI TR 102 647 V1.2.1 (2006-10) for OAM&P, one learns that 84% of all management standards are related to Resource Management & Operations. An additional 4% deals each with intra-provider Service Management and Operations and Customer Relationship Management. Finally, 8% address inter-provider Supplier/Partner Relationships and are usually spanning Service Management Layers or Service Management to Resource (Network) Management Layers. For the most part, providers have viewed internal interface descriptions as strategic, proprietary and unsuitable for standardization. This fact explains the paucity of intra-provider OAM&P interfaces. Supplier/Partner Relationship standards were promoted by regulatory requirements such as the Federal Communications Commission (FCC) guidelines arising from the 1996 Telecommunications Act as well as the obvious need to have common billing settlements arrangements between providers in our current diversely owned and managed telecommunications infrastructure.

APPENDIX E: FRAMEWORK-USE CASE MAPPING

Having established the foundation of an EGC framework, this appendix applies the framework to create an end-to-end and top-to-bottom flow of a convergence use case. Specifically, the Service Transfer use case of Section 4 is selected with the caveat that, at this stage of convergence, any flow must be considered an example given the "example" state of the EGC architecture details. The focus of the example flow, therefore, is on reference points between frames (and subframes). The more finely detailed level of work is left for the proverbial interested-reader and work groups as appropriate.

Recalling the Service Transfer use case, the stated and reasonably deduced conditions are summarized:

- Jim has basic SD television service from Service Provider A
- an HD pay-per-view fight is available via an on-line order system
- a confirmation email is part of the order confirmation
- Jim has authorized single-sign-on identity management
- a mobile option for viewing is available (with downloadable mobile client)
- Tom's PDA is from Service Provider B
- Jim's email is password protected from "untrusted" devices (e.g., Tom's PDA)
- Jim downloads the mobile client to Tom's PDA
- "starts the fight" implies tuning the mobile viewer to the fight broadcast
- a remote-control feature is part of the mobile client and allows control of the TV
- a notification on the TV that the pay-per-view event has started but is currently being viewed on another device is consistent with the purchased content rights
- an option exists to move the viewing rights to the TV (using the TV remote)
- displaying the fight on the TV followed (immediately) by replacing the fight on the PDA with a notification is consistent with the purchased content rights.

The implied and reasonably assumed conditions follow:

- Jim has an ISP service with browser-based email from Service Provider A
- Jim starts a PC with standard browser (a PC TV-client is not required)
- Jim's Set Top Box (STB) and TV support HD
- DRM for the fight is provided to Jim's STB following the purchase order
- Tom has an ISP service with broadband mobile access
- Service Pack (SP)-A and SP-B have a business relationship for E2E QoS
- the mobile client is compatible with Tom's PDA
- the mobile remote-control allows device selection based on Jim's profile.

With this understanding of the scenario, the flow is more easily discussed in a step by step manner; however, the following is not intended as a complete treatment. Rather, the figures indicate many of the interactions between frames with a hint toward candidate reference points involved for this use case.

For the **first step** of this scenario flow (depicted in Figure E-1):

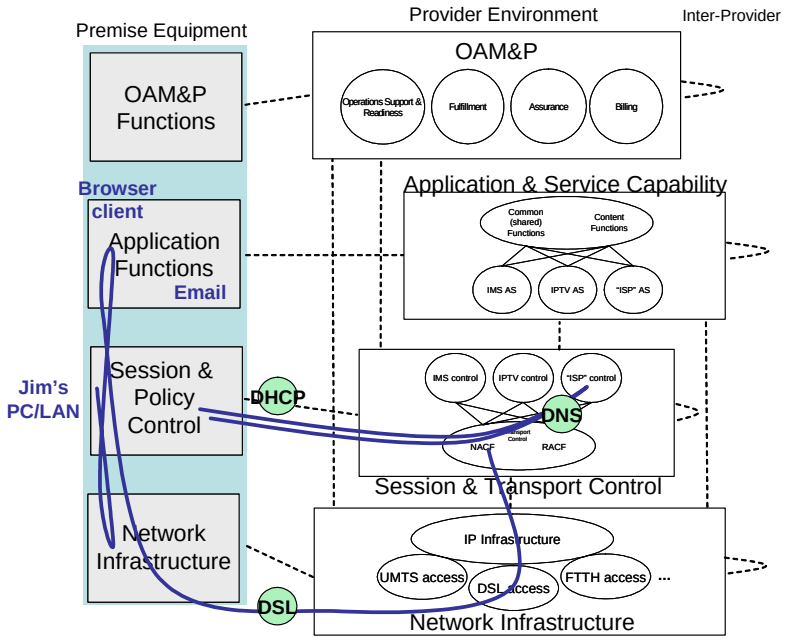


Figure E-1

- Jim has an ISP service with browser-based email from Service Provider A
- Jim starts a PC with standard browser (a PC TV-client is not required for this use case.)

For the **second step** indicated in Figure-E-2:

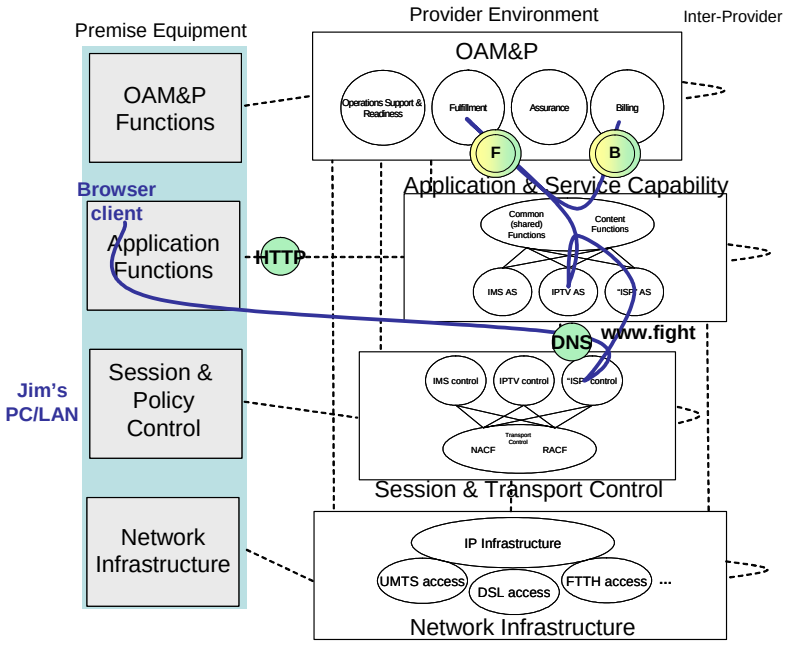


Figure E-2

- Jim has basic SD television service from Service Provider A
- An HD pay-per-view fight is requested via an on-line order system
- A mobile option for viewing is available (with downloadable mobile client)

For the **third step** as indicated in Figure E-3:

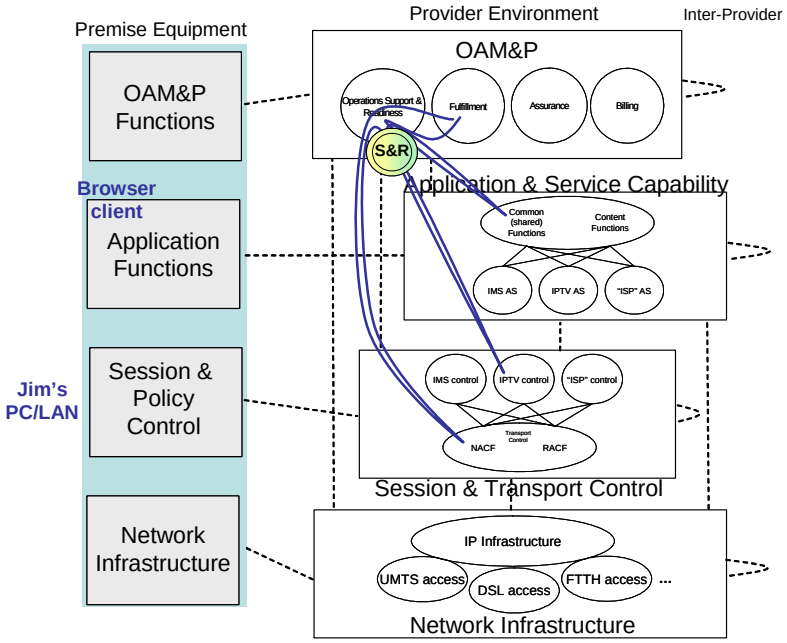


Figure E-3

- Jim now has HD pay-per-view service from Service Provider A

- Jim's STB and TV support HD

The **fourth step**, as indicated in Figure E-4:

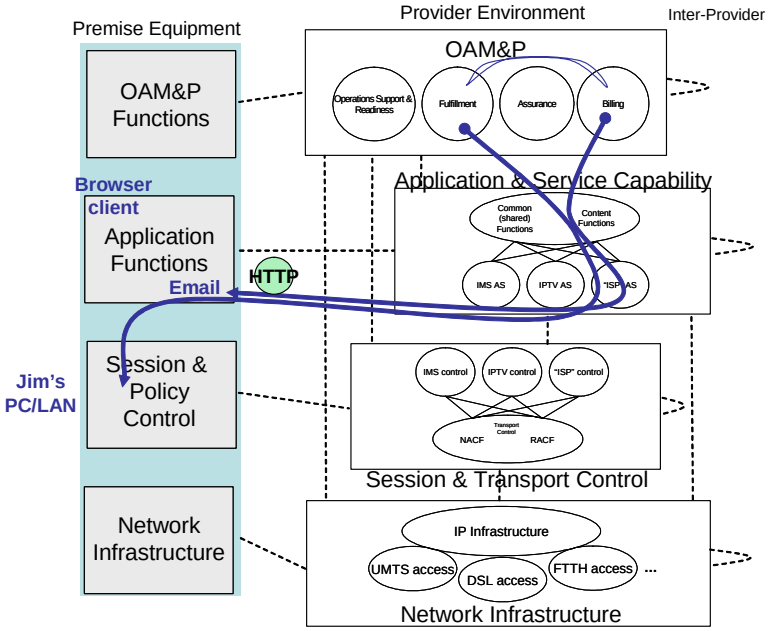


Figure E-4

- A confirmation email is part of the order confirmation
- DRM for the fight is provided to Jim's STB following the purchase order

For the **fifth step**, as indicated in Figure E-5:

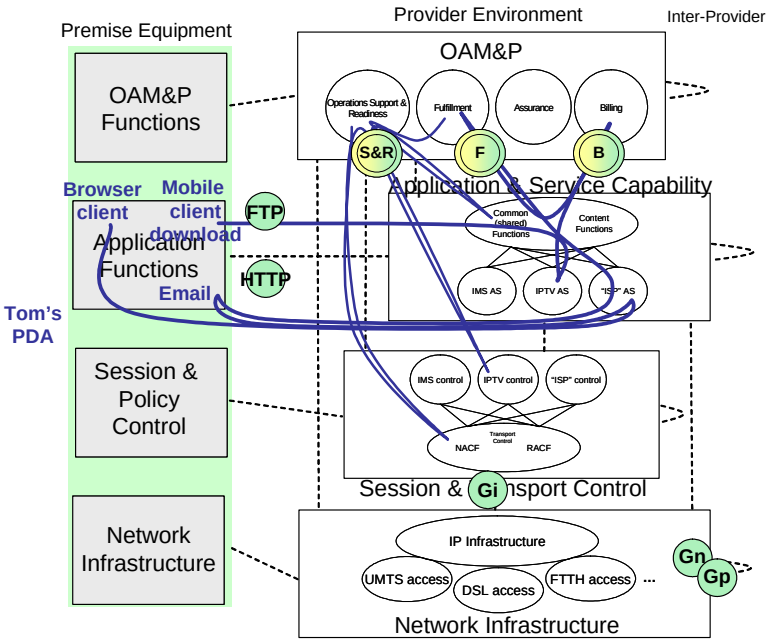


Figure E-5

- Tom's PDA is from Service Provider B with broadband mobile access
- Jim's email is password protected from "untrusted" devices (eg, Tom's PDA)
- Jim has authorized single-sign-on identity management
- Jim downloads the mobile client to Tom's PDA

The **sixth step**, as indicated in Figure E-6:

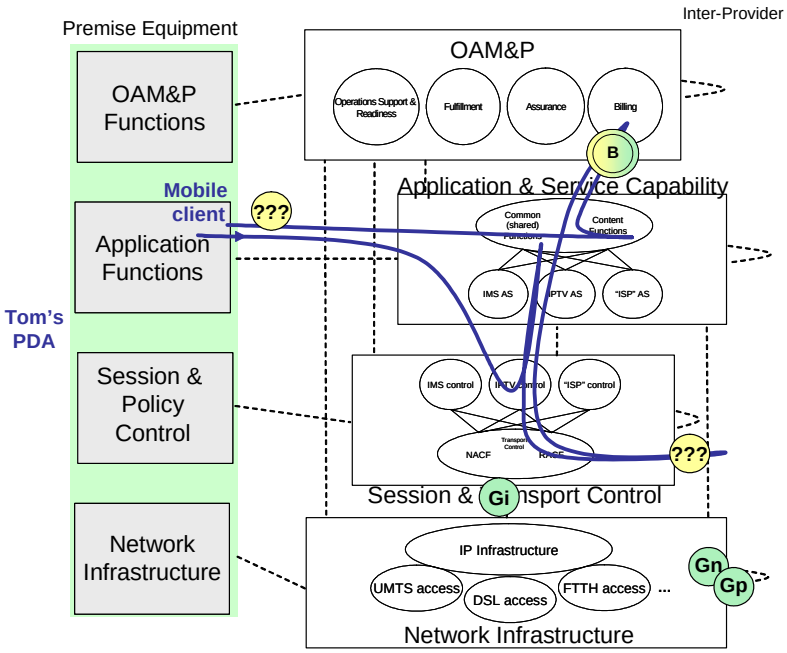


Figure E-6

- The mobile client is compatible with Tom's PDA
- "Starting the fight" implies tuning the mobile viewer to the fight broadcast
- SP-A and SP-B have a business relationship for E2E QoS

The **seventh step** as indicated in figure E-7:

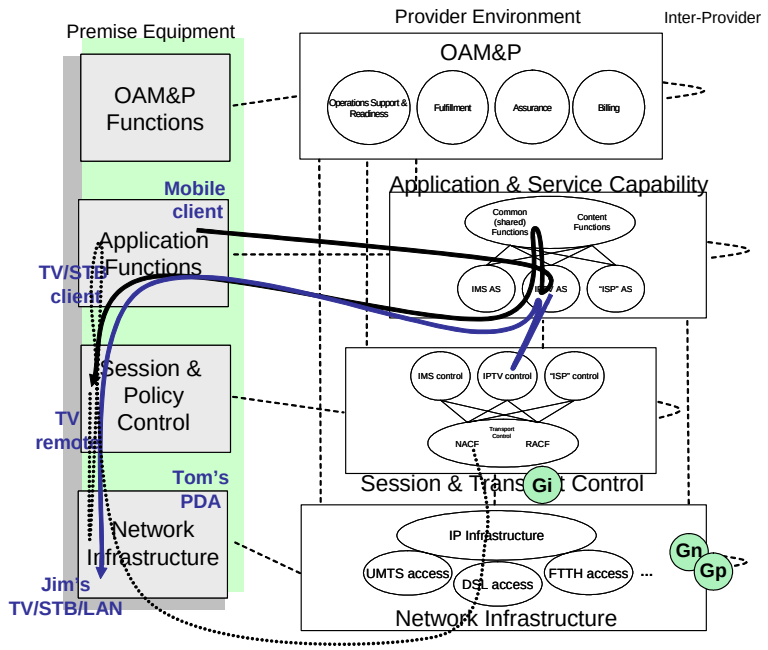


Figure E-7

- A remote-control feature is part of the mobile client and allows control of the TV
- The mobile remote-control allows device selection based on Jim's profile (TV and mobile)
- A notification on the TV that the pay-per-view event has started but is currently being viewed on another device is consistent with the purchased content rights

In the **final step**, as indicated in Figure E-8:

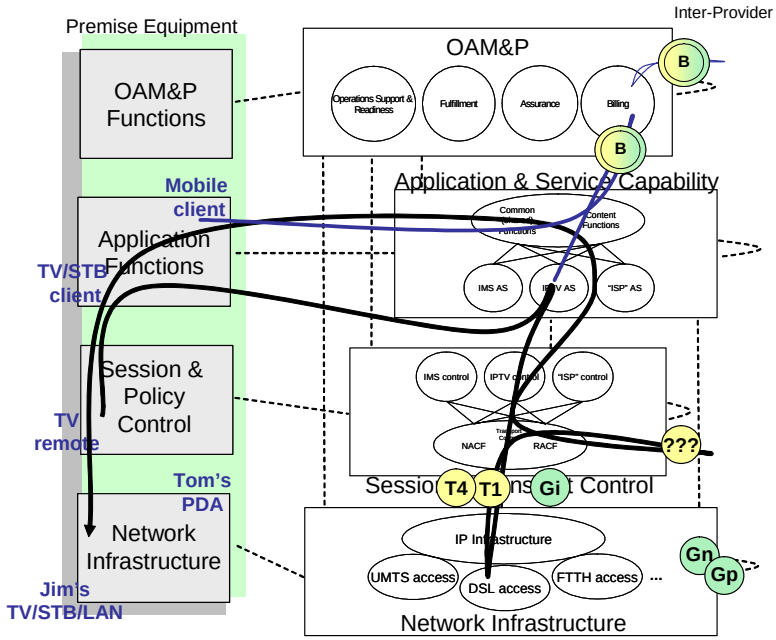


Figure E-8

- The option is exercised to move the viewing rights to the TV (using the TV remote)
- Displaying the fight on the TV followed (immediately) by replacing the fight on the PDA with a notification is consistent with the purchased content rights

APPENDIX F: TUPLE CONCEPT EXPLANATION

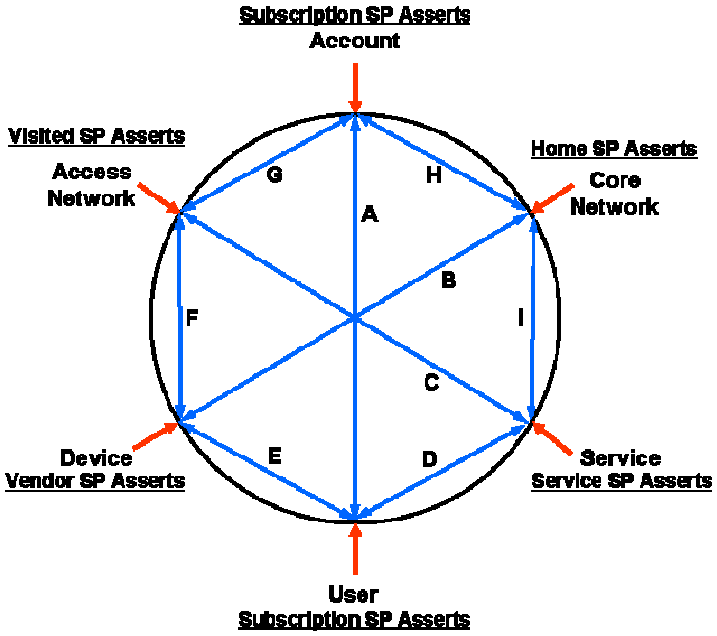
The following is offered as food for thought on how to provide flexibility through identification of atomic components that can be derived separately, but compose a coherent composite profile.

To support the concept of a Flexible User Profile, it is recognized that what once was a single monolithic object making assertions by one service provider about one service type for one device connected to one network and used by one user needs to evolve to a composite object that can make multiple assertions from multiples of each dimension. In database terms, a given instance of a record has several attributes, each of which may take various values. In telecommunications terms, an assertion of a service instance is composed of a combination of various assertions about the nature of that service instance. A tuple is simply a reference to a combination:

> Service Instance = (User, Device, AccessNetwork, CoreNetwork, ServiceType, Account)

That is, a collection of discrete assertions are aggregated into a composite description of the authorizations currently in effect that determine what services may be provided by the system as a whole. Actual service usage results in certain profile data being recorded in detail records.

It is also useful to differentiate between Authentication and Authorization. Authentication involves validating an assertion of Identity. Authorization involves an assertion that a user (authenticated or not) may use a service, in effect binding the Identity of the user to the Identity of the service. One may infer that asserting an association between a User or Device to a Network Type also infers basic (Best Effort) data transport service over that network. The identity and association assertions may be depicted as follows:



The red arrows external to the circle represent Identity assertions or assignments that could be made using cryptographic certificates. The blue arrows inside the circle represent assertions about an association between two elements that could also be done by certificates, but is more likely to be represented by state in the network. In other words, the red and blue arrows represent the authentication and authorization aspects. These arrows could mean the following:

A: A User instance is associated with a instance of an Account (e.g., N:1 shared account)

B: A Device instance is associated with an instance of a Core Network (e.g., N:1 homed).

C: A Service instance is associated with an instance of a Access Network (e.g., N:1 services).

D: A User instance is associated with an instance of a Service (e.g., 1:N possible).

E: A User instance is associated with an instance of a Device (e.g., N:1 or 1:N sharing).

F: A Device instance is associated with an instance of a Access Network (e.g., N:1 registered).

G: An Account instance is associated with an instance of a Access Network.

H: An Account instance is associated with an instance of a Core Network.

I: A Service instance is associated with an instance of a Core Network (e.g., N:1 service offered).

With respect to Accounts, a given user could be associated with multiple accounts, for example, one for personal home use and another for strictly business use, assigned by their employer. It may also be possible for Account numbers to be assigned by multiple service providers providing components of the whole service. In such a case, a composite service could be charged to multiple accounts, which might complicate the goal of providing a single bill to the user. Finally, given that a user can roam across multiple access networks, it may be better to view each connection as a Service or Access Network instance rather than a new account instance for logging and settlement purposes.

An additional possibility would be to assert an additional identity to distinguish the various Roles that a use might take. Thus, a User is not one-dimensional but takes on different facets, depending on the activity being pursued at the time. Although this adds to complexity, it also allows more granular means of authorizing and accounting for services rendered.

The concept of a Service identity may be defined as the addition of a QoS flow to enable some real-time service that requires jitter, delay and loss characteristics. In general, a

Service may be associated with a particular Application running over based IP transport service. It could also be related to some minimal sustained data flow rate that is better than best effort. A Service could also represent a transaction type for which there is a per transaction charge, such as download of music, videos, or ring-tones. Some thought should be given to what is the minimum level of service included in Access or Core network instances and what constitutes an additional level of service to be identified separately as a Service instance.

Of course, this barely covers all the possible permutations of Identities. Each of the above could be represented as a tuple with some null attributes using the following as a template:

(User, Device, AccessNetwork, CoreNetwork, ServiceType, Account)

Thus, as an example, a series of assertions as follows:

(User, Device, ~, ~, ServiceType, Account) by the subscription provider
(~, Device, AccessNetwork, ~, ServiceType, Account) by the access provider

(~, Device, ~, CoreNetwork, ServiceType, Account) by the home provider could collectively define the whole service instance:

(User, Device, AccessNetwork, CoreNetwork, ServiceType, Account)
meaning that this User on this Device can get this ServiceType through these Access and Core networks, to be charged to this Account.

Note, there may be additional Identities that need Authentication and Associations that need to be Authorized. The above merely shows that when multiple players are involved, discrete assertions should be collectible into a unified expression that is referred to here as the Tuple. The format for expressing that Tuple should be the focus of a standardization effort so that different players can contribute their part across administrative domains.

Another dimension to the above is the concept of the time over which the various assertions are made. A given call or service could span multiple Access Networks due to mobility, and thus a complete call may be represented by a series of service instances that are identical except for the changing identity of the access network. Each of those tuples would be referred to as a call segment, where each segment is delimited by a start and stop time. Care should be given to how time is accounted. Similar to the User case above, time could also be characterized by whether it is part of a "busy" hour, business hours or conversely off hours for authorization and accounting purposes.

APPENDIX G: SERVICE INTERACTION MANAGEMENT

Service Interaction Management can be divided into five categories using four characteristics. The characteristics are defined as follows.

1. Linear versus Dynamic Interaction Management
    a. Linear - Scripted response to initial filter criteria such as supplied by IMS user profile. These interactions follow a linear execution of features or applications and do not vary based on the condition/state of the user or network.
    b. Dynamic - Variable invocation of applications based on the condition/state of the user or network. This variable response can impact the order that the features or applications are invoked.
2. Support for Single versus Multiple Services
    a. Single – Combines multiple applications for the delivery of a single service to the user or network.
    b. Multiple – The interaction supports multiple discrete services.
3. Loosely Coupled versus Tightly Coupled Interactions
    a. Loosely Coupled – This interaction is usually stateless but reliable.
    b. Tightly Coupled – The interaction is session oriented. Data is maintained as part of the session either as state or stored data.
4. IMS, Web Services, or NGN interfaces
    a. IMS – These support interactions as defined in 3GPP IMS.
    b. Web Services – Uses web services in a service oriented architecture.

NGN supports a superset of a and b. The 5 types of service interaction management have combinations of the above characteristics. Those combinations are presented in the table below. This table shows that Service Interaction Management is not a point solution but rather a spectrum of solutions optimized for specific functions.

The requirements of an individual service interaction management type are specified by the checked columns in the table. For example, an IMS CSCF shall support linear service invocation. It shall support multiple services. The interaction shall be tightly coupled. It shall support interfaces as specified in IMS.

It also follows that a system supporting all of the above functions but also supporting web services interfaces is not a CSCF but a service broker.

These requirements define the required characteristics of service interaction managers, but they can also be used to classify existing systems. The intent is to refine a previously ambiguous topic so that individual functions can be specified.

Function	Linear Invoke	Dynamic Invoke	Single Service	Multiple Service	Loose Couple	Tight Couple	IMS	Web Services	NGN
IMS S-CSCF	X			X		X	X		
Application Server		X	X			X	(X)	(X)	X
IMS SCIM		X		X		X	X		
Service Orchestration		X		X	X			X	
Service Broker		X		X		X	(X)	(X)	X

Figure G-1

An additional description of each service interaction type follows:

1) Serving Call Session Control Function (S-CSCF) –

The serving-CSCF is the first point of service interaction for IMS services in the 3GPP subsystem model. The S-CSCF uses the initial filter criteria associated with the public user entity

2) Application Server

An application server can manage the interactions required for delivery of a single service. The application coordinates the response of network resources or applications for the delivery of a service. For example, an IM application delivers a text message service after coordinating a routing rules application and a presence application. The delivery of the service is dependent on the response that the IM application receives from the other applications. (Routing Application: No sessions after 10PM, Presence Application: User is registered on mobile device.)

3) SCIM (Service Capability Interaction Manager) function -
This refers to the 3GPP definition in TS 23.002. The current version is v7.1.0 published 2006-03.

The figure below depicts an overall view of the functional architecture for services.

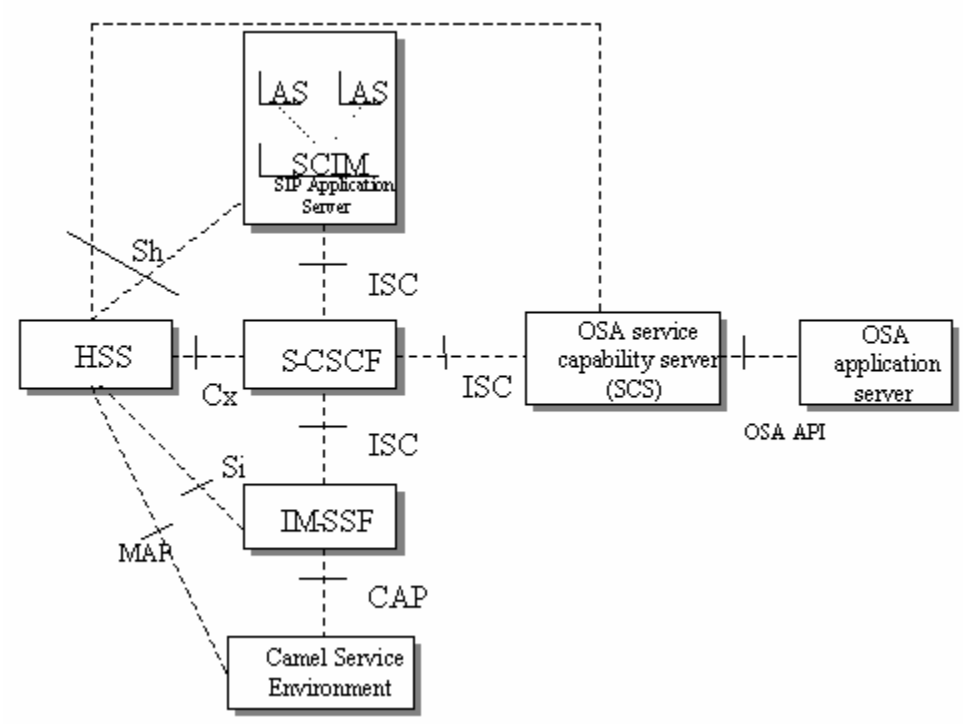


Figure G-2: Functional architecture for the provision of service in the IMS

The application server may contain SCIM functionality and other application servers. The SCIM functionality is an application which performs the role of interaction management.

4) Service Orchestration function –
Service orchestration is most often associated with the flow of business processes. Given a reasonable separation of Application and Service Capabilities including SCIM and Service Brokers from Service Operations, it follows to reserve the use of "service orchestration" to the realm of service operations.

Service Orchestration is the management of business processes within the flow of service operations.

Proposed new definition: Service orchestration is a loosely coupled interaction manager that provides a middle layer interface abstraction between applications. Orchestration provides a publish/subscribe delivery mechanism for application events. This model is useful in the management of business processes as well as service models where multiple applications want specific event information for unrelated purposes.

5) Service Broker function -
More generally, *Service Broker manages the interactions between service capabilities that are exposed using SOA and NGN technology abstractions (including but not limited to IMS service capabilities).*

This function necessarily involves abstraction of the SIP protocol as the IMS service control (ISC) interface; however, other technologies such as Web Service Definition

Language (WSDL) and Simple Object Access Protocol (SOAP) allow the invocation of non-IMS features. Implementations generally model interactions between services as business processes.

The service broker may abstract specific protocols. In this way, the service broker is the protocol agnostic version of the SCIM.

APPENDIX H: ACRONYMS & ABBREVIATIONS

Acronym	Definition
1xRTT	Single Carrier Radio Transmission Technology
3GPP	3rd Generation Partnership Project
A&SC	Application and Service Capabilities
AAA	Authentication, Authorization and Accounting
A-BGF	Access Border Gateway Function
ADSL	Asymmetric Digital Subscriber Line
AF	Application Functions
AGW	Access GateWay
AI	Airborne Internet
AM-FE	Access Management Functional Entity
ANI	Application-to-Network Interface
AP	Access Point
API	Application Programming Interface
AR	Antonymous Registration
AS	Application Server / Autonomous System
ASN	Abstract Syntax Notation
ASP	Applications Service Providers
ATIS	Alliance for Telecommunications Industry Solutions
BE	Border Element
BGWF	Border GateWay Function
BS	Base Station
BSS	Business Support System
CAPEX	Capital Expenditure
CCF	Charging Collector Function
CDMA	Code Division Multiple Access
CGF	Changing Gateway Function
CMIP	Common Management Information Protocol
CPE	Customer Premises Equipment
CRM	Customer Relationship Management
CS	Circuit Switched
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DRM	Digital Rights Management
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data rates for GSM Evolution
ePDIF	Enhanced Packet Data Interworking function
EGC	Exploratory Group on Convergence
EIR	Equipment Identity Registers
eTOM	Enhanced Telecom Operations Map
ETS	Emergency Telecommunications Service
ETSI	European Telecommunications Standards Institute
e-VCC	enhanced Voice Call Continuity
EVDO	Evolution Data Optimized
FA	Foreign Agent
FCC	Federal Communications Commission
FTP	File Transfer Protocol
FTTH	Fiber-To-The-Home
FTTN	Fiber-To-The-Node

GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture (Liberty Alliance)
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communications
GUI	Graphical User Interface
GUP	Generic User Profile
GW	Gateway
HA	High Availability
HGWC-FE	Home GateWay Configuration Functionality Entity
HLR	Home Location Register
HRPD	High Rate Packet Data
HSS	Home Subscriber Server,
IBCF	Interconnect Border Control Function
ID-FF	Identity Federation Framework (Liberty Alliance)
ID-WSF	Identity Web Services Framework (Liberty Alliance)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
I-ENUM	Infrastructure ENUM
IETF	Internet Engineering Task Force
iFC	Initial Filter Criteria
IIF	IPTV Interoperability Forum (ATIS)
IM	Instant Messaging
IMS	Internet Protocol Multimedia Subsystem
IP	Internet Protocol
IPDR	Internet Protocol Detail Record
IPSEC	Internet Protocol Security
IPTV	Internet Protocol Television
ISC	IMS Service Control
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU-Telecommunications Standardization Sector
IWF	Interworking Function
LAN	Local Area Network
LAP	Liberty Alliance Project
LMA	Link Management Agent
LTE	Long Term Evolution
MAG	Multicast & Anycast Group
MCU	Multipoint Control Unit
MGWF	Media Gateway Function
MME	a file in the Multi-purpose internet Mail Extensions
MRFP	Multimedia Resource Functions Platform
MSC	Media Server Control
MSF	Multiservice Switching Forum
NACF	Network Access Control Function
NAC-FE	Network Access Configuration Function – Functional Entity
NAT	Network Address Translation
NGN	Next Generation Network
NGNSP	Next Generation Network Service Provider

NGOSS	Next Generation Operation Support System
NNI	Network-to-Network Interface
NWG	WiMax Networking Group
OAM&P	Operation, Administration, Maintenance and Provisioning
OASIS	Organization for the Advancement of Structured Information Standards
OBF	Ordering and Billing Forum (ATIS)
OMA	Open Mobile Alliance
OPEX	Operational Expenditure
OSS	Operation Support System
PC	Personal Computer
PCC	Policy and Charging Control
PCS	Personal Communications Services
P-CSCF	Proxy - Call Session Control Function
PDA	Personal Digital Assistant
PDF	Policy Decision Function
PD-FE	Policy Decision Functional Entity
PDP	Policy Decision Point
PDSN	Packet Data Servicing Node
PLMN	Public Land Mobile Network
PMIP	Proxy Mobile IP
PEP	Policy Enforcement Point
PRQC	Network Performance Reliability and Quality of service Committee (ATIS)
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies & Systems Committee (ATIS)
QoE	Quality of Experience
QoS	Quality of Service
RACF	Resource and Administration Control Functions
RFID	Radio Frequency Identification
RM	Resource Management
RM&O	Resource Management & Operations
SAC	Service Access Code/Special Area Code
SAE	System Architecture Evolution
SCF	Service Control Function
SCIM	Service Capability Interaction Manager
S-CSCF	Serving – Call Session Control Function
SCTE	Society of Cable Telecommunications Engineers
SD	Secure Digital card
SDE	Service Delivery Environment
SDO	Standards Development Organization
SGF	Signaling Gateway Function
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLF	Subscriber Location Function
SMB	Server Message Block protocol
SM&O	Service Management & Operations
SMS	Short Message Service
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol

SOHO	Small Office/Home Office
SP	Service Provider
S/PRM	Supplier/Partner Relationship Management
SRNC	Signaling Radio Control
STB	Set Top Box
S&TC	Session & Transport Control
SUP	Subscriber Update Protocol
TA	Terminal Adapter
TAA-FE	Transport Authentication and Authorization Functional Entity
TDM	Time Division Multiplex
TIA	Telecommunications Industry Association
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TLM-FE	Transport Location Management Functional Entity
TMF	TeleManagement Forum
TMOC	Telecom Management and Operations Committee (ATIS)
TOPS	(ATIS) Technology and Operations Council
TRC-FE	Transport Resource Control Functional Entity
TUP-FE	Transport User Profile Functional Entity
TV	Television
UDDI	Universal Description Discovery and Integration
UE	User Equipment
UICC	UMTS Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
UNI	User Network Interface
UPSF	User Profile Server Function
URI	Uniform Resource Identifier
VCC	Voice Call Continuity
VDSL	Very high data rate Digital Subscriber Line
VLR	Visitors Location Register
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WEP	Wired Equivalent Privacy
WiFi	A term developed by the Wi-Fi Alliance to describe WLAN (WLAN) products that are based on the IEEE 802.11x standards.
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WSDL	Web Service Definition Language
WTSC	Wireless Technologies and Systems Committee (ATIS)
XDR	External Data Representation
XML	Extensible Markup Language

APPENDIX I: EGC MEMBERS

Company	Name
Chair	
AT&T	Chris Rice
Members	
Alcatel- Lucent	Gary Hanson*
Alcatel-Lucent	Igor Faynberg
Alcatel-Lucent	Ken Biholar
Alcatel-Lucent	Larry O'Pella*
AT&T	Phyllis Anderson
AT&T	Chuck Bailey
AT&T	Chuck Dvorak
AT&T	Bob Hall
AT&T	Gary Munson*
AT&T	George Stanek*
AT&T	Randy Wohlert*
AT&T	Hank Kafka
AT&T	Steven Wright*
AT&T	Tom Anschutz*
BT	Graham Travers
Ciena	Michael Gazier*
Cisco	Art Reilly
Cisco	Chip Sharp
Cisco	Darren Beers
Cisco	Kenny Hong*
Cisco	Michael Hammer*
Ericsson	Asok Chatterjee
Ericsson	George Foti
Hewlett-Packard	Marc Brandt
Hewlett-Packard	Mark Gullett*
Intel	Walt Brown
Intrado	Larry Ciesla
Juniper	Carl Engineer*
Leapstone	Stuart Walker
NeuStar	Tom Ely
Nokia, Inc.	Ed Ehrlich
Nortel	Jim McEachern*
Qwest	Andrew White*
Qwest	Mike Fargano*
RIM	John-Luc Bakker
Siemens Communications	David Francisco
Siemens Communications	Felipe Alvarez Del Pino*
Siemens Communications	Victor Coello
Syniverse Technologies	Lou Grilli
TDS Telecom	Kenneth Paker
Trendium	Dr. Sameh Yamany
U.S. Cellular	Narothum Saxena
Verizon	Naseem Khan*
Verizon	Tom Helmes
ATIS Staff	
ATIS	Tim Jeffries
ATIS	Martha Ciske
ATIS	Lisa Wiseman

**Denotes section and subgroup contribution.*