Chicago, Illinois - USA
29 May – 2 June 2006

SOURCE: **ATIS**

TITLE: **ATIS NGN Framework, Part III: Standards Gap Analysis**

AGENDA ITEM: **GSC11 OPENING; 4.3**

DOCUMENT FOR:

Decision	
Discussion	
Information	**XX**

1 DECISION/ACTION REQUESTED

N/A

2 REFERENCES

N/A

3 RATIONALE

This document has been prepared by the ATIS Next Generation Networks Focus Group (NGN-FG) as the third part in a series of documents intended to identify the requirements, objectives, and priorities for the NGN from the perspective of ATIS member companies, and the identification and creation of standards for a global NGN.

The first document released by ATIS in November 2004 was the ***ATIS Next Generation Network (NGN) Framework Part I: NGN Definitions, Requirements, and Architecture, Issue 1.0****. The Part I document contains a snapshot of NGN target architectures, requirements, and features for which phased implementation requirements will be developed. In August 2005, the second document, the* ***ATIS NGN Framework Part II: NGN Roadmap 2005*** *was released. Part II built upon Part I to identify the primary criteria for an NGN Roadmap. The Roadmap focused on the necessary components and capacities of an infrastructure that enables the flexible creation of new NGN services and identified the underlying service enablers that will allow new services to be efficiently introduced.*

Part III builds upon the previous documents, in particular the requirements identified in Part I and priority enablers identified by service providers in Part II, to identify standards activities and assess the potential impacts of NGN across other priority issues specified by the ATIS Technology and Operations (TOPS) Council. Through a bottom-up assessment of NGN service enablers, based on company focus, resources, and standards activities, an assessment of the progress of NGN standards development is provided. Where gaps are identified, additional issues are proposed.

4 CONSEQUENCES AND IMPLICATIONS

N/A

5 ISSUES FOR DISCUSSION

N/A

ATIS Next Generation Network (NGN) Framework, Part III: Standards Gap Analysis

Issue 1.0
May 2006

ATIS 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** >

Next Generation Network (NGN), Part III: Standards Gap Analysis

Is an ***ATIS Work Plan*** developed by the **Next Generation Network Focus Group** 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 © 2006 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

EXECUTIVE SUMMARY **7**
1 INTRODUCTION **8**
2 UNIFIED USER PROFILE **9**
2.1 REQUIREMENTS 9
2.2 FUNCTION/SERVICE ENABLED 10
2.3 CURRENT STANDARDIZATION ACTIVITIES 10
2.3.1 ETSI-TISPAN 10
2.3.2 3GPP 10
2.3.3 ATIS 11
2.3.4 Open Mobile Alliance (OMA) 12
2.3.5 W3C 12
2.4 IDENTIFIED GAPS 12
2.5 PROPOSED WORK ITEMS 13
3 SECURITY **15**
3.1 CONTEXT 15
3.1.1 Security Architecture & Framework Overview 15
3.2 CURRENT STANDARDIZATION ACTIVITIES 19
3.2.1 Activities by Organization 19
3.2.2 Activities by Technology 24
3.3 ASSESSMENT (IDENTIFIED GAPS) 25
3.3.1 Security architectures 25
3.3.2 Security standards technical alignment 25
3.3.3 Authentication 25
3.4 PROPOSED WORK ITEMS 25
4 SERVICE DECOUPLING **27**
4.1 REQUIREMENTS 27
4.1.1 Access Criteria for NGN Conformance 27
4.1.2 Service Definition Environment 28
4.2 FUNCTION/SERVICE ENABLED 28
4.3 IDENTIFIED GAPS 28
4.4 PROPOSED WORK ITEMS 29
5 PRESENCE **29**
5.1 REQUIREMENTS 29
5.2 FUNCTION/SERVICE ENABLED 29
5.3 CURRENT STANDARDS ACTIVITIES 30
5.3.1 IETF 30
5.3.2 3GPP/3GPP2 IMS 30
5.3.3 OMA and IMPS 31
5.3.4 Parlay Group's PAM specification 31
5.3.5 Presence Functional Architecture 31
5.4 IDENTIFIED GAPS 36
5.5 PROPOSED WORK ITEMS 36
6 SERVICE TRANSPARENCY **36**
6.1 REQUIREMENTS 36
6.2 FUNCTION/SERVICE ENABLED 37
6.3 CURRENT STANDARDIZATION ACTIVITIES 37
6.3.1 End-to-end Transparency 37
6.3.2 Service Interworking Transparency 38
6.4 IDENTIFIED GAPS 39
6.4.1 End-to-end transparency 39
6.4.2 Service Interworking Transparency 40
6.5 PROPOSED WORK ITEMS 40
6.5.1 End-to-end Transparency 40
6.5.2 Service Interworking Transparency 40
7 QOS **40**
7.1 REQUIREMENTS 40
7.1.1 QoS Specification 41
7.1.2 QoS Signaling 44

7.1.3 *Resource Management* 46
7.2 FUNCTION/SERVICE ENABLED 47
7.3 CURRENT STANDARDIZATION ACTIVITIES 48
7.3.1 *QoS Specification* 48
7.3.2 *QoS Signaling* 49
7.3.3 *Resource Management* 51
7.4 IDENTIFIED GAPS 51
7.4.1 *QoS Specification* 51
7.4.2 *QoS Signaling* 52
7.4.3 *Resource Management* 53
7.5 PROPOSED WORK ITEMS 53
7.5.1 *QoS Specification* 54
7.5.2 *QoS Signaling* 56
7.5.3 *Resource Management* 56
8 RESOURCE AND ADMISSION CONTROL 58
8.1 REQUIREMENTS 58
8.2 FUNCTION/SERVICE ENABLED 59
8.3 CURRENT STANDARDIZATION ACTIVITIES 59
8.3.1 *Session Management* 59
8.4 IDENTIFIED GAPS 61
8.5 PROPOSED WORK ITEMS 62
9 SETTLEMENT 63
9.1 REQUIREMENTS 63
9.2 FUNCTION/SERVICE ENABLED 63
9.3 CURRENT STANDARDS ACTIVITIES 65
9.3.1 *ATIS* 65
9.4 IDENTIFIED GAPS 66
9.5 PROPOSED WORK ITEMS 66
10 NGN MANAGEMENT (OAM&P) 67
10.1 REQUIREMENTS 67
10.1.1 *Specifications for NGN Management* 68
10.1.2 *Generic telecommunications management specifications, reused for NGN* 68
10.1.3 *Specifications for the management of NGN functions* 68
10.1.4 *Other relevant specifications* 69
10.2 IDENTIFIED GAPS 72
10.2.1 *Harmonization Issues* 72
10.2.2 *N.A. Specific Gaps* 73
10.3 PROPOSED WORK ITEMS 74
11 LOCATION BASED SERVICES 74
11.1 REQUIREMENTS 74
11.2 FUNCTIONS/SERVICES ENABLED 75
11.3 CURRENT STANDARDIZATION ACTIVITIES 75
11.3.1 *IETF* 75
11.3.2 *ETSI/TISPAN* 76
11.3.3 *ATIS ESIF and NENA* 76
11.3.4 *Open Geospatial Consortium* 76
11.3.5 *OASIS* 77
11.3.6 *EPCglobal* 77
11.3.7 *OMA* 77
11.3.8 *MAGIC Services Initiative* 77
11.3.9 *GSM Association* 77
11.4 IDENTIFIED GAPS 77
11.5 PROPOSED WORK ITEMS 78
12 MULTICAST 78
12.1 REQUIREMENTS 78
12.2 FUNCTION/SERVICE ENABLED 78
12.3 CURRENT STANDARDIZATION ACTIVITIES 78
12.3.1 *IETF* 79
12.3.2 *ATIS IPTV Interoperability Forum* 80
12.3.3 *DSL Forum* 80
12.3.4 *Other (non IP) Multicast Fora and Capabilities* 81

12.4 IDENTIFIED GAPS 81
12.5 PROPOSED WORK ITEMS 82
13 ADDRESS RESOLUTION (E.164 / SIP) 82
13.1 REQUIREMENTS 82
13.2 FUNCTION/SERVICE ENABLED 82
13.3 CURRENT STANDARDIZATION ACTIVITIES 82
13.3.1 ATIS 82
13.3.2 IETF 83
13.3.3 ITU-T 83
13.3.4 ETSI 83
13.3.5 EIDQ 83
13.4 IDENTIFIED GAPS 83
13.4.1 ENUM 83
13.4.2 VoIP Interconnection 83
13.4.3 Number portability correction 83
13.5 PROPOSED WORK ITEMS 83
14 DIGITAL RIGHTS MANAGEMENT 84
14.1 REQUIREMENTS 84
14.1.1 Top Level DRM System Objectives 84
14.2 OVERVIEW OF EXISTING RELEVANT SPECIFICATIONS 85
14.2.1 DRM in the Context of NGN 85
14.2.2 NGN DRM Standards/Technology Gaps (for Standards available by EOY 2007) 86
14.3 PROPOSED WORK ITEMS 86
15 USER CONTROL OF PROFILE/SERVICES 87
15.1 REQUIREMENTS 87
15.1.1 3rd Party Access 87
15.2 FUNCTION/SERVICE ENABLED 88
15.3 CURRENT STANDARDIZATION ACTIVITIES 88
15.3.1 ETSI 88
15.3.2 3GPP 88
15.3.3 ATIS 89
15.4 IDENTIFIED GAPS 89
15.5 PROPOSED WORK ITEMS 89
16 MEDIA RESOURCE FUNCTIONS 90
16.1 REQUIREMENTS 90
16.2 FUNCTION/SERVICE ENABLED 90
16.3 CURRENT STANDARDIZATION ACTIVITIES 91
16.3.1 Media Resource Function Architectures 91
16.3.2 Control Protocols/Languages for Media Resource Function 93
16.4 IDENTIFIED GAPS 95
16.5 PROPOSED WORK ITEMS 96
17 GROUP MANAGEMENT 97
17.1 REQUIREMENTS 97
17.2 FUNCTION/SERVICE ENABLED 98
17.3 CURRENT STANDARDIZATION ACTIVITIES 98
17.3.1 OMA 98
17.3.2 IETF 99
17.3.3 ETSI / 3GPP 99
17.4 IDENTIFIED GAPS 99
17.5 PROPOSED WORK ITEMS 99
18 EMERGENCY RELATED SERVICES 100
18.1 EMERGENCY TELECOMMUNICATIONS SERVICE (ETS) 100
18.1.1 Requirements 101
18.1.2 Current Standardization Activities by Organization 101
18.1.3 Identified Gaps 103
18.1.4 Proposed Work Items 103
18.2 NEXT GENERATION 9-1-1 (NG9-1-1) EMERGENCY SERVICES 103
18.2.1 Requirements 103
18.2.2 Function/Service Enabled 104
18.2.3 Current Standardization Activities 104

18.2.4 Identified Gaps *109*
18.2.5 NG9-1-1 Proposed Work Items *110*
18.3 AUTOMATIC (CRASH) NOTIFICATION CAPABILITY 113
18.4 EMERGENCY ALERT SERVICE 113
19 WIRELESS/WIRELINE CONVERGENCE 113
19.1 GENERAL DESCRIPTION 113
19.2 REQUIREMENTS 113
19.3 FUNCTION/SERVICE ENABLED 113
19.4 CURRENT STANDARDIZATION ACTIVITIES 114
19.4.1 3GPP *114*
19.4.2 ATIS *114*
19.4.3 ETSI *114*
19.4.4 ITU *114*
19.4.5 IETF *114*
19.5 IDENTIFIED GAPS 114
19.6 PROPOSED WORK ITEMS 114
APPENDIX A: NGN ACRONYMS 116
APPENDIX B: NGN FOCUS GROUP MEMBERS 122

EXECUTIVE SUMMARY

This document has been prepared by the ATIS Next Generation Networks Focus Group (NGN-FG) as the third part in a series of documents intended to identify the requirements, objectives, and priorities for the NGN from the perspective of ATIS member companies, and the identification and creation of standards for a global NGN.

The first document released by ATIS in November 2004 was the *ATIS Next Generation Network (NGN) Framework Part I: NGN Definitions, Requirements, and Architecture, Issue 1.0*. The Part I document contains a snapshot of NGN target architectures, requirements, and features for which phased implementation requirements will be developed. In August 2005, the second document, the *ATIS NGN Framework Part II: NGN Roadmap 2005* was released. *Part II* built upon *Part I* to identify the primary criteria for an NGN Roadmap. The Roadmap focused on the necessary components and capacities of an infrastructure that enables the flexible creation of new NGN services and identified the underlying service enablers that will allow new services to be efficiently introduced.

This document builds upon the previous documents, in particular the requirements identified in *Part I* and priority enablers identified by service providers in *Part II*, to identify standards activities and assess the potential impacts of NGN across other priority issues specified by the ATIS Technology and Operations (TOPS) Council. Through a bottom-up assessment of NGN service enablers, based on company focus, resources, and standards activities, an assessment of the progress of NGN standards development is provided. Where gaps are identified, additional issues are proposed.

While engaging in this gap analysis, the NGN-FG sought to identify gaps, overlaps, and synergies in the existing and anticipated standards activities taking place within ATIS as well as external organizations such as 3rd Generation Partnership Project (3GPP), European Telecommunication Standards Institute (ETSI), and the International Telecommunication Union (ITU).

Government mandates such as the Communications Assistance for Law Enforcement Act (CALEA) and lawful intercept are not addressed in this document. Industry responds to these mandates as they are required with the development of appropriate standards. Hence, the identification of standards gaps in the implementation of government mandates, although priority service enablers, are not fully explored in this gap analysis.

As with any new area of standards development, the process and progress of the NGN and its implementation is an ongoing activity. ATIS thus intends this document as a work in progress, expects its periodic revision, and welcomes any comments on its content and conclusions.

1 INTRODUCTION

The purpose of this Gap Analysis is to identify standards activities and assess the potential impacts of NGN across other TOPS priority issues in support of the timely development of the NGN.

The ATIS NGN Focus Group is an activity of the TOPS Council, a standing committee of the ATIS Board of Directors. The NGN-FG inherently involves the executive level of ATIS member companies in its participants and perspectives. Unique to this Gap Analysis is also the participation of the elected leaders of the ATIS committees and fora. These leaders formally provided input, feedback, and assessment of the content of this analysis from the perspectives of their various committees.

The topics addressed in this gap analysis should, by and large, be familiar to the reader of the previously released *ATIS NGN Framework (Part I)* and *Roadmap (Part II)* documents. While the initial intent of this document was to assess standard needs with respect to the service enablers previously identified and ranked by service providers in order of importance in *Part II*, in recognition of the emergent nature of the NGN, additional areas, such as Wireless/Wireline Convergence and Emergency Related Services are included. Each section addresses an area from which a function or service of the NGN is enabled. In most cases, each section will provide information on the following:

1. Requirements
2. Function/Service Enabled
3. Current Standards Activity
4. Identified Gaps
5. Proposed Work Items

The Requirements sections contain a definition of the character of the NGN which must or should be developed in order to fulfill the expectation of a function or service. The Function/Service Enabled is a description of what the fulfillment of the requirements will allow to take place. The Current Standards Activities references the activities and documents undergoing work within standards development committees, within ATIS, and externally. The Identified Gaps defines where and what is not being addressed by the current activity.

Proposed work items are the suggested activities which need to take place to close the gap left by current activities. The work items vary in their specificity. When appropriate, a specific committee or organization has been named as a primary or secondary recipient of the work item. The nature of the work items is that they can build upon current work taking place, are akin to an Issue statement, give general direction, propose a new group or committee, and propose inter-committee and organization harmonization activity. The work items are as varied as the topics they address. When known, a timeline or target completion date is given.

It should be noted that Section 2, "Unified User Profile" and Section 15, "User Control of Profile/Services" both deal with the subject of User Profiles but from different perspectives. Section 2 relates to providing a consistent, unified user profile that encompasses communication services and web services, provided by a range of service providers. Section 15 relates to providing the end user with control over the services that they subscribe to. To provide a complete picture of the standards gaps related to user profiles, the reader is advised to examine both of these sections.

It is intended that the information in this analysis present an accurate snapshot of the telecommunications industry standards development activities surrounding the NGN at the time of this analysis' publication (May 2006). The attempt has been made to provide complete and accurate reference to current standards activities and documents. Updates on ATIS issues and documents are accessible on an ongoing basis via the ATIS website and document store.

2 UNIFIED USER PROFILE

This section addressing the Unified User Profile relates to providing a consistent, unified user profile that encompasses communication services and web services provided by a range of service providers.

2.1 Requirements

In today's networks, the user experience is greatly defined by the terminal characteristics and the user location. A trivial example is dialing and number plans: a user familiar with the North America (N.A.) Numbering Plan has a very difficult time placing a local or long-distance call when traveling outside N.A. In the NGN, users may have *profiles* that allow uniform network interfaces (regardless of location) and service ubiquity (i.e., the users' subscribed services are also available on a "host" network). Thus, users may need to identify the person they wished to call ,and the profile will interact with the network to "dial" the call irrespective of which country they may be in.

The management and application of these profiles reflect the interaction characteristics of a user at a specific time (i.e., reflect the "role" they have chosen at a time). The system should recognize and modify its presented interface to properly reflect the user "role." The roles of users are independent and dynamic.

The *personal profile* is the cornerstone of an end-user-centric world. Today, end-users are confronted with fragmented service, requiring them to enter and maintain equivalent information several times – for example: address books, buddy lists, billing and payment preferences, phone numbers, presence, and ring-tones.

Ideally, the end-user would only require one, single personal-profile containing all of his personal information and preferences. In order for such a profile to be attractive for the end-user, a number of prerequisites must be fulfilled. The profile must be delivered in a

simple way that is manageable by the end-user. It also must address fundamental core end-user values such as privacy, security, intimacy, life enrichment, and simplification.

2.2 Function/Service Enabled

This enables service capabilities to be accessed from a range of locations and devices. Beyond this, many of the services enabled are in theory possible by manually provisioning the same information on multiple devices. However, in practice this is awkward, and will not be done. Therefore, in practice, the unified user profile enables (i.e., makes practical) any services that link together separate devices or appearances of a user (e.g., logging in from another user's soft client). It also forms the foundation for functionalities based on who is calling.

2.3 Current Standardization Activities

2.3.1 ETSI-TISPAN

Current standardization activities taking place are the development of ETSI materials, such as: STF265, TISPAN 02027. TISPAN defines the USPF for this, which is the Home Serving System (HSS) minus the Home Location Register (HLR) functionality.

- User Profile Management
  ETSI Doc. No. - EG 202 325 V1.1.1 (2005-10)

- NGN R1 Functional Architecture; Organization of user data, NGN User data
  ETSI Doc. No. – TR 182 005 (Not Published, Target 03.30.2006)

- Work Item Reference DTR/TISPAN-02027-NGN-R1
  TISPAN WG2

2.3.2 3GPP

3GPP materials include T2/SMG1 and SA1. Additional work being done is as follows:

- Multiple Subscriber Profile (MSP) Phase 2; Service description; Stage 1
  Spec No. - 22.097
  WG - S1

- Technical Specification Group Core Network and Terminals; Organization of Subscriber Data
  Spec No. 23-008

This document includes definition of data for IP Multimedia domain in Section 3. Examples include private user identity, public user identity, registration data, and authentication data.

- Multiple Subscriber Profile (MSP) Phase 1; Stage 2
  Spec No. - 23.097

WG – C4

- 3GPP Generic User Profile (GUP) Requirements; Architecture (Stage 2)
  Spec No. – 23.240
  WG – S2

- 3GPP Generic User Profile (GUP); Stage 2; Data Description Method (DDM)
  Spec No. – 23.941
  WG – C4

- 3GPP Generic User Profile (GUP) Common objects; Stage 3
  Spec No. - 24.241
  WG – C4

- 3GPP Generic User Profile (GUP); Stage 3; Network
  Spec No. – 29.240
  WG – C4

2.3.3 ATIS

The following work is in progress in ATIS committees and should be reviewed for relevance and impact to the User Profile requirements. Based on the issue description, the work may impact the implementation of a user profile. Additional investigation is needed.

Packet Technology & Systems Committee (PTSC)

- Create a Generic Control and Signaling Plane Standard
  Subgroup: Security (SEC)
  Issue # S0004

- Create a standard defining the Network-to-Network Interface (NNI) for IP-IP Network Interconnection Supporting Multimedia Services
  Subgroup: Signaling, Architecture and Control (SAC)
  Issue # S0009

- NGN Architecture Technical Report
  Subgroup: SAC
  Issue #S0018

- IP Device (SIP UA) to Network Interface Standard
  Subgroup: SAC
  Issue #S0027

- US Standard For IP-IP Network Interconnection - Roadmap Standard
  Subgroup: SAC
  Issue #S0028

- End to End User Authentication and Signaling Security
  Subgroup: SEC
  Issue #S0033

Telecom Management & Operations Committee (TMOC)

- VoIP Accounting Management NE/Operations Support Systems (OSS) Interface – American National Standard (ANS)
  Subgroup: AIP-AccMgt
  Issue #57

- VoIP Accounting Management NE/OSS Interface - ITU-T
  Subgroup: AIP-AccMgt
  Issue #58

- IPTV Accounting Management
  Subgroup: AIP-AccMgt
  Issue #76

IPTV Interoperability Forum (IIF)

- IPTV Requirements and Roadmap
  Subgroup: ARCH-TF
  Issue: #10

2.3.4 *Open Mobile Alliance (OMA)*

- User Agent Profile Version 20-May-2003
  Doc. No. - OMA-UAProf-v2_0-20030520-C

- Enabler Release Definition for User Agent Profile Version 20- May-2003
  Doc. No. - OMA-ERELD-UAProf-v2-0-20030520-C

This document is useful for translating device properties to applications. It defines a framework of device hardware capabilities, device software capabilities, and access network capabilities.

2.3.5 *W3C*

- World Wide Web Consortium (W3C) Composite Capability/Preference Profiles (CC/PP): Structure and Vocabularies 1.0, W3C Recommendation 15, January 2004

2.4 *Identified Gaps*

The identified gaps for unified user profile are:

- Standardization of IP Multimedia Subsystem (IMS) user profile is focused on communication capabilities such as call hold, call forwarding, and call waiting.

The IMS user profile standards need to be expanded to account for web, content, or gaming services and preferences.

- There is a need for the development of user profiles for web, video, and mobile access.
- The need for resolution is required between Network, Consumer Premises Equipment (CPE), and Web models for user preferences.
- Preferences are static items. There is a need for the definition of Mechanisms for the dynamic creation of preferences based on user behavior.
- Mechanisms should be defined to distribute profile stores across providers and provide extensible meta-system definitions for management of the resulting logically unified (but physically distributed) profile. (See also Section 15 on User Control of Profile/Services over a multitude of access networks.)

2.5 Proposed Work Items

Work Item A: Primary: ATIS PTSC, IIF
Title: Define profile elements for IPTV

Business Need:

Video and audio content services such as broadcast TV, video on demand, pay per view, and music are being deployed. Users have preferences for the types of shows and music that they watch or listen to, parental controls, volume, subtitles, and other delivery attributes. These are user profile attributes that should be stored in the HSS.

Recommended Approach:

The PTSC should, in close cooperation with the IIF, understand the impact of this work within the context of PTSC Issue S0027 IP Device (SIP UA) to Network Interface Standard and/or determine the possible need for a new standard.

Target Date: 1Q2007

Work Item B: Primary: PTSC, Secondary: IIF
Title: Web & NGN profile integration

Business Need:

The web and NGN are proceeding down separate competing paths for the storage and access of profile information. This results in conflicts for a service provider attempting to provide blended services. The web session and applications running within the Java Virtual Machine (JVM) should be equivalent to other communication or content sessions within the NGN. Reconciliation is required between the two approaches to facilitate blended applications and eliminate the need for proprietary integration between the two infrastructures.

Recommended Approach:

The PTSC should understand how the external standards work is proceeding with regards to Web and NGN profiles. The PTSC should propose a United States (US) position with regards to Web and NGN profile integration and generate a US standard to capture this position. This standard should be promoted as a global solution. This converged profile solution should allow for dynamic profiles. The PTSC position should include a recommendation on how to ensure the coordination of user profile information and structure to resolve conflicting data.

Target Date: 4Q2007

Work Item C: Primary: IIF
Title: Dynamic Profile

Business Need:

Web providers are moving away from static profiles and are using data mining or search techniques to dynamically determine profile attributes based on past user behavior. As long as the privacy concerns are addressed, this mechanism is valuable because it does not rely on user input of the profile attribute. The IPTV system, for example, can suggest content based on the movies that have been previously selected without requiring the user to define those preferences. This passive collection eliminates a barrier to usage of the new service and improves the user experience.

Recommended Approach:

The IIF should develop a requirements document that defines the incremental capabilities required by IPTV to collect passive data that may be used to update a converged Web/NGN profile database.

Target Date: 4Q2007

Work Item D: Primary: PTSC
Title: Profile NNI

Business Need:

An end-user's profile may be distributed between multiple providers' network profiles. Each provider may know the end-user by separate public and private entities. This profile information is often relevant to applications associated with all of the end-users' public entities.

There currently is no method of logically representing these disparate profiles in the context of a single providers' profile interface such that the profile appears associated with that providers' user identifiers and associated credentials (e.g., private identity).

Recommended Approach:

A global standard NNI interface that defines the transfer and update of user profile information between providers. This interface needs to perform the mapping between public and private identities and their associated credentials.

Target Date: 4Q2007

3 SECURITY

3.1 Context

3.1.1 Security Architecture & Framework Overview

The NGN should provide the same level of, or better, security as the current PSTN. To be successful, effective security policies must be developed and implemented in a systematic, consistent, and rigorous manner for these services and networks. Developing effective security policies is best achieved by using a comprehensive security architecture. Two such security architecture documents used as foundations are the ITU-T X.800 and ITU-T X.805 Recommendations. Both X.800 and X.805 allow for a structured approach to developing security policies and determining what security mechanisms need to be deployed. The use of these (or another) security architecture is essential when examining gaps in security standards that can be barriers to implementing security policies needed for Next Generation Networks (NGN). These policies must take into account the risks and benefits of deploying specific security technologies by systematically evaluating a service in light of each of the five major "Security Services" identified within X.800 (Authentication, Access Control, Confidentiality, Integrity, and Non-repudiation) delineated in Figure 2 below. Figure 1 below depicts a simplified view of these services from the X.805 perspective of 'security dimensions'.

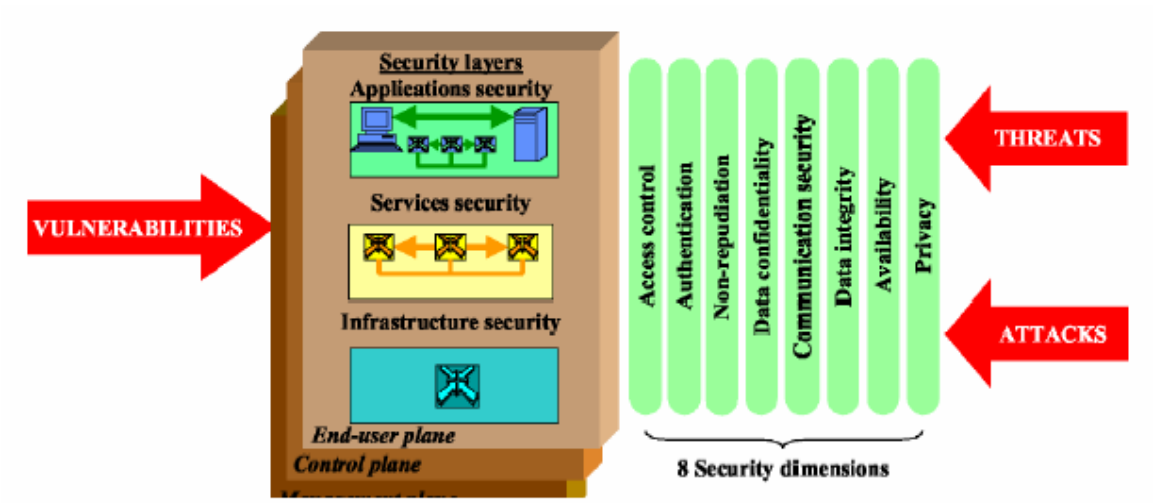

Figure 1: X.805 perspective on security

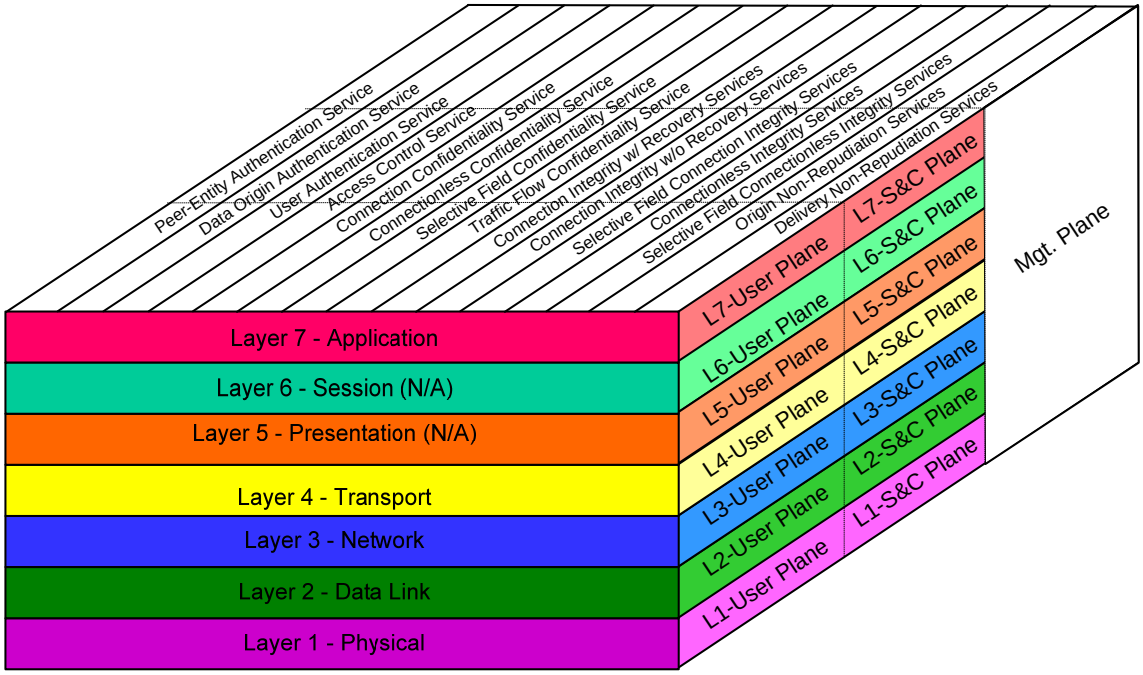

Figure 2: Security Services vs. Functional Planes and Protocol Layers

As shown in the above figure, each of the five X.800 security services decompose into the following:

1) Authentication
   - 1a) Peer entity authentication
   - 1b) Data origin authentication
2) Access control
3) Data confidentiality
   - 3a) Connection confidentiality
   - 3b) Connectionless confidentiality
   - 3c) Selective field confidentiality
   - 3d) Traffic flow confidentiality
4) Data integrity
   - 4a) Connection integrity with recovery
   - 4b) Connection integrity without recovery
   - 4c) Selective field connection integrity
   - 4d) Connectionless integrity
   - 4e) Selective field connectionless integrity
5) Non-repudiation
   - 5a) Non-repudiation with proof of origin
   - 5b) Non-repudiation with proof of delivery

Both X.800 and X.805 distinguish between User Plane (a.k.a. Media) traffic and Signaling and Control traffic within each protocol layer. Furthermore, X.800 specifies that Security

Services, as well as X.805 security dimensions, apply to each functional plane within each protocol layer independently of what occurs in other protocol layers. Moreover, the requirements and specifications being developed within ATIS Technical Committees and adopted specifications by ITU-T and IETF need to be reviewed for adoption within the NGN security framework for both internal and inter-carrier functions.

Each Security Service may be instantiated through the use of one or more security mechanisms. X800 identifies the following specific security mechanisms that may be incorporated into the appropriate functional plane of each protocol layer in order to provide the aforementioned security services.

- Encipherment
- Digital signature mechanisms
- Access control mechanisms
- Data integrity mechanisms
- Authentication exchange mechanism
- Traffic padding mechanism
- Routing control mechanism
- Notarization mechanism

There are a number of mechanisms which are not specific to any particular service, thus they are not explicitly described as being in any particular protocol layer. Some of these pervasive security mechanisms can be regarded as aspects of security management. The importance of these mechanisms is, in general, directly related to the level of security required.

- Trusted functionality
- Security labels
- Event detection
- Security audit trail
- Security recovery

X.805 does not reach the same level of detail as X.800, nor does X.805 identify explicit security mechanisms necessary to instantiate the X.805 security dimensions.

3.1.1.1 Security mechanism mapping to services and protocol layers

Not all security services pertain to the user (media) plane or the signaling and control plane within each protocol payer. For example commercial networks generally:

- do not require authentication, access control or non-repudiation services at layer one (1)
- require confidentiality and integrity services at layer one (1)
- do not require any non-repudiation services at layer two (2)
- require authentication, access control, confidentiality and integrity services at layer two (2)

- do not require any non-repudiation services at layer three (3) or confidentiality services for signaling & control
- require authentication, access control, confidentiality and integrity services at layer three (3)
- do not require any non-repudiation services at layer four (4)
- require authentication, access control, confidentiality and integrity services at layer four (4)
- require all security services at layers five through seven (5-7) be provided.

The following table delineates what security services and specific security mechanisms are needed within each protocol layer by either user (media) or by the signaling & control functional plane within that protocol layer.

Table 1: Security Services and specific security mechanisms by protocol layer and functional plane

	Layer 1 - Physical								Layer 2 - Data Link								Layer 3 - Networking								Layer 4 - Transport								Layer 5/6/7 - Application							
	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
User (Media) Plane																																								
Authentication																																								
Peer entity authentication	.	.	.	.	.	.	.	.	Y	Y	.	.	Y	.	.	.	Y	Y	.	.	Y	.	.	.	Y	Y	.	.	Y	.	.	.	Y	Y	.	.	Y	.	.	.
Data origin authentication	.	.	.	.	.	.	.	.	Y	Y							Y	Y	.	.	.	.	.	.	Y	Y	.	.	.	.	.	.	Y	Y	.	.	.	.	.	.
Access control	.	.	.	.	.	.	.		.		Y	.	.	.			.		Y	.	.	.			.		Y	.	.	.			.		Y	.	.	.		
Data confidentiality																																								
Connection confidentiality	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.
Connectionless confidentiality	.	.	.	.	.	.	.	.	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.
Selective field confidentiality	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	.	.	.	.	.	.
Traffic flow confidentiality	Y	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	.	.	.	Y	Y	.
Data integrity																																								
Connection integrity with recovery	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.
Connection integrity without recovery	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.
Selective field connection integrity	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	.	Y	.	.	.	.
Connectionless integrily	Y	Y	.	Y	.	.	.	.	Y	Y	.	Y	.	.	.	.	Y	Y	.	Y	.	.	.	.	Y	Y	.	Y	.	.	.	.	Y	Y	.	Y	.	.	.	.
Selective field connectionless integrity	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	Y	.	Y	.	.	.	.
Non-repudiation																																								
Non-repudiation with proof of origin	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	Y	.	.	.	Y
Non-repudiation with proof of delivery	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	Y	.	.	.	Y
Signaling & Control Plane																																								
Authentication																																								
Peer entity authentication	.	.	.	.	.	.	.	.	Y	Y	.	.	Y	.	.	.	Y	Y	.	.	Y	.	.	.	Y	Y	.	.	Y	.	.	.	Y	Y	.	.	Y	.	.	.
Data origin authentication	.	.	.	.	.	.	.	.	Y	Y	.	.	.	.	.	.	Y	Y	.	.	.	.	.	.	Y	Y	.	.	.	.	.	.	Y	Y	.	.	.	.	.	.
Access control	.	.	.	.	.	.	.		.		Y	.	.	.			.		Y	.	.	.			.		Y	.	.	.			.		Y	.	.	.		
Data confidentiality																																								
Connection confidentiality	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.	.	.	.	.	.	.	.	.	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.
Connectionless confidentiality	.	.	.	.	.	.	.	.	Y	.	.	.	.	.	Y	.	.	.	.	.	.	.	.	.	Y	.	.	.	.	.	Y	.	Y	.	.	.	.	.	Y	.
Selective field confidentiality	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	.	.	.	.	.	.
Traffic flow confidentiality	Y	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	.	.	.	Y	Y	.
Data integrity																																								
Connection integrity with recovery	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.
Connection integrity without recovery	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.	Y	.	.	Y	.	.	.	.
Selective field connection integrity	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	.	.	Y	.	.	.	.
Connectionless integrily	Y	Y	.	Y	.	.	.	.	Y	Y	.	Y	.	.	.	.	Y	Y	.	Y	.	.	.	.	Y	Y	.	Y	.	.	.	.	Y	Y	.	Y	.	.	.	.
Selective field connectionless integrity	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y	Y	.	Y	.	.	.	.
Non-repudiation																																								

3.2 Current Standardization Activities

3.2.1 Activities by Organization

3.2.1.1 3GPP

3GPP Security mechanisms are detailed in the following specifications:

- ♦ TS 33.203, Access Security for IP based services.
- ♦ TS 33.210, Network Domain Security: IP network layer security.

Access security relies on the use of USIM Integrated Circuit Card (UICC) as the platform in which all IMS authentication keys and functions at the user side will be stored.

TS 33.203 sets specific requirements on the ISIM application to support IMS access security, so that the service is not provided until a security association is established between the UE and the network. The IMS AKA method is used for authentication as defined in TS 33.203.

For network domain security, 3GPP has specified security to be provided at the network layer using hop-by-hop security protocols as defined by TS 33.210. For intranetwork security, TS 33.210 specifies the use of security gateways between disparate networks and the use of IKE to negotiate and establish secure ESP tunnels between the gateways. Internetwork security is optional, but TS 33.210 recommends the use of IPsec with ESP and IKE.

The security services that have been identified in 3GPP as needed are: confidentiality, integrity, authentication, authorization, and anti-replay protection. These are ensured by standard 3GPP procedures, based on cryptographic techniques.

3.2.1.2 ETSI TISPAN

ETSI TISPAN is endorsing the security mechanisms specified by 3GPP for access and network security, and further enhancements are being studied to accommodate those requirements not currently considered by 3GPP. The already standardized security services and mechanisms in 3GPP will need to be reviewed in conjunction with the requirements and specifications being developed within ATIS and ETSI TISPAN, for adoption within the NGN security framework for both internal and inter-carrier functions.

3.2.1.3 ATIS-PTSC

A new security subcommittee has been formed and is working to develop signaling control plane security for the future (S0003 Security Roadmap). Five documents are underway and cover many aspect of security directly applicable to NGN. This is a very broad topic and has growing support. Of particular interest in this suite is the User to Network Interconnection standard, using IP, for multimedia services (see Issue S0007). This will be a critical element of NGN.

3.2.1.4 ATIS-TMOC

Significant work has been done to date on Management Plane Security both in ATIS/TMOC and TMOC's driving work in ITU-T SG4 (T1.276, T1.276 Supplement, and M.3016). TMOC is completing a new standard on security management systems (LB M035) titled "Draft Proposed American National Standard – Guidelines and Requirements for Security Management Systems" which, when approved, will be contributed to ITU-T for consideration as an ITU recommendation.

3.2.1.5 ATIS-PRQC

Within PRQC work was completed on:

PRQC-2005-185R1, Draft Technical Report "Security for Next Generation Networks – An End User Perspective".

3.2.1.6 ATIS-NIIF-NIOC

Within NIIF-NIOC work is under way on Issue #0258: National Security/Emergency Preparedness (NS/EP) calls may encounter difficulties when some portion of the call is served by VoIP technology.

3.2.1.7 ITU-T

ITU-T security related materials include: X.273, X.274, X.500, X.509, X.736, X.740, X.800, X.803, X.805, X.810 through X.816, X.1051 and M.3016.0 through M.3016.4.

Among them, X.1051 is presently under revision. In addition, a set of new Recommendations relevant to NGN security are under development, including:

- Password-authenticated Key Exchange Protocol (PAK)
- Security Requirements for NGN Release 1
- Guidelines for NGN Security Release 1
- Network security certification based on ITU-T Recommendation X.805
- Overview of cybersecurity
- Security for home networks
- Authentication architecture in mobile end-to-end data communications
- Guidelines on strong password authentication protocols
- Framework for authentication and key management for link layer security in NGN
- Security assertion markup language
- Extensible access control markup language
- Methods for countering spam by technical means
- The use of telebiometrics for securing networks
- Multimedia security in Next Generation Networks

3.2.1.8 IEEE

IEEE security related materials include: 802.1Q, 802.1X, 802.11 series, 802.15 series and 1363 series. A number of current projects include:

- P802.1AE, "Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security"
- 802.1af, "Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control - Amendment 1: Authenticated Key Agreement for Media Access Control (MAC) Security"
- 802.11i-2004, "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks- Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements"
- 802.11w, "Amendment to Standard [FOR] Information Technology-Telecommunications and Information Exchange between systems-Local and Metropolitan networks- Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Protected Management Frames"
- P802.15.4-REVb, "Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPAN) "
- P1363.1, "Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices"
- P1363.2, "Standard Specification for Password-Based Public-Key Cryptographic Techniques"
- P1700, "Standard for Information System Security Assurance Architecture (ISSAA)"
- P2200, "Standard for Baseline Operating Systems Security (TM) (BOSS TM)"

3.2.1.9 IETF

The IETF Security Area is responsible for developing security-specific RFCs. All RFCs are required to have a Security Considerations section to address security issues specific to that RFC. In addition, other IETF working groups can use mechanisms and RFCs developed by the Security Area in their work; for example, the SIP WG has developed an RFC utilizing SMIME to security SIP exchanges.

3.2.1.10 OIF

OIF security related materials include:

- OIF-SEP-01.0 - Security Extension for UNI and NNI
- OIF-SEP-02.0 - Addendum to the Security Extension for UNI and NNI
- OIF-SMI-01.0 - Security for Management Interfaces to Network Elements
- OIF-SMI-02.0 - Addendum to the Security for Management Interfaces to Network Elements

3.2.1.11 NIST

Within the US Government, the primary group working on non-military security for NGNs is the National Institute for Science and Technology (NIST). NIST has produced a

key component for securing NGN infrastructures in the form of the Common Criteria (CC), which is now captured in the ISO standards 15408-1 through -3. Another security effort within NIST is the Draft Special Publication 800-73-1, *Interfaces for Personal Identity Verification*. This NIST effort has resulted in the issuance of FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. NIST standards are not directly binding on commercial NGN design and deployment, but indirectly impact service providers within the USA, as these providers routinely supply communications services to the government and therefore need to consider government's unique requirements.

3.2.1.12 OASIS

The OASIS charter focuses on defining and maintaining a standard, XML-based framework for creating and exchanging security information. As such, OASIS has produced a number of security related documents, specifically:

- Application Vulnerability Description Language (AVDL) v1.0
- Common Alerting Protocol v1.0
- Common Alerting Protocol (CAP) v1.1
- Darwin Information Typing Architecture (DITA) v1.0
- Directory Services Markup Language (DSML) v2.0
- DocBook v4.1
- ebXML Collaborative Partner Profile Agreement (CPPA) v2
- ebXML Message Service Specification v2.0
- ebXML Registry Information Model (RIM) v2.0
- ebXML Registry Information Model (RIM) v3.0
- ebXML Registry Services Specification (RS) v2.0
- ebXML Registry Services Specification (RS) v3.0
- Extensible Access Control Markup Language (XACML) v1.0
- eXtensible Access Control Markup Language TC v2.0 (XACML)
- OpenDocument Format for Office Applications (OpenDocument) v1.0
- Security Assertion Markup Language (SAML) v1.0
- Security Assertion Markup Language (SAML) v1.1
- Security Assertion Markup Language (SAML) V2.0
- Service Provisioning Markup Lanaguage (SPML) v1.0
- Universal Description, Discovery and Integration (UDDI) v2.0
- Universal Description, Discovery and Integration (UDDI) v3.0.2
- Universal Business Language (UBL) v1.0
- Universal Business Language Naming & Design Rules v1.0 (UBL NDR)
- WS-Reliability (WS-R) v1.1
- Web Services for Remote Portlets (WSRP) v1.0
- Web Services Security v1.0 (WS-Security 2004)
- Web Services Security SAML Token Profile v 1.0 and REL Token Profile v1.0
- WSDM Management Using Web Services v1.0 (WSDM-MUWS)
- WSDM Management Using Web Services v1.0 (WSDM-MOWS)
- XML Catalogs v1.1

- XML Common Biometric Format (XCBF) v1.1

3.2.1.13 ISO

ISO-IEC security related materials include: 7498-2, 9798-2 through 9798-5, 10164-7, 10164-8, 10736, 10745, 10181-1 through 10181-7, 11577, and 15408-1 through 15408-3.

3.2.1.14 3GPP2

Security related materials include:

- S0014-B, "Interoperability Specification (IOS) for cdma2000 11 Access Network Interfaces — Part 4 (A1, A2, and A5 12 Interfaces)", 4/2004
- P0039, "Enhanced Subscriber Privacy for cdma2000 High Rate Packet Data", 2/2006
- P0067-0, "Generic Key Exchange Protocol for High Rate Packet Data Systems", 5/2005
- S.P0098-0, "Wireless LAN Security Framework", 10/2003
- S.P0103-0, "Network Firewall Configuration and Control Stage 1", 3/2004
- S.P0104-0, "HAT (Hybrid Access Terminal) Authentication System Requirements", 4/2004
- S.P0109, "Generic Bootstrapping Architecture (GBA) Framework", 12/2005
- S.P0110-0, "Location Services Security Framework", 2/2005
- S.P0112-0, "Generic Bootstrapping Architecture (GBA) Security System Requirements Document", 4/2005
- S.R0037-0, "IP Network Architecture Model for cdma2000 Spread Spectrum Systems", 10/2004
- S.P0114-0, "Security Mechanisms using GBA", 12/2005
- X.P0027-002, "Presence Security", Work in Progress

3.2.1.15 TIA

Security related documents published by the TIA include:

- TIA-1053, “Broadcast/Multicast Security Framework ", January 2005
- EIA-679, “National Renewable Security Standard (NRSS)", September 1998
- TIA-102.AAAB, “APCO Project 25 - Digital Land Mobile Radio, Security Services Overview ", August 2002)
- TIA-102.AAAB-A, “Project 25 - Digital Land Mobile Radio - Security Services Overview (R2005)", January 2005
- EIA-803, “Mobile Electronics Wiring Designations for Audio and Vehicle Security ", November 1999TIA/EIA-732-406, " Cellular Digital Packet Data System Specification - Part 406 Airlink Security", July 2001
- TIA/EIA-570-A-1, "Residential Telecommunications Cabling Standard Addendum 1 - Security Cabling for Residences ", March 2002
- TIA-102.AACA-1, "APCO Project 25 - Digital Radio Over-the-Air-Rekeying (OTAR) Protocol - Addendum 1 - Key Management Security Requirements for Type 3 Block Encryption Algorithms ", December 2002

- TSB-902.AAAA, "Wideband Data System Security Services - Overview Public Safety Wideband Data Standards Project ", May 2004
- TSB-102.AAAB, "Security Services Overview - New Technology Standards Project - Digital Radio Technical Standards ", January 1996)

The main working groups and engineering committees dealing with security are:

- WG-8.3 Encryption
- TR-30 Engineering Committee, Multi-Media Access, Related Protocols and Interfaces
- TIA TR-41 Engineering Committee, User Premises Telecommunications Requirements
- TR-45 Engineering Committee, Mobile, and Personal Communications Systems

3.2.2 Activities by Technology

3.2.2.1 Architecture, Frameworks and General Security

ISO-IEC materials include: 7498-2, 9798-2 through 9798-5, 10164-7, 10164-8, 10736, 10745, 10181-1 through 10181-7, 11577.

ITU-T materials include: X.273, X.274, X.736, X.740, X.800, X.803, X.805, X.810 through X.816.

ETSI materials include TISPAN 01020, TISPAN 07016, TS 187 001, DTS/TISPAN-07014-NGN-R1, TS 187 003, DTS/TISPAN-07015-NGN, TS, DTS/TISPAN-07017-NGN-R1.

3GPP materials include T2/SMG4.

3.2.2.2 Authentication, including Single Sign On (SSO)

ISO-IEC materials include: 7498-2, 9594-8, 9798-1, 10181-2.

ITU-T materials include: X.800, X.805, X.811.

ETSI SSO related materials include DTS/TISPAN-03016-NGN-R2, TS , TISPAN 07012, and TISPAN 07017. TISPAN Note: SSO is a broad concept. To some extent, TISPAN already addresses this in various forms. By using ISIM based authentication for SIP, sign on from any device and for any service can be provided (WI 07017). By using the Authentication proxy as specified in WI 03046, SSO can also be achieved for the http/xcap as well. The Liberty Alliance has defined a general framework for SSO, but this has not been addressed in TISPAN R1.

3GPP materials include Doc. Nb. TS 121 111 Ver. 6.2.0, Ref. RTS/TSGC-0621111v620 and (3GPP CT6 TS 21.111 version 6.2.0 Release 6).

3.2.2.3 Roaming (Mobility) Security
ETSI materials include TISPAN 02025, TR., DTR/TISPAN-01020-NGN, TR.

ECMA materials include ECMA tc31-tg17-2005-017.

3.2.2.4 Inter-provider (NNI) security (FW/Border Element, etc.)
ETSI materials include TISPAN 02021, TISPAN 03041, and TISPAN 03042 .

3.2.2.5 Risk Analysis
ETSI materials include TR 187 002 and DTR/TISPAN-07016-NGN-R1.

3.2.2.6 Device Authentication
3GPP materials include Doc. Nb. TS 121 111 Ver. 6.2.0, Ref. RTS/TSGC-0621111v620 and (3GPP CT6 TS 21.111 version 6.2.0 Release 6).

3.2.2.7 Security Management
ANSI materials include T1.276 and ATIS-0300074.

3.3 Assessment (Identified Gaps)

3.3.1 Security architectures
X.800 and X.805 have been selected by virtually all SDOs as the basis for their respective work on security. However, X.800 notes that security for non-communications functionality and capabilities is outside of the scope of X.800. On the other hand, X.805 says that it considers all infrastructure functionality, from end-to-end, is within scope, and yet fails to address the security needs of said non-communications functionality. There is a need for an overall information security architecture that is not fully met by any existing standards, since these are predominantly communications security-specific.

3.3.2 Security standards technical alignment
It is readily apparent that many different SDOs are involved with security issues within their areas of activity. Concern has been expressed that there may be a technical misalignment between ISO 7498-2 / ITU-T X.800 and ITU-T X.805 recommendations. Use of a consistent set of security standards is critical to ensure interoperability within a heterogeneous infrastructure.

3.3.3 Authentication
All service providers have existing authentication infrastructures that are not likely to be replaced in the near future. Therefore, the NGN should allow a variety of authentication techniques to be used against the single user profile, such as name and password, SIM card, smart card, token, etc. Thus the NGN may require an authentication broker and the IMS architecture may need to be expanded to support it.

3.4 Proposed Work Items

Work Item A: (Primary: PTSC/PRQC/TMOC)

Title: Establishment of an ATIS Security baseline

Business Need:

Continued use of different security architectures will interfere with integration of different SDO security related standards, frameworks, and guidelines resulting in delay in convergence on a common NGN infrastructure.

Recommended Approach:

- Assessment of the degree of technical misalignment between ISO 7498-2 / ITU-T X.800 and ITU-T X.805 recommendations.
- Recommendation on a unified ATIS approach to security based on this assessment.
- Provide contributions to other standards bodies (e.g., ITU-T) as appropriate.

Target Date: 4Q2006

Product: Resolution of any identified misalignment between security standards.

Work Item B: (Primary: PTSC, Secondary: TMOC)
Title: Definition of NGN alternative authentication mechanisms

Business Need:

As service providers migrate to an NGN infrastructure, NGN authentication mechanisms need to accommodate an evolutionary approach for this migration. If transition to an NGN requires wholesale replacement of existing deployed authentication then NGN adoption will be delayed as service providers refuse to write-off in-use authentication assets.

Recommended Approach:

Determine if the scope of Issue S0033 is intended to address the identified business need. If not, an appropriate issue statement should be generated.

Target Date: Assessment by 2Q2006; Standard by 2Q2007.

Product: An appropriate standard.

Work Item C: Primary: PTSC, or possibly a new committee, Secondary: TMOC, PTSC
Title: Definition of a comprehensive service provider security architecture

Business Need:

The existing national and international standards regarding security only directly address communications security; information systems security is only touched on in passing. As a result, very little consistent work has been done within individual SDOs that address all security needs within a service provider infrastructure resulting in:

- Communications security is a subset of information security, and this can lead to contradictory results.
- Inability to systematically determine gaps in a TSP infrastructure security posture resulting in exploitable vulnerabilities.

Recommended Approach:

Identify those aspects of information security that still need to be addressed (such as discretionary vs. mandatory access controls, infrastructure and services policy management and enforcement). This effort should build on ITU-T and ISO standards for communications security rather that repeat that work. Areas in need of development and standardization are concerned with information security.

Target Date: Assessment by 2Q2006; Standard by 2Q2007.

Product: An appropriate standard.

4 SERVICE DECOUPLING

4.1 Requirements

Services in the NGN should be defined in a way that is independent of specific access technologies. Provisioning a service on a specific technology will still be possible, but the remainder of this section deals with the case where services are not tied to a specific access.

Service decoupling applies in particular where services have specific performance requirements. There are three access-independent mechanisms that support this requirement:

- services request specific performance and access allows/refuses (e.g., CAC)
- access networks limit what can be provided, and services adapt or fail
- services declare what they need, and the access adapts.

Access Independence: It must be possible for services to be defined and delivered independent of a specific access technology. This does not imply that all services will work completely with all access technologies.

4.1.1 Access Criteria for NGN Conformance

As previously noted in the NGN Framework document, Section 2.1.6, one of the key objectives of the NGN is having services independent of access. It will achieve this by defining technology independent requirements for NGN access. Key requirements are that the access technologies:

- shall provide IP transport.

- shall support the provision of Quality of Service (QoS) consistent with the end-to-end objectives of ITU-T Recommendation Y.1541.
- shall be domain specific if encryption is provided at the transport level, rather than end-to-end.
- may provide a mechanism to permit or deny a session, based on the user and the service.

4.1.2 Service Definition Environment

It is important that the technology for developing services should be network and application protocol independent.

An important capability to achieve this is for service capabilities to be accessible by applications and end users through Application Protocol Interfaces (APIs). Applications could be under direct management of the NGN provider or could be provided by third parties. APIs capture service capability features. For example, OSA/Parlay X specifies web services APIs for Third Party Call, Network-Initiated Third Party Call, Short Message Service (SMS), Multimedia Message, Payment, Account Management, User Status, and Terminal Location services.

The Parlay/OSA model should be given consideration as an appropriate model for the interface that is presented to the outside world. In particular, 3GPP OSA Release 6 has defined several service interfaces based on Parlay X Web Services. The Web Services 6 Framework adds a level of abstraction and flexibility to service creation. Parlay X Web Services can be published through a registry, making them available for discovery.

While SIP is the core signaling protocol in IMS, it should be as transparent as possible to application developers. SIP application servers will continue to play an important role in providing services. The development of APIs that abstract protocols generally lags behind the development of those protocols. This is especially true for a protocol that is as extensible as SIP. Nevertheless, the goal should be to bring new capabilities into a higher-level API such as Parlay/OSA.

In order to fulfill their role and depending on the services requested, service capability servers could access IMS components such as S-CSCF, HSS, PDF, and Media Resource Functions (MRF). Interactive Voice Response (IVR) systems, announcement systems, and media servers are examples of MRFs.

4.2 Function/Service Enabled

This enables services to be defined and delivered independent of a specific "vertical" network function. This also enables a flexible service environment, including third party services. Although the use of open APIs is not, strictly speaking, necessary for this, it will dramatically improve the level of technology independence.

4.3 Identified Gaps

A key component of decoupling is a vertical signaling interface to allow services to communicate their requirements to the transport layer. This is sometimes known as the Resource and Admission Control Function (RACF). ETSI-TISPAN, ITU-T, and ATIS all include a function that performs essentially this role. However, there are some important differences. ETSI-TISPAN and ITU-T identify this as a discrete subsystem, 3GPP uses functions in the radio access, and ATIS is currently considering a range of options, including the option of aspects of it being included in the Session Border Control (SBC) function. The differences may be partially a function of terminology, but the different mechanisms for resource control need to be rationalized. Abstract (i.e., non-SIP) network interfaces should be considered for HSS, PDF, and MRF NGN components. Abstract interfaces should also be considered for x-CSCF NGN components.

4.4 Proposed Work Items

There are no work items proposed specific to this section. The aforementioned gaps are being addressed in Section 8 (Resource and Admission Control) of this document.

5 PRESENCE

5.1 Requirements

Some NGN services require an indication of presence or connectivity – for example, extensions of Instant Messaging (IM) services. *Presence* is a set of attributes characterizing the current properties (e.g., status, location, etc.) of an entity. An *entity* in this respect is any device, service and application that is capable of providing presence information. *Availability*, on the other hand, denotes the ability and willingness of an entity to communicate based on various properties and policies associated with that entity (e.g., time of day, device capabilities). The terms presence and availability are almost always used together to provide a complete set of presence information. However, presence is not usually a service that is offered as a stand-alone service, but rather in conjunction with other services. Presence is often referred to as an "enabler" in that it enables other services and applications to exist by providing presence information to that service or application.

The next section provides a short overview of standards activities for presence. The following section discusses presence in the context of SIP/SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) protocol. This discussion assumes the use of the SIP Event Package with SIP SUBSCRIBE and SIP NOTIFY methods and the Event State Publication Extension for SIP with SIP PUBLISH method. The NGN should focus on Presence in the SIP/SIMPLE networks as SIP is the prevailing VoIP protocol in the NGN (3GPP2 IMS and the IETF SIMPLE).

5.2 Function/Service Enabled

Presence information can be used by a variety of other applications. For example, a "find me follow me" application could use presence to remove an unregistered cell phone from the called devices.

5.3 Current Standards Activities

This section provides short description for:

1. Presence protocols (SIMPLE. XMPP)
2. Reference architectures using presence (IMS, OMA/IMPS) and
3. An API set for presence within OSA/Parlay framework.

5.3.1 IETF

IETF SIMPLE

SIMPLE is a working group within the IETF dedicated to producing interoperable standards for services compatible with the SIP and Common Presence and Instant Messaging (CPIM). While SIP is proposed by the IETF group for real time VoIP activities, SIMPLE identifies SIP-based mechanisms to be used for communicating presence information (SIP PUBLISH, SIP SUBSCRIBE, SIP NOTIFY) and for instant messaging (SIP MESSAGE).

While SIP defines ways for initiating and ending sessions between users, SIMPLE allows notifying users of other users' presence status changes in a SIP-based network.

SIMPLE is the proposed protocol in the IMS and OMA frameworks. The value of SIMPLE is that it leverages existing SIP infrastructure to introduce presence features.

IETF XMPP

XMPP (Extensible Messaging and Presence Protocol) uses an XML-based protocol for instant messaging, and presence. The XMPP standard is arguably the most commonly used presence protocol today. There are XMPP gateways (e.g., Jabber) between almost all IM systems/protocols. This protocol is important as it allows aggregation of buddies/presence from disparate and proprietary IM systems such as AOL, MSN, Yahoo! etc. XMPP was accepted as an IETF standard in January, 2004.

5.3.2 3GPP/3GPP2 IMS

3GPP and 3GPP2 have both created standards based upon SIMPLE for Presence Services (3GPP Release 6, 3GPP2 MMD Release A). IETF and IMS (3GPP/3GPP2) Presence architectures are similar. However, the IMS presence ref. architecture shows more functional entities as presence information suppliers (external and network agents in addition to the user agent). Presence in this environment may be based on a number of pieces of information; for example, mobile device status (Idle, Busy) and location

(Serving VLR, Cell Identity, etc.). It may also take into consideration the capabilities of the mobile device (e.g., SMS, WAP).

IMS architecture brings a broader view of presence suppliers and consumers. The 3GPP2 specification defines three general types of presence suppliers:

1. **Presence External Agents (PEA) –** these entities provide presence information from elements or applications typically outside of the provider's network.
2. **Presence User Agents (PUA) –** these entities provide presence information from or about a user. Users may be using a diverse set of devices or applications, each of which is represented by a device/application-based PUA or network-based PUA.
3. **Presence Network Agents (PNA) –** these entities provide presence information from network elements.

5.3.3 OMA and IMPS

OMA is currently focused on the IETF SIMPLE-based presence, Group List Management (GLMS), and Instant Messaging. The presence work takes place in the OMA Presence and Availability Group (PAG). Earlier releases of the OMA Presence specifications include Wireless Village (WV), and Instant Messaging and Presence Services (IMPS) as a supported auxiliary technology.

The OMA SIMPLE presence model heavily utilizes the 3GPP and 3GPP2 models.

5.3.4 Parlay Group's PAM specification

Parlay Group's PAM (Presence and Availability Management) Working Group - under OSA/Parlay organization - continues the work started at *PAM Forum.* Lucent, Bell Labs and Novell formed the *PAM Forum* consortium in 2000 with the objective of establishing and promoting PAM Forum specification as an industry standard enabling advanced communications and messaging services seamlessly across various telephony and IP networks. The OSA Presence & Availability Management SCF (Service Control Function) defines its own terminology and model for presence. OSA/Parlay PAM Presence API is based on multiple specifications such as JAIN, Parlay X, and CORBA. SIP may also be used as a transport protocol.

5.3.5 Presence Functional Architecture

For a user, presence services involve publishing that user's presence information, identifying interest in other users' presence data and receiving the updates when those users' presence data change.

Sources or suppliers of presence data are typically called **Presence User Agents** (PUA)[1]. For example, a PUA may represent an IM PC client or a cell phone. PUA's publish presence information coming from different sources to a **Presentity**, which is an aggregation of the presence for an entity such as a user. The Presentity is often referred

[1] In IMS, the PUA notion extends also to a PNA and a PEA.

to as a Presence Agent (PA). The PA can be collocated with the user's client or with the presence server.

Watchers, or Presence Consumers, represent interest by other entities in a particular Presentity. That is, Presentity informs Watchers of changes in presence data. Such Watchers, using notification mechanism, are called *subscribers.* Another type of Watcher is a *fetcher*. A *fetcher* simply requests the current value of a Presentity's presence information. A special kind of fetcher, a *poller,* is one that fetches information on a regular basis.

To manage the complexity of communications, presence services are usually defined in terms of a **Presence Server**, which collects aggregates and distributes presence information as it is added or modified in the network. The Presence Server may store presence information via Presence Information Data Format (PIDF), and manage subscriptions to presence services.

A presence protocol defines the interaction between the Presence Server, Presentities and Watchers. It carries the presence information. Both the Extensible Messaging and Presence Protocol (XMPP) and SIP are the leading presence protocols: XMPP primarily for more of the public Internet-based applications, and increasingly SIP, and its corresponding extensions for the telecommunications industry.

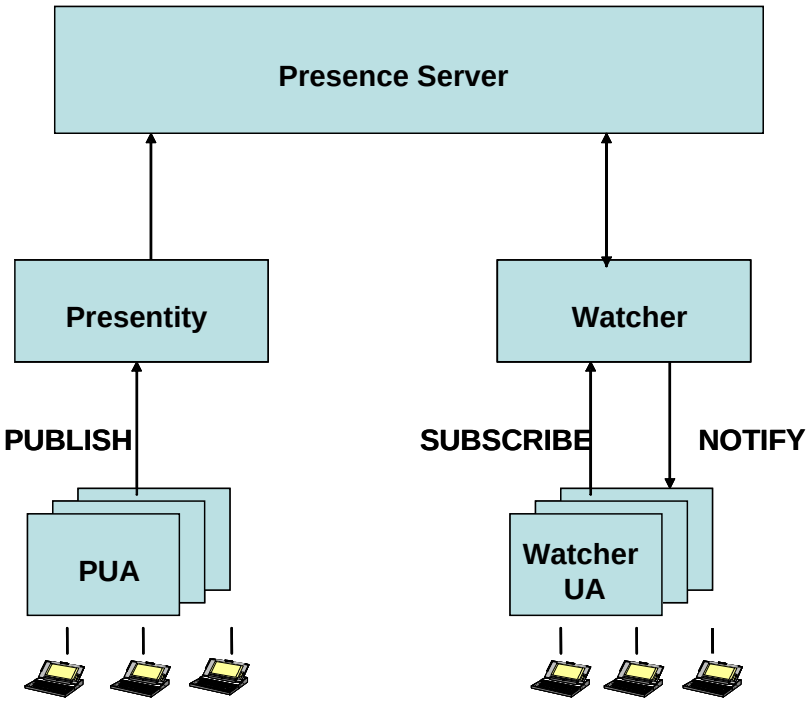

Figure 3: Presence Service Architecture

5.3.5.1 Presence Publication

A Presence User Agent (PUA) is responsible for getting events from the external environment and informing the Presence System of the change. There are essentially

two types of PUA: one collocated with the event source and another that is network-based. The PUA generates a SIP PUBLISH message and sends it to the corresponding Presentity. The presence update information or PIDF is contained in the SIP PUBLISH. The Presentity is responsible for accepting presence updates from PUAs, composing the aggregate presence state for the entity into a normalized PIDF, and then informing all relevant Watchers.

5.3.5.2 Presence Subscription and Notification

Watchers represent interest in changes to a particular Presentity's state. A Watcher may exist on a user's device or as a distinct application. Watcher-subscriber uses a SIP SUBSCRIBE message to request updates of the (future) changes in a Presentity's presence information (full or partial PIDF). Subscriptions are subject to authentication and authorization policies. When presence information changes, the Presentity sends a SIP NOTIFY request with current PIDF.

5.3.5.3 Presence Data Model

The model is based on the XML schema namespace representing the PIDF. The model has evolved through several stages and is described in many IETF RFC documents. It describes Presentity consisting of four components: Presentity URI, the person (or entity), the service, and the device (Figure 4).

The PIDF contains dynamic and transient information about the services and devices the user or person is using. In other words, this is dynamic session or context information. From the transport viewpoint, the PIDF is basically a payload, which can be carried, for example, within SIP requests.

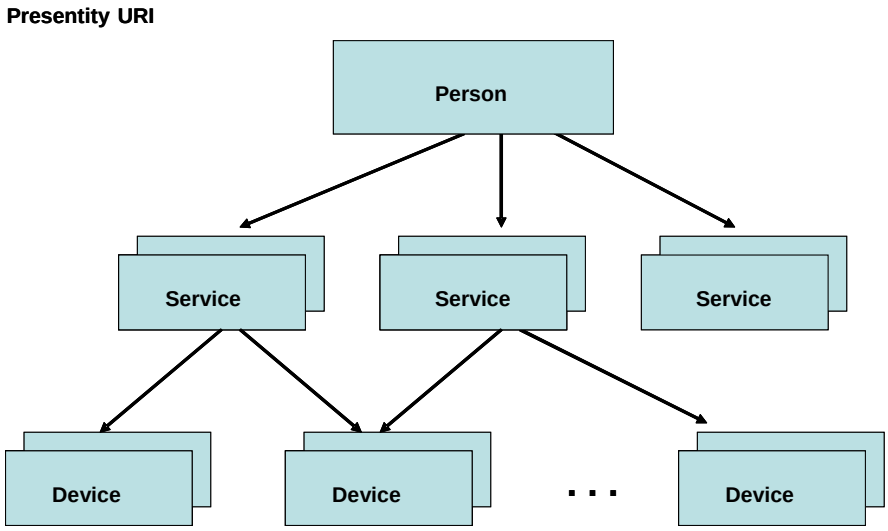

Figure 4 : Presence Data Model

5.3.5.4 Presence Extensions

Presence extensions allow us to include in the presence information document detailed and rich information about a Presentity. For example, the extended presence information may include:

- *Where am I?:* Location (LBS).
- *What context am I in?:* Home, restaurant, professional.
- *Who do I know?:* Address book, buddy lists, buddies' location, favorite links.
- *Which access means/devices do I use?:* PC, cellular phone, PDA.
- *Which access rights do I have?:* Parental controls (credit limits, content restrictions).
- *How do I pay?:* E-payment, wallet, split billing, creative pre/post paid.
- *Which identifiers (e.g., numbers, SIP addresses, etc.) do I have?:* Fixed, mobile, SIP-Url, IM-ID.
- *How do I want to appear?:* Ring-tones, ring-back tones, logos, avatars.
- *How to I want to manage elements in the future?* (Such as "My voice-print" for speaker recognition).
- *What is my willingness to accept various types of communication?*

These extensions take different forms and are introduced in different (draft) IETF specifications.

The Rich Presence Information Data Format (RPID) is an extension to the PIDF. As an example, the RPID may describe detailed *activities* of the Presentity: being in the meeting, traveling, in transit, on the phone. The *place-type* attribute may specify: home, work, hotel, public transport, etc. The *privacy* attribute may point to the level of availability.

The Contact Information in Presence Information Data Format (CIPID) may provide references to a Presentity's vCard, home web page and a photograph.

Timed extensions to the PIDF allow for a good integration with calendaring software and may render a timeline of what Presentity was doing in the near past and in the immediate future.

Presence capabilities extension allows watchers to know a Presentity's supported features such as type of device, media supported (text, voice, video) and similar.

Geographical location information is another extension. The PIDF gets extended to allow the encapsulation of pre-existing location information formats within a presence document.

5.3.5.5 Presence Composition and Processing

Presence servers manage presence data for a given Presentity or a user. It composes all presence documents–from diverse set of user's devices – into one PIDF using composition policy and privacy filtering. The general outline for composition policies has been specified by IETF although the standard is yet to be formulated. For filtering,

Presentity-side and watcher-side filters can be applied. For Presentity, the process allows maintaining user's privacy and also applying adaptive availability concept to watchers – i.e., a Presentity's status can be rendered differently to different watchers. Watcher-specified filtering rules ensure that a watcher gets only this part of PIDF it is interested in.

5.3.5.6 Cross-domain Presence Infrastructure and Services

In an end-user centric world, it is the end-user who decides which access means or which device to use. This end-user decision will be based on a trade-off between access means and devices depending on his personal preference or need of the moment:

- At home;
- On the pause (nomadicity);
- On the move (mobility); and
- In the enterprise.

The decision on which access will be based on the application, service availability, and price without the need to understand the technical attributes of one access mechanism versus another. However, this trade-off will implicitly be based on parameters such as required bandwidth, cost, mobility, QoS needs, ergonomic requirements, and the like. Given the very different nature of these parameters and the applications that heavily exploit one or many of these attributes, the current proliferation of devices (PC, blackphone, cellular phone, multimode/WiFi phone, PDA, TV) and access types (PSTN, fixed broadband access, cellular access, WiFi, WiMax) will continue to exist.

This implies that the end-users will value services that can be delivered over any access means and any device allowing them maximum freedom and control –- including the capability to apply the same personalization settings to any of these devices. A typical illustration is the recently introduced IM on mobile phones, which has long been available on PCs. The introduction of IM on mobiles has given people greater freedom to communicate in this form (i.e., being in touch with "buddies" the same as if they were sitting at their PC).

Another example of presence-bound service is Push to Talk or POC, which may provide the contact availability information to the potential caller. Some other presence services examples are: presence-based dynamic call routing, presence-based rendezvous or callback services, presence and buddy list based call screening, presence-enabled address book or phone book, and presence and location integrated services.

Moving towards an end-user centric vision opens the door to many new service opportunities that will cross the traditional boundaries of fixed, mobile, broadband, Internet Service Provider (ISP), and portal businesses. It is anticipated that the migration to these new services will be phased over time, in line with the capability build-up of service providers and the adoption of end-users.

5.4 Identified Gaps

Existing fragmentation in Presence standards necessitates acknowledgment of other non SIP-based presence environments and brings up the interoperability issues. Examples include XMPP-based networks and OSA/Parlay groupings.

Consequently, there is a need for the NGN to work out the requirements for the functional presence gateway entity to translate the presence information between these different environments. As an example, the 3GPP/3GPP2 IMS Presence Reference Architecture could be enhanced to provide such a solution by extending the functions of the Presence External Agent or other entities.

The NGN should investigate the issue of the dynamic and transient user data stored by presence. Just as the unified user profile contains the static user data, the presence contains dynamic user information. It may be beneficial for the NGN services to aggregate dynamic user data such as location information, and calendar information as presence information.

5.5 Proposed Work Items

None. IETF SIMPLE is currently addressing this area.

6 SERVICE TRANSPARENCY

6.1 Requirements

Service transparency of NGN carries two essential requirements:

- Maintaining end-to-end transparency of Internet.
- Maintaining transparency of service interworking with non-NGN networks.

Both should be done to the maximum extent possible.
End-to-end transparency ensures that end-user data applications from the existing best effort Internet continue to work on the NGN, in the same way they work today. However, it is recognized that there may be a conflict between end-to-end transparency and some NGN capabilities (e.g., NAT/Firewall for security). Even so, the NGN should strive to offer backwards compatibility to the existing best effort Internet. This may imply additional network functionality will be required in the NGN for this backward compatibility.

For service interworking transparency, the manner of access, transport, or switching (circuit-switched PSTN or packet-switched IP network) technology used inside the network, should not affect the user's terms of service (subject to inherent limitations of the access technology, such as maximum bandwidth). In addition, NGN services such as voice should be able to interwork fully with compatible PSTN services. The burden of

assuring such service transparency should be the concern of the NGN service providers and equipment vendors. It should not be turned into a dilemma for a user.

6.2 Function/Service Enabled

The service enabled by end-to-end transparency is the ability of the user to utilize any service reachable over the NGN independent of the access service provider, given that the service does not require any additional network performance or functionality.
If the end-to-end service requires extra functionality provided by the NGN (e.g., QoS, specific bandwidth), then a method must be in place for the service to request such functionality from the NGN.

End-to-end transparency might be constrained by the following:

- Access Bandwidth
- Network Address Translation
- IP Version used (IPv4 or IPv6)
- Security services offered by the NGN, such as:
    - Packet filtering
    - Anti-spoofing protection
    - Firewall protection

Moreover, NGNs will continue to support most, if not all, end-user applications from the existing non-NGN networks. In particular, this applies to data services such as web browsing, email, presence, messaging, IP multimedia service, file transfer, and games. Likewise, the NGN will support transparent voice services interworking with PSTN such as allowing voice call continuity between Circuit Switched (CS) and IMS. Lastly, the NGN must support IP Version Interworking (IPv4 vs. IPv6) and Application Level Interworking in SIP and mobility management.

6.3 Current Standardization Activities

6.3.1 End-to-end Transparency

The IETF has defined standards for routing packets end-to-end through the network in a connectionless manner.

The main standardization activity in the IETF in terms of end-to-end transparency is how to maintain such transparency considering the existence of functions in the middle of the network that break the natural end-to-end capability of the Internet. This work is being done in a number of working groups such as MMUSIC (ICE) and BEHAVE.

Also, there is effort in the IPv6 working group in recommendations for designing an IPv6 network to meet the perceived security and connectivity requirements implicit in

the current usage of IPv4 NATs, while maintaining the advantages of IPv6 end-to-end transparency as described in IPv6 Network Architecture Protection. [2]

6.3.2 Service Interworking Transparency

6.3.2.1 IP multimedia (IM) service

- 3GPP TS29.162: "Interworking between the IM CN subsystem and IP networks"

TS29.162 details the interworking between the IM CN subsystem and external IP networks for IM service support. It addresses the issues of control plane interworking, user plane interworking, and IP version interworking.

6.3.2.2 Presence service

- 3GPP TS 23.141: "Presence service; Architecture and functional description; Stage 2"

- 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3"

- 3GPP TS 33.141: "Presence service; Security"

TS23.141, 24.141, and 33.141 detail the realization of presence service in IMS by defining new functional elements, interface points, and security mechanisms.

6.3.2.3 Messaging service

- 3GPP TS 24.247: "Messaging using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3"

TS24.247 details the realization of session-based messaging service in IMS by defining new call flows and procedures.

6.3.2.4 Voice service interworking with PSTN/PLMN

- 3GPP TS 23.279: "Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services; Stage 2."

- 3GPP TS 23.806: "Voice Call Continuity (VCC) between Circuit Switched (CS) and IP Multimedia Subsystem (IMS) Study."

TS 23.279 provide architectural details to combine CS services and IMS services for using them in parallel between the same two users in a peer-to-peer context. The document provides a detailed description of how capabilities and identities are exchanged to enable the combination of CS and IMS services between the same two UEs.

---

[2] draft.ietf-v6ops-nap-02

TS 23.806 considers overall requirements, architectural requirements, and alternative architectures of the support of the active voice call continuity between Circuit Switched (CS) domain and the IMS. It also addresses voice call related functionality, including the need for Regulatory issues (e.g., Text Telephone - TTY as defined in TS 26.226), Emergency Call and support for supplementary services.

6.3.2.5 PSTN/ISDN Emulation and Simulation

There are two important standard activities in offering PSTN/Integrated Services Digital Network (ISDN) services transparently to users, referred to as *PSTN/ISDN Emulation and Simulation*. *PSTN/ISDN Emulation* provides PSTN/ISDN-like service capabilities using session control over IP interfaces and infrastructure. On the other hand, *PSTN/ISDN Simulation* provides PSTN/ISDN service capabilities and interfaces using adaptation to an IP infrastructure. PSTN/ISDN Simulation is considered as a specific implementation of IM services. The idea of PSTN/ISDN Emulation is to create a service in an NGN that is effectively identical to the PSTN, with the same feature set and user ergonomics. This means that, as far as the end user is concerned, nothing has changed. In contrast, PSTN Simulation provides something that looks generally like a PSTN or ISDN service, but doesn't resemble it in all respects. For example, it can use a variety of new terminal types, offer new value-added features, but also not offer some old ones. Simulation is more about allowing evolution into a new NGN environment than replicating the old environment exactly.

The ITU-T FGNGN has addressed emulation and simulation in:

- ITU-T FGNGN: "The PSTN/ISDN Emulation Architecture"; and
- ITU-T FGNGN: "PSTN/ISDN Emulation and Simulation."

6.4 Identified Gaps

6.4.1 End-to-end transparency

End-to-end transparency of best effort services is well defined on the Internet. However, gaps still exist on how to achieve end-to-end transparency with the presence of middle boxes such as NAT. These gaps are being worked in the IETF in MMUSIC (ICE) and BEHAVE (STUN, TURN, etc).

In the development of the NGN, new middle box functions may be defined that could interfere with end-to-end communications, thus creating a gap. Examples include:

- Signaling and control of Hosted NAT, Network Address Translation-Protocol Translators NATP(-PT) and/or Topology Hiding function in Border Gateway Functions (BGFs) by Application Function or in Session Border Controllers in a NGN for end-to-end transparency.
- Modification of P-CSCF (acting as Application Function) procedures to accommodate the above signaling and control.

6.4.2 Service Interworking Transparency

The gaps exist in the following areas:

- Service interworking transparency for IP multimedia services across NGN and non-NGN networks including those issues above network layer, such as unified user profile and service adaptation.
- Enhancement of IMS messaging systems to seamlessly interwork with existing messaging systems.
- Enhancement of IMS presence systems to seamlessly interwork with existing presence systems.
- Detailed flows of how VCC provides voice call continuity between 3GPP CS domain and 3GPP IP-Connectivity Access Network (IP-CAN) based on IMS.

6.5 Proposed Work Items

6.5.1 End-to-end Transparency

None. End-to-end transparency issues are being adequately addressed by IETF and ETSI TISPAN-NGN.

6.5.2 Service Interworking Transparency

The following PTSC Issues are intended to expand and resolve the identified gaps in NGN service interworking transparency. Thus no further work items are required at this time.

S0009 - Create a standard defining the NNI for IP-IP Network Interconnection Supporting Multimedia Services
S0020 - Supporting phased migration of existing services and CPE to an IP environment
S0024 - Session/Border Control Function Definition and Requirements
S0025 - NNI Numbering and Routing Capabilities and Procedures
S0028 - US Standard for IP-IP Network Interconnection - Roadmap Standard

7 QoS

7.1 Requirements

A key challenge in realizing the NGN will be to standardize, implement, and deploy a QoS solution that enables interworking IP-based networks to support services with assured quality levels, end-to-end, while simultaneously (and efficiently) sharing network resources with traditional "best effort" IP applications. An NGN QoS standards solution meeting this challenge will comprise three elements:

- *Specification* standards for defining the user QoS requirements (and associated traffic and priority attributes) for particular IP packet flows.

- *Signaling* standards for communicating the user requirements to the serving IP network and among independently-operated IP networks.
- *Resource management* standards for coordinating network resource allocation and traffic control mechanisms across networks to support the specified and signaled user requirements.

Standards in the first category are needed to specify the syntax and semantics of the *content* communicated from users to NGN providers, and among independent NGN providers, in establishing IP flows that meet user requirements. Standards in the second category are needed to define the *protocols* to be used in communicating such content across NGN UNIs and NNIs. Standards in the third category are needed to define individual network *responses* to the communicated content, insofar as such responses change or interpret the content in ways that must be coordinated among networks.[3] In the latter category, the goal of standardization is not to mandate the use of particular resource management or traffic control mechanisms within networks, but to ensure that the various mechanisms that may be used will interwork in a multi-provider environment.

The NGN should enable end-to-end QoS across different infrastructure technologies and multiple service providers to the extent possible based on the capabilities of those technologies and agreements between service providers – both Application Service Providers (ASPs) and Next-Gen Service Providers (NGSPs). An NGSP may provide service and connectivity to service providers that do not support QoS coordination. In these cases, the services requiring QOS may not be available end-to-end or may operate in a degraded manner.

The basic thrust is that QoS is multi-faceted, covering not just transmission quality, but also reliability, availability, and functions such as call set-up. Where QoS is provided end-to-end, it must operate across combinations of access and backbone networks, and also across paths that span multiple carriers and service providers. A feasible NGN QoS solution will, of necessity, evolve incrementally from current (non-QoS-enabled) networks.

The following sections define NGN requirements related to QoS specification, QoS signaling, and resource management respectively.

7.1.1 QoS Specification

ITU-T SG12's Recommendation G.1010 provides a model for categorizing multimedia QoS from the viewpoint of the end user (e.g., human listener, viewer, or terminal operator), and identifies broad QoS categories and performance limits based on user tolerance to information loss and delay. G.1010 and related SG12 Recommendations provide a basis for specifying NGN QoS objectives by defining the end user QoS requirements for key applications NGN will support. An essential point is that *these QoS*

[3] Such responses may be enabled by off-line Operational Support System (OSS) functions.

requirements are driven by the end user's perception – and not the underlying networks or technology platforms. Different networks and technology platforms affect end user applications in a variety of ways, but the user's requirements are network and technology independent.

With this user-oriented approach, and SG12's results in characterizing terminals, ITU-T SG13 has developed two Recommendations that specify QoS objectives and related traffic characteristics for IP-based networks. The first, Y.1541, specifies UNI-to-UNI performance objectives for IP-based networks and clusters them in six IP network QoS classes. A recent revision of Y.1541 defines two additional QoS classes that specify requirements for demanding applications such as IPTV. The second Recommendation, Y.1221, defines the key elements of a *traffic contract* that complements a QoS request by describing associated flow characteristics and limits. The two Recommendations together define the essential data that must be communicated from the originating user to the network or service provider, and among cooperating providers, in establishing assured-quality IP flows in an NGN. Y.1541 provides guidance on how its QoS classes can be used to support IP network applications, including VoIP, and identifies associated network resource sharing mechanisms. Some of the many available mechanisms are described briefly in 7.1.3.

The process of setting UNI-to-UNI performance objectives can be affected by performance degradation (e.g., delay) or performance protection (e.g., packet loss concealment) in customer equipment. Recommendation Y.1541 provides examples of such interactions (for VoIP, TCP file transfers, and IPTV with forward error correction/interleaving), and the Y.1541 QoS classes take typical customer equipment performance characteristics into account. However, further study may be needed as new services (e.g., IPTV) and new customer equipment types evolve.

Although Recommendation Y.1541 is directly applicable to NGN, it does not address all issues of importance to NGN QoS. In particular, it does not specify parameters or objectives for IP network session establishment and release ("call processing"). Such specifications will need to be developed after the signaling protocols for IP-based NGNs are defined. NGN service availability objectives will also need to be specified.

NGN QoS requirements to support a given level of QoS will often be documented in Service Level Agreements (SLAs). The Y.1541 QoS classes and Y.1221 traffic descriptors provide a common basis for such agreements. Although the QoS parameters of principal interest will depend on the service being offered, certain parameters (MTTF, MTTR, etc.) will be pertinent to all services. SLAs may be defined for both the "signaling and control plane" and for "transport plane" for services on the basis of end-to-end and per network segment (both intra- and inter-provider).

Standards will also be required to ensure comparability among perception-based QoS measurements. Algorithms have been standardized to predict customer quality assessments for given combinations of network equipment and defects in existing networks. An example is the E-model for voice. In the NGN context, a variety of other

services are to be offered, and indeed those services present much of the rationale for evolution beyond the PSTN to an NGN. Perceptual quality metrics equivalent to Mean Opinion Score (MOS) will be required for the following other NGN services:

- IPTV
- High Definition IPTV
- Web site browsing
- Multimedia conferencing
- IP radio (broadcast radio over IP)
- High definition (stereo) audio

Other services may also require such metrics as the services become better defined and more widely available. The quality prediction mechanisms for non-voice NGN services will be based largely on network performance metrics and codec options. While standard IP network performance metrics will probably be usable, the codec information may be more complex. For example, in the case of MPEG4 implementation options for decoding and error concealment can impact perceived quality in the presence of errors and loss.

The performance of the NGN infrastructure is expected to significantly affect the perceived performance of NGN applications. Performance metrics associated with individual NGN functions will also be required, particularly when they are invoked in response to human-triggered actions. Latencies associated with service selection or session establishment are examples of areas where such NGN performance metrics will be required. Performance metrics will also be required for new NGN service capabilities. Examples include presence and location, where there will be a need to specify parameters such as update times. This will also extend to web based services such as click-to-call. Where NGN related databases (e.g., user profiles) and functions (e.g., provisioning) are provided via Web Services, appropriate performance metrics for those Web Services may be required. For an IPTV service, the channel change time may be an important performance metric. Such service specific performance metrics may well be impacted by the performance of various network service enablers. These factors may affect the choice of QoS allocations and admission control mechanisms.

It will be important to be able to measure service quality actively for each NGN service. The definition of appropriate metrics and best practices for QoS measurement methodologies are required. The mechanisms to concatenate these metrics across multiple domains are also items for further study. Measurement frequency will depend on the SLA and other factors. IPTV QoS measurement may require time and frequency to be provided throughout the network, including the home network. The time and frequency synchronization specifications that apply to IPTV may be different from those identified in existing Recommendations (e.g., G.823/824, G.8261).

7.1.2 QoS Signaling

ITU-T Q-Series Supplement 51 specifies a comprehensive set of *technology independent* QoS signaling requirements for IP-based multi-service networks.[4] These requirements apply to signaling messages exchanged at two types of interfaces: the UNI and the NNI. They provide a basis for defining interoperable NGN QoS control architectures and protocols and a "common language" for NGN QoS and traffic control in situations where independent providers and different technologies interwork. It is emphasized that these requirements apply to fully developed NGN solutions, to which IP-based networks will evolve incrementally over time.

Because NGN will integrate packet- and circuit-switched technologies, the NGN QoS solutions will likely include both "path-coupled" and "path-decoupled" signaling approaches. In *path coupled* solutions, the signaling messages that control the network QoS mechanisms travel between end systems and their serving networks (and among networks) on the same path that carries the user data flow. In *path decoupled* solutions, the signaling messages that control the network QoS mechanisms may travel on paths distinct from the path that carries the user data flow. The QoS signaling requirements defined in Supplement 51 accommodate both approaches.

To be useful in NGN, the standardized QoS signaling protocols must meet the following general requirements:

1. enable independent IP network and service providers to communicate and apportion QoS requirements among NGN elements in different jurisdictions;
2. enable interworking among different networks and access technology platforms in support of end-to-end QoS delivery; and
3. be implementable in products that are reliable, scalable, robust (fault-tolerant), flexible, secure, and manageable.

The Supplement 51 requirements apply to standard signaling protocols for communicating QoS and related traffic information among two types of entities:

1. users and their terminal equipment (TE); and
2. network service providers/operators and their equipment, especially the equipment that implements interworking.

7.1.2.1 UNI QoS signaling requirements

Supplement 51 specifies that it must be possible for the serving network entity to derive the following service level parameters from a user's QoS request at the UNI:

1. QoS class from Y.1541
2. Peak rate in bytes/second
3. Peak bucket size in bytes

---

[4] ITU-T Q-Series Supplement 51, *Signalling Requirements for IP-QoS*, December 2004.

4. Sustainable rate in bytes/second
5. Sustainable bucket size in bytes
6. Maximum allowed packet size in bytes.

Additional guidance on how to specify these parameters for a given application is an area for further work.

The serving network entity should also be able to derive a specification of the reliability/priority with which the service is to be sustained.

The ITU-T Supplement notes that a TE may compose a QoS request on the user's behalf, possibly based on configurations set by the user or equipment installer. Many TEs will have the flexibility to match the user's request for application quality with network QoS classes by selecting parameters such as source codec type and packet size. Alternatively, a user may specify a general application type and quality level in requesting a well-defined service such as voice telephony, and the detailed QoS and traffic attributes may be derivable from this information. In some cases, the access network may perform additional optimization based on knowledge of other application or media parameters. For example, when the user/TE request is a voiceband channel (to support speech or a voiceband modem), the QoS request (or other associated message) should contain the preferred codec and packet size. Other optional parameters may be included to indicate, for example, the use of silence suppression, the need for network echo cancellation, and alternate codecs/packet sizes.

In responding to the user/TE initiating a QoS request, the network service provider must be able to communicate the following information:

1. An identification code for the request exchange, to be used in this response and all related messages that follow.
2. A simple acknowledgement and acceptance of the user/TE request.
3. The performance level expected, and optionally, the network's ability to achieve a performance level better than that specified in the request for one or more QoS parameters.
4. The ability to reject a request and, at the same time, to offer a modified service level that can be met. The response may modify the request and may include commitments to an alternate QoS class or a lower capacity.

Networks may wish to indicate a maximum time interval for which the response is valid.

The user/TE not originating the QoS request for a particular flow will also be involved in the NGN QoS signaling protocol exchange. Messages exchanged between a non-originating user/TE and its serving network provider will be similar in form to those exchanged at the originating user/TE interface. A non-originating user/TE may reject an offered session based on the offered QoS levels or other factors.

7.1.2.2 NNI QoS signaling requirements

In Supplement 51, the term NNI includes both QoS related interfaces between interworking network providers and interfaces between such providers and separate service providers that do not provide the network transmission facilities. NNI signaling is the principal way for providers to ensure multi-network compliance with QoS and associated traffic classes. The Supplement specifies that NNI QoS signaling must support determination of the QoS that can be offered to a requesting user/TE *by communicating both the network QoS class requested, and the extent to which each specified parameter is already consumed*. This requirement implies that each network knows the performance it can (or will) support from the entrance node to the exit node(s), and the most likely impact this choice will have on the ability of the session to meet the end-to-end QoS request. In processing a QoS request from another network, a receiving network must determine if the requested capacity and reliability are available from entrance to exit node(s). The attributes of an NNI QoS request include those listed for the UNI above, but also the interconnecting point(s) where user/TE traffic will leave the requesting network and enter its downstream peer.

In responding to an NNI QoS request, the receiving provider must be able to communicate a set of information elements equivalent to those identified above for the network response to a UNI request. At both interfaces, users and networks must be able to signal requests to release, and confirm the release of, allocated resources.

The Supplement also defines QoS signaling protocol performance and other requirements -- e.g., regarding symmetry of information transfer capability, contention resolution, error reporting, handling of unrecoverable failures, forward and backward compatibility, QoS resource modification, and emergency service.

7.1.3 Resource Management

A variety of network-based mechanisms are required to support different aspects of QoS for different services and infrastructure contexts. In IP (and other packet) networks, one of the major concerns for QoS is developing mechanisms to manage congestion. Admission control – the most fundamental mechanism for limiting network congestion – is discussed in detail in Section 8. Within networks, congestion can be managed by complementary techniques that operate on several timescales -- e.g., network engineering, traffic engineering, and packet scheduling. These techniques are discussed in Part I of the ATIS NGN Framework.[5] Network mechanisms will also be needed to re-route critical IP flows rapidly (e.g., <100 ms) when link or node failures occur. IP network mechanisms analogous to TDM automatic protection switching are becoming available. Protocols to support the use of reserve network capacity are of particular importance at network interfaces where they must operate across administrative boundaries. Consider load balancing as a generic mechanism to provide resiliency and increased capacity at a network interface. This can be applied at layer 1 (e.g., current

[5] IP QoS error control mechanisms are also addressed in *ATIS Next Generation Network (NGN) Framework Part I: NGN Definitions, Requirements, and Architecture; Issue 1.0*, November 2004.

work on "G.Bond" in the context of DSL), Layer 2 (e.g., 802.1ad), or Layer 3 (ECMP) as appropriate.

Several different resource management mechanisms are expected to be used in NGNs, and they will not necessarily need to be standardized. Within the IP core, where traffic of multiple classes from multiple customers is aggregated, an operator may rely on Best Effort services with appropriate network and traffic engineering support. Access networks are likely to rely on packet scheduling mechanisms to support QoS requirements. These mechanisms are not unique to IP protocols. NGN may incorporate IEEE 802.1p classification and scheduling mechanisms in devices that are not IP-aware. Other link specific scheduling mechanisms may be required for other lower layer technologies (e.g., IEEE 802.11e for WiFi and similar mechanisms for Bluetooth, HomeplugAV, etc.).

Packet classification and scheduling mechanisms cannot be assumed to be uniform across the domain of a single operator, let alone the multiple operators that may exist in the context of an NGN service. For example, an operator may choose to implement an expedited service with a priority scheduling mechanism at the edge of the network where latency is a concern, and with a WFQ scheduling mechanism in the core where cost allocation across multiple services may be a concern. For this reason, the packet classification and scheduling mechanisms are specified as policies (see 2.4.3 in the *ATIS Next Generation Network (NGN) Framework Part I* for more details concerning policies) rather than specific mechanisms, providing for some flexibility in terms of network implementation.

Many of the techniques for QoS in IP networks have been designed for operation within a single Autonomous System. Some service providers span multiple Autonomous Systems. The IP peering between service providers, however, is typically at an Autonomous System boundary. NGN resource management standards will likely focus on interworking among Autonomous Systems, and among different resource management mechanisms. Further study is required to assess the nature and scope of such standards. There appear to be two potential mechanisms to support QoS sensitive routing across an Autonomous System boundary: 1) QoS extensions to BGP; or 2) Application Layer Routing (e.g., using tunnels between Session Border Controllers).

Resource management across service provider (or administrative) domains will require appropriate "non-real-time" OSS-to-OSS ordering transaction support, controls, and security (e.g., non-repudiation) to provide for basic service ordering and to enable the appropriate "real-time" signaling interactions. Complementary and supporting OSS applications (e.g., accounting management, trouble administration, service level agreement management) will also be needed.

7.2 Function/Service Enabled

The basic function enabled is the ability to isolate QoS assured flows from other interfering traffic, both within a given service and across multiple services. It is worth

noting that QoS mechanisms cannot create capacity where it does not exist. Examples of the services enabled by QoS include VoIP, multimedia conferencing, IPTV, and network gaming.

7.3 Current Standardization Activities

The following sections summarize current standardization activities related to QoS specification, QoS signaling, and resource management respectively.

7.3.1 QoS Specification

Current standardization work is addressing two QoS specification problems: 1) QoS class mapping; and 2) performance apportionment or accumulation. The first problem is the need to relate the end-to-end QoS classes defined in Recommendation Y.1541 with the distinct QoS levels available in particular technologies that may support an end-to-end NGN IP flow. PRQC has made an effort to address one instance of this problem by defining a specific mapping between the Y.1541 QoS classes and an associated set of 3GPP UMTS QoS classes defined for wireless networks based on the 3GPP specifications in the "Quality of Service (QoS) concept and architecture," 3GPP Technical Specification 23-107 V5.10.0, September 2003.[6] Work begun in TISPAN WG 5 and now continued in ETSI STQ is standardizing that mapping in the "QoS Framework and Requirements," Draft ETSI DTS/TISPAN-05008-NGN v0.0.2. The PRQC recommends changes in the ITU-T and 3GPP specifications that would substantially improve this particular mapping, and SG12 has accomplished the recommended changes affecting Y.1541 by defining two new QoS classes (see 7.1.1). 3GPP has thus far been unwilling to contemplate any changes to the defined UMTS QoS classes.

Other instances of the mapping problem will undoubtedly arise. Differences among QoS specifications are evident in the case of access technologies (e.g., DSL, IPCablecom, Ethernet, Wi-Fi, Wi-Max). PRQC has recently begun to explore such differences and the associated mapping issues. Various QoS mapping approaches are being examined, and associated compatibility issues have been identified in PRQC contributions.[7] One important access technology whose QoS mapping implications PRQC has not been fully considered is DSL. Another is Ethernet.

The second standards problem identified above is the need to share a UNI-to-UNI impairment budget (e.g., for packet transfer delay) among the individual networks that collectively support the IP path. ITU-T's classical "static allocation" approach would be difficult to implement in an IP infrastructure because the number of networks in a UNI-to-UNI IP path may be quite variable. PRQC has worked with ITU-T and its FGNGN to

---

[6] "Mapping between ITU-T (Y.1541/Y.1221) and 3GPP (TS 23-107) QoS Classes and Traffic Descriptors," T1A1/2003-075, February 2004.

[7] "Summary of IP QoS signalling work in the IETF NSIS Working Group," PRQC-2005-066, April 2005 and "QoS provisions in IEEE 802.11-based wireless LANs," PRQC-2005-069, April 2005.

sort out the possibilities, but no specific approach has been agreed.[8] A new specification defining various alternatives and criteria was begun at the April 2005 meeting of ITU-T's FGNGN.[9] This work is being continued in SG12, since the FGNGN ended its work in November 2005. Prior PRQC contributions on this topic are provided in the "Proposal on performance management for multi-network QoS in the NGN," PRQC-2005-115, June 2005 and "Process for achieving network QoS objectives in a multi-provider environment with impairment accumulation," PRQC-2005-116, June 2005. A draft ITU-T Recommendation reflecting results of these contributions was begun in the FGNGN and is now being progressed in SG12.[10]

ATIS IIF and other groups -- e.g., the Digital Video Broadcasting (DVB) project – are investigating end-to-end error control techniques, including forward error correction, retransmission, and error concealment as they relate to UNI-to-UNI performance objectives for IPTV services. The IIF is also developing approaches for the measurement of IPTV service quality as perceived by the user (including the measurement of response times to user initiated service changes), and for IPTV time and frequency synchronization.

In a recent contribution, PRQC has identified two IP network QoS specification approaches that further enlarge the set of variables to be considered in NGN QoS specification: "non-parametric" QoS specification and application QoS classes.[11]

As noted earlier, NGN QoS specification fully considered includes other performance attributes such as call processing performance and service availability in addition to the performance of IP packet transfer. PRQC has begun a project to define SIP-based call processing performance parameters, and has contributed initial results to ITU-T SG12.[12]

7.3.2 QoS Signaling

QoS signaling is perhaps the most challenging and least fully defined NGN QoS solution element. Some very fundamental current work is aimed at standardizing an NGN QoS signaling architecture. Two relevant specifications are the TISPAN's Resource and Admission Control Subsystem (RACS) and the ITU-T FGNGN/SG13 Resource and Admission Control Functions (RACF). These specifications and related protocol standardization activities are described in 8.3.1.3. Both specifications address QoS signaling in the broader context of resource- and policy-based admission control, which includes border control (e.g., NAPT, NAT traversal, and gating) in addition to QoS

---

[8] "Impairment targets," PRQC-2005-052, April 2005.

[9] "Algorithms for achieving end-to-end performance objectives," FGNGN-OD-135, April 2005.

[10] "Framework for achieving end-to-end IP objectives," Draft ITU-T Recommendation G.FEPO, SG 13 TD 36 (WP 4/13), January 2006.

[11] "Towards an NGN QoS Solution: New Information and Related Discussion Issues," PRQC-2005-180, October 23, 2005.

[12] "SIP-Based Call Processing Performance in NGNs, PRQC-2005-143, August 9, 2005.

control. Relevant ETSI specifications include TISPAN 05007 and TISPAN 05008.[13] The TISPAN approach is to provide QoS via managed allocation of resources in the access network, assuming adequate QoS is achieved by over-provisioning in the core. RACS defines inter-provider interfaces in the access network to support separation of applications from the network (Gq') and to support wholesale bandwidth business models.

Most work in IETF related to QoS signaling is taking place in the Next Steps in Signaling (NSIS) Working Group. NSIS is responsible for "standardizing an IP signaling protocol with QoS signaling as the first use case. The intention is to re-use, where appropriate, the protocol mechanisms of RSVP, while at the same time simplifying it and applying a more general signaling model." NSIS is developing a QoS model which is a defined mechanism for achieving QoS as a whole. The specification of a QoS model includes a description of its QSPEC parameter information and how that information should be treated or interpreted in the network. The QSPEC contains a set of parameters and values describing the requested resources. The Resource Reservation Protocol (RSVP) originally defined in RFC2205 defines a resource reservation setup protocol. RSVP has been updated and modified by a number of RFCs since its publication.

PTSC-SAC contributed strongly to early progress in the QoS signaling area by spearheading the development of Q-Series Supplement 51, as described in 7.1.2. More recently, PTSC-SAC participants have contributed to the development of a QoS model and QSPEC template consistent with Supplement 51 and Y.1541 in the IETF's Next Steps in Signaling (NSIS) Working Group.[14] PTSC is also progressing work on an NNI for IP networks supporting multi-media services, focusing initially on VoIP.[15] In April of 2005, PTSC approved a new Issue to develop requirements for one key element of the NGN QoS solution – a vertical signaling interface for communicating IP traffic priority and QoS parameters between applications and the IP transport.[16]

A PRQC contribution to PTSC-SAC defines a generic list of priority and QoS parameters that will need to be communicated from applications to the layer 3 setup processes via

---

[13] A recent draft of the ITU-T Recommendation on RACF is provided in "Functional architecture and requirements for resource and admission control functions in next generation networks," ITU-T Study Group 13 TD 81 Rev.2 (WP 4/13), January 2006. The TISPAN Release 1 version of RACS is provided in "Resource and admission control subsystem (RACS) functional architecture," ETSI ES 282 003, V.1.6.8, December 2005.

[14] See "Y.1541-QOSM -- Y.1541 QoS model for networks using Y.1541 QoS classes," *draft-ietf-nsis-y1541-qosm-00.txt*, August 2005 and "QoS-NSLP QSPEC Template," *draft-ietf-nsis-qspec-08.txt*, December 2005.

[15] "U.S. standard defining the NNI for IP-IP network interconnection supporting multi-media services," PTSC Issue S0009, May 2004.

[16] "Vertical signaling interface to communicate QoS and reliability/priority parameters between the application layer and the user plane in IP networks," PTSC Issue S0023, April 2005. A recent draft of the vertical interface signaling specification is provided in "Vertical signaling interface for communicating priority and QoS parameters from applications to layer 3 setup processes in IP networks," PTSC-SAC-2006-018, January 2006.

the proposed vertical signaling interface.[17] In related work, PTSC-SAC has approved an Issue Statement (Issue 27) under which it proposes to define a standard signaling/control interface between an end user's SIP User Agent (UA) and an IP service provider, with the focus on layer 4 and above (application signaling and control). This document is planned to also include procedures and call/signaling flows for device bootstrap, discovery, and data profile configuration. PTSC-SAC is also contributing to Y.RACF in ITU-T.

7.3.3 Resource Management

PRQC and PTSC have focused less on resource management and traffic control mechanisms than on the other NGN QoS solution elements. The IETF has a strong work program in this area, and it appears that practical, implementable solutions are emerging. As an example, IETF's TE Working Group defined protocol extensions and bandwidth constraint models for support of Differentiated-Service-aware MPLS Traffic Engineering (DS-TE), which can be used to reserve bandwidth and control queues for particular classes of traffic in IP networks.[18] Regarding OSS support to resource management, there is existing work underway in (or existing standards from) TMOC, Ordering and Billing Forum (OBF), Tele-Management Forum (TMF), ITU-T SG4, and the ITU-T NGNMFG that needs to be completed, verified, revised, and utilized (as appropriate) in order to provide a complete solution.

7.4 Identified Gaps

The following sections identify potential gaps in current standardization activities related to QoS specification, QoS signaling, and resource management respectively.

7.4.1 QoS Specification

As noted in 7.3.1, solutions are lacking for two important QoS specification problems: QoS class mapping and performance apportionment or accumulation. Although PRQC and cooperating standards organizations are working to address these problems, a more energetic and broad-based industry commitment to this effort is needed. New industry efforts will be required to standardize the QoS attributes not fully addressed in existing specifications (e.g., call processing performance, service availability, and perception-based quality measures). The ultimate development of this information into useful operational reports must also be considered.

QoS specification standards are also needed to define:

---

[17] "Draft Technical Requirements Document on Priority and QoS Parameters for Communication from Applications to Layer 3 Setup Process in IP Networks via Proposed Signaling Interface," PTSC-SAC-2005-220, June 2005.

[18] "Protocol extensions for support of Differentiated-Service-aware MPLS Traffic Engineering," RFC4124, December 2004 and "Mechanisms for IP priority services and standards implications," T1A1/2003-127, May 2004.

- Metrics and (perhaps) target values for NGN call processing performance and service availability.
- Perception-based quality metrics, equivalent to MOS, for non-voice NGN applications, including IPTV.
- Performance metrics for individual NGN functions (e.g., service selection, IPTV channel change time), new service capabilities (e.g., presence, location), and web-based services (e.g., browsing).
- Methods for NGN performance measurement and reporting, and for concatenating NGN performance metrics across multiple domains.

There is also a need for more comprehensive and detailed guidance on how to map the end-to-end (e.g., mouth-to-ear) QoS requirements for particular user applications to IP network (UNI-to-UNI) QoS classes.

7.4.2 QoS Signaling

A key challenge in the QoS signaling area is that multiple standards-based solutions are being defined. QoS signaling work is being conducted in several different forums, reflecting different technology assumptions and business objectives, and the results are correspondingly divergent. A variety of proposed solutions, differing in important respects, may be standardized – and several may be implemented in early NGN products.

As noted above, the proposed solutions include both path coupled and path decoupled approaches. In addition to the ITU-T, TISPAN, and ATIS initiatives described in 7.3.2, there is work under way in ITU-T SG16 to develop a QoS signaling solution for H.323 based multimedia communications.[19] SG 16 recently began work on a fundamentally new multimedia signaling protocol -- H.325, which could be proposed as a replacement for both H.323 and SIP, and has QoS implications. A recent PRQC contribution identifies another relevant development: a proposal for NSIS "path decoupled" signaling.[20]

In this complex environment, it will be important for ATIS member organizations to identify their common business interests and public service responsibilities in IP/NGN QoS and traffic control, and to ensure that those interests and responsibilities are adequately addressed in NGN-related ATIS and international standards. Taking into account the results of the NGN-FG's *Part III* gap analysis, ATIS members and standards committees should review the various IP/NGN QoS signaling solutions being developed, and consider whether a particular solution (or a multi-solution hybrid with associated interworking arrangements) should be specified as the preferred ATIS solution. To support a phased deployment of NGN capabilities, a series of incremental technology steps leading to the preferred signaling solution should also be defined.

---

[19] "Draft new Recommendation H.mmqos, "End-to-End Quality of Service (QoS) and Service Priority Control and Signaling in H.323 Systems," PRQC-2005-169, October 20, 2005.

[20] "A Problem Statement for Path-Decoupled Signalling in NSIS," draft-hancock-nsis-pds-problem-02.txt, July 18, 2005.

7.4.3 Resource Management

A number of NGN resource management mechanisms are being standardized and developed, as discussed briefly in section 7.1.3. New standards will likely be required to enable some of these mechanisms to interwork across network provider boundaries. Interworking standards may also be required to coordinate resource management among providers in situations where different solutions are implemented. A PRQC contribution describes one particular NGN resource management solution (DS-TE), identifies some of the necessary interactions with SIP, and lists the minimum information that would need to be transmitted via the PTSC-proposed vertical interface in implementing it.[21] This list is highly relevant if DS-TE has general support as a resource management and traffic control solution. A more complete and detailed assessment of NGN resource management mechanisms and interworking requirements will be needed to establish actionable standardization goals.

7.5 Proposed Work Items

This section outlines a set of proposed work items and associated outputs that collectively address the NGN standardization gaps identified in section 7.4. The proposed work items are grouped in three categories consistent with those identified earlier: QoS specification, QoS signaling, and resource management. Although some proposed interim outputs are ATIS documents, all of the NGN QoS standards should ultimately be international in scope.

Within each of the three categories described above, the proposed work items are of three general types: *new work*, *existing work augmentation*, and *overlap analysis*.

1. *New work* is recommended when, in the judgment of the NGN-FG, a standard is needed to plan, implement, operate, or maintain an NGN facility or service and no suitable standard exists. Items listed in this category are intended to motivate new Issue Statements in target ATIS committees, or equivalent detailed work proposals in other SDOs. The desired end result is a new standard that meets ATIS member goals.
2. *Existing work augmentation* is recommended when, in the judgment of the NGN-FG, an existing standards development activity should be expanded in scope or needs stronger industry participation to achieve ATIS member goals. Items listed in this category are intended to motivate revised Issue Statements or resource requests. The desired end result is a more technically complete or timely standard, consistent with ATIS member goals.
3. *Overlap analysis* is recommended when, in the judgment of the NGN-FG, two or more different solutions to an NGN standards problem have been or are being standardized. Items listed in this category are intended to motivate technical or

[21] "Enabling Priority, Availability, and QoS in IP/MPLS Networks with DiffServ-Aware Traffic Engineering, PRQC-2005-161, October 2005.

business evaluation leading to a consensus standard that defines the preferred ATIS solution or required interworking arrangements.

7.5.1 QoS Specification

Work Item A: New Work - Primary: PRQC; Collaborators: IIF, ITU-T SG12 and SG13, Title: NGN Performance Metrics

Business Need:

Uniformly-defined performance metrics will be needed to plan, deploy, and operate NGN systems and services that provide assured network QoS in a multi-provider environment, and to match offered systems and services with user application needs.

Recommended Approach:

In close collaboration with ITU-T SG12 and SG13, ATIS PRQC should define network performance metrics for NGN call processing and service availability, and application QoS metrics for individual NGN functions (e.g., service selection) and new NGN service capabilities (e.g., presence, location, web-based services).[22] The ATIS IIF QOSM Task Force is expected to be an interested user and may be a contributor in this area.

Target Date: 4Q2007

Work Item B: Existing Work – Augmentation -Primary: ITU-T JRG-MMQA; Collaborators: ITU-T SG9 & 12, ATIS PRQC, IIF
Title: Perception-Based Quality Metrics for NGN Services

Business Need:

NGN providers will need objective, perception-based quality metrics to support deployment and operation of audio, video, and multimedia equipment and services. Such metrics will need to be standardized to enable network interworking and comparison of service alternatives. The services of interest will include high-definition audio distribution, IPTV, mobile wireless multimedia distribution, and multimedia conferencing among others.

Recommended Approach:

ITU-T's Joint Rapporteur Group on Multimedia Quality Assessment (JRG-MMQA) should motivate and coordinate the development of perception-based quality metrics for NGN services. This activity will require substantial standards activities in each of JRG-MMQA's participating SDOs (SG9 and SG12) and in other cooperating SDOs (e.g., ITU-T SG16, ITU-R WP 6Q). ATIS PRQC should support and contribute technically to this ITU work.

---

[22] The latter work should take into account the IP application performance metrics already defined in ATIS TR 83-2003 "Performance Parameters for IP-based Applications," T1.TR.83-2003, December, 2003.

The ATIS IIF QOSM Task Force is also expecting to work in this area. The Task Force will have an interest in the relationships between service layer and NGN (IP) layer performance metrics, and in describing the baseline NGN performance expectations for IPTV applications.

Target Dates:

Will depend on the particular metrics being standardized. An ITU-T Recommendation for objective perception-based audio/video quality assessment, applicable to IPTV and other services, is targeted for 4Q2007.[23] Such a specification could probably be approved as an ATIS standard somewhat earlier.

Work Item C: Existing Work – Augmentation- Primary: SG12; Collaborators: SG13, PRQC, IIF
Title: NGN QoS Mapping

Business Need:

To provide assured-quality NGN services, providers will need standard ways to:

- Dynamically apportion or accumulate performance values among independently operated networks to achieve requested UNI-to-UNI QoS levels for NGN flows.
- Relate UNI-to-UNI QoS levels (e.g., Y.1541 QoS classes) for particular services with the distinct QoS categories or mechanisms available in particular network technologies (e.g., UMTS bearer service attributes, Ethernet priority classes).

Recommended Approach:

To meet the first need, ATIS should strengthen and broaden its contribution to ITU-T work on Q11/12, *QoS interworking and apportionment of performance parameter values between networks*. A specific goal should be to complete draft new Recommendation G.fepo, *Framework for achieving end-to-end IP performance objectives*. In related work, SG12 should supplement Recommendation Y.1541 with additional, more comprehensive guidance on how to map end user QoS requirements for individual IP applications into corresponding UNI-to-UNI QoS classes.

As a first step towards meeting the second need, PRQC should develop a technical report that describes and evaluates the QoS control mechanisms likely to be most widely used in NGN component networks, putting particular emphasis on access networks.

[23] This standards will be based on the requirements of ITU-T Recommendation J.148. See "Requirements for an Objective Perceptual Multimedia Quality Model," ITU-T Recommendation J.148, May 2003.

To advance both goals, SG13 and 12 (and SG4) should collaborate in completing draft Recommendation Y.pmm, *Performance measurement and management for NGN*.

The ATIS IIF QoS QOSM Task Force is expected to be an interested user and may be a contributor in this area.

Target Dates:

Will depend on the particular standards development activity. A goal should be to complete all four documents by 4Q2007.

7.5.2 QoS Signaling

Work Item D: Standards Gap / Overlap Analysis, Primary: PTSC
Title: QoS Signaling Technology Assessment

Business Need:

A number of different NGN QoS signaling solutions are being developed in standards committees, and several may be implemented in early NGN products. Resulting incompatibilities could make it difficult or impossible to establish end-to-end, assured quality IP flows on request in a multi-provider, hybrid technology NGN environment.

Recommended Approach:

ATIS member organizations should identify their common business interests and public service responsibilities in IP/NGN QoS and traffic control, and contribute actively in ITU-T SG13, 11, and 12 and IETF to ensure that those interests and responsibilities are adequately addressed in NGN related international standards. Taking into account the results of the NGN-FG's *Part III* gap analysis, PTSC and PRQC should review the various IP/NGN QoS signaling solutions being developed and determine whether a particular solution (or a multi-solution hybrid with associated interworking arrangements) should be specified as the "preferred ATIS solution." The recommended signaling solution(s) should meet the technology-independent QoS signaling requirements defined in ITU-T Q-Series Supplement 51. To support a phased deployment of NGN capabilities, a series of incremental technology steps leading to the preferred signaling solution should also be defined. These results should be document in an PTSC technical report.

Target Date: 3Q2007

7.5.3 Resource Management

Work Item E: New Work, Primary: PRQC, Collaborator: PTSC
Title: Resource Management Technology Assessment

Business Need:

Many different NGN resource management mechanisms have been defined (or are being defined) in standards committees, and may be implemented in early NGN products. At least some interworking among mechanisms (e.g., Diffserv, MPLS) and cross jurisdictional boundaries will be required to support requested QoS levels end-to-end in a multi-provider, hybrid technology NGN environment. Interworking among resource management mechanisms at different layers in layered NGN architectures may also be needed, and could require standardization if jurisdictional boundaries are involved.

Recommended Approach:

PRQC and PTSC should review the various IP network resource management mechanisms defined in IETF and other standards committees, and assess the most probable deployment scenarios and associated interworking requirements. The results could be documented in a PRQC technical report to identify required interworking standards. Among other uses, this report is expected to serve as input to ATIS NIOC on NIIF Issue #0254, "IP QoS and IP/PSTN Convergence as it relates to the PRQC Work."

Target Date: 4Q2006

Work Item F: New Work, Primary: ATIS OBF, Secondary: TMOC, TMF, and ITU-T SG4
Title: Inter-Administration OSS-to-OSS Ordering in Support of QoS/Resource Management

Business Need:

QoS/Resource Management across service provider (or administrative) domains will require appropriate "non-real-time" OSS-to-OSS ordering transaction support, controls, and security (e.g., non-repudiation) to provide for basic service ordering to enable service delivery. The intent is to enable the appropriate "real-time" network QoS/Resource Management signaling interactions across service provider (or administrative) domains.

Recommended Approach:

Build this *OSS-to-OSS Ordering in Support of QoS/Resource Management* work into the existing interconnection ordering work program in OBF. In addition, complementary and supporting applications (e.g., accounting management, trouble administration, service level agreement management, etc.) will be needed. There is existing work underway in (or existing standards from) TMOC, OBF, TMF ITU-T SG4, that needs to be completed, verified, revised, and utilized (as appropriate) in order to provide a complete solution.

Target Date: 3Q2007

Work Item G: New Work, Primary: ATIS TMOC
Title: Inter-Administration OSS-to-OSS Resource Management Study

Business Need:

In the long term, resource management across service provider (or administrative) domains may require more features/functions regarding "non-real-time" OSS-to-OSS resource management transaction support, controls, and security (e.g., non-repudiation) where the networks provide significant flexibility to provision and partition services. The intent is to enable the appropriate resource boundaries for "real-time" network resource management signaling interactions across service provider (or administrative) domains.

Recommended Approach:

A study should be done to examine the business needs, technology, and operations issues regarding robust OSS-to-OSS resource management transaction support, controls, and security (e.g., non-repudiation). For example, one or more layers of non-real-time OSS-to-OSS resource management could be provided to allow services providers to interconnect and enable the appropriate boundaries for real-time network resource management signaling interactions. These layers could be *High Level Enablement* (e.g., service ordering) and *Low Level Enablement* (e.g., network resource configuration management). Another approach could be to minimize OSS-to-OSS interactions and build more interconnection control features/functions into the network elements (e.g., via signaling). In addition, complementary and supporting applications (e.g., accounting management, trouble administration, service level agreement management, etc.) will be needed. There is existing work underway in (or existing standards from) TMOC, OBF, TMF ITU-T SG4, that needs to be completed, verified, revised, and utilized (as appropriate) in order to provide a complete solution. The results should be documented in an TMOC technical report.

Target Date: 4Q2007

8 RESOURCE AND ADMISSION CONTROL

8.1 Requirements

Resource and admission control includes but is not limited to capabilities that support QoS. It also addresses network border control issues such as topology hiding or packet filtering. Therefore, resource and admission control can be seen as a separate enabler for the NGN and is dealt with separately in this Gap Analysis.

The NGN must provide a means to allow an application to request transport resources dynamically in a transport-technology independent way. In order to respond to the request, the NGN must support various aspects of resource control (concerning resource reservation, opening or closing of gates, NAPT, hosted NAT traversal, etc.). It shall be possible to control transport resources according to domains or network segments and to coordinate the controls across domains or network segments.

The NGN must support admission control to allow the admission of the user traffic into the NGN to be based on certain criteria. For example, an admission decision can be based on the availability of adequate network resources to meet the performance objectives of a particular service request or on policy rules for administering, managing, and controlling access to network resources. The policy rules can be specific to the needs of the service provider, or reflect the agreement between the customer and service provider, which may include reliability and availability requirements over a period of time. To satisfy the reliability and availability needs for certain services (e.g., emergency communications), associated traffic can be given higher than normal priority for admission to the network.

It must be possible for admission control to be integrated with session management such that only sessions that can achieve some defined level of QoS and security are admitted. There are four primary mechanisms for QoS-related session admission control that should be supported in the NGN:

1. *Maintaining session counts*, which admits session requests according to the knowledge of how many sessions (or how much bandwidth) has been allocated;
2. *Out-of-band measurement*, which admits session requests based on measured network resource availability through periodic polling of routers or switches;
3. *In-band measurement*, which admits session requests based on the measured network performance through active probes or other in-band performance metrics; and
4. *Reservation based mechanisms*, which admit sessions or flows only if an explicit request for bandwidth reservation for that session/flow is successful.

In addition, the admission control mechanisms must span multiple service types (e.g., voice and video).

8.2 Function/Service Enabled

This function enables the reliable delivery of real time services with the desired QoS. There may also be applications that need relatively better services than other applications, perhaps just for a defined period of time (i.e., differentiated services). In addition, this function enables communication between entities behind NAT devices.

8.3 Current Standardization Activities

8.3.1 Session Management

8.3.1.1 SIP

The IETF has specified the following RFCs to allow SIP session control to take into consideration QoS, policy, and session mobility:

- RFC 3312 - Integration of Resource Management and Session Initiation Protocol (SIP).

- RFC 3313 - Private Session Initiation Protocol (SIP) extensions for media authorization.
- RFC 4032 – Update to the SIP preconditions framework (updates RFC 3312 to include guidelines on defining new precondition types and how to use preconditions involving session mobility).

Presently the IETF is developing the following mechanisms that can influence session admission:

- Communications resource priority for the Session Initiation Protocol (RFC 4412) through two new SIP header fields (Resource-Priority and Accept-Resource-Priority); the Resource-Priority header field can influence the behavior of SIP user agents.
- Session policy framework and dataset to allow network-based session policy to be part of end-to-end session negotiation.[24]

8.3.1.2 IMS

3GPP and 3GPP2 have (such as specified in TS 24.229) prescribed the use of RFC 3312, RFC 3313, and RFC 4032 to integrate QoS admission control with IMS session control.

8.3.1.3 Resource- and Policy-based Admission Control

The IETF RFC 2753 specifies a framework for policy-based admission control. This framework underpins the IMS service-based local policy control as specified in 3GPP TS 23.207, which, in turn, has become the basis for the resource- and policy-based admission control mechanisms being standardized in both the TISPAN and ITU-T.

The emerging standard mechanisms are to allow the admission decision for a service request (IMS- or non-IMS supported) to take into consideration policy as well as transport resource availability. They enable performance assurance and border control (e.g., NAPT, NAT traversal and gating) through bridging service control and transport resource management. The mechanisms are defined as part of the RACS in TISPAN and the RACF in the ITU-T.
RACF and RACS, however, show differences in their specifics. For example:

- RACF addresses QoS end-to-end (encompassing access, core and inter-provider-domain), while RACS addresses only access QoS to date.
- RACF supports both the push and pull models for policy installation, while RACS supports only the push model.
- RACF supports the selection of firewall working modes of varied levels of security strength, but RACS does not.
- RACF and RACS specify similar but not identical functional entities and reference points.

[24]See IETF documents draft-hilt-sipping-session-policy-framework-00.txt; draft-ietf-sipping-media-policy-dataset-00.txt; and draft-hilt-sipping-policy-package-00.txt.

The following RACS-related specifications for Release 1 have been approved:

- Functional architecture for RACS.
- Gq' interface based on the DIAMETER protocol.
- e4 interface based on the DIAMETER protocol.
- Stage 3 specification of the Rq interface based on the DIAMETER protocol.
- H.248 profile for the Ia Interface.
- Effort is currently under way in TISPAN to develop the specifications for post-Release 1 features.

The RACF-related specifications under development in the ITU-T include:

- Functional requirements and architecture for resource and admission control in next generation networks (Y.RACF).
- Protocol at the Rs interface (Q.rcp.1) [Note that Rs is closely related to Gq′].
- Protocol at the Rp interface (Q.rcp.2).
- Protocol at the Rw interface (Q.rcp.3) [Note that Rw is closely related to Ia].
- Protocol at the Rc interface (Q.rcp.4).

Note that the Rs and Gq′ protocols are aligned, but there is no consensus on the Rw protocol choice.

PTSC-SAC has an open issue (S0018) for a technical report that defines an implementable architecture for N.A. networks in support of resource and admission control and serves as the basis for related USA/company contributions to the ITU.

PRQC has published the following specifications defining user plane reliability/priority classes for admission control and network restoration, respectively:

- User Plane Priority Levels for IP Networks and Services, PRQC Technical Report, Pre-Publication Version – Contribution T1A1/2003-196 R3
- Service Restoration Priority Levels for IP Networks, Draft ATIS Technical Report, PRQC-2005-021R5, May 2005

8.4 Identified Gaps

- Service admission control taking into consideration signaling resource availability, separate from media resource availability. So far the standards efforts have yet to address the performance requirements specific to service control signaling. Additional measures (e.g., overload indication of signaling resources) may be needed to ensure that the desired performance of service control signaling (such as certain "session" setup delay target or unconditional delivery) can be met.

- Harmonization of resource and admission efforts across relevant SDOs (e.g., 3GPPs, ATIS, ETSI, and ITU-T). A consistent approach to resource and admission control is key to reducing the complexity of dynamic support for QoS and network border control to diverse applications over a packet transport infrastructure that employs varying transport technology. ATIS should contribute to the formulation of a harmonized solution.

There is general agreement within the industry on the need for some mechanism to control the allocation of resources. However, when one moves beyond that general agreement, there is not a widespread consensus on how strong the mechanism should be, how widely it should apply, and the relative priority of individual work items within this. This lack of consensus at this "detail, two layers down" level is believed to be the main reason for the lack of industry alignment and progress on a single solution.

8.5 Proposed Work Items

Work Item A: Primary: PTSC, Secondary: IIF
Title: Resource and admission control for signaling resources

Business Need:
The capabilities for resource and admission control for signaling resources give service providers another dimension of control of user experience (i.e., the real-time setup delay of NGN services).

Recommended Approach:
PTSC to develop an ATIS view and, if required, contribute it to the development of the global standard solution in the ITU-T. This is within scope of Issue S0039.

Target Date: 4Q2006

Work Item B: Primary: PTSC, Secondary: IIF
Title: Harmonization of related resource and admission control standards efforts

Business Need:
Resource and admission control capabilities give service providers control of user experience (in terms of assured quality of service and unimpeded communication in the presence of NAPT devices). The capabilities also allow service providers to protect transport resources. There is a strong need for a harmonized approach to resource and admission control to reduce implementation and operation costs.

Recommended Approach:
Continue the work currently being done in PTSC on this issue as part of Issue S0019.

Target Date: 1Q2007

9 SETTLEMENT

9.1 Requirements

NGN services need to support a variety of commercial arrangements for settlement of transactions, both with the service providers and between the communicating entities. Telephone service billing has also been used to support other billing arrangements. Perhaps the stereotypical example is the ability to use a mobile phone to purchase a soda from a vending machine. A further extension would be the ability to transfer value between communicating consumers, rather than just select merchants.

Flexible settlement arrangements may be required. It is desirable that these arrangements be based on consistent, scaleable accounting metrics and settlement models (e.g., "sender pays," "receiver pays," etc.), and a level of aggregation that supports scalability. It shall also be possible to charge through various techniques such as prepay, post pay, advice of charge, and third party charging.

The generic requirements for all commercial arrangements/application types along with the suggested level of requirements, per application, for every single requirement, are specified in section 7 of ATIS-0300075 Revision 10.

Specific service requirements (such as VOIP) are described in separate documents. This document is part of the IPDR suite of documents located at < http://www.ipdr.org >.

9.2 Function/Service Enabled

1. *Retail Billing* – The rendering of an invoice for charges due to a Service Provider by a Subscriber to their services, as per an agreed rate plan and service agreement.
2. *Wholesale Billing* – The rendering of an invoice for charges due to a Network Operator from a Service Provider for access or transport services via which the Service Provider's services were delivered.
3. *Intercarrier Settlement* – The process by which Service Providers determine the periodic net charges due from one party to another for services rendered by each of the parties on behalf of the other's Subscribers.
4. *Internal Cost Accounting (e.g., Chargeback)* – Use of accounting information by a commercial Subscriber for separating the aggregate usage into sub-accounts associated with the enterprises' financial components.
5. *Customer Care* – All those activities associated with the sustenance of satisfactory Subscriber service levels, including inquiries, account changes, restoration, and termination.
6. *Marketing Information* – Demographic, financial, statistical, geographical, and temporal data used to aid in decision making and direction setting for product and services positioning and introduction by a Service Provider.

7. *Support for Law Enforcement* – Capture of targeted service usage entries, requested by a legal order for use by various agencies of law enforcement.
8. *Capacity Planning* – Predictive extension of existing usage patterns to allow for adequate resources to be staged in such a timeframe as to ensure continuity of agreed service levels.
9. *Traffic Profiling* – Statistical portrayal of usage information for characterizing the patterns of usage levels and concentrations at nodal points and across transport boundaries.
10. *Traffic Engineering* – Use of traffic profile information to manage the configuration of infrastructure resources so as to ensure service level continuity.
11. *Performance Management* – Use of statistical data derived from network and service element telemetry to adapt the configuration of those elements to ensure service level continuity.
12. *Revenue Assurance* - Any activity an organization performs to ensure that processes, practices, and procedures result in revenue that is billed and collected completely, accurately, and in a timely manner. This involves all areas of the organization, from customer care and network systems to invoicing and collections and finance, crossing all boundaries. Revenue leakage is revenue the company has earned, but has neither billed for nor collected. This revenue is lost. Revenue assurance includes *Fraud Abatement e.g., Attack/Intrusion Detection*, which is the use of statistical and pattern recognition results to detect, prevent, and interdict in usage by Service Consumers not authorized for such usage by a Subscription agreement.
13. *QoS Monitoring/SLA Management* – Use of all varieties of network and BSS data in the tracking and adaptation of network behavior to ensure service level continuity.

Target Network/Service Elements that are involved in some way with the handling of, or are aware of packet-based services, and where packet-based accounting protocol can be implemented and reside include:

- Soft-switches
- Passive/active Probes
- Firewalls
- Web/Proxy servers
- Application servers
- Edge access devices (such as: router, CSUs/DSUs and modems)

There are additional Network/Service Elements that switch, route, handle, treat differentially, or recognize packet-based data, but are dedicated to a specific application or service (such as VoIP traffic or signaling Network/Service elements). The packet-based accounting protocol can be implemented in these Network/Service Elements as well.

9.3 Current Standards Activities

9.3.1 ATIS

OBF

ATIS OBF has a structure in place to address the ordering needs of companies as new services are defined. Currently, ordering standards are developed and maintained by Wireless, LSOP, and ISOP committees via their documents WICIS, LSOG and ASOG, respectively. Various interface specifications are published to support these standards and include paper form, batch processing, and UOM (XML) processing. For NGN based services, the XML interface specification as defined within the UOM documentation will most likely be the basis for ordering NGN-based services. The batch process interface specifications are defined in the *ASR Mechanized Interface Specifications*, ATIS-0404100, for transmission between trading partners. The UOM interface utilizes the specifications defined in the ATIS TMOC Transport profile (TCIF-03-003) for transmission between trading partners.

OBF-IP-NNI

- VoIP Ordering and Billing Issues and Concerns Document Summary - Issue 1 - September 2005

This document is a compilation of questions, comments, concerns and assumptions identified by the OBF Strategic Advisory Group (SAG) Committee's VoIP Sub-team surrounding VoIP and the related challenges for intercarrier ordering and billing. It outlines, via call flows, some of the issues and concerns developing due to the implementation of VoIP in the absence of industry standards for VoIP business processes.

- **Issue 2949:** (Intercompany Data Exchange for Packet Based Services) are intended to resolve the identified gaps.
- **Issue 3025:** Identification of Data Exchange Use Cases for IPTV Services.
- **Issue 3026:** Billing & Collection Services for 3rd Parties, Partners, and Affiliates – Exchange of Billing Events Data Standards Needed.
- **Issue 3027:** Billing & Collection Services for 3rd Parties, Partners, and Affiliates – Application Authentication & Authorization Standards Needed.
- **Issue 3028:** VoIP Data Element Matrix.

TMOC

- ATIS-0300075 - Usage Data Management for Packet-Based Services—Service-Neutral Architecture and Protocol Requirements Document.
- ATIS-0300075.1-2005 Usage Data Management for Packet-Based Services -- Service-Neutral Protocol Specification for Billing Applications.
- IPDR.org Business Solution Requirements: Network Data Management-Usage (NDM-U) 3.5.0.1 specification, Chapter 4 information model of the IPDR NDM-U.
- IPDR/File Transfer Protocol 3.5.0.1 specification.
- IPDR/SP Protocol Specification 2.1.

- IPDR/XDR File Encoding Format 3.5.1 specification.

3GPP submitted IMS as a standard to ITU-T for consideration. Concern was expressed to ITU-T regarding the inability of IMS to handle large record volumes needed to manage accounting and settlements. Thus, the alternative for accounting management submitted by TMOC was also given consideration. TMOC submitted their proposal to the following ITU-T Study Groups 4 and 13.

A Task Force of TMOC and a subgroup of 3GPP met to reach an agreement on NGN Harmonization. Agreement was reached and is in the process of being finalized by both committees. Each committee will submit a liaison to the ITU-T with the same attachment as agree to as an outcome of the harmonization meeting.

TMOC has developed the Intra-provider accounting and settlements service-neutral standard. The OBF IP-NNI committee will work with TMOC-AIP to develop the Inter-provider standard for Next Generation Networks.

9.4 Identified Gaps

The following gaps have been identified:

- Identification of Services is needed for the development of ordering and billing standards. A standard to support the ordering of new services requires a clear definition of these services.
- If ordering standards are required, it is important that these services be identified as quickly as possible so that ordering standards can be developed for effective and timely product delivery using the above listed ATIS structure.
- If the products identified are not accommodated by the existing OBF structure, then changes will be made to this structure -- i.e., new committees will be developed within the OBF as required -- or existing committee mission statements will be modified appropriately. For example, Service Descriptions and network architectures need to be defined by the ATIS member companies. Additional work cannot begin until these items are provided and resources are identified if needed.
- The work in IETF IPFIX WG needs to be considered for integration with the accounting management work in TMOC.

9.5 Proposed Work Items

Work Item A: Primary: TMOC
Title: Issue 81 (Inter-administration Accounting Management)

Target Date: Ongoing

Work Item B: Primary: OBF IP-NNI
Title: OBF IP-NNI NGN Work Items

Target Date: Ongoing

10 NGN MANAGEMENT (OAM&P)

10.1 Requirements

As noted in Part I of the ATIS NGN Framework, ATIS fully supports a consistent set of global NGN standards. NGN Management is an essential part of the overall NGN infrastructure. Implementation of NGN cannot be realized without a satisfactory management solution.

The objective of this section is to identify and analyze the available standards specifications that are applicable to NGN Management. Through the analysis, OAM&P areas where lacking NGN Management support will be identified for pursuing. On the other hand, competing solutions, if any, will also be identified for harmonization.
ITU-T (in collaboration with other committees/forums, including TMOC) initiated a NGN Management Focus Group (NGNM FG) in November 2004 to coordinate NGN Management (OAM&P) work efforts across the telecom industry. Participation is open to individuals from organizations with expertise and specifications applicable to NGN Management interfaces, including the following:

- ITU-T SG4 and SG15
- ATIS TMOC
- ETSI TISPAN WG 8
- 3GPP SA5
- 3GPP2 TSG-S WG5
- TeleManagement Forum
- IETF Operations and Management
- OASIS

The NGNM FG is undertaking a centralized approach regarding specification of NGN Management related to FCAPS interfaces. FCAPS interfaces are generally understood to include NE-OS, OS-OS, and NE/OS-WS interfaces in support of element, network, service, and business management. The result of this effort has been produced in a roadmap document, which lists the existing specifications that are candidates for a suite of management specifications. The roadmap document also identifies the gaps which have to be filled and areas for harmonization. The current content is relevant for ITU-T NGN Release 1; information regarding later Releases will be added when needed.

The set of NGN Management specifications described in the NGNM FG roadmap is separated in four categories. The following text is taken directly from the ITU-T NGNM FG Roadmap (TD55 WP1/13 Rev1 20060123).

10.1.1 Specifications for NGN Management

Specifications are listed under this category if they have been written specifically for NGN Management and their scope is the NGN as a whole -- i.e., they are not related to a specific functional entity in the NGN.

10.1.2 Generic telecommunications management specifications, reused for NGN

Specifications will be listed under the first category, if they have not been written specifically for management of the NGN. The indication "NGN" does not appear anywhere in the titles of these documents, yet they are recognized as applicable for management of the NGN because of their generic applicability to telecommunications management.

Dependent on their main subject areas, specifications within this category are identified as generic or according to their relation with the FCAPS and other functional areas.

10.1.3 Specifications for the management of NGN functions

Specifications will be listed under this category if their scope is the management of one or more specific functional entities in the NGN. This category includes specifications which have been written specifically for the management of NGN functions, and specifications which have been written for the management of non-NGN functional entities which are re-used in the NGN.

Specifications in this category are identified according to their main application area in terms of the functional entities of the NGN as they are defined in Y.NGN-FRA, "Functional Requirements and Architecture of the NGN" (FGNGN-OD-192R1), Figure 3. These entities are:

- *Service Stratum*:
  - Application Functions
  - User Profile Functions
  - Service and Control Functions:
  - Other Multimedia Components
  - Streaming Services
  - PSTN/ISDN Emulation
  - IP Multimedia Component including PSTN/ISDN Simulations
- *Transport Stratum*:
  - Network Access Attachment Function
  - Resource and Admission Control Functions
  - Access Functions
  - Access Transport Functions
  - Edge Functions
  - Core Transport Functions

- *CPE*:
  - Legacy Terminals
  - Gateways
  - NGN Terminals
  - Customer Networks

10.1.4 Other relevant specifications

Specifications considered relevant for the management of the NGN, which do not belong to another category.

The following is an extraction from the NGNM FG roadmap document for the identified OAM&P specifications.

10.1.4.1 Specifications for NGN Management

Subcategory	Document ID	Title	Notes/Issues
Requirements	ETSI TS 188 004	NGN Management; OSS Vision	
	IETF RFC 3535	Overview of the 2002 IAB Network Management Workshop	
	ITU-T M.3060	Management of Next Generation Networks	
Management Architecture	ITU-T M.3060	Management of Next Generation Networks	Harmonization issue with ETSI TS 188 001 (See also Section 9.6.1)
	ETSI TS 188 001	NGN Management; OSS Architecture	Harmonization issue with ITU-T M.3060 (See also Section 9.6.1)

10.1.4.2 Generic telecommunications management specifications reused for NGN

Subcategory	Document ID	Title	Notes/Issues
Generic	ITU-T M.3050 series	Enhanced Telecom Operations Map	1) Equal to TMF eTOM v4 GB921 2) NGN relationship explained in M.3060 and in TS 188 001
	TMF 053B, C, D, and F	NGOSS Technology-Neutral Architecture v4.5	
Fault	X.733.1	Protocol-Neutral UML Description of the Alarm Reporting Function	
Configuration			

Subcategory	Document ID	Title	Notes/Issues
Accounting	ATIS-0300075-2005 and ATIS-0300075.1-2005	Usage Data Management for Packet-Based Services - Service-Neutral Architecture and Protocol Requirements -Service-Neutral Protocol Specification for Billing Applications	Harmonization issue with 3GPP IMS Charging specifications (See also Section 9.6.3)
Performance	ATIS-030004	NIIF Interconnection Template	
	ATIS-03000032	NIIF Reference Document Part X- Interconnection Between LECs-Operations Handbook Local Interconnection Service Arrangement	
Security	M.3016 series	Security of the management plane	NGN relationship explained in M.3060
Service Management	ITU-T M.3341	QoS/SLA management service requirements	
	ITU-T M.3350	Emergency telecommunication service management requirements	
Protocol	IETF Netconf	NETCONF configuration protocol	For interfaces to the NE, for configuration
	IETF STD 62	Simple Network Management Protocol version 3	For interfaces to the NE, primarily monitoring (including event reporting)
	OASIS WSDM MUWS	WSDM Management Using Web Services (WSDM-MUWS) v1.0	For non-NE interfaces
Interface definition language	IETF STD 58	Structure of Management Information version 2	To support SNMP; recommended MIBs are for further study

10.1.4.3 Specifications for the management of NGN functions

Subcategory	Document ID	Title	Notes/Issues
Core Transport Functions	ITU-T G.7718/Y.1709	Framework for ASON Management	
	ITU-T G.7718.1/Y.1709.1	Protocol-neutral management information model for the control plane view	
	TMF 513	MTNM Business Agreement (part of TMF MTNM Solution Suite)	Harmonization issue with 3GPP 32.111 and 32.671-675 (see also sections 9.6.2 and 9.6.4)
	TMF 608	MTNM Information Agreement (part of TMF MTNM Solution Suite)	
	TMF 814	MTNM Solution Set in CORBA IDL with Supporting Documentation (part of TMF MTNM Solution Suite)	
	TMF 814A	MTNM Implementation Statement Templates for CORBA (part of TMF MTNM Solution Suite)	
Access Transport Functions	TMF MTNM Solutions Suite (see Core Transport Functions)		
Service Stratum	ATIS TMOC Usage Data Management specifications (see table in 9.2)		
IMS	3GPP TS 32.111-1 to -4	Fault Management IRP	Harmonization issue with TMF MTNM Solution Suite (See also section 9.6.2)
	3GPP TS 32.301-304	Notification IRP	
	3GPP TS 32.311-314	Generic IRP	
	3GPP TS 32.601-604	Basic CM IRP	
	3GPP TS 32.621-625	Generic NRM IRP	
	3GPP TS 32.631-635	Core NRM IRP	
	3GPP TS 32.661-664	Kernel CM IRP	

Subcategory	Document ID	Title	Notes/Issues
	3GPP TS 32.671-675	State Management IRP	Possible harmonization issue with TMF MTNM Solution Suite (See also section 9.6.4)
	3GPP TS 23.125, 32.240, 32.260, 32.296-299	IMS Charging Management	Harmonization issue with TMOC Usage Data Management specifications (See also section 9.6.3)

10.1.4.4 Other relevant specifications

Subcategory	Document ID	Title	Notes/Issues
	IETF RFC 3444	On the Difference between Information Models and Data Models	

10.2 Identified Gaps

The following table identifies areas for which suitable specifications candidate could not be identified. The NGNMFG has brought the gap areas to the attention of the organizations listed in the third column, on the assumption that they will address the gap.

Area	**Reference**	**Organization**
Exchange of service orders, trouble tickets, etc	NGNMFG-ID-028 NGNMFG-OD-006	ITU-T SG4 ATIS-TMOC
NGN function oriented NE MIBs	TBD	TBD

10.2.1 Harmonization Issues

10.2.1.1 Management Architecture

ITU-T M.3060 and ETSI TS 188 001.

10.2.1.2 Fault Management

TMF MTNM Solution Suite, 3GPP 32.111, and X.733.1 regarding alarm reporting.

10.2.1.3 Accounting Management

3GPP Charging and TMOC Usage Data Management specifications.

10.2.1.4 State Management
TMF MTNM Solution Suite and 3GPP 32.671-675.

10.2.2 N.A. Specific Gaps
ATIS TMOC is already involved within the ITU-T NGNM FG. As the ITU-T NGNM FG progresses in its definition of NGN OAM&P, TMOC has an action item to monitor, review and, if necessary, provide inputs regarding N.A. requirements. Table 2 lists issues currently being worked on within TMOC that are relevant or intended to fill gaps within the N.A. perspective on NGN OAM&P.

Table 2: Current TMOC issues relevant to NGN OAM&P

Issue Number within TMOC	Issue Title
12	T1.202: Future Study Item - IP Focus
14	ETS Work Items related to ITU-T Study Group 4 (ETS Subset of Issue 60)
54	TMOC support for GTDD
56	Security Management System (near completion)
57	VoIP Accounting Management NE/OSS Interface - ANS
58	VoIP Accounting Management NE/OSS Interface - ITU-T
61	WAE OAM and Network Management
62	ITU-T NGN Management Focus Group (NGN Subset of Issue 60)
63	Instant resolution of ITU Carrier Codes (ICCs) as NGN identifiers
76	IPTV Accounting Management

Table 3: Current NIIF issues related to NGN OAM&P

Issue Number within NIIF	Issue Title
0247	Network Management Controls for High Volume Call In (HVCI) Events when VoIP Technology is Involved
0269	Call Forwarding is Causing Looping When New Technology is Involved
0266	Mass call blast impact on Telecommunication Networks

10.3 Proposed Work Items

Work Item A: Continuation of existing TMOC work (Issue 62)
Title: OAM&P Harmonization

Business Need:

NGN would benefit greatly from an integrated rather than fragmented OAM&P approach.

Recommended Approach:

ITU-T SG4 has already formed an NGN Management Focus Group involving key OAM&P standard forums and organizations. TMOC is one such organization already part of the focus group. In the sprit of integration and harmonization, TMOC should be left in charge of monitoring and influencing, if needed, the work of the NGNM-FG with a N.A. focus in mind.

Target Date: The deliverable should be timed with those of the ITU NGNM-FG.

11 LOCATION BASED SERVICES

11.1 Requirements

Some NGN services may require location information for devices, people, or both. These entities (endpoints or users) can be static, nomadic, and mobile.

Static users have a fixed location, and that does not change during or between the communication (e.g., wireline, DSL, or cable modem) endpoints. Nomadic users do not change location during communication but can change location in between (e.g., call made from a WiFi endpoint). Mobile users can change location during and in between communications (e.g., cellular calls).

Mechanisms to determine, acquire, verify and report location information will generally vary by technology and service platform. Location may also be delivered by the CPE to an NGN platform -- for example, doing a query of a Global Positioning System (GPS) chipset on the CPE. Location information can also be obtained from RFID based readers and savants that provide agent-based means for communicating location information. An NGN can also facilitate additional capabilities to authenticate location information to prevent fraudulent or erroneous location information.

The new ITU-T Directory Interoperability specification, E.115-2005, was developed to provide a standard NGN mechanism for maintaining and exchanging of location info among NGN service providers. However, not all providers may want to use this capability, and other Location Based Services (LBS) mechanisms will likely need to be supported.

Regulatory, legal (lawful intercept), consumer, and homeland/national security requirements must be taken into account when defining location based services. Various kinds of personal profile mechanisms can provide a means for the user to control the availability of location information.

11.2 Functions/Services Enabled

Services typically fall into four categories: family safety, presence & availability, push advertising, and government mandates. *Family safety* services generally allow family members to share their location information or even vehicle speed, in order to ensure the safety of children or knowledge of a parent's whereabouts. The *presence & availability* services typically provide the subscriber/user with the ability to facilitate or manage communication with family or friends. *Push advertising* allows local enterprises – both commercial and non-commercial – to make user/subscribers with their permission, aware of local opportunities of various kinds. Advertisers will want the information to guide potential customers to nearby shops or restaurants including weather, traffic report, pop-ups (real-estate reports, proximity based service ads, etc.). Users will want directions to required services or destinations.

Lastly, a growing array of *government mandates* are emerging worldwide that include personal safety such as E9-1-1, Emergency Messaging Services that allow local authorities to warn of disasters, "Amber Alert" services that provide notice of a missing child, National Security/Emergency Preparedness (NS/EP) capabilities that allow locating needed officials, and law enforcement/security requirements that require the availability of this information with the appropriate authorizations or as part of a data retention/preservation mandate.

11.3 Current Standardization Activities

11.3.1 IETF

11.3.1.1 Geographic Location/ Privacy (GEOPRIV)

- RFC 4119, A Presence-based GEOPRIV Location Object Format
- RFC 3925 describes the situation where the network determines the location and sends it to the end device via DHCP. The end device can then include the location in its communications.
- Geopriv requirements (Info, RFC 3693)
- Threat Analysis of the GEOPRIV Protocol (Info, RFC 3694)
- Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information (Std., RFC 3825)
- A Presence Architecture for the Distribution of GEOPRIV Location Objects (Info, RFC 4079)
    - draft-ietf-geopriv-dhcp-civil-07.txt
    - draft-ietf-geopriv-policy-07.txt
    - draft-ietf-geopriv-pidf-lo-03.txt
    - draft-ietf-geopriv-common-policy-06.txt

- draft-ietf-geopriv-radius-lo-04.txt
- draft-ietf-geopriv-location-types-registry-03.txt
- draft-ietf-geopriv-pdif-lo-profile-01.txt

Work is needed to develop new DHCP option to convey verifiable location info in a access network independent fashion.

11.3.1.2 Internet Emergency Preparedness (IEPREP)

- Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP) (RFC 3487)
- Internet Emergency Preparedness (IEPREP)Telephony Topology Terminology (RFC 3523)
- IP Telephony Requirements for Emergency Telecommunication Service (RFC 3690)
- General Requirements for Emergency Telecommunication Service (RFC 3689)
- Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony (RFC 4190)
- Emergency Telecommunications Services (ETS) Requirements for a Single Administrative Domain (RFC 4375)

These activities do not address protocol or protocol feature development, and do not focus on particular national regulations.

11.3.2 ETSI/TISPAN

TISPAN ES 282 004 (WI02021), "NGN Functional Architecture: Network Attachment Subsystem," is expected to be published April 14, 2006. The Network Access configuration Function (NACF, DHCP server) should be able to provide unique access network identifier to the CPE. Application can use this information to locate the Connectivity/Session Location and Repository Function (CLF). The transport of the access network identifier depends on extension in existing protocols (e.g., new DHCP option). The IP address alone is not sufficient to identify/locate the access network; especially there are private IP addresses, mobile IP or nomadic network scenarios. WI02021 needs a new DHCP option. The work looks to IETF for a solution.

11.3.3 ATIS ESIF and NENA

ATIS, ESIF, and NENA are working collaboratively to develop protocols and network architecture for delivering emergency calls to PSAPs. In the i2 and i3 architecture for E9-1-1, NENA is developing stage -1 (user requirements) and stage-2 (FE). ESIF is addressing stage 2 and stage-3 (implementation details).

11.3.4 Open Geospatial Consortium

Open GIS Consortium, OGC's, OpenLS Initiative brings together key industry players to build and consolidate the standards infrastructure for these interoperating location-based software services via Geography Markup Language (GML). The OpenLS mission is to specify standard interfaces and protocols which developers can use to integrate geospatial data and geoprocessing resources into location services and

telecommunications infrastructure and to demonstrate these capabilities for a wide variety of applications for consumers, businesses and governments.

11.3.5 OASIS

OASIS is the principal global body for developing and making available XML based schema for exchanging information. A significant array of government agencies and industry have developed the Common Alerting Protocol, currently in Version 1.1 that includes an ability to bind geospatial information to a CAP message.

11.3.6 EPCglobal

EPCglobal is the worldwide consortium of all the vendors of product codes -- which joined with the AutoID consortium to develop a global means of reading RFID based information, binding information to that object through network based services, and retrieving that information. As part of this activity, means for associating geospatial information with objects were standardized and providing LBS capabilities. Work includes the EPCglobal Architecture Framework and EPC Information Services (EPCIS).

11.3.7 OMA

The OMA mission is to grow the market for the entire mobile industry by removing the barriers to global user adoption and by ensuring seamless application interoperability while allowing businesses to compete through innovation and differentiation.

11.3.8 MAGIC Services Initiative

Mobile/Automotive Geo-Information Services Core (MAGIC) Services Initiative was founded with the goal of defining and promoting open industry specification for delivering navigation, telematics, and related geographic information services across multiple networks, platforms and devices. The MAGIC Services Initiative is a group of companies - TeleAtlas, NavTech, Microsoft, MobileGIS, and others -- defining and promoting the open industry specification for delivering navigation, telematics, and related geographic information services across multiple networks, platforms, and devices. Some of the existing in-car navigation and telematics applications will ultimately prove successful and useful, and will dominate the future of mobile electronic interaction. MAGIC seeks to define a minimal set of generic geo-information services that will be found in these and other mobile Internet ventures. There is significant membership overlap between MAGIC and OGC.

11.3.9 GSM Association

The GSM Association Services Group (SerG) addresses location based services via the Permanent Reference Document (PRD SE.23) on Location Base Services (LBS).

11.4 Identified Gaps

- Location acquisition, verification and dissemination.
- Audio and video applications over IP.
- Real-time monitoring and transmission of emergency data on persons condition to doctors or emergency service facility to/from locations of danger/disaster.

- Personalized and automated emergency calls.
- Location and device sensitive information dissemination.

11.5 Proposed Work Items

Work Item A: Primary: PTSC-SAC
Title: Monitor progress of work in the IETF GEOPRIV WG to develop new DHCP option to convey verifiable location info in access network independent fashion

Recommended Approach:
Monitor

Target Date: Ongoing

12 MULTICAST

12.1 Requirements

Multicast capabilities are required for efficient delivery of some services, but these capabilities are not easy to operate in a multi-provider, multi-infrastructure context. Mechanisms are needed to deploy and operate scalable multicast services supported by a single NGNSP and which span multiple transport service providers.

- One-to-many
- Many-to-many
- Many-to-one

12.2 Function/Service Enabled

One to Many (source specific, unidirectional) multicast services are expected to be required for some instantiations of mass market entertainment services (e.g., IPTV).

12.3 Current Standardization Activities

One-to-many
Streaming services are not likely to be included in release 1 in TISPAN.

Many-to-many
These services are not mentioned in ETSI WI01025 "Service Requirements".

Many-to-one
These services are not mentioned in ETSI WI01025 "Service Requirements". 3GPP has addressed many to one in TS 25.324 Broadcast/Multicast Control (BMC).

12.3.1 IETF

The IETF has a number of groups that have been working on standards in the area of multicast, as a network transport service in the context of both IPv4 and IPv6. A brief listing of the relevant working groups and their published RFCs is provided below. The default IETF model for multicast services is the any source multicast (asm) model, where any source in the multicast group may transmit traffic onto the multicast group -- although there has been some more recent work in the area of source specific work.

While there has been some deployment experience with multicast through the MBONE network, this is primarily restricted to academic institutions and multicast services are typically not available to consumers in commercial residential Internet access services. Guidance for operation of multicast based services is relatively limited; for example, there is only a framework for the potential interactions between MPLS and multicast IP services, rather than detailed specifications.

Multicast Security (msec):

- RFC 3547 The Group Domain of Interpretation
- RFC 3740 The Multicast Security Architecture
- RFC 3830 MIKEY" Multimedia Internet KEYing
- RFC4046 Multicast Security (MSEC) Group Key Management Architecture
- RFC 4082 Timed Efficient Stream Loss-tolerant Authentication(TESLA): Multicast Source Authentication transform Introduction

Multicast & Anycast Group Membership (Magma):

- RFC 3228 IANA Considerations
- RFC 3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
- RFC 3678 Socket Interface Extensions for Multicast Source Filters
- RFC 3810 Multicast Listener Discovery Version 2(MLDv2) for IPv6
- RFC 4286 Multicast Router Discovery

Reliable Multicast Transport (rmt):

- RFC 2887 The Reliable Multicast Design Space for Bulk Data Transfer
- RFC 3048 Reliable Multicast Transport Building Blocks for One-to-Many Bulk-Data Transfer
- RFC 3269 Author Guidelines for RMT Building Blocks and Protocol Instantiation documents
- RFC 3450 Asynchronous Layered Coding protocol instantiation
- RFC 3451 Layered Coding Transport (LCT) Building Block
- RFC 3452 Forward Error Correction Building Block
- RFC 3453 The use of Forward Error Correction in Reliable Multicast
- RFC 3695 Compact Forward Error Correction (FEC) Schemes

- RFC 3738 Wave and Equation Based Rate Control building block
- RFC 3926 FLUTE - File Delivery over Unidirectional Transport
- RFC 3940 NACK-Oriented Reliable Multicast Protocol (NORM)
- RFC 3941 NACK-Oriented Reliable Multicast (NORM) Building Blocks

Protocol Independent Multicast (PIM):

- RFC 3973Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)

MBONE Deployment (MBONED):

- RFC 2365Administratively Scoped IP Multicast
- RFC 2588IP Multicast and Firewalls
- RFC 2770GLOP Addressing in 233/8 obsoleted by RFC 3180
- RFC 2776Multicast-Scope Zone Announcement Protocol (MZAP)
- RFC 3138Extended Allocations in 233/8
- RFC 3171 IANA Guidelines for IPv4 Multicast Address Assignments
- RFC 3170 IP Multicast Applications: Challenges and Solutions
- RFC 3180 GLOP Addressing in 233/8
- RFC 3446Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
- RFC 3956 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

Multiprotocol Label Switching (MPLS):

- RFC 3353 Framework for IP Multicast in MPLS

Source Specific Multicast (SSM):

- RFC 3569 An Overview of Source-Specific Multicast(SSM)

12.3.2 ATIS IPTV Interoperability Forum

The ATIS IIF has started collecting requirements for the IPTV service, and some initial documents to satisfy their issue statements were scheduled for closure in March 2006. While the discussions at the IIF have not yet reached this level of detail, presumably this body would be concerned with service specific issues related to the use of multicast by an IPTV service. Multicast address allocation and binding mechanisms between content (e.g., program guides) and multicast addresses may be examples of such service specific uses of NGN multicast capabilities.

12.3.3 DSL Forum

Work in progress at the DSL Forum (WT101) covers the application of IP multicast in DSL access networks.

12.3.4 Other (non IP) Multicast Fora and Capabilities

There are various Layer 2 protocols of interest to NGN service providers that also provide native multicast capabilities. For example, various PON systems, WiFi and WiMax, Ethernet and some Ethernet derived protocols for home networks (HPNA v3, MoCA, etc.) provide some native multicast capability. The interaction between these native Layer 2 multicast capabilities and an IP multicast service are not always well documented. In some cases, this is referred to as *IGMP snooping* or *IGMP proxy functions*. If the NGN is to be efficient, as well as Layer 2 agnostic, we need standard mechanisms to allow IP to leverage Layer 2 multicast capabilities.

12.4 Identified Gaps

Maintenance and diagnostics associated with the operation of large scale multicast networks. This should include the identification and localization of transport failures or routing failures. Given the secured nature of the content to be delivered over these channels, best practices for assuring the functionality of the multicast service without exposing the content would be useful.

Performance metrics associated with changing the multicast session to which a client is attached:

- NGN based QoS and admission control services are currently mainly concerned with unicast services. This work should be extended to consider the resource impacts of deployment at scale of unidirectional, source specific multicast services.
- The msec work is primarily concerned with prevention of unauthorized access to multicast streams. An area of concern for operators is the potential for multicast based services to be mis-configured or hijacked in ways that could cause denial of service attacks on other network services. This is an area where the potential security vulnerabilities could be investigated further.
- The entertainment services proposed for use over unidirectional (ssm) multicast network services require high reliability that typically assumes some redundancy in the networks to support these services. Interactions between network redundancy mechanisms and multicast services should be investigated further.
- Most IETF applications of multicast assume a public address space. The DSL based applications of multicast for IPTV assume the existence of a residential gateway performing a NATPT function to translate addresses between the public (WAN) and private (LAN) network. There is no standard application layer gateway function to support multicast services through NATPT.
- Traffic measurement and accounting arrangements are often considering the amount of traffic sent on a particular interface. Packet counting is relatively straightforward for unicast services. Packet accounting for multicast services may be somewhat more complex, and be dependent recording additional information regarding the degree of packet replication involved, the location within a multicast tree, etc.

12.5 Proposed Work Items

The IIF should review the identified gaps for an assessment of whether these are being addressed by the current IIF work program.

13 ADDRESS RESOLUTION (E.164/SIP)

13.1 Requirements

The NGN has the following requirements for address resolution:

- The NGN must:
  - Translate from an E.164 number to a SIP URI for routing within an IMS/SIP network.
  - Correct for number portability, unambiguously, even when legacy and NGN mechanisms co-exist.
  - Identify appropriate NGN interconnection points (SIP/IP), whether session was initiated with an E.164 number, or a SIP URI.
  - Provide unambiguous guidelines for the use of User, Infrastructure and Private ENUM.
- The NGN should:
  - Identify the optimum PSTN breakout point for calls that terminate on the PSTN.
  - Establish extensible address resolution capabilities that support new services.

13.2 Function/Service Enabled

An NGN address resolution capability will allow NGN sessions to be initiated with either an E.164 number or a SIP URI. Numbers will be corrected for number portability whether the call terminates or originates on the NGN or on the legacy PSTN. It will enable direct, secure (SIP) interconnection of NGN networks.

13.3 Current Standardization Activities

13.3.1 ATIS

- PTSC-SAC Issue Number S0025: **NNI Numbering and Routing Capabilities and Procedures**
  - PTSC-SAC-2005-284R1
  - PTSC-SAC-2005-378
- Industry Numbering Committee (INC)

13.3.2 IETF

- ENUM WG
- Infrastructure ENUM

13.3.3 ITU-T

The ITU-T work on address resolution is being carried out in SG2, SG11, and SG17. SG11 has initiated a project to define NNI for NGN. This relates directly to the corresponding work in ATIS PTSC-SAC.

13.3.4 ETSI

TISPAN has initiated activity within Working Group 4. Documents include:

- ETSI TR 102 055, "ENUM scenarios for user and infrastructure ENUM," 3 May 05
- ETSI TR xxx xxx, "Interconnect issues related to Numbering Naming and Addressing (NAR)." Draft available as Work Item 04006
- ETSI TS 102 172, "Minimum requirements for interoperability of ENUM implementations," 26 April 05

13.3.5 EIDQ

EIDQ is the industry maintaining consortium for the E.115 standard.

13.4 Identified Gaps

13.4.1 ENUM

Basic resolution protocol mechanism standardized as RFC 3761.

13.4.2 VoIP Interconnection

PTSC-SAC is currently working on standardization of an NNI to support VOIP interconnection (Issue number S0025). This work is closely following the standards work in IETF ENUM (Infrastructure ENUM) working group. Once the IETF WG completes standardization, it is expected that PTSC-SAC will align with this work if possible. To provide the required functionality until IETF standards are complete, PTSC-SAC is defining interim mechanisms. ITU-T SG11 has recently started work on an NGN NNI based on the work being done in PTSC-SAC.

13.4.3 Number portability correction

It is assumed that ENUM mechanisms will be number portability corrected.

13.5 Proposed Work Items

PTSC and INC need to be engaged in implementations that satisfy industry and government requirements as they emerge. At this time existing Issue statements address all known requirements, and no additional work items are required.

14 DIGITAL RIGHTS MANAGEMENT

14.1 Requirements

Digital Rights Management (DRM) represents a range of techniques that use information about rights and rights holders to manage copyright material and the terms and conditions on which that material is made available to users. The NGN should permit DRM techniques to ensure the legal rights of all stakeholders of the content in the NGN including creators, producers, publishers, traders, and receivers. DRM is an application layer enabler and should not affect the NGN transport. The NGN may provide authentication or location information to a DRM application.

The NGN service provider may make content available through a DRM system. This NGN DRM requires all contents to be not only systematically identified, but also the information about their legal rights holders and their legal rights associated with the contents faithfully recorded. The NGN DRM uses copyright protection techniques such as encryption, digital watermarking, and digital signatures to ensure these rights are lawfully enforced. To facilitate wide scale adoption, the use of the NGN DRM must be relatively easy. In most cases, the users should not be aware of the DRM system until they attempt unauthorized access to the content in the NGN. Also, different methods of payment should be offered under the NGN DRM. As digital transactions may involve small volumes of material, there will be a need for efficient and cost-effective payment methods such as micro-payments. The NGN DRM should not restrict private fair use of copyrighted material. Neither should it restrict copying of material for personal use by the user (e.g., making backup copies). It should facilitate the ability for the user to be able to use the content on multiple personal devices.

The NGN DRM services do not restrict applications from providing their own DRM mechanisms. Other NGN capabilities (e.g., network security capabilities such as authentication) may also be useful to application DRM mechanisms.

14.1.1 Top Level DRM System Objectives

DRM systems are closely related to copyright laws/treaties and content protection and management. DRM systems can impact the privacy interests of users/subscribers, and can impact usability by users/subscribers. Thus the following high level objectives provide the context and framework for IPTV DRM systems:

1. The DRM system shall be consistent with all applicable laws and treaties (e.g., Digital Millennium Copyright Act [DMCA]).
2. The DRM system shall provide for appropriate content usage controls (e.g., copy controls) by the service provider and content owner.
3. The DRM system shall provide for appropriate content usage flexibility (e.g., private fair use) by the user/subscriber.
4. The DRM system shall provide for a secure environment such that threats to content ownership and management (e.g., content theft or pirating) are eliminated or reasonably mitigated.

5. The DRM system (in conjunction with other NGN components) shall not compromise the appropriate privacy interests of users/subscribers.
6. The DRM system functions should generally be transparent to the user in that the user should generally be unaware of the DRM functions under normal situations; however under user-observable restriction of rights instances (e.g., a user attempt to make an inappropriate copy of content), the DRM system functions (in conjunction with subscriber management system and user interface) shall provide for usability (e.g., notices, guidance, interactions, etc.) that have the following characteristics:
    a. The DRM usability provided to the user/subscriber shall be generally user friendly and easy to understand, and shall be characterized as simple, clear, direct, manageable, practical and non-technical.
    b. DRM interactions with user/subscriber should not cause misunderstandings and thus should not induce the user/subscriber to invoke follow up (service provider) customer care interactions based on user/subscriber misunderstandings.

From the objectives listed above it is clear that the NGN DRM system is related to and impacts other key areas (e.g., subscriber management).

14.2 Overview of existing relevant specifications

DRM is a major issue in the industry, and possible solutions are being worked in multiple industry forums. The following are organizations or groups that have developed or are developing relevant specifications:

- OMA (http://www.openmobilealliance.org)
- DVB Project - Content Protection and Content Management (http://www.dvb.org)
- ISO (http://www.iso.org)
- ETSI (http://www.etsi.org)
- IETF MSEC (http://www.ietf.org/html.charters/msec-charter.html)
- ATIS IIF DRM Task Force

Prior work on DRM interoperability includes the following:

- Leonardo Chiariglione's – the DMP: IDP & List of TRUs
- The work of the Coral Consortium - NEMO - Service provider architecture.
- The ATIS IIF DRM TF will examine the NEMO Functionality Mapping onto DRM Basic Reference Model.

14.2.1 DRM in the Context of NGN

For the planning period that is the scope of this document (i.e., standards available by EOY 2007 for implementations 12, 18, or 24 months thereafter), DRM systems in an NGN environment are expected to be service and application specific (e.g., DRM for IPTV). This is not to say that there will not be commonality of technology and underlying standards in service/application specific DRM systems. However, services/applications

are expected to drive DRM solutions during the planning period in question, given the tight coupling of services/applications with DRM.

In order for the NGN to accommodate DRM systems for a variety of service and applications, the following capabilities must be provided.

The NGN (and/or NGN based platform) shall support:

1. The ability to route broadcast content through the NGN DRM encryption component for encryption;
2. The ability for the DRM encryption component to access the clear video-on-demand content for encryption;
3. The ability for the DRM components to upload encrypted video-on-demand content to a video-on-demand server;
4. The ability to exchange rights and keys between the DRM management component on the head-end and the DRM component hosted on the NGN terminal using IP (both UDP and TCP);
5. The ability to securely download a DRM component to the NGN terminal; and
6. The ability for the DRM components to securely communicate between each other and also to the other middleware components on the head-end.

The NGN based terminal shall support:

1. The ability to host a downloadable DRM component;
2. The ability to uniquely identify the NGN terminal to the DRM components;
3. The ability to provide secure non-volatile memory to the DRM component;
4. The ability to provide a secure processing environment to the DRM component; and
5. The ability for the DRM component to control the anti-taping/anti-copying on the output if the NGN terminal.

From a NGN perspective (as an enabler), gaps in the above listed capabilities will be create issues regarding NGN accommodation of DRM systems as discussed below.

14.2.2 NGN DRM Standards/Technology Gaps (for Standards available by EOY 2007)

No gaps have been identified from a generic NGN enabler perspective to date (for the planning period in question). However, it should be noted that there are significant service/application specific DRM standards works in progress (e.g., IPTV DRM standards). In addition, it is expected that more and more commonality of technology and underlying standards in service/application specific DRM systems will occur as the NGN evolves.

14.3 Proposed Work Items

From a DRM commonality perspective (not NGN per-se), the following standards work areas can be seen:

- Guidelines regarding subscriber fair-use and privacy; this would give service providers and vendors some level of guidance regarding these sensitive issues.
- Lack of a widely-accepted common rights expression language.

These common DRM areas are important but are generally independent of NGN standards (for this planning period). Thus, from a service/application independent NGN perspective, there are no new standards work items regarding DRM. In addition, the previously noted significant service/application specific DRM standards work items that are planned by industry forums and standards bodes (e.g., IIF) should be monitored.

15 USER CONTROL OF PROFILE/SERVICES

This section relates to providing the end user with control over the services that they subscribe to. As previously noted in Section 2, Unified User Profile, the personal profile is the cornerstone of an end-user-centric world. Beyond the creation of a unified user profile is the need for the end user to enact control over that profile and service subscriptions.

15.1 Requirements

15.1.1 3rd Party Access

A list of business requirements for third-party access relates to the need to benefit from a single user profile, even when this user is not on the home network of the service provider**:**

1. End-users should be able to access their services through a simple access and service authentication process.
2. Service providers must be capable of securely accessing specific user profile information (e.g., preference settings) from different networks.
3. The NGN should support flexible consolidated collection of settlement information, such as usage. For example, all services for an end-user may be charged through a single bill for postpaid, or a single account for prepaid, for seamless roaming services between access types such as mobile access and wireless broadband access.
4. Service providers must also be capable of collecting user information from different access networks to the service providers' home network (e.g., location information).

Another set of business requirements relate to the challenge of delivering the same service from the service provider who owns the end-user profile (including the service subscriptions) over a third party access network:

1. Communication services must be delivered from any access network or technology to any other access network or technology.
2. Application and content services must be delivered from the Service Delivery Environment to any access network.
3. The solution architecture must accommodate different types of mobility between access networks (e.g., nomadic services, roaming seamless handover, etc.), depending on the service providers' offering and interconnection relationships.

Business requirements that relate to the handling of the different access characteristics are inherent to each access medium (e.g., DSL broadband versus wireless 2.5G):

1. Services must be adjusted to fit the terminal and media characteristics of each access network (e.g., bandwidth, QoS).
2. Where necessary, different session related control protocols in access networks must be interworked with SIP in the NGN core.
3. QoS and security (data integrity, data confidentiality, network security) must be maintained from a user viewpoint (or managed within the constraints of different technologies) across the access networks and the NGN core.
4. The end-to-end service instance may span access networks that are independently administrated by separate service providers or use different technologies.

15.2 Function/Service Enabled

Functions enabled include single sign on, location based services, 3rd party applications, mobility and nomadicity. See also the related functions and services enabled by unified interfaces, personal profiles, and service ubiquity as noted in Section 2.

15.3 Current Standardization Activities

15.3.1 ETSI

While there are no explicit requirement for user control of profiles and services in the WI01025 R1 Service Requirements, it does assume that users can subscribe to services which may allow them to set up preferences. Also, the DT supplementary services include an interface to control the service. It is not clear, however, that DT supplementary services will actually be complete in R1 given issues such as "what is network determined user busy?" in the NGN.

15.3.2 3GPP

- IP Multimedia (IM) session handling; IM call model; Stage 2
  Spec No. - 3GPP TS 23.218 V6.3.0 (2005-03)
- IP Multimedia Subsystem (IMS); Stage 2
  Spec No. - 3GPP TS 23.228 V6.12.0 (2005-12)

- IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents
  Spec No. - 3GPP TS 29.328 V6.8.0 (2005-12)

15.3.3 ATIS

The following work is in progress in ATIS committees and should be reviewed for relevance and impact to the User Control of profile/services requirements. Based on the issue description, the work may impact the implementation of a user profile. Additional investigation is needed.

PTSC

- Create a Generic Control and Signaling Plane Standard
  Subgroup: SEC
  Issue # S0004

- Create a standard defining the NNI for IP-IP Network Interconnection Supporting Multimedia Services
  Subgroup: SAC
  Issue # S0009

- US Standard For IP-IP Network Interconnection - Roadmap Standard
  Subgroup: SAC
  Issue #S0028

- End to End User Authentication and Signaling Security
  Subgroup: SEC
  Issue #S0033

15.4 Identified Gaps

The enablers required for users to access their services from a foreign network are defined at a high level by the specifications listed in 15.3.2. For example, IMS, Stage 2 (Spec No. 3GPP TS 23.228 V6.12.0) describes the support of roaming users. The specification could be improved by adding further description of how visiting network applications, such as location, are federated between the two networks. This is not a service offered by the visiting P-CSCF as with QoS, and the use of Parlay OSA for this function requires non-standard integration between the visiting network P-CSCF and Parlay service to determine authorized endpoints.

15.5 Proposed Work Items

Work Item A: Primary: PTSC-SAC
Title: Define standard inter-service provider interconnect methods that specify federated service and profile data.

Business Need:

Home service providers will want to receive location information from the visited network.

Recommended Approach:

Standards should be developed that define the data or services provided by and to the visited network for roaming users. These future groups will use existing service enablers in a structured way to improve and speed interconnect between carriers. The relevance of related work in OMA, Liberty Alliance, and others should be considered. This work can potentially be included in either Issue S0009 or S0028.

Target Date: 4Q2006

16 MEDIA RESOURCE FUNCTIONS

16.1 *Requirements*

Media resources in the NGN provide many roles in conjunction with traditional voice processing services and user interactions via voice and DTMF. These are expanded in the NGN with new data, video and content services. *Media Servers (MS)* are network elements providing the media resource functions such as:

- Recorded and composed announcements
- Interactive voice response
- Audio recording
- Voice mail
- Advanced speech recognition
- Text to speech
- Audio conference bridge
- Video/data bridges
- Media forking
- Media insertion (e.g., image, text, video) in multimedia stream
- Content caching/hosting/serving
- Transcoding

MS terminate media streams using standard signaling interfaces, and interact with the media session under programmatic control of application functions. The application functions typically reside in Application Servers (AS) external to Media Servers. An AS can invoke call control and media control functions in a MS using open industry standard interfaces/control languages such as SIP, H.248 and W3C VoiceXML and CCXML.

16.2 Function/Service Enabled

Services enabled include conferencing, pre-paid or calling card calling, voice-activated dialing, unified messaging, toll-free calling, and network gaming.

16.3 Current Standardization Activities

16.3.1 Media Resource Function Architectures

There is not a single standard media resource function architecture that is collectively agreed upon by ATIS, ITU-T, and 3GPP. This section describes current status and planning directions for those forums, and also the IETF where there is related work going on. 3GPP IMS is described first, because that serves as an underlying basis for the ITU-T and ATIS specified NGNs. In any case, the topic of media resource function architecture is a work in progress.

16.3.1.1 3GPP

The architecture concerning the Multimedia Resource Function in 3GPP is specified in TS 23.228 and presented below.

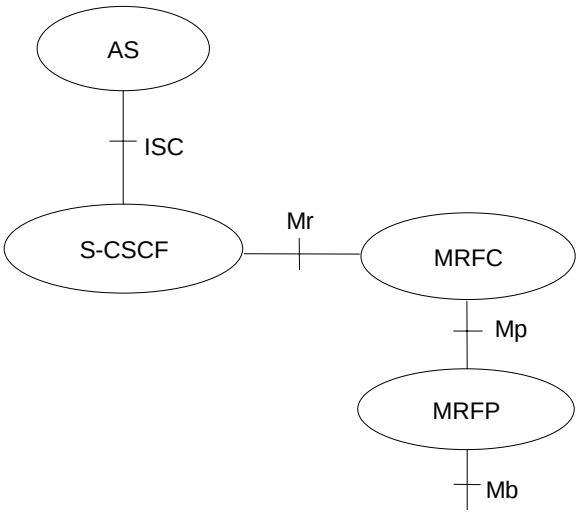

Figure 5: 3GPP Architecture of MRF

The MRF is split into Multimedia Resource Function Controller (MRFC) and Multimedia Resource Function Processor (MRFP). In this architecture, there is no functional element or collection of elements that is referred to as a "Media Server."

The protocol used for the Mr reference point is SIP, as defined by RFC 3261, other relevant RFCs and additional enhancements have been introduced to support 3GPP´s needs.

The Mp reference point allows an MRFC to control media stream resources provided by an MRFP. The Mp reference point is fully compliant with the H.248 standard.

MFRC may be made available directly to a UE for cases like ad-hoc multi-party sessions initiated by the UE. In addition, the MRFC/MRFP resources may also be used, based on service control in an IMS network, for services such as multiparty sessions,

announcements, or transcoding. In this case, an Application Server interacts with an MRFC. Session control messages are passed between the AS and the MRFC via the S-CSCF.

There have not been any recent contributions on media resource management related to the MRF in 3GPP. The view in 3GPP is still that an MRFC function controls and allocates the media resources for a service on one or many MRFP's.

A work item has just been approved in the 3GPP protocol group -- CT1 -- to define a media server control protocol to be used between the AS and the MRF. The work proposes to study protocols such as those discussed below in the IETF work. At the time of this publication, there has been agreement on this work item, but it has not yet been formally approved. There may be architectural impacts identified during this work.

One final area in 3GPP that has not yet been defined is how an AS locates an MRF. In 3GPP, although a user's services, signaling, and associated application server or servers are invoked in a users home network, user's may use MRF resources in a visited network (e.g., to perform transcoding).

16.3.1.2 ITU-T

The items that are currently in the ITU-T NGN description that are in addition to or different from the 3GPP media resource function architecture are:

a. the addition of a Media Resource Broker (MRB[25]), with an interface to the AS (introduced through the PTSC). The MRB assigns a Media Server to provide specific media resources to Application Servers as required, for the purpose of more efficient utilization of shared media resources, and
b. an interface between the AS and MRC-FE (i.e., the 3GPP MRFC).

3GPP is developing an H.248 profile for Mp, incorporating existing H.248 packages developed by ITU-T SG16.

The work within ITU-T is currently in the form of draft Recommendations, which have not yet been consented to.

16.3.1.3 ATIS

The PTSC-SAC was the source of the work on the MRB in the ITU-T and aligns with the description there. Work within the PTSC-SAC on MRB has included the following, all of which was shared with the ITU-T FGNGN:

[25] The term MRB is used in the ITU-T and so we will use it throughout this section. It may be useful to the reader to be aware that work done on that topic within the ATIS PTSC-SAC used the term Media Server Resource Broker (MSRB).

- requirements that the use of MRB needs to support,
- how MRB works in a call flow, and
- what kind of information MRB receives through an operations-type interface.

The PTSC-SAC view of the NGN also identifies the 'Media Server' as the combination of the control part of the 3GPP MRFC[26] with the MRFP.[27] The PTSC SAC has also identified SIP as the basis for AS-MS interaction.

16.3.1.4 IETF

The XCON WG, with other work from the SIPPING WG, is developing a centralized conferencing framework (focus, participants, conference server, etc.) and a common conference data model (represented by the "Conference Package" XML schema), a Binary Floor Control Protocol, and a Centralized Conference Control Protocol. The IETF conferencing framework decomposition and scope differs from any of the 3GPP IMS, ITU-T NGN or ATIS NGN architectures, and where there is commonality, there is no official mapping defined. ATIS may continue to reference the IETF work, as it deems appropriate, to progress its NGN MRF definition.

A proposal is being developed for the use of SIP to create an AS-MS communication channel over which control protocols would run.[28] There is also an associated activity underway to specify 'control packages' (i.e., control protocols) for different types of general applications, the first being for IVR.[29]There is also work attempting to define a single AS-MS control protocol for sophisticated conferencing applications; eventually leading to a formal Media Control BOF.[30] These informal activities are expected to lead to a formal Media Control BOF, which in turn could either result in establishing a new WG or extending the XCON or other WG charter.

16.3.2 Control Protocols/Languages for Media Resource Function

The table below lists the current predominant AS-MS control protocols/languages. There is no consensus on the need to specify a single AS-MS control protocol to support all applications. Some believe it is better to have specific control protocols for each fundamentally different application domain such as IVR, conferencing, and sophisticated speech.

---

[26] MRFC is aggregated with MRFP into the MS, in the sense of local and granular control. However, from a service-level point of view, it is still an AS that controls the MS.

[27] See PTSC Issue S0018.

[28] A Control Framework for the Session Initiation Protocol (SIP) – draft-boulton-sip-control-framework.

[29] An Interactive Voice Response (IVR) Control Package for the Session Initiation Protocol (SIP) – draft-boulton-ivr-control-package.

[30] Media Control Protocol Framework – draft-dolly-xcon-mediacntrlframe).

Table 4: AS-MS Control Protocols/Languages

Control Protocol/Language	Application Area	Status (all of these are implemented in vendor products)	Comments
VXML	▪ Announcements ▪ IVR ▪ Simple speech recognition ▪ Simple text to speech ▪ Simple conferencing	W3C Standard	
H.248/MEGACO	▪ Announcements ▪ IVR ▪ Simple conferencing	IETF Proposed Standard RFC 3525	Really designed for Media Gateway control
MGCP	▪ Announcements ▪ IVR ▪ Simple conferencing	IETF Informational RFC 3435	Really designed for Media Gateway control; predecessor of H.248
MSCP	▪ Announcements ▪ IVR ▪ Semi-sophisticated conferencing	IETF individual internet draft (work in progress)	This is a relatively recent internet draft.
MSCML	▪ Sophisticated audio conferencing	IETF individual internet draft (work in progress)	Can work with VXML
MSML/MOML	▪ Sophisticated audio conferencing	MSML: expired IETF individual internet draft (withdrawn by IETF); MOML: IETF individual internet draft	Can work with VXML
MRCP[31]	Sophisticated speech processing ▪ Speech recognition ▪ Speaker verification ▪ Text to speech ▪ Recording	IETF WG internet draft (Speechsc WG)	Uses W3C markup languages. MRCP may also run from one MS to a "Speech Server"

SIP "NetAnn"	▪ Announcements ▪ IVR (pointer to) ▪ Simple conferencing	IETF Informational RFC 4240	NetAnn identifies to the MS the basic type of function that the MS should perform (announcement, IVR, conferencing). The level of AS-MS 'control' provided by NetAnn is relatively limited. For IVR, there is a pointer to a VXML script. For conferencing, there is a Conference ID passed.

All of the above listed protocols/languages are generally undergoing continued extension/expansion/evolution. MSCML and MSML/MOML address the same application space – sophisticated conferencing – and are competing protocols, which is undesirable from a standards point of view. Work is under way to extend both to support multi-media conferencing. CCXML is a language that gets executed in the AS, or as some may argue possibly in the MS. It has not passed to the MS in any control protocol as of yet.

16.4 Identified Gaps

The capability set supported by Media Servers support is in a state of ongoing extension and evolution, as well as the corresponding work on the AS-MS control protocols/languages (e.g., video conferencing, Baudot tone user input, more speech grammers, more codecs, etc.). A specific list of desired future MS capabilities is not provided as no particularly pressing needs for specific MS functions have been identified at this time. However, the overall architectural context and the specific protocols within that architecture are an area of active discussion, with no obvious consensus yet.

As stated above, MRB has been introduced through PTSC into the ITU-T NGN. That concept needs to be solidified as the ITU-T NGN work progresses. There have been alternative views expressed in the industry about how MRB might work that do not meet all of the identified service provider needs.

Additionally, there especially needs to be closure on:

- a single standard AS-MS conference control protocol - continue to help progress this work in the IETF (currently the informal group of IETF participants mentioned above);

- the AS-MRB protocol – proposed to be worked in the PTSC-SAC and then brought to the ITU-T; the likelihood is that an existing protocol would be used (e.g., http or SIP) to pass information, but the structure and scope of the information passed also needs to be defined (The latter might possibly be addressed in the IETF.); and
- the details of how to establish an AS-MS control channel – continue to monitor/ help progress this work in the IETF, and have this concept reflected in the NGN architecture.

Finally, the work on AS-MS control protocols/languages -- which is largely being done in the IETF and W3C -- should be monitored, with the intent to discourage any unnecessary multiplicity of such interfaces within each of the various fundamental application domains.

16.5 Proposed Work Items

All of the work in the Media Resource Functions area should be part of the ITU-T NGN global standard, either directly or by reference, and not just as a national standard. In ATIS, addressing gaps in this area and/or and influencing related work in other SDOs/forums falls within the charter of the PTSC-SAC.

It is proposed that the following work items be carried on under the existing PTSC-SAC Issue S0018 "NGN Architecture Technical Report." A contribution to the March 2006 PTSC-SAC meeting will confirm that Issue S0018's scope is appropriate for this work. The business need is for more efficient sharing of MS resources across multiple Application Servers and the use of a reasonable and standard set of AS-MS protocols.

Work Item A: Primary: PTSC
Title: AS-MRB interface specification

Recommended Approach:
Recommendation for the basic AS-MRB interface protocol

Target Date: 3Q2006

Work Item B: Primary: PTSC
Title: AS-MRB interface information content and structure

Recommended Approach:
1) Define requirements for the information payload content of the AS-MRB interface.
2) Initiate work in the appropriate SDO (TBD) to define payload structure.

Target Date: 1) 3Q2006, 2) 4Q2006

Work Item C: Primary: PTSC
Title: AS-MS interface rationalization

Recommended Approach:

Contribute to the outcome of a rational set of AS-MS protocols (standard, few in number, meet services needs, technically sound, etc.).

Target Date: Ongoing

In advancing this work, the PTSC-SAC should work with the appropriate SDOs/forums, especially the ITU-T NGN effort, the 3GPP IMS effort, and the ATIS Wireless Technology and Systems Committee (WTSC), to align/harmonize to a single media resource function, architecture, and protocols/languages view. Additionally, the ATIS PTSC should liaise to and work with the ATIS IIF to identify and address MRF gaps with respect to IPTV, as the work on IPTV in the IIF progresses.

17 GROUP MANAGEMENT

Network resident group management mechanisms are fundamental to the NGN. Group management systems provide Service Provider subscribers the ability to establish and maintain group lists, while promising access to those lists from a complete suite of end user devices and applications.

17.1 Requirements

a. Group management systems shall provide the ability for users to create groups that can be utilized in context of different services. There are several roles within group management, most notably group administrators, group members, and additional entities or parties that may leverage the groups.
b. Group members shall consist of member identification properties, such as globally unique addressable identifiers. The NGN Group Management systems shall provide the capability to associate properties for each group members, such as member rights indicating what action the member can perform
c. Group members or authorized users shall be able to subscribe to different events concerning the group. For example, if an event occurs that entities are interested in, the event shall trigger a notification to the respective member or user.
d. NGN Group lists shall include group identifiers, group specific information, group properties such as group visibility and duration, and conceivably could include specific information that may indicate how the group should be used for a specific service.
e. Group management systems shall support various aspects to define how lists are leveraged within specific services. As examples, “Accept”, “Reject”, and “Politely block” are authorization policies that shall be supported.
f. Group management systems shall provide capabilities in a secure manner. When appropriate, systems shall authenticate and authorize users and/or applications

accessing the group content. Detection of fraudulent or unauthorized activity shall be supported.

g. Group management systems shall provide collection of accounting data necessary to support various methods of charging, such as pay per transaction or volume based charging. The data collection and transmission of accounting data by the group management system should be sufficient to support both Offline and Online charging models.

17.2 Function/Service Enabled

a. Instant Group Communication (audio conferencing, IM, keyboard chatting, content sharing sessions) Enablement
Instant Communication Services that can be invoked to multiple parties will leverage the group management system**.**
b. Store and Forward Messaging Enablement (e.g., email, SMS, etc.)
Establishing email communication via Group Lists is common today, and will be supported as part of the Next Generation Network**.**
c. Presence Enabled via Group Management: XDMS – {OMA definition}
Presence Enabled XDMS stores subscription authorization and presence content authorization XML documents. These documents may be accessed by end user clients or Presence Servers.
d. PoC Enabled via Group Management: XDMS {OMA definition}
PoC Enabled XDMS stores PoC Groups and PoC User Acess Policy. These documents may be accessed by end user clients, PoC Servers, and other application servers.
e. Shared Groups: XDMS {OMA definition}
A Shared XDMS condition may be specified and stored in a URI list. Each URI list contains a collection of URIs that may be shared by multiple end users or resources.

17.3 Current Standardization Activities

17.3.1 OMA

- OMA XML Document Management Architecture OMA-AD-XDM-V1_0-20060110-C January 2006
- OMA XML Document Management (XDM) Specification OMA-TS-XDM_Core-V1_0-20060110-C January 2006
- OMA Shared XDM Specification OMA-TS-XDM_Shared-V1_0-20060110-C January 2006
- OMA Resource List Server (RLS) XDM Specification OMA-TS-Presence_SIMPLE_RLS_XDM-V1_0-20051122-C November 2005.
- OMA Presence XDM Specification OMA-TS-Presence_SIMPLE_XDM-V1_0-20051122-C November 2005
- OMA XML Document Management Requirements OMA-RD-XDM-V1_0-20050317-C March 2005
- Push-to-talk over Cellular (PoC) Architecture, v2.0.8, June 2004

- Push-to-talk over Cellular (PoC) List Management and Do-not-Disturb, v2.0.6, June 2004

17.3.2 IETF

- IETF The Extensible Markup Language (XML) Configuration Access Protocol (XCAP), draft-ietf-simple-xcap-05, November 2004
- IETF Extensible Markup Language (XML) Formats for Representing Resource Lists, draft-ietf-simple-xcap-list-usage-05
- IETF An Extensible Markup Language (XML) Document Format for Indicating Changes in XML Configuration Access Protocol (XCAP) Resources draft-ietf-simple-xcap-package-03, July 2004
- IETF A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages October 2004
- IETF A Framework for Session Initiation Protocol User Agent Profile Delivery, draft-ietf-sipping-config-framework-05, October 2004
- IETF RFC 3856 A Presence Event Package for the Session Initiation Protocol (SIP), August 2004
- IETF A Document Format for Expressing Privacy Preferences, draft-ietf-geopriv-common-policy-04.txt, February 2005
- IETF Presence Authorization Rules, draft-ietf-simple-presence-rules-02.txt, February 2005
- RFC 3265 SIP Specific Event Notification, June 2002
- RFC 2617 HTTP Authentication: Basic and Digest Access Authentication, June 1999
- RFC 2818 HTTP over TLS, May 2000

17.3.3 ETSI / 3GPP

- ETSI TS 122 250 V6.0.0 (2002-12) Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS) Group Management; Stage 1

17.4 Identified Gaps

Based on the current definition of NGN Group Management, no gaps have been identified relative to industry coverage of the Group Management domain. It is recommended that ATIS and its member companies participating in these initiatives continue to monitor and influence appropriate OMA, IETF, and 3GPP groups that have been established to cover this domain.

17.5 Proposed Work Items

Work Item A: ATIS staff to identify and initiate the mechanism to monitor and influence this area.

Target Date: Ongoing

18 EMERGENCY RELATED SERVICES

Emergency Telecommunications Service (ETS) and Next Generation 9-1-1 (NG9-1-1) services are distinct and separate services in support of, responding to and resolving emergency events in an NGN based telecommunications environment. The same NGN infrastructure is able to support both services. A general description of these services is as follows:

- ETS requires priority treatment in the IP network infrastructure in support of National Security/Emergency Preparedness (NS/EP) communications. ETS has capabilities to increase the probability of successful completion of calls, sessions, or other communications, initiated by government authorized users over the public network infrastructure. ETS also includes legacy circuit-switched NS/EP services such as Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS). ETS provides government-authorized users priority telecommunication services in support of management, control and recovery operations during emergency events where telecommunications congestion may be high due to unusually high general usage and/or diminished telecommunications capabilities due to damage or loss.
- NG9-1-1 service allows the general public to access and communicate with appropriate (e.g., local) Public Safety Answering Points (PSAPs) and corresponding first responders (e.g., police), by using an address (e.g., 911 or other special user enterable address or identifier for non-PSTN emulated services).

The following two sections describe the ETS and NG9-1-1 Service standards work plans.

18.1 Emergency Telecommunications Service (ETS)

The NGN Framework will facilitate the creation of ETS that will significantly enhance the nation's safety. In particular, the NGN is envisioned to enable improved communication between and among the government-authorized users from agencies charged with the protection of citizens, as well as calls originated by government-authorized users. While E9-1-1 (and NG9-1-1) concerns itself with enabling a caller to contact local authorities and government agencies via PSAPs and first responders during an individual or public emergency situation, the NGN Framework will provide priority ETS calling by government authorized users during an emergency crisis or catastrophic event utilizing ETS capabilities.

Providing government-authorized users with priority access and calling service during an emergency crisis, regardless of the type of communications device or network access used, is critical. To ensure that only authorized users can have access to the ETS, and to protect network resources from excessive use or abuse, the NGN must support appropriate authentication and authorization mechanisms. In general, these mechanisms should be as robust as possible. The authorization mechanisms should also be flexible enough to provide various levels of restriction and privilege as needed.

As NGN capabilities supporting user and device nomadicity/mobility increases, it shall be possible to: (a) support ETS in such environment; and (b) utilize these NGN capabilities to ensure subscribers can be contacted easily and quickly at any time. The capability to contact important public officials and key industry leaders, regardless of where they might be or which network they might be on, can also significantly improve our nation's ability to respond during an emergency crisis, or catastrophic event.

18.1.1 Requirements

ETS requirements and standards are currently under development in ATIS committees (e.g., PTSC, PRQC and TMOC), and others to provide services somewhat analogous to the GETS deployed in the PSTN.

The NGN Framework consisting of architecture, protocols, and network elements shall be highly resistant and resilient to denial of service attacks or other types of harm that might be perpetrated on the NGN by terrorists or miscreants. Implicit in the idea that the NGN will provide an efficient and improved ETS is the notion that the NGN itself is secure, robust, and constantly available for use during an emergency crisis, although it may experience congestion, thereby requiring priority calling treatment for ETS.

18.1.2 Current Standardization Activities by Organization

18.1.2.1 ATIS

TMOC

TMOC has one significant standard, *T1.202-2004 - Internetwork Operations - Guidelines for Network Management of the Public Telecommunications Networks under Disaster Conditions*, along with a recently created supplement with includes IP networks. A new revision to this standard is underway that will incorporate NGN concerns.

PTSC

PTSC developed a standard, *T1.628-2000 (R2005) - Emergency Calling Service*, that was revised in 2005. In addition, PTSC has a number of active issues on ETS and has developed or is in the process of developing the following standards and technical reports on ETS over the past four years:

- Issue S0010: Create an Addendum to T1.679
- Issue: S0016: Support of ETS in IP Networks
- Issue S0041: Support of ETS in IP Networks – Phase 2
- Revision of ANSI T1.631, SS7 HPC Network Capability (Pre-publication)
- Technical Report on Service description of ETS (Pre-publication)
- Standard on ETS (Pre-publication)
- Standard on Support of ETS in IP Networks (Under Letter Ballot)

PRQC

PRQC has two active issues on ETS and has issued one standard and 5 Technical reports directly relevant to ETS:

- Issue: A021 Revision of T1.TR.79-2003 "Overview of Standards in Support of Emergency Telecommunications Service (ETS)" (Revision in Progress)
- Issue: A019 "Requirements for ETS Authentication in Multiple IP-based Service Domains" (In Progress)
- ATIS-0100001.2004 User Plane Security Guidelines And Requirements For ETS (Published)
- ATIS Technical Report "Availability and Restorability Aspects of Emergency Telecommunications Service (ETS)" (Pre-publication)
- T1.TR.84 "IP Network Traffic Priorities and ETS" (Published)
- "User Plane Priority Levels for IP-Based Networks and Services," ATIS/PRQC Draft Technical Report (Pre-publication)
- "Service Restoration Priority Levels for IP Networks,"ATIS/PRQC Draft Technical Report (Pre-publication)

NIIF-NIOC

- Issue #0258: "National Security/Emergency Preparedness (NS/EP) calls may encounter difficulties when some portion of the call is served by VoIP technology"

18.1.2.2 IETF

The IEPREP (Internet Emergency Preparedness) and SIP working groups have issued the following RFCs on ETS and GETS:

- RFC 3487, "Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP)
- RFC 3523, "Internet Emergency Preparedness (IEPREP) Telephony Topology Terminology"
- RFC 3690, "IP Telephony Requirements for Emergency Telecommunication Service"
- RFC 3689, "General Requirements for Emergency Telecommunication Service "
- RFC 4190, "Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony"
- RFC 4412, "Communications Resource Priority for the Session Initiation Protocol (SIP)"
- RFC 4375: Emergency Telecommunications Services (ETS) Requirements for a Single Administrative Domain

In addition, a number of Internet-Drafts are under development, such as:

- "TRIP Attribute for Resource Priority", draft-carlberg-trip-attribute-rp-00.txt, (Internet Draft, September 15, 2005)

18.1.2.3 ITU-T

Recommendations I.255.3, E.106 (IEPS), and H.460.4 cover ETS requirements for the International Emergency Preference Scheme (IEPS) for disaster relief operations. SG 11 has approved a signaling requirements document and amendments to a number of protocols (ISUP, BICC, DSS2, and AAL2) for supporting IEPS. SG2 is in the process of developing E.ets that provides a description of ETS and interconnection of ETS national implementations. SG11 and SG13 have initiated or are in the process of initiating requirements and protocol work for supporting ETS in NGNs. SG16 has completed H.460.4 and is in the process of initiating additional work in support of ETS in H.323 systems.

18.1.3 Identified Gaps

As illustrated by the standards work currently underway, ETS is receiving extensive attention in ATIS, IETF, and ITU-T.

The main issues to address are:

a. User equipment signaling to the NGN that a call should have ETS priority, and signaling between various NGN network elements for supporting ETS;
b. Authentication and authorization of the caller for ETS access;
c. Specification of priority treatment mechanisms applicable to ETS in NGNs;
d. ETS security; and
e. ETS support for services beyond VoIP.

18.1.4 Proposed Work Items

Current standard activities are already addressing the identified gaps and, therefore, no new work items have been identified at this time.

18.2 Next Generation 9-1-1 (NG9-1-1) Emergency Services

18.2.1 Requirements

NG9-1-1 requirements are currently under development in ATIS committees (e.g., ESIF, PTSC, and WTSC) and others (e.g., NENA) to provide services somewhat analogous to the legacy E9-1-1 deployed in the PSTN.

The NGN Framework consisting of architecture, protocols and network elements shall be highly resistant and resilient to denial of service attacks or other types of harm that might be perpetrated on the NGN by terrorists or miscreants. Implicit in the idea that the NGN will provide an efficient and improved NG9-1-1 is the notion that the NGN itself is secure, robust, and constantly available for use during an emergency crisis.

It is important to note that in North America the three-digit number "9-1-1" is used as the "Emergency Number" to request emergency assistance, while different number combinations are used in other parts of the world. For example, "1-1-2" is used by most authorities in Europe. Today, most of the population in North America is covered by

the E9-1-1 emergency service. In the future, the NGN should provide a set of multimedia NG9-1-1 emergency services that will enhance public safety in North America.

NG9-1-1 includes:

- The NG9-1-1 provides an opportunity for major improvements of the current E9-1-1 infrastructure in North America.
- The NGN will enable the delivery of the Location Object (LO) with the voice call to the PSAP along with associated multimedia applications and information (e.g., video streaming, caller's medical record, maps, etc.).
- The NG9-1-1 should enable the interworking with legacy E9-1-1 networks.
- The NG9-1-1 emergency services should provide improved communication(s) between PSAPs, and between the first responders (Law Enforcement, Fire, and EMS) and the users. The first responders must be protected from improper communications from users that would disrupt their systems (e.g., denial of service attacks).
- The NG9-1-1 primary concern is to enable a caller to contact first responders via PSAPs during an emergency situation. The NGN will provide more efficient ways for the citizens, PSAPs, relevant government agencies, and first responders to communicate among themselves during an emergency situation.

18.2.2 Function/Service Enabled

The NG9-1-1 emergency services, in the context of an IMS-based service, should enable an emergency service network to determine the physical location of the caller and the correct routing to an appropriate PSAP for that caller given the location (location-based routing).

The nomadicity/mobility of the NG9-1-1 users implies that an emergency service network must identify the current location of the calling party, and route the emergency call to the appropriate PSAP (based on the caller' location). It must also provide that location along with other multimedia data associated with the call context to the appropriate PSAP. It is important to consider that nomadicity/mobility across multiple emergency service networks must not preclude the caller's ability to contact the correct PSAP nor the PSAP's ability to callback the original caller during an emergency situation.

NG9-1-1 users should be able to communicate with PSAPs and first responders during an emergency situation using devices other than traditional phones and wireless handsets (e.g., PDAs, WiFi phones, email, Multimedia IM services, etc.).

18.2.3 Current Standardization Activities

18.2.3.1 ATIS

ESIF

ESIF's Task Force 34 has completed a draft American National Standard for Telecommunications standards *Emergency Services Network Interfaces (ESNI)*, for

trial use. ATIS-PP-0500002-200X, *Emergency Services Messaging Interface (ESMI) Document* will provide a standard for interconnections between next generation PSAPs and the Emergency Services Network (ESNet) after the call arrives at the appropriate PSAP. The ESMI Task Force is also currently working on the Emergency Information Services Interface (EISI) standard to provide access to services within or external to the ESNet, as well as a standard for the Emergency Services Network to Emergency Services Network (ENEN) interface to allow the interconnection and exchange of services between ESNets.

PTSC

PTSC has accepted the following NGN "9-1-1" Service issue at the January 2006 meeting (Issue Number S0038):

Issue Statement/Business Need: The PSTN has a special design for E9-1-1 systems which includes dedicated high reliability trunks and tandem switches, as well as special call handling based on the dialed digits "9-1-1". Now that we are moving to the next generation network, there is a need to address network infrastructure required to support this next generation service. The FCC continues to mandate the provision of 9-1-1 capability.

Suggested Solution: The PTSC should develop a standard applicable to managed IP networks using an NGN architecture to support "9-1-1" Service. This standard will reference existing standards and other documents, where appropriate.

Related work required for the solution to this issue to be implementable by the industry:

- Issue S0009: NNI interface to promote IP-IP interconnection between carriers in support of multi-media services.
- Issue S0027: IP Device (SIP UA) to Network Interface Standard
- Issue S0031: Packet Priority and Priority Call Processing
- Issue S0018: NGN Architecture Technical Report
- NRIC Best Practice documents, e.g., NRIC BP 6-6-3205
- ATIS.PP.0500002.200x, *Emergency Services Messaging Interface (ESMI) ESIF Document*
- 3GPP TS 23.167 Internet Protocol (IP) based IP Multimedia Subsystem (IMS) emergency sessions; Stage 2

It is anticipated that the PTSC will provide contributions on this subject to 3GPP, ITU-T and ESIF as appropriate, to ensure coordination of activities.

WTSC

- T1.709-1999, *Stage 1 Service Description for Personal Communications Services (PCS) - Emergency Services Call Supplementary Service.*

18.2.3.2 3GPP

The 3GPP Technical Report (TR) 23.837 V7.1.0, a published report dated December 2005, outlines the Stage 1 definition of requirements for SIP Emergency Sessions in the context of the IMS architecture for wireless users. Emergency Services are being defined by 3GPP Service Architecture 1 & 2 Working Groups. 3GPP has initiated work on 23.167, the Technical Specification (TS) for IMS emergency calls.

In addition, 3GPP has adopted and adapted the NENA i2 requirements to be applicable to wireless and for interworking with wireless LAN's.

18.2.3.3 ETSI

TISPAN Working Groups 2 and 3, and ETSI Special Committee EMTEL (Emergency Telecommunications) are working on the definition of NG1-1-2 Emergency Services Requirements in the context of TISPAN Release 1 & 2.

18.2.3.4 IETF

The IETF has standard activities underway for the definition of IP protocols for NG9-1-1 Emergency Services.

- *ECRIT (Emergency Context Routing with Internet Technologies)***:** The charter of this working group is to address requirements for routing of emergency call services based on the location of the caller (using a location mapping protocol). ECRIT is developing its requirements and proposals independent of an emergency service provider (although an emergency service provider should be able to use the output of ECRIT) and is mostly defined in the context of the Internet.
- *GEOPRIV (Geographic Location and Privacy)*: This working group defines the location payload and associated privacy policies for location conveyance (determination and acquisition) that can be used for emergency services. The location payload is carried in other protocols (e.g., SIP) for emergency services.

18.2.3.5 TIA

Within the TIA Engineering Committee TR41, a VoIP emergency services working group, TR41.4, is primarily focused on enterprise IP PBX Emergency Services interfaces definition, which could be extended to connectivity with the NGN.

18.2.3.6 NENA

NENA has several initiatives underway for the definition of NG9-1-1. It is not yet clear if these initiatives are fully aligned with the ATIS NGN Framework or the IMS standard. NENA has relationships in place with both ESIF and TIA for ANS work and with IETF for its work in ECRIT and GEOPRIV. NENA's VoIP and NG9-1-1 activities are summarized as follows:

- NENA's Standards Development Organizations (SDO) TID 08-504 Issue 2 includes a complete description of VoIP and NG9-1-1 global SDO initiatives and is provided in the summary table below.

- NENA's Interim VoIP Architecture for Enhanced 9-1-1 Services (i2) was published in December 2005.
- NENA i3 Technical Requirements Document (TRD); which will be published by the VoIP Long Term Definition working group in 2006 focuses on NG9-1-1.
- There are other TRDs that will be published by the VoIP Location Determination and IP-enabled PSAP working groups.

18.2.3.7 NRIC

The Network Reliability and Interoperability Council (NRIC) VII completed its reports in December 2005. While not a standards organization, NRIC makes recommendations to the FCC on technology policies. The major part of the NRIC VII reports focused on near term public safety issues and the evolution of emergency services through 2010. It is expected that the FCC will Charter the NRIC-VIII Report either in 2006 or 2007 in order to address next generation emergency services.

18.2.3.8 Department of Homeland Security

It is also important to note that the Department of Homeland Security (DHS) has partnered with ANSI in order to create the ANSI Homeland Security Standards Panel (HSSP). The latter acts as a coordination entity for all standards related activities in identified areas of concern for the DHS, including next generation emergency services.

18.2.3.9 Summary

The current NG9-1-1 standardization activities are summarized in the table below, as referenced from NENA's SDO TID 08-504 Issue 2; January 2006.

Table 5: Summary of Current NG9-11 Standardization Activities

SDO	Subcommittee/ Work Group	Activity
3GPP 3GPP2	SA WG1 (Services) & SA WG2 (Architecture)	3GPP TR 23.837 Version 7.1.0 Requirements for IP Multimedia System (IMS) Emergency Sessions, December 2005.
ATIS	ESIF	ESIF is a primary venue for the telecommunications industry, public safety & other stakeholders to develop & refine technical & operational interconnection issues that will ensure this life-saving service is available for everyone in all situations.
ETSI	TISPAN WG 2 and 3 EMTEL	The EMTEL Special Committee, along with TISPAN WGs 2 and 3 is in charge of standardizing Emergency Services for IMS in the context of wireline/wireless integration for Fixed/Mobile Convergence (FMC). Note that, EMTEL has an emphasis on 1-1-2 since in the EU and also has the charter to interface with ITU for input on the NGN global standard. SR 002 180 Requirements for Communication of citizens with

		authorities/organizations in case of distress (emergency call handling), Published and freely available. SR 002 181 Requirements for Communication between authorities/organizations in case of distress, to be published. TR 102 197 Preliminary analysis of EMTEL and local Emergency Service Requirements for IP networks and Next Generation Networks, Published and freely available. TS 102 164 Location Information Handling for Emergency Situations, Published May 2004. TS 102 410 The present document addresses the requirements for communication facilities among citizens and to authorities/ organizations, Non Governmental Organizations (NGOs) and media in the case of emergencies, not including alerting communication. To be Published.
IETF	GEOPRIV	The primary task of this working group will be to assess the authorization, integrity and privacy requirements that must be met in order to transfer such information, or authorize the release or representation of such information through an agent. Define mechanism to allow IP device to become location aware at time of network connection. Define a protocol or requirements for transport of location information with appropriate privacy protections.
	Sipping	The Session Initiation Protocol Project INvestiGation (SIPPING) working group is chartered to document the use of SIP for several applications related to telephony and multimedia, and to develop requirements for extensions to SIP needed for those applications.
	ECRIT	The Emergency Context Resolution with Internet Technologies (ECRIT) working group is chartered to provide requirements and recommend protocols for use of location data to determine call routing information at different steps in session setup to enable communication between a user and a relevant emergency response center.

ITU	Study Group 13	Responsible for studies relating to the architecture, evolution, and convergence of next generation networks including frameworks and functional architectures, signaling requirements for NGN, NGN project management coordination across study groups and release planning, implementation scenarios and deployment models, network and service capabilities, interoperability, impact of IPv6, NGN mobility and network convergence, and public data network aspects.
NRIC VII[32]	Focus Group 1A	Enhanced 911 – Near Term Issues
	Focus Group 1B	Enhanced 911 – Long Term Issues
	Focus Group 1C	Enhanced 911 – Network Outages and Best Practices
	Focus Group 1D	Enhanced 911 – PSAP, Emergency Communications beyond 911 (First Responders)
TIA	TR41.4	TSB 146 reviews the problems that must be solved to support Emergency Calling Service (ECS) from IP Telephony terminals connected to an Enterprise IP network. It addresses various Enterprise Network (EN) topologies, and describes possible solutions. This mechanism follows NENA's Model Legislation (utilizing ERLs & ELINs).

18.2.4 Identified Gaps

There is a lack of coordinated NG9-1-1 standards activities in North America in the context of the ATIS NGN Framework for addressing the convergence of wireline and wireless networks (FMC), the PSTN migration to VoIP, along with upcoming deployments of IMS for the support of NG9-1-1 emergency services. PTSC is addressing network infrastructure aspects of NG9-1-1.

A major gap is that the location-based routing attributes and capabilities of the S-CSCF (as defined in 3GPP Technical Report (TR) 23.837 V7.1.0) in the context of Emergency Services have not yet been fully specified by 3GPP. As a result, IMS does not currently support the routing and location determination of emergency calls. The S-CSCF that handles Emergency Services calls is being referred to as a "pre-configured" S-CSCF that is available for call processing in the serving IMS network. Whether the 911 caller is actually in a visited network or registered in their home network, it is the responsibility of the serving network to process the 911 call per the 3GPP requirements.

[32] The FCC Charter for NRIC VII ended December 31, 2005. Each FG produced Reports addressing their assigned deliverables. Those are available on the NRIC web site shown above.

In every case, the specific S-CSCF handling Emergency Services must have the capability to map a geographical location to a particular PSAP boundary at runtime. The method and means by which location information is determined, acquired and supplied is for further study per 3GPP TR 23.867 and must include all VoIP type of users. It appears this gap may be addressed in TS 23.167. Requirements are being developed to insure this is a serving system function, and will have the capability of providing calls without assistance from the home network.

3GPP is also producing requirements for determining PSAP routing for wireless and nomadic callers, with nomadic callers accessing the network via the I-WLAN standard (TS23.234 and related) produced by 3GPP. Continued monitoring of this activity is required by ATIS to determine if 3GPP fully addresses the problem. If it is determined that 3GPP is not fully addressing this problem, additional work will be required by ATIS.

The IETF's ECRIT Working group is investigating a number of issues important for accessing emergency services such as:

- How to identify that a session set-up request is for an emergency response center.
- Strategies for associating session originators with physical locations.
- How to route an emergency call based on location information.
- How to discover the media stream types an ERC supports.

While ECRIT doesn't currently call out the IMS CN architecture for the NGN Framework explicitly, its work is intended to be applicable to all systems utilizing SIP Proxy Server(s) such as IMS's CSCF. The same applies to GEOPRIV for Location Object delivery in the context of the NGN Framework. Note that there is an initiative led by 3GPP to introduce IMS call routing requirements into ECRIT. ATIS should monitor the work in ECRIT to determine if it addresses the requirements. In addition, ATIS may need to develop specifications on how the work in ECRIT and GEOPRIV will be applied to the ATIS NGN.

ATIS NG9-1-1 Framework does not reference the NENA i3 Requirements. This is a current gap as E9-1-1 system requirements today are based on stakeholder agreements and government policy, not just standards developed by various SDOs. NENA relies on IETF, ESIF, and TIA for standards development work beyond its own scope and charter for the 9-1-1 System. As a result, further standardization work should be undertaken with the cooperation of NENA. This may be facilitated by ESIF, which is responsible for the interconnection between 9-1-1 Systems and access networks, in order to map NENA i3 Requirements into the ATIS NGN Framework, as well as by PTSC.

18.2.5 NG9-1-1 Proposed Work Items

Work Item A: Primary: ATIS ESIF - Next Generation Emergency Services Subcommittee

Proposed Work Plan and Deliverables:

- Formulate the NG9-1-1 end-to-end service architecture for the ATIS NGN Framework taking into account the 3GPP IMS standard and NENA's i3 requirements.
- Map NENA's i3 Stage 2 and Stage 3 standard to the ATIS NGN Framework and identify issues as appropriate.
- Track progress of 3GPP Service Architecture 1 & 2 working groups and provide input for consideration into 3GPP Technical Report (TR) 23.837 V7.1.0 and TS 23.167 for IMS Emergency Sessions to meet ATIS NGN requirements.
- Coordinate joint reviews with ETSI EMTEL on Emergency Services for a global standard coordination effort on NG9-1-1 and NG1-1-2 emergency services initiatives between North America and Europe.

Work Item B: Primary: ESIF
Title: "NG9-1-1 Technical Requirements & Architectural Analysis (for IMS networks)"

Business Need:

One important point is that some industry groups, like 3GPP, are industry groups that do not in themselves develop standards, but make recommendations on Technical Specifications, Functional Architectures, and provide input to SDOs (e.g., ETSI, ITU, TIA and IETF).

The NGN standard development is globally focused; therefore, the NG9-1-1 standard needs to follow the same path. There is a current need for ESIF to help shape NG9-1-1 in a global standard environment by acting as a technical coordination group between 3GPP, ETSI, ITU, TIA, IETF, and NENA. This will ensure that the standard process is followed for the development of a global NG9-1-1 standard for North America.

Recommended Approach:

The role of the ESIF standard committee is to help define the NG9-1-1 standard for North America in the context of the IMS global standard. The latter must be accomplished by having ESIF and NENA work closely together on standards coordination for the work being produced by NENA, such as NENA's i3 requirements, while assuming a coordination and liaison role with other global standard development organizations (3GPP, ETSI, ITU, IETF, and TIA) as listed in previous sections.

One final recommendation is that ESIF establishes a new Subcommittee – Next Generation (NG) Emergency Services -- that will address the proposed work items previously listed. This new ESIF Subcommittee will carry the mission to enable the coordination and liaison amongst global SDOs for the standards development of Next Generation (NG) Emergency Services.

Target Date:

The deliverables listed above NG9-1-1 Technical Requirements & Architectural Analysis must be delivered in accordance with the 3GPP IMS Release 7 schedule in 2006 and 2007. IMS emergency calls will be supported in 3GPP Release 7.

ESIF has a target date of 3Q2006 for completion of the deliverables.

Work Item C: Primary: ATIS PTSC
Title: "NG9-1-1 Emergency Services Network Specifications"

Proposed Work Plan and Deliverables:

- Develop NG9-1-1 Emergency Services Functional Network Architecture Specifications.
- Develop NG9-1-1 Emergency Services Network Design Recommendation.

Business Need:

The NG9-1-1 emergency services network architecture should recognize that the role of the emergency service provider and the emergency service network will change drastically as IP technology expands beyond traditional wireline fixed location telephones (VoIP, UMA, 3G, etc.) with the ATIS NGN Framework. The type of information needed by the PSAP is increasing beyond what the existing emergency network infrastructure can support. At the same time, service reliability and availability must be maintained by NG9-1-1 emergency services with the ATIS NGN Framework.

Recommended Approach:

The NGN FG, PTSC, and ESIF should work together. The NG9-1-1 standard should be considered in the context of a "global standard" and part of the umbrella ITU NGN and 3GPP IMS standards for Emergency Services. The role of the ESIF standard committee is to help define the NG9-1-1 standard for North America in the IMS global standard context. The latter must be accomplished by having ESIF and NENA work closely together on standards coordination for the work being produced by NENA, such as NENA's LTD i3 Requirements, while assuming a coordination and liaison role with other global standard development organizations (3GPP, ETSI, ITU, and TIA) as listed in previous sections.

Target Date:

The deliverables listed above NG9-1-1 Emergency Services Functional Network Architecture Specifications and Network Design Recommendations must be delivered in accordance with the 3GPP IMS Release 7 schedule in 2006 and 2007. IMS emergency calls will be supported in 3GPP Release 7.

PTSC has a target date of 4Q2006 for completion of the deliverables.

18.3 Automatic (Crash) Notification Capability

This section has not yet been addressed and is included for inclusion of information derived from future study.

18.4 Emergency Alert Service

This section has not yet been addressed and is included for inclusion of information derived from future study.

19 WIRELESS/WIRELINE CONVERGENCE

19.1 General Description

As NGNs evolve and are deployed, there will exist an increasing need to provide continuity of service between access networks and a consistent user perspective. To support the needed equipment interworking, standards are needed that specify service requirements, architecture, and signaling interfaces. The requirements of Fixed, Nomadic, and Mobile oriented services including Voice, Video, and Data, need to be taken into consideration, although the initial focus may be constrained to dual mode user equipment (e.g., WLAN / GSM) for Voice services (due to pressing market needs). Areas for consideration include the following:

a. Seamless handover between different access networks (e.g., Circuit Switched GSM and IP WLAN) and associated core network interworking (e.g., Circuit Switched and IMS).
b. Interoperability between independent IMS and CS core networks.
c. Coordination of service data in and between user equipment, access networks, and core networks for a consistent user experience.
d. Flexible subscriber addressing, including multiple directory numbers (e.g., two E.164 numbers).
e. Network/Domain selection for originating and terminating calls.
f. Supplementary Services support (e.g., Call Forwarding, Call Waiting, Call Hold, etc.).
g. Security.
h. Quality of Service.
i. Multimedia support (e.g., Voice, Video, Data).

19.2 Requirements

A definitive list of requirements has not yet been established.

19.3 Function/Service Enabled

Service continuity for Voice, Video, and Data between different access networks is provided. The initial focus will be on voice service. Further study is needed to identify a full list of functions enabled.

19.4 Current Standardization Activities

19.4.1 3GPP

- Approved a Release 7 "Voice Call Continuity" work item.
- Requirements documented in TS 22.101 (IMS Requirements).
- Architecture work under way in TS 23.206 (VCC Architecture).

19.4.2 ATIS

19.4.2.1 WTSC

- Approved a Voice Call Continuity work item (WTSC-2006-020Rx).

19.4.2.2 PTSC

- Approved an issue statement to address Service Continuity Between Access Networks (PTSC Issue #44).

19.4.3 ETSI

To be determined.

19.4.4 ITU

To be determined.

19.4.5 IETF

To be determined.

19.5 Identified Gaps

Current work under way in the industry does not include, or requires further specification for:

- Independent core network interfaces (e.g., for subscriber service data synchronization).
- Emergency Call continuity between access networks.
- Multimedia (e.g., Video) continuity between access networks.

19.6 Proposed Work Items

The ATIS TOPS Council should consider the appropriate mechanism to fully identify and address these gaps. Possibilities include:

Work Item A: Primary: ATIS
Title: New Focus Area

Business Need:

It may be appropriate to consider formation of a focus area dedicated to addressing wireless/wireline convergence issues.

APPENDIX A: NGN ACRONYMS

3G	Third Generation
3GPP	Third Generation Partnership Project
AD	Administrative Domain
AIP- AccMgt	Architectures Interfaces and Protocols - Account Management Taskforce (within the ATIS TMOC AIP Subcommittee)
AKA	Authentication and Key Agreement
AMPS	Advanced Mobile Phone System
ANS	American National Standard
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials International, Inc.
API	Application Programming Interface
AS	Autonomous System
ASOG	Access Service Ordering Guidelines
ASON	Automatically Switched Optical Network
ASM	Any Source Multicast
ASP	Application Service Provider
ATIS	Alliance for Telecommunications Industry Solutions
BGP	Border Gateway Protocol
BMC	Broadcast/Multicast Control
BOF	Business Operations Framework
BOSS	Baseline Operating Systems Security
BSS	Base Station Switching System
CAC	Connection Admission Control
CALEA	Communications Assistance to Law Enforcement Act
CCXML	Call Control eXtensible Markup Language
CDMA	Code Division Multiple Access
CIPID	Contact Information in Presence Information Data Format
CLF	Connectivity/Session Location and Repository
CM	Configuration Management
CN	Core Network
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
CPIM	Common Presence and Instant Messaging
CS	Circuit Switched
CSCF	Call Session Control Function
CSU	Channel Service Unit/ Channel Sharing Unit
DDM	Data Description Method
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DIAMETER	An IETF AAA protocol
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DS-TE	Differentiated-Service - Traffic Engineering
DSU	Digital Service Unit
DT	Direct Termination
DTMF	Dual Tone Multi-Frequency
DTR	Data Terminal Ready
DTS	Draft Technical Specification
DVB	Digital Video Broadcast

ECMA	European Computer Manufacturers Association
ECMP	Equal Cost Multipath Routing
ECRIT	Emergency Context Resolution with Internet Technologies
EISI	Emergency Information Services Interface
ELIN	Emergency Location Identification Number
EMI	Exchange Message Interface
EMTEL	Emergency Telecommunications
EN	Enterprise Network
ENEN	Emergency Services Network to Emergency Services Network
ENUM	Electronic NUMber
EOY	End of Year
ERL	Emergency Response Location
ES	Errored-Second/ End System
ESA	Enhanced Subscriber Authentication
ESMI	Emergency Services Messaging Interface
ESNet	Emergency Services Network
ESNI	Emergency Services Network Interfaces
ESP	Enhanced Subscriber Privacy
eTOM	enhanced Telecom Operations Map
ETS	Emergency Telecommunications Service
ETSI	European Telecommunications Standards Institute
EU	European Union
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FCC	Federal Communications Commission
FEC	Forward Error Correction
FFS	For Further Study
FGNGN	ITU-T Focus Group on Next Generation Networks
FLUTE	File Delivery over Unidirectional Transport
FMC	Fixed/Mobile Convergence
FW	FireWire
GBA	Generic Bootstrapping Architecture
GEOPRIV	Geographic Location and Privacy
GETS	Government Emergency Telecommunications System
GLMS	Group List Management
GTDD	Generic Telecom Data Dictionary
GUP	Generic User Profile
HAT	Hybrid Access Terminal
HLR	Home Location Register
HPNA	Home Phoneline Networking
HSS	Home Subscriber Server
HSSP	Homeland Security Standards Panel
HTTP	HyperText Transfer Protocol
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICC	ITU Carrier Code
ID	Identifier
IDL	Interactive Data Language
IDP	InterDigital Pause
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IEPREP	Internet Emergency Preparedness
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Procotol

IIF	IPTV Interoperability Forum
IKE	Internet Key Exchange
IM	IP Multimedia
IM	Instant Messaging
IMPS	Instant Messaging and Presence Services
IMS	IP Multimedia Subsystem
IOS	Interoperability Specification
IP-CAN	IP-Connectivity Access Network
IPDR	Internet Protocol Detail Record
IPFIX	IP Flow Information Export
IPTV	Internet Protocol Television
IRP	I/O Request Packet
ISDN	Integrated Services Digital Network
ISIM	IP Multimedia Services Identity Module
ISO	International Standards Organization
ISOP	Interconnection Service Ordering and Provisioning Committee
ISP	Internet Service Provider
ISSAA	Information System Security Assurance Architecture
ITU	International Telecommunication Union
ITU-T	ITU- Telecommunications Standardization Sector
IVR	Interactive Voice Response
I-WLAN	Internetworking Wireless LAN
JAIN	Java APIs for Integrated Networks
JRG-MMQA	Joint Rapporteur Group on Multimedia Quality Assessment
JVM	Java Virtual Machine
LAN	Local Area Networks
LBS	Location Based Services
LCT	Layered Coding Transport
LDAP	Lightweight Directory Access Protocol
LLC	Logical Link Control
LO	Location Object
LSOG	Local Service Ordering Guidelines
LSOP	Local Services Ordering and Provisioning Committee
LTD	(NENA LTD) Long Term Direction working group
MAC	Media Access Control
MAGMA	Multicast & Anycast Group Membership
MAN	Metropolitan Area Network
MBONE	Multicast Backbone
MBONED	MBONE Deployment
MEGACO	MEdia GAteway COntrol
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MIKEY	Multimedia Internet KEYing
MLD	Multicast Listener Discovery
MoCA	Multimedia over Coax Alliance
MOML	Media Objects Markup Language
MOS	Metal Oxide Semiconductor/ Mean Opinion Score
MPEG	Moving Pictures Experts Group
MPLS	MultiProtocol Label Switching
MRB	Media Resource Broker
MRC-FE	Media Resource Control Functional Entity
MRCP	Media Resource Control Protocol
MRF	Media Resource Function

MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MS	Mobile Station/ Message Switch
MSCML	Media Server Control Markup Language
MSCP	Media Server Control Protocol
MSDP	Multicast Source Discovery Protocol
MSEC	Multicast Security
MSML	Media Server Markup Language
MSP	Multiple Subscriber Profile
MTNM	Multi-Technology Network Management
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
MUWS	Management Using Web Services
MZAP	Multicast-Scope Zone Announcement Protocol
NACF	Network Access Control Function
NACK	Negative-Acknowledge Character
NAPT	Network Address Port Translation
NAT	Network Address Translation
NAT-PT	Network Address Translation – Protocol Translator
NE	Network Element
NEMO	Network Mobility
NENA	National Emergency Number Association
NE-OS	Network Element to Operations System
NE/OS-WS	Network Element/Operations System to Work Station
NETCONF	Network Configuration
NG	Next Generation
NGN	Next Generation Network
NGNMFG	NGN Management Focus Group
NGNSP	Next Generation Network Service Provider
NGO	Non Governmental Organizations
NGOSS	New Generation Operations Support and Software
NGSP	Next Generation Service Provider
NNI	Network to Network Interfaces
NORM	NACK-Oriented Reliable Multicast
NRIC	Network Reliability and Interoperability Council
NRM	Normal Response Mode
NRSS	National Renewable Security Standard
NSIS	Next Steps in Signaling
NSLP	NSIS Signalling Layer Protocol
NTP	Network Termination Point/ Network Time Protocol
OAM&P	Operation, Administration, Maintenance and Provisioning
OASIS	Organization for the Advancement of Structured Information Standards
OBF	Ordering and Billing Forum
OD	(FGNGN-OD) Output Document
OIF	Optical Internetworking Forum
OMA	Open Mobile Alliance
OSA	Open Services Architecture/ Open System Adapter
OS-OS	Operations System to Operations System
OSPF	Open Shortest Path First
OSS	Operations Support System
OTAR	Over-the-Air Rekeying
PA	Presence Agent
PAG	Presence and Availability Group

PAK	Password-authenticated Key Exchange Protocol
PAM	Presence and Availability Management
PBX	Private Branch eXchange
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PDF	Portable Document Format
PEA	Presence External Agents
PHY	Physical Layer
PIDF	Presence Information Data Format
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast – Dense Mode
PNA	Presence Network Agents
PoC	Push-to-talk over Cellular
PON	Passive Optical Network
PRQC	Network Performance, Reliability, and Quality of Service Committee
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee
PUA	Presence User Agents
QoS	Quality of Service
QOSM	Quality of Service Management
QSPEC	Quality of Service Specification
RACF	Resource and Admission Control Functions
RACS	Resource and Admission Control Subsystem
RD	Routing domain/ Route Distinguisher
RFC	Request for Comment
RLS	Resource List Server
RMT	Reliable Multicast Transport
RP	Rendezvous Point
RPID	Rich Presence Information Data Format
RSVP	Resource Reservation Protocol
SA	Source Address
SAC	Service Access Code/ Special Area Code
SBC	Session Border Control
SCF	Service Control Function
S-CSCF	Serving- Call Session Control Function
SDO	Standards Development Organizations
SDU	Service Data Unit
SEC	(PTSC SEC) PTSC Security Subcommittee
SG	Signaling Gateway
SIM	Subscriber Identity Module
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SIPPING	Session Initiation Protocol Project INvestiGation
SLA	Service Level Agreement
SMS	Short Message Service
SNMP	Signaling Network Management Protocol/ Simple Network Management Protocol
SSM	Source-Specific Multicast
SSO	Single Sign On
STD	Subscriber Trunk Dialing
TCP	Transmission Control Protocol

TD	Temporary Document
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TE	Terminal Equipment
TESLA	Timed Efficient Stream Loss-tolerant Authentication
TIA	Telecommunications Industry Association
TID	Terminal Identification
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TMF	TeleManagement Forum
TMOC	Telecom Management and Operations Committee
TOPS	Technology and Operations Council
TRD	Technical Requirements Document
TR-RACF	Technical Report on Resource and Admission Control Functionality
TRU	Tone Receiver Unit
TS	Technical Specification
TSG-S	3GPP2 Services and Systems Aspects Technical Specification Group
TTY	Text Telephone
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
UICC	USIM Integrated Circuit Card
UMA	Upper Memory Area
UML	Unified Modified Language
UMTS	Universal Mobile Telecommunications System
UNI	User Network Interface
UOM	Unified Ordering Model
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module
UPSF	User Profile Server Function
VCC	Voice Call Continuity
VLR	Visitors' Location Register
VoIP	Voice Over Internet Protocol
VXML	Voice Extensible Markup Language
W3C	World Wide Web Consortium
WAE	Wide Area Ethernet
WAN	Wide Area Network
WAP	Wireless Application Protocol
WFQ	Weighted Fair Queuing
WG	Working Group
WICIS	Wireless Intercarrier Communications Interface Specification
WP	Working Party
WPAN	Wireless Personal Area Networks
WSDM	Web Services Distributed Management
WTSC	Wireless Telecommunications Systems Committee
WV	Wireless Village
XCAP	XML Configuration Access Protocol
XCON	IETF Centralized Conferencing WG
XDM	XML Document Management
XDMS	XML Document Management Server
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

APPENDIX B: NGN FOCUS GROUP MEMBERS

Company	Name
Chair	
Lucent Technologies, Inc.	Janet Davidson
Technical Lead	
Nortel	Jim McEachern*
Members	
ADC Wireline Business Unit	Dieter Nattkemper
ADTRAN	Marc Kimpe, Ph.D.*
Alcatel	Frederick H. Skoog
Alcatel	Gary Hanson
Alcatel	Ken Biholar
Alcatel North America	Larry O'Pella
AT&T	Chuck Bailey
AT&T Labs	Charles Dvorak
AT&T Labs	Bernard Ku
AT&T Labs	Robert (Bob) Hall
AT&T	Gary Munson*
BellSouth	David Whitney*
BellSouth	Shirley Loewen
BellSouth	Steven Wright*
BT Group	Graham Travers
Cisco	Catagay Buyukkoc
Cisco	Chip Sharp
Cisco	Art Reilly
Cisco	Dave Meyer
Cisco	Kyung-Yeop Hong
Ericsson, Inc.	Asok Chatterjee
Ericsson, Inc.	Susana Sabater
General Bandwidth	Don Sparks
HP	Lionel Lapras
HP	Mark Gullett*
HP	Marc Brandt
Intel	Walt Brown*
Intrado	Christian Militeau*
Lucent Technology, Inc.	Hui-Lan Lu*
Lucent Technology, Inc.	Stu Goldman
Nokia	Ed Ehrlich
Nokia	Curt Wong
Nokia	Gabor Bajko
Nokia	Matti Alkula
Nokia	William Plummer
Qwest	Mike Fargano*
Qwest	Andrew White*
Qwest	Glenn Morrow*
Samsung	Howon Choe
Siemens ICN	Rudolf Brandner
Siemens ICN	David Francisco
Siemens ICN	Derek Underwood
Sprint	Dale Baldwin
Telcordia	Cliff Halevi
Telcordia	Fuchun Joe Lin*
T-Mobile	Gary Jones
Verisign	Tony Rutkowski
Verizon	Bhumip Khasnabish*
Verizon	Tom Helmes*
Verizon	Stu Jacobs*
Committee Chairs	
ESIF Chair	Maureen Napolitano
ESIF First Vice Chair	Bob Montgomery
ESIF Second Vice Chair	David Irwin*
IIF Chair	Dan O'Callaghan
IITC Chair	Jim Neises
IITC Vice Chair	Guerin Goldsmith
INC Chair	Ken Havens
INC Vice Chair	Adam Newman
NIIF Co-Chair	Stu Goldman
NIIF Co-chair	Robert Schafer
OBF Co-Chair	Dave Thurman
OBF Co-Chair	Dawn Kaplan
OBF/SAG Co-Chair	Stephanie Cowart
OBF/SAG Co-Chair	Chris Read
OPTXS Chair	Ken Biholar
OPTXS Vice Chair	Mark Jones
PRQC Chair	Randy Wohlert*
PRQC Vice Chair	Neal Seitz*
PTSC Chair	Bob Hall
PTSC Vice Chair	Joe Zebarth
TFPC Chair	Mark Yelchak
TFPC Vice Chair	Mark Kearns-Banks
TMOC Chair	Mike Fargano
TMOC Vice Chair	Ron Roman
ATIS Staff	
ATIS	Tim Jeffries*
ATIS	Martha Ciske*
ATIS	Meghan Ewell

*Contributing Section Author