ATIS-1000055.2013

EMERGENCY TELECOMMUNICATIONS SERVICE (ETS): CORE NETWORK SECURITY REQUIREMENTS

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle — from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000055.2013, *Emergency Telecommunications Service (ETS): Core Network Security Requirements*

Is an American National Standard developed by the **Signalling, Architecture, and Control (SAC) Subcommittee** under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

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

ATIS-1000055.2013

American National Standard for Telecommunications

Emergency Telecommunications Service (ETS): Core Network Security Requirements

Alliance for Telecommunications Industry Solutions

Approved August 12, 2013

American National Standards Institute, Inc.

Abstract

The integrity, confidentiality, and availability of Emergency Telecommunication Service (ETS) in a multi-provider Next Generation Network (NGN) environment will depend on the security of each individual network involved in an end-to-end communication. To allow network provided security of end-to-end ETS communications in a multi-provider environment, intra-network domain and inter-network domain security requirements for ETS protection are needed. This ATIS standard provides a minimum set of common (i.e., independent of network type or technology) and core network security requirements for the protection of ETS in a multi-provider NGN environment.

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global information and communications technology (ICT) companies to advance the industry's most-pressing business priorities. ATIS serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, PTSC, which is responsible for the development of this Standard, had the following leadership:

M. Dolly, PTSC Chair(AT&T)
V. Shaikh, PTSC Vice Chair (Applied Communication Sciences)
M. Dolly, PTSC SAC Chair (AT&T)
R. Singh, Technical Editor (Applied Communication Sciences)
C. Underkoffler, ATIS Chief Editor

The Signalling, Architecture, and Control (SAC) Subcommittee was responsible for the development of this document.

Table of Contents

1 SCOPE, PURPOSE, & APPLICATION 1

1.1 SCOPE 1
1.2 PURPOSE 1
1.3 APPLICATION 1
1.4 RELATIONSHIP OF CONCEPTS & TERMS 1
1.5 SECURITY THREATS & RISKS 2
1.6 REFERENCE ARCHITECTURE 2
1.7 ASSUMPTIONS 3

2 NORMATIVE REFERENCES 4

2.1 ATIS REFERENCES 4
2.2 ITU-T REFERENCES 5
2.2 OTHER 5

3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS 5

3.1 DEFINITIONS 5
3.2 ACRONYMS & ABBREVIATIONS 6

4 GENERAL SECURITY OBJECTIVES & REQUIREMENTS 8

4.1 GENERAL OBJECTIVE 8
4.2 GENERAL GUIDELINES 9
4.3 ETS FUNCTIONAL REQUIREMENTS 10
4.4 GENERAL REQUIREMENTS 11
4.5 PROTECTION OF PRIORITY SERVICES USER INFORMATION 12
4.6 COMMON REQUIREMENTS 12

5 NGN PS AUTHENTICATION & ACCESS CONTROL 13

5.1 PROTECTION AGAINST UNAUTHORIZED ACCESS 13
5.2 ENHANCING DEVICE SUBSCRIPTION VALIDATION 13
5.3 ENHANCING PIN AUTHENTICATION & AUTHORIZATION FOR VOICE SERVICES 14
5.4 AUTHENTICATION OF NGN PRIORITY SERVICES, SERVICE PROVIDER 17

6 NETWORK-TO-NETWORK INTERFACE 18

6.1 AUTHENTICATION 18
6.1.1 Mutual Authentication of Service Provider 18
6.2 ACCESS CONTROL 18
6.3 INTEGRITY 19
6.4 CONFIDENTIALITY 20

7 USER-TO-NETWORK INTERFACE 21

7.1 AUTHENTICATION 21
7.2 ACCESS CONTROL 22
7.3 INTEGRITY 22
7.4 CONFIDENTIALITY 23
7.5 DATA COMMUNICATIONS BETWEEN AUTHORIZED GOVERNMENT AGENCY & SERVICE PROVIDER 23
7.5.1 Authentication 23
7.5.2 Access Control 24
7.5.3 Integrity 24
7.5.4 Confidentiality 24

8 APPLICATION/SERVER-TO-NETWORK INTERFACE 24

8.1 AUTHENTICATION 24
8.2 ACCESS CONTROL 25
8.3 INTEGRITY 26
8.4 CONFIDENTIALITY 26

9 INTRA-NETWORK COMMUNICATIONS 26

9.1 AUTHENTICATION 27
9.2 ACCESS CONTROL 27
9.3 INTEGRITY 28
9.4 CONFIDENTIALITY 28

10 SECURITY FOR THE MANAGEMENT PLANE 29

10.1 MANAGEMENT PLANE SECURITY REQUIREMENTS 30
10.1.1 Identification 30
10.1.2 Authentication 30
10.1.3 Authorization & Privilege Management 31
10.1.4 Access Control 32
10.1.5 System & Data Integrity 34
10.1.6 Data Confidentiality 36
10.1.7 Management Communications 37

11 IP TRANSPORT NETWORK SECURITY 38

11.1 INTRA-NETWORK IP TRANSPORT 38
11.1.1 General 38
11.1.2 Routing Functions & Protocols 39
11.1.3 Use of Encryption 39
11.2 INTER-NETWORK IP TRANSPORT 40
11.2.1 General 40
11.2.2 Routing Functions & Protocols 41
11.2.3 Use of Encryption 42

12 MANAGEMENT OF SECURITY FOR NGN PRIORITY SERVICES 42

12.1 GENERAL OBJECTIVES & REQUIREMENTS 42
12.2 RISK ASSESSMENT 43
12.3 SECURITY ARCHITECTURE & SOLUTIONS 44
12.3.1 Security Policies 44
12.3.2 Security Architecture Design 45
12.4 SECURITY OPERATIONS 46
12.4.1 Organizational Structure, Roles, & Responsibility 46
12.4.2 Security Training & Awareness 47
12.4.3 Management of Insider Threats 47
12.4.4 Collaboration for Cyber Security Information Exchange 47
12.4.5 Management of Incident Response & Recovery from Security Events 48
12.4.6 Management of Supply Chain 48

13 AVAILABILITY 48

13.1 INTRODUCTION 48
13.2 GENERAL OBJECTIVES 49
13.3 PROTECTION FROM SERVICE DEGRADATION 50
13.4 AVAILABILITY PROTECTION 50
13.4.1 Denial of Service 50
13.4.2 Resource Exhaustion 50
13.5 DIVERSITY & REDUNDANCY FOR SURVIVABILITY 51
13.6 SECURITY MONITORING AT NGN PS SPECIFIC EQUIPMENT 52

14 BIBLIOGRAPHY 53

A EXAMPLE SERVICE LEVEL AGREEMENT (SLA) TEMPLATE FOR NS/EP NGN-PS SECURITY 54

A. 1 GENERAL SLA CONCEPTS 54
A.1.1 Overview of the M.3342 SLA Templates 55
A.2 SPECIAL CONSIDERATIONS FOR NETWORK-TO-NETWORK INTERFACE 56
A.3 SPECIAL CONSIDERATIONS FOR INTERNETWORK IP TRANSPORT 58
A.4 NGN-PS SECURITY TEMPLATES 59

A.4.1 Proforma for "NGN PS Security Point of Contact" *59*
A.4.2 Proformas for "NGN PS Security Parameters" *61*
A.4.3 Proforma for "NGN PS Security Design Information" *63*
A.4.4 Proforma for "NGN PS Security Recovery Mechanisms" *63*
A.4.5 Proforma for "NGN PS Security Report" *64*

Table of Figures

FIGURE 1 - RELATIONSHIP OF CONCEPTS AND TERMS 2
FIGURE 2 – NGN CONNECTIVITY AND INTERFACES [ITU-T Y.2012] 3
FIGURE 3 - EXAMPLE OF END-TO-END COMMUNICATION ACROSS DIFFERENT SERVICE PROVIDER DOMAINS 9
FIGURE 4 – IP NETWORK INTERCONNECTION SCENARIOS 40
FIGURE 5 – EXAMPLE SECURITY ARCHITECTURE FOR CORE NETWORK 46

FIGURE A.1 - SLA SCENARIO SCHEMATIC 54
FIGURE A.2 - BASIC COMPOSITION OF SLA CONTENT (PER 1/M.3342) 55
FIGURE A.3 - SLA CONTENT STRUCTURE 58

Table of Tables

TABLE 1: ORIGINAL TABLE OF ETS FUNCTIONAL REQUIREMENTS [ATIS-0100009] 11
TABLE 2: NGN PRIORITY SERVICES EXISTING AND PROPOSED ENHANCED AUTHENTICATION AND AUTHORIZATION METHODS FOR VOICE SERVICES 16

TABLE A.1 - NGN PS AUTHENTICATION AT NNI" PROFORMA 56
TABLE A.2 - NGN PS ACCESS CONTROL AT NNI" PROFORMA 57
TABLE A.3 - "NGN PS INTEGRITY AT NNI" PROFORMA 57
TABLE A.4 - NGN PS CONFIDENTIALITY AT NNI" PROFORMA 58
TABLE A.5 - NGN PS SECURITY FOR INTERNETWORK IP TRANSPORT" PROFORMA 59
TABLE A.6 - NGN PS SECURITY FOR IP ROUTING FUNCTIONS AND PROTOCOLS" PROFORMA 59
TABLE A.7 - NGN PS SECURITY FOR IPSEC TUNNELS" PROFORMA 59
TABLE A.8 - "NGN PS SECURITY POINT OF CONTACT" PROFORMA 60
TABLE A.9 - "NGN PS SECURITY METRICS" PROFORMA 61
TABLE A.10 - NGN PS SECURITY KPI DEFINITION" PROFORMA 62
TABLE A.11 - –"NGN PS KQI DEFINITION" PROFORMA 62
TABLE A.12 - NGN PS SECURITY DESIGN INFORMATION" PROFORMA 63
TABLE A.13 - "NGN PS SECURITY RECOVERY MECHANISMS" PROFORMA 64
TABLE A. 14 - "NGN PS SECURITY REPORT" PROFORMA 64

American National Standard for Telecommunications–

Emergency Telecommunications Service (ETS): Core Network Security Requirements

1 Scope, Purpose, & Application

1.1 Scope

The integrity, confidentiality, and availability of Emergency Telecommunication Service (ETS) in a multi-provider Next Generation Network (NGN) environment will depend on the security of each individual network involved in an end-to-end communication. To allow network provided security of end-to-end ETS communications in a multi-provider environment, intra-network domain and inter-network domain security requirements for ETS protection are needed. This ATIS standard provides minimum security requirements for the security protection of ETS in a multi-provider NGN environment.

The scope of this ATIS standard is common (i.e., requirements that are independent of network type or technology) and core network security requirements in the context of supporting ETS in a multi-provider NGN environment. The scope of the security requirements includes integrity, confidentiality, and availability protection for ETS communications within a network and across network boundaries (i.e., between different network domains).

1.2 Purpose

The purpose of this ATIS standard is to provide a minimum set of security requirements that can be used to facilitate the security protection of ETS communications across directly or indirectly interconnected networks. The requirements in this standard are intended to protect ETS applications and resources against security threats, including protection of the network infrastructure supporting the ETS applications.

Another purpose of this standard is to promote interoperability in a multi-network, multi-service provider, and multi-vendor environment.

1.3 Application

This standard is applicable to public networks supporting ETS. Private enterprise networks may also use this standard.

1.4 Relationship of Concepts & Terms

National Security/Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS), Legacy Government Emergency Telecommunication Service (GETS), and Wireless Priority Service (WPS) are all facets of the U.S.A. instantiation of the international standard for ETS [E.107]. The relationship of the terms is portrayed in Figure 1.

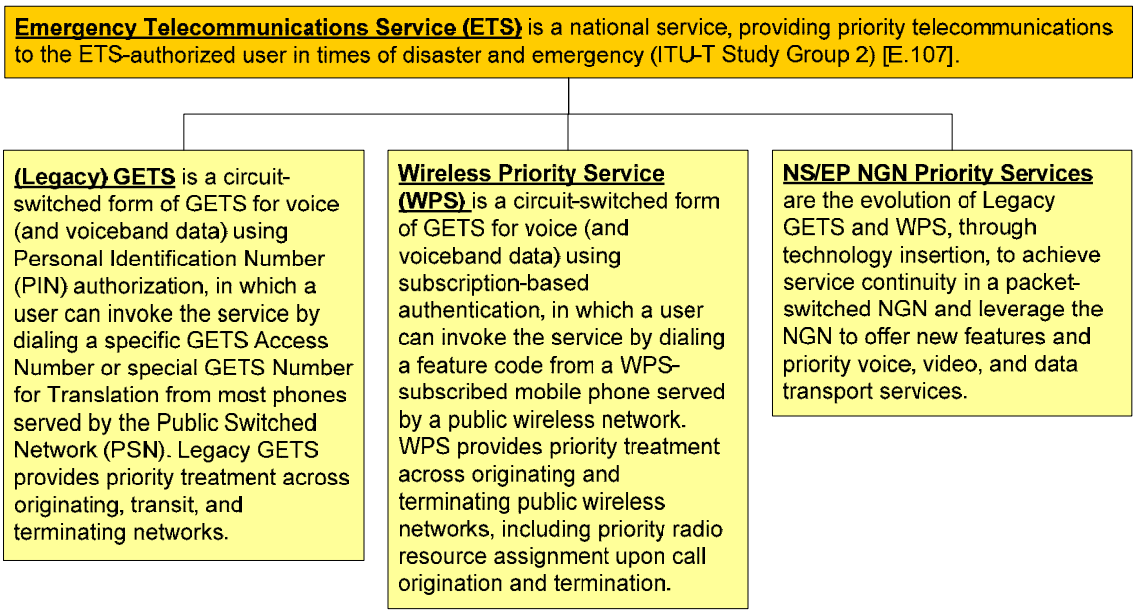

Figure 1 - Relationship of Concepts and Terms

1.5 Security Threats & Risks

ETS communications may be targeted for cybersecurity attacks because of the critical nature of the communications. The source of threats or malevolent actions intent on disrupting, misusing, manipulating, or otherwise harming ETS could originate from a variety of sources including interconnected networks. For example, ETS may be targeted for cybersecurity attacks for reasons such as to:

- Disrupt the ability of disaster recovery personnel to communicate.
- Obtain sensitive information by eavesdropping on ETS calls/sessions.

A threat is viewed as a security weakness or potential vulnerability that if exploited may negatively affect the availability, integrity, or confidentiality of ETS communications.

This ATIS standard focuses mainly on threats pertaining to network interconnection for ETS. Example threats relating to network interconnection include, but are not limited to:

- *General Interconnection Threat*: Security weaknesses or potential vulnerabilities associated with connecting the network (e.g., NGN) to other managed and unmanaged networks, such as the public Internet.
- D*esign and Implementation Threat*: Security weaknesses or potential vulnerabilities in the network interconnection architecture and implementation designs.
- *Management, Operational, and Insider Threat*: Security weaknesses or potential vulnerabilities in the command and control functions for ETS and their underlying infrastructure.
- *Transport and Facilities Threat*: Security weaknesses or potential vulnerabilities associated with the underlying transport network (e.g., routing, network duplication, diversity, resiliency), support systems (e.g., power, environmental), and physical protection of network assets.

1.6 Reference Architecture

This ATIS standard relies on the functional architecture and network connectivity model defined in [ATIS-1000018] and [ITU-T Y.2012] and shown in Figure 2.

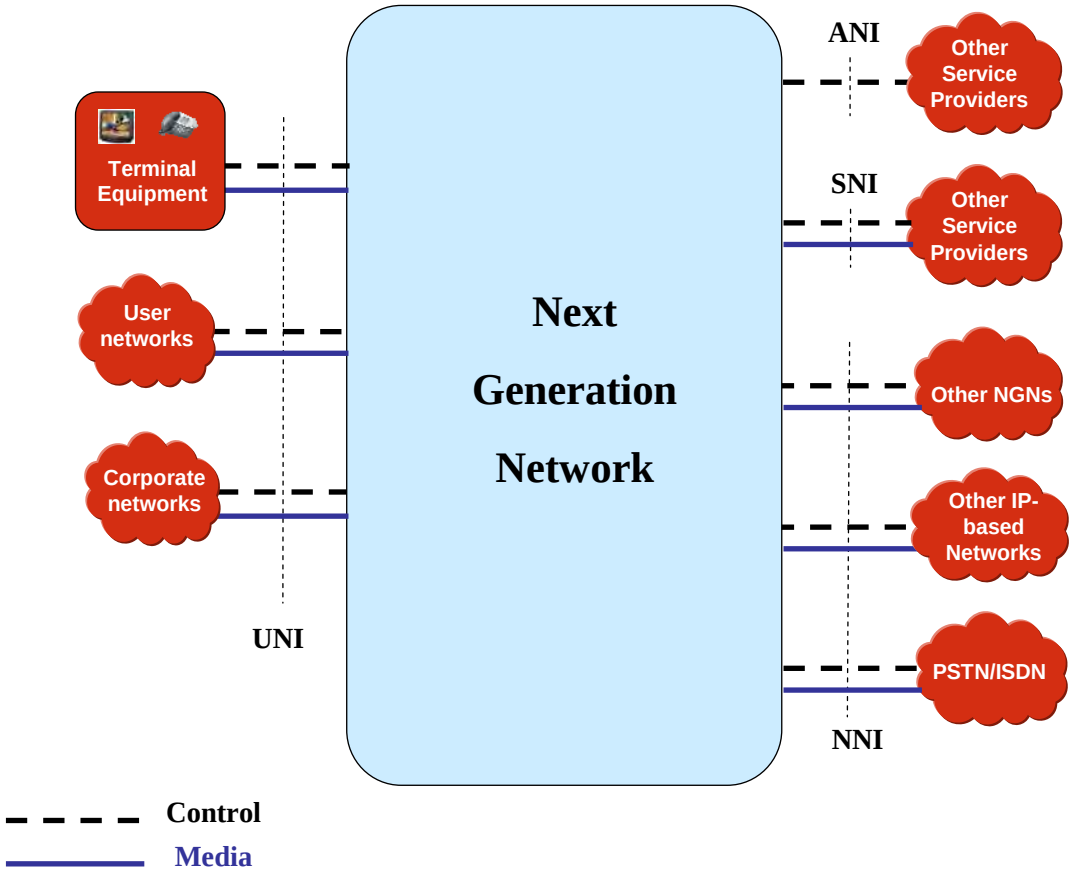

Figure 2 – NGN Connectivity and Interfaces [ITU-T Y.2012]

The interfaces pertaining to network interconnections are:

- Application Network Interface (ANI)
- Service Network Interface (SNI)
- Network-Network Interface (NNI)

Refer to [ATIS-1000018] and [ITU-T Y.2012] for descriptions of the ANI, SNI and NNI.

1.7 Assumptions

The following assumptions are made in this document:

1. An entity (i.e., user or device) must be authorized for ETS by the appropriate U.S. government agency. This includes the enrolment, assignment or issuance, update or change of any identity and the associated attributes or privileges (e.g., role) for ETS.
2. The security (i.e., integrity, confidentiality, authenticity, and availability) of ETS depends on the security of the NGN supporting the ETS communications. It is assumed that the Service Providers will protect the NGN by supporting and adopting security best practices and applicable security standards.
3. This document focuses on network provided security for ETS. Therefore, the requirements should be interpreted as requirements on the Service Provider of ETS.

4. It is assumed that end-to-end ETS communication may traverse different Service Provider domains and that each Service Provider is responsible for security within its domain.
5. Network Elements (e.g., Femtocells), end user equipment, and customer enterprise networks not under the full control of the Service Provider (i.e., in the un-trusted domain) are outside the scope this document.
6. Security requirements for specific access network type and technologies are outside the scope of this document.
7. The security of ETS will be based on mutual agreement and documented in the Service Level Agreement (SLA) between the Authorized Government Agency (currently the Office of Emergency Communications – OEC) and the Service Provider.
8. The security of ETS across Service Provider's networks (including any 3rd-party Provider) will be mutually agreed and documented in the SLA between the Service Providers.
9. The requirements in this specification for the ANI and the SNI only apply to applications or services recognized as ETS.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

2.1 ATIS References

[ATIS-0100004], ATIS-0100004, *Availability and Restorability Aspects of Emergency Telecommunications Service* (ETS).[1]

[ATIS-0100009], ATIS-0100009, *Overview of Standards in Support of Emergency Telecommunications Service* (ETS).[2]

[ATIS-0100016], ATIS-0100016, *End-to-End Service Availability*: *General Definition.*[3]

[ATIS-0100036], ATIS-0100036.2013, *Media Plane Performance Security Impairments for Evolving VoIP/Multimedia Networks.*[4]

[ATIS-1000018], ATIS-100018, *NGN Architecture.*[5]

[ATIS-0100026], ATIS-0100026, *A Methodology for Design of End-To-End Network Reliability for Proactive Network Reliability Planning.*[6]

[ATIS-1000029], ATIS-1000029.2008 (R2013), *Security Requirements for NGN*.[7]

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=23976 >.

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=22974 >.

[3] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=22935 >.

[4] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=27867 >.

[5] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=22964 >.

[6] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=25611 >.

[ATIS-0300276], ATIS-0300276.2008, *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*.[8]

2.2 ITU-T References[9]

[ITU-T E.107], ITU-T Recommendation E.107, *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS.*

[ITU-T M.3342], ITU-T Recommendation M.3342, *Guidelines for the definition of SLA representation templates.*

[ITU-T Y.2012], ITU-T Recommendation Y.2012, *Functional Requirements and Architecture of the NGN of Release 1.*

[ITU-T Y.2701], ITU-T Recommendation Y.2701, *Security requirements for NGN release 1.*

[ITU-T X.800], ITU-T Recommendation X.800, *Security architecture for Open Systems Interconnection for CCITT applications.*

[ITU-T X.811], ITU-T Recommendation X.811, *Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework.*

[ITU-T X.1500], ITU-T Recommendation X.1500, *Overview of cybersecurity information exchange (CYBEX).*

[ITU-T X.1520], ITU-T Recommendation X.1520, *Common vulnerabilities and exposures (CVE).*

[ITU-T X.1521], ITU-T Recommendation X.1521, *Common vulnerability scoring system.*

[ITU-T X.1570], ITU-T Recommendation X.1570, *Discovery mechanisms in the exchange of cybersecurity information*.

2.2 Other[10]

[RFC 2474], IETF RFC 2474, Nichols, K., S. Blake, F. Baker, D. Black. *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* .

[RFC 2475], IETF RFC 2475, Blake, S. et al. *An Architecture for Differentiated Services.*

[RFC 4412], IETF RFC 4412, Schulzrinne, H., and J. Polk. *Communications Resource Priority for the Session Initiation Protocol (SIP)*.

3 Definitions, Acronyms, & Abbreviations

3.1 Definitions

3.1.1 Authentication [X.811]: The provision of assurance of the claimed identity of an entity.

3.1.2 Authorization [X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.3 Claimant [X.811]: An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

---

[7] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=27970 >.

[8] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=25578 >.

[9] These documents are available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[10] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

3.1.4 Emergency Telecommunications Service (ETS): A national service, providing priority telecommunications to the ETS-authorized user in times of disaster and emergency (ITU-T Study Group 2) [E.107].

3.1.5 Government Emergency Telecommunications Service (GETS): One facet of the U.S.A. instantiation of ETS using public telecommunications networks, offered by the government[11] to authorized users for NS/EP purposes. GETS is a circuit-switched form of ETS for voice (and voiceband data) using PIN authorization, in which a user can invoke the service by dialing a GETS-AN or GETS-NT from most phones served by the Public Switched Network (PSN). GETS provides priority treatment across originating, transit, and terminating networks.

3.1.6 NS/EP NGN-Priority Services (NS/EP NGN-PS): The evolution of Legacy GETS and WPS to achieve service continuity in the packet-switched NGN and leverage the NGN to offer new features and priority multimedia services.

3.1.7 NS/EP NGN-PS Data Transport Service: A Service Provider NS/EP service that provides priority transport of non-Gigabit Rate (GBR) data traffic. Invocation and revocation of the service is supported either via Session Initiation Protocol (SIP)-based interactions with an IP Multimedia Subsystem (IMS) Core Network or via Secure Hypertext Transfer Protocol (HTTPS)-based interactions.

3.1.8 NS/EP NGN-PS GBR Data Service: A Service Provider NS/EP service that provides priority transport of GBR data traffic. Invocation and revocation of the service is supported either via SIP-based interactions with an IMS Core Network or via HTTPS-based interactions.

3.1.9 NS/EP NGN-PS Voice Service: A Service Provider NS/EP voice service supported by an IMS Core Network.

3.1.10 NS/EP NGN-PS Video Service: A Service Provider NS/EP video service supported by an IMS Core Network.

3.1.11 Wireless Priority Service (WPS): A circuit-switched form of ETS for voice (and voiceband data) using subscription-based authentication, in which a user can invoke the service by dialing a feature code from a WPS-subscribed mobile phone served by a public wireless network. WPS provides priority treatment across originating and terminating public wireless networks, including priority radio resource assignment upon call origination and termination.

3.1.12 Service Provider (SP): A public telecommunications service provider authorized by the OEC to provide NS/EP NGN-Priority Services.

3.1.13 Priority Treatment: Refers to mechanisms and features that support a greater probability of service success when NS/EP NGN-PS is invoked by a Service User.

3.2 Acronyms & Abbreviations

ANI	Application Network Interface
API	Application Programming Interface
BGP	Border Gateway Protocol
CMIP	Common Management Information Protocol
COS	Class of Service
DBF	Data Border Function
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Control Protocol
DHS	Department of Homeland Security
DN	Directory Number
DNS	Domain Name System
DoS	Denial of Service

[11] NOTE: the Department of Homeland Security Office of Emergency Communications (DHS/OEC) is the government agency responsible for granting ETS privileges to individuals.

EPS	Evolved Packet System
ETS	Emergency Telecommunications Service
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FE	Functional Entity
GBR	Gigabit Rate
GDSRT	Guidelines for the Definitions of SLA Representation Templates
GETS	Government Emergency Telecommunications Service
GETS-AN	Government Emergency Telecommunications Service Access Number
GETS-FC	Government Emergency Telecommunications Service Feature Code
GETS-NT	Government Emergency Telecommunications Service Number Translation
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating Call Session Control Function
IdM	Identity Management
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Protection System
IPsec	IP security
IS-IS	Intermediate System-to-Intermediate System
KPI	Key Performance Indicator
KQI	Key Quality Indicator
LDP	Label Distribution Protocol
LTE	Long Term Evolution
MPLS	Multi-Protocol Label Switching
MS	Media Server
NANP	North American Numbering Plan
NE	Network Element
NGN	Next Generation Network
NIST	National Institute of Standards and Technology
NNI	Network-to-Network Interface
NS	Network System
NS/EP	National Security/Emergency Preparedness
OA&M	Operations, Administration, and Maintenance
OAM&P	Operations, Administration, Maintenance, and Provisioning
OEC	Office of Emergency Communications
OSPF	Open Shortest Path First
OSS	Operations Support System
PBX	Private Branch Exchange
P-CSCF	Proxy Call Session Control Function
PII	Personally Identifiable Information
PIN	Personal Identification Number
PS	Priority Services

PSN	Public Switched Network
QoE	Quality of Experience
QoS	Quality of Service
RBAC	Role Based Access Control
RPH	Resource Priority Header
S&P	Systems and Platforms
SBC	Session Border Controller
SC	Service Customer
S-CSCF	Serving Call Session Control Function
SDP	Service Description Protocol
SEG	Security Gateway
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNI	Server-to-Network Interface
SNMP	Simple Network Management Protocol
SP	Service Provider
SPoC	Single Points of Contact
TL1	Transaction Language 1
TSP	Telecommunications Service Priority
UE	User Equipment
UNI	User-to-Network Interface
URL	Universal Resource Locator
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPS	Wireless Priority Service
XML	Extensible Markup Language

4 General Security Objectives & Requirements

4.1 General Objective

The general objective is to provide network security protection of end-to-end ETS communications that may traverse different network provider domains where each network is responsible for security within its domain on a hop-by-hop basis.

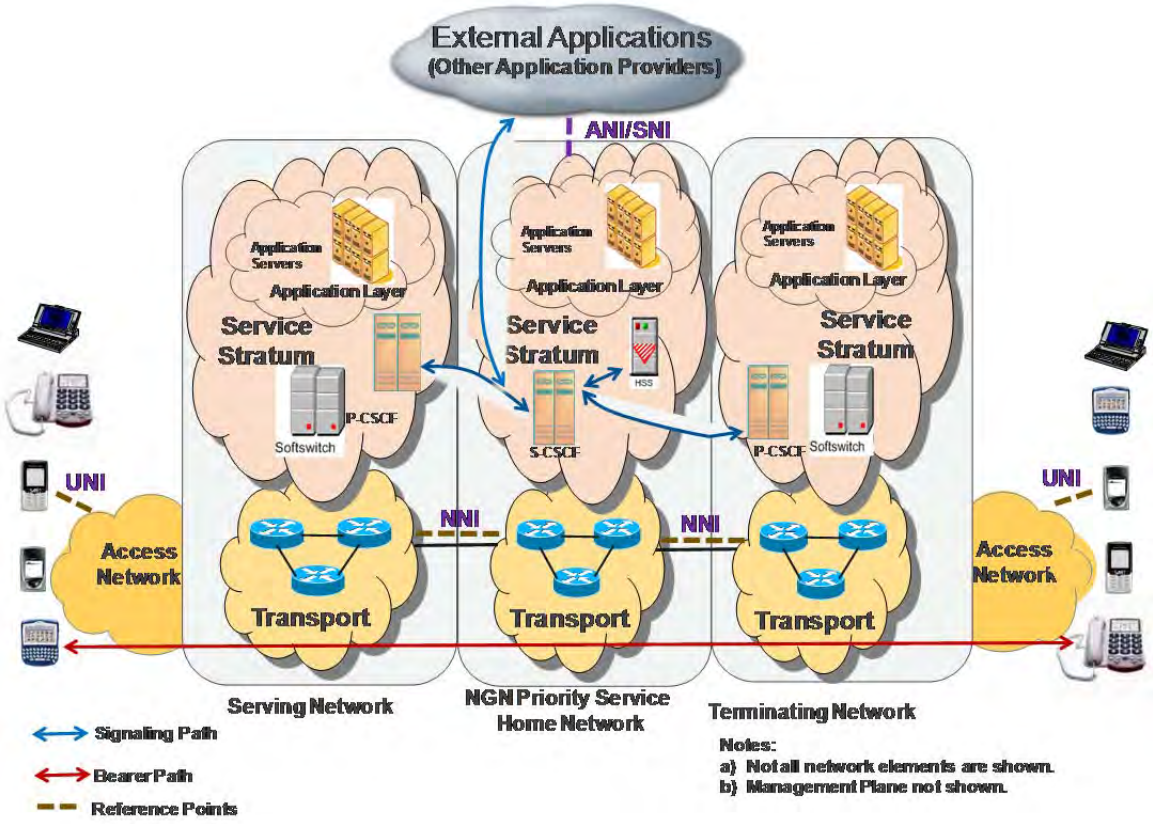

Figure 3 - Example of end-to-end communication across different Service Provider domains

Figure 3 illustrates an example end-to-end architecture including applicable reference points for an end-to-end ETS communication. It shows access networks (in-dependent of specific fixed or wireless technology) that, upon User Equipment (UE) attachment requests, allow network authentication and registration to general-purpose and fixed UEs, and wireless UEs. Figure 3 also illustrates that ETS communications can traverse multiple provider administrative domains. Each provider administrative domain consists of one or more security zones having different degrees of trust (i.e., trusted, trusted but vulnerable, and untrusted) to protect its network elements and its communications. In general, it should be assumed from the perspective of each provider domain that other interconnecting provider domains are untrusted and appropriate security measures need to be considered.

The general objective is for each of the interconnected networks along the path of the end-to-end ETS communication to provide the necessary security protection within its domain including the interconnection to the adjacent network so that the integrity, confidentiality, and availability of the end-to-end ETS communication are not compromised.

4.2 General Guidelines

A structured approach and methodology should be established and implemented between interconnecting networks for ETS through the use of Service Level Agreements (SLAs). This should include:

1. *Security Risk Assessment*: Risk assessment of ETS assets, threats, and vulnerabilities related to interconnection of ETS. It is critical that security risk assessment be performed periodically and when changes, new technology, services, or applications are introduced.
2. *Security Architecture and Solution*: Establishing security policy, security architecture design, and specification of solutions to mitigate identified threats to ETS. This includes establishing the necessary bi-lateral or multi-lateral SLAs for ETS security ([ITU-T M.3342] and [b-TMF GB917] for information on SLAs). Areas addressed include security policies, requirements, architecture design, situational awareness and forensics tools, and infrastructure security to be included in SLAs for interconnection.

3. *Security Implementation*: Implementation and deployment of the security architecture and solutions based on the bi-lateral or multi-lateral SLAs as appropriate for ETS interconnection security.
4. *Security Operations*: Operational measures for the management of the security solutions for ETS interconnection should be specified and implemented. For example, management of insider threats, management of configurable parameters and default values, resiliency and failure recovery operations, ETS security testing, and logging and auditing of ETS security related events.

4.3 ETS Functional Requirements

According to the list of basic functional requirements documented and summarized in Table 1 of [ATIS-0100009], included here for convenience, NS/EP NGN-PS must be protected against unauthorized access.

The Service Provider is required to provide protection to prevent unauthorized access to NGN Priority Services.

This requirement is supported by a number of NS/EP Functional requirements shown in Table 1 of [ATIS-0100009]. The items directly related to Priority Services security are highlighted in blue. They include: Secure Networks, Anonymity, Restorability, Survivability/Endurability, and Reliability/Availability.

Table 1: Original Table of ETS Functional Requirements [ATIS-0100009]

NS/EP Telecommunication Services Functional Requirement	Description
a. Enhanced Priority Treatment	Services supporting NS/EP missions must be provided priority treatment over other traffic.
b. Secure Networks	Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
c. Non-Traceability	Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).
d. Restorability	Should a disruption occur, services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
e. International Connectivity	Services must provide access to and egress from international carriers.
f. Interoperability	Services must interconnect and interoperate with other selected government or private facilities, systems, and networks.
g. Mobility	The communications infrastructure must support transportable, redeployable, or fully mobile communications (e.g., personal communications service, cellular, satellite, high frequency radio).
h. Ubiquitous Coverage	Services must be readily accessible to support the national security leadership and inter- and intra-agency emergency operations, wherever they are located.
i. Survivability/Endurability	Services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or man-made disaster up to and including nuclear war.
j. Voice-Band Service	The service must provide voice-band service in support of presidential and other communications.
k. Broadband Service	The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, web access, and multimedia).
l. Scalable Bandwidth	NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.
m. Affordability	Services must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf technologies, and services).
n. Reliability/Availability	Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

4.4 General Requirements

The Service Provider is required to protect NS/EP NGN-PS communications from security events (e.g., unauthorized access, interception, hijacking, and replay) that would compromise the security of NS/EP NGN-PS in accordance with commercially-available security best practices while the PS traffic is traversing the Service Provider's Network domain.

The following high-level general requirements come as a corollary to the White House mandate.

R-1. The Service Provider shall protect NS/EP NGN-PS communications from security events that would compromise the authenticity of NS/EP NGN-PS in accordance with commercially-available security best practices while the PS traffic is traversing the Service Provider's Network domain.

R-2. The Service Provider shall protect NS/EP NGN-PS communications from security events that would compromise the integrity of NS/EP NGN-PS in accordance with commercially-available security best practices while the PS traffic is traversing the Service Provider's Network domain.

R-3. The Service Provider shall protect NS/EP NGN-PS communications from security events that would compromise the confidentiality of NS/EP NGN-PS in accordance with commercially-available security best practices while the PS traffic is traversing the Service Provider's Network domain.

R-4. The Service Provider shall protect NS/EP NGN-PS communications from security events that would compromise the availability of NS/EP NGN-PS in accordance with commercially-available security best practices while the PS traffic is traversing the Service Provider's Network domain.

In the above requirements, a *domain* is a physical or logical "network segment" over which the Service Provider exercises full administrative and operational control, management, maintenance, and security. A building such as a data center or network operations center might be a trusted zone within a domain, as might each logical partitioning of a network into administrative regions over which the Service Provider has full control of all network equipment and the operating environment.

4.5 Protection of Priority Services User Information

According to the original set of White House requirements, selected users must be able to use NGN Priority Services without risk that the Priority Services User or his location will be identified. This means that selected Priority Services Users must be given anonymity protection.

R-5. Service Provider shall allow selected Priority Services Users to use NGN Priority Services anonymously.

R-6. Service Provider shall protect the confidentiality of selected Priority Services User identities.

R-7. Service Provider shall protect the confidentiality of the location of selected Priority Services Users.

O-1. It is desirable that the Service Provider protect against unauthorized observation or disclosure of NGN Priority Services usage information (e.g., observation of network activities such as web sites that an PS User has visited, PS User IP addresses, or usage patterns such as NGN Priority services traffic volume, locations, time, frequency).

NOTE: The above requirements and objective pertain to the protection of the Service User information with regard to Priority Services. The Service User has certain responsibilities to protect sensitive information (e.g., identities and location). Specifically, it is possible that certain information could be obtained as a result of the Service User's activities outside of Priority Services (e.g., visited web sites) that could be correlated to the Service User subsequent usage of Priority Services. Therefore, it is assumed that the Service User must take certain precautions in this regard.

Anonymity services and features for Priority Services (e.g., priority voice, video, and data transport services) are not within the scope of this document.

4.6 Common Requirements

It is expected that Service Providers would be supporting and using a wide range of security tools and capabilities to protect both NGN PS and the entire network and all supported applications. It is important that appropriate measures be taken to ensure that the use of these security capabilities do not negatively impact the performance of NGN PS or introduce any unintended security compromises to NGN PS.

R-8. Service Provider use of security mechanisms (e.g., intrusion detection systems, deep packet inspection, and encryption) shall not interfere with the priority treatment mechanisms used to support Priority Services.

O-2. It is desirable that the Service Provider use of security tools and capabilities include appropriate measures to minimize negative impacts on NGN Priority Services Quality of Service (QoS) (e.g., by minimizing the introduction of delays).

5 NGN PS Authentication & Access Control

This clause summarizes the current method of authenticating a legacy GETS user and provides requirements that address authentication, authorization, and access control for NGN Priority Services. It also explores the notion of enhanced authentication of Priority Services Users and the NGN to address potential risks related to unauthorized access.

5.1 Protection Against Unauthorized Access

Because the legacy GETS and WPS are to be used only by authorized individuals, it is currently set up to verify authorization via either a Personal Identification Number (PIN) method or by a subscription-based method respectively. These work as follows:

1. The GETS-AN, 8YY GETS-AN, and GETS-NT priority calling methods are currently authenticated and authorized by means of a 12-digit PIN and Priority Services User privileges. The PINs are static and, unlike account passwords, cannot be changed by the Priority Services User. Consequently, industry best security practices for password protection, such as password aging, cannot be applied.
2. The GETS-FC priority calling method currently involves authentication and authorization based on the subscription profile information associated with a particular terminal or service user device. The service user device or terminal identity is authenticated as part of the Service Provider normal registration and authentication, and individual priority calls/sessions are authorized by checking the service subscription profile (i.e., verifying whether the service subscription allows priority calls/session from the device).

In the legacy Public Switched Network (PSN), the methods just described represent the full capability of the authorization process. In an NGN, Priority Services calling methods follow up the legacy authentication and authorization procedures (e.g., PIN Authentication or device subscription validation) by requiring that the NGN Priority Services User register with the IMS Core Network prior to accessing voice priority services.

The methods – PIN verification and device subscription – suffer drawbacks that permit unauthorized access by persons who purloin either a subscriber's PIN or, in the case of GETS-FC, the subscriber's user equipment (e.g., mobile phone). In the case of PINs, the drawback lies in the fact that an unauthorized person who obtains a legitimate Priority Services User's PIN can place priority calls as though he were the legitimate Priority Services User. In the device subscription method, the drawback lies in the fact that device subscription does not explicitly authenticate the Priority Services User; it authenticates only the device, which allows anyone possessing the device to invoke Priority Services.

The remainder of this clause discusses methods to address the drawbacks of each of these methods.

5.2 Enhancing Device Subscription Validation

The drawback to device subscription validation is that it does not explicitly authenticate the Priority Services User, but rather the PS User's device, as was mentioned above. Two methods of resolving the weakness of this approach use the notion of a secret possessed by the device owner:

1. The Priority Services User can be required to use the capabilities available in many, if not all, modern UE devices that force the PS User to supply an authenticator (e.g., an *n*-digit PIN) that the UE must recognize before it will permit itself to be used. Such an authenticator would bind the PS User to the device, and thus, in essence, authenticate the PS User during the device subscription validation process.
2. Alternatively, the Priority Services User can be required to provide a Priority Services PIN that authenticates the PS User in exactly the same way it authenticates the GETS-AN user. To support this alternative, Identity Management (IdM) mechanisms could be used to correlate and bind the authorization of a Priority Services User via his Priority Services PIN with the identification and authentication of a subscribed user device based on a subscription profile. For example, to accomplish this, after a Priority Services User attaches to the access network and registers with the Core IMS, and a Priority Services

session is invoked, an IdM application requests device identification and authentication from the Home Subscriber Server (HSS) and then sends a challenge to the Priority Services User to request his assigned PIN. The Priority Services User authentication is correlated with and bound to the device information to verify authorization for the NGN Priority Services.

O-3. For NGN GETS-FC, it is desirable that Service Providers offer a capability to authenticate both the UE and the Priority Services User and bind the two to verify authorization to use NGN Priority Service.

As also shown in Table 2, this is applicable to the NGN GETS-FC Invocation.

The first option can be enforced through OEC policy that, if not already in existence, can be produced and levied on each Priority Services User.

The second option requires that the Service Provider support a new authentication method. This will require necessary prototyping and testing prior to mandating the support of such mechanism.

5.3 Enhancing PIN Authentication & Authorization for Voice Services

The current method by which a Priority Services User authenticates himself is to dial an NGN Priority Services special telephone number (e.g., 710-NCS-GETS) and then enter the 12-digit PIN on the telephone keypad. The PIN may be sent across the network to the verifying mechanism in an unprotected fashion, suggesting that it is vulnerable to discovery. Such a vulnerability could open the door to access by unauthorized callers and to possible eavesdropping on Priority Services Users during emergencies.

The following explores a number of scenarios whereby PIN mechanism vulnerabilities can be exploited by adversaries. It assumes that one or more PINs have been compromised by adversaries having serious malicious intentions. PINs might be compromised in many ways such as, through social engineering schemes and eavesdropping on the start of a Priority Services call, when the Priority Services User provides the PIN and it is transmitted unprotected across the network.

If an attacker obtains a PIN and the PIN compromise is not discovered, unauthorized priority calls to a destination of choice can be made using a GETS-AN to any routable number, based on the Priority Services User's assigned privileges. A consequence of this threat is that during severe network congestion (e.g., as a result of a terrorist attack), the attackers could be motivated to use Priority Services because it might be their only means to communicate with one another. Priority calls can also be made to a GETS-NT, but since the call destination is not controllable by the PS User, the benefit could be very limited to the casual attacker attempting to exploit the system, unless the destination allows call redirection or re-origination. A consequence of this threat is that savvy attackers might be able to glean a certain amount of intelligence. For example, attackers might be able to masquerade as NS/EP personnel and obtain information about emergency operations, participant identities, and their locations. In addition, this threat could have wider consequences because the NGN Priority Services does not prevent the sharing of PINs.

Formidable adversaries (e.g., nation states, terrorist organizations, and organized crime) who are able to obtain valid PINs in advance might use them to initiate Denial of Service (DoS) and network congestion attacks during a disaster event. For example, a coordinated attack involving the use of computer-generated calls could generate a large volume of NGN Priority Services calls using valid PINs and directory numbers from multiple locations and different regions. Such an attack would render Priority Services ineffective, since an overwhelming volume of priority calls would mean that Priority Services Users would be contending for resources just as ordinary service users would.

The above discussion suggests that PIN-based authentication might be insufficient to mitigate the risk of attacks by adversaries who come into possession of PINs. It further suggests that enhanced authentication be considered as an alternative or in addition to PIN-based authentication. A number of methods are available, including:

1. Verification of the Priority Services User by an audio query-response in which the PS User, after entering the PIN, is prompted by the network to respond to a pre-arranged question (e.g., mother's maiden name). This enhancement counters the threat of compromised PIN, and while it can be defeated by eavesdropping, the attacker must work harder to do so (by positioning himself to intercept all of the Priority Services User's calls in hopes of listening in on the PS authentication process). The prearranged

question and answer would need to be negotiated when the PS User's Priority Services account is initialized. It should be noted that this verification method does not depend on voice recognition; only the correct answer to the query. (It is unclear how reliable voice recognition would be, since stress can cause changes in the speaker's voice, which could lead to a large number of failed recognitions.)

2. Use of hardware tokens carried by each Priority Services User and verifiable by an NGN Priority Services application. One-time PINs generated by a hardware token and synchronized with the application would overcome most, if not all, of the problems associated with theft of PINs.

Both of these methods are *two-factor* authentication schemes that require two pieces of information from the user prior to granting access. The first uses two things the user knows (a PIN and an answer); the second uses one thing he possesses (a one-time PIN on a token) and one thing he knows (a permanent PIN). Other two-factor authentication schemes exist, but they typically work for more sophisticated devices than a phone and so are not practical as a general authentication method for Priority Services.

As an aside, it was stated earlier that the PIN cannot be changed by the Priority Services User. Though this might seem a drawback, it is probably a reasonable limitation, since allowing the Priority Services User to change his PIN also permits an attacker who has compromised the PIN to change it and thus deny service to the PIN's owner. Furthermore, an attacker who has stolen the PINs of many Priority Services Users could easily engineer large-scale denial of service of those users whose PINs had been stolen. (By contrast, an attacker who has merely stolen a PIN can use it to place calls and perhaps listen in on NS/EP conference calls, but cannot deny service to the PIN owner.)

The capability to allow the Priority Services User to change his PIN safely could be managed via a PIN-changing application that prompts the Priority Services User for a special PIN (a PIN-update PIN) before it will change the PIN. However, the degree of risk mitigation gained by allowing Priority Services Users to change their PINs must be evaluated before such an application is considered. In particular, its advantage over the current no-change strategy must be determined, especially since Priority Services Users have no obvious incentive to change their PINs unless forced to do so.

Table 2 summarizes various NGN Priority Services voice call invocation types, current authentication and authorization methods, and suggested future authentication and authorization methods to be considered. It is self-explanatory – except possibly for the rightmost column, *Authentication and Authorization Proposed Enhanced Methods*, which is intended to reflect the idea that the present methods are to be augmented by the proposed methods in this column. The fact that several proposed methods are listed is merely to suggest the alternatives and does not imply that all are to be used simultaneously.

Table 2: NGN Priority Services Existing and Proposed Enhanced Authentication and Authorization Methods for Voice Services

Service Invocation Type	UE Type	Destination DN Type	Authentication and Authorization Present Methods	Authentication and Authorization Proposed Enhanced Methods
GETS-AN or 8YY GETS-AN	Any general purpose UE (fixed or mobile) that supports basic voice calls	Normal NANP or E.164 number (or a number that has been forwarded to such number)	PIN Authentication Calling Privileges Authorization	Audio-based Query-response[12] One-time PIN
		GETS-NT or a DN forwarded to GETS-NT	PIN Authentication Calling Privileges Authorization Number Translation	Audio-based Query-response One-time PIN
		GETS-PDN or a DN forwarded to GETS-PDN		
		DN forwarded to GETS-AN[13]		Limit forwarding to GETS-AN as a Destination DN
GETS-NT		Translated routable number	PIN Authentication Calling Privileges Authorization Number Translation	Audio-based Query-response One-time PIN
GETS-FC	Voice-capable UE with subscription	Normal NANP or E.164 number (or a number that has been forwarded to such number)	UE authentication and Subscription Validation Calling Privileges Authorization	Audio-based Query-response Priority Services User and UE Authenticator Binding of Priority Services User and UE authentication
		GETS-NT or a DN forwarded to GETS-NT		
		GETS-AN or a DN forwarded to GETS-AN		

The proposed authentication and authorization methods are expected to have a low to medium effect on the user in terms of additional time and effort needed to invoke Priority Services. This “user experience” is an important

[12] One approach is to have the network prompt the NGN Priority Service User to respond with a secret after a successful PIN authentication. It is assumed that the Service User has pre-recorded a secret audio response when prompted during the initial NGN Priority Service activation process and that the response has been acknowledged by the Service User and then securely stored by the network. The network will play back the pre-recorded query to allow the NGN Priority Service User to provide the correct response and thus authenticate himself.

[13] This will result in a recursive looping scenario if attackers using stolen PINs reenter the same destination DNs. In extreme cases, this may cause localized network congestion.

consideration, since it must not pose a distraction or an impediment to the user. The usability of any replacement method should, in fact, be better in terms of ease of use (such as remembering pieces of information, keeping track of and manipulating a token, typing a PIN or password, and speedily completing the authentication process).

The proposed authentication and authorization methods are expected to provide a medium to high level of protection when compared to the current methods, which are estimated to be below par by today's security conventions. On the down side, they are expected to impose some increases in the complexity of:

- The user experience, which is likely to vary from application to application (e.g., authentication for an e-mail versus for voice calls).
- Operations – the administrative effort needed to support Priority Services.

These complexities, along with the technical complexity associated with these proposed methods, should be tagged as areas for careful study should the proposed methods be deemed worth implementing.

In addition, these enhancements should be considered in the context of Priority Services applications beyond voice applications. Specifically, applications such as priority data services would require a higher degree of assurance or confidence of the Priority Services User's identity and of the level of authorization to access the application and its associated resource. In addition, enhanced authentication mechanisms may not necessarily have to be supported for all applications and all Priority Services Users. For example, strong authentication could be applied to a smaller population of Priority Services User as a factor of the privileges or resources being authorized.

O-4. In addition to the existing PIN-based and subscription-based (single-factor) authentication methods, it is desirable that the Service Provider offer capabilities for two or more factor authentication of the Priority Services User for selected Priority Services.

Proposed enhanced authentication methods may include the use of:

(a) Audio-based query-response using speech or voice recognition technology.

(b) One-time authentication.

(c) Binding of the Priority Services User and UE authentication.

(d) Biometric methods.

In addition to enhanced capabilities for authenticating the user, NGN Priority Services will need to be augmented with capabilities that permit monitoring of PIN and subscription validation activities for Priority Services usage. The following requirements address these points.

5.4 Authentication of NGN Priority Services, Service Provider

Priority Services Users of GETS-AN, 8YY GETS-AN, GETS-NT, and GETS-PDN services authenticate themselves to the Service Provider using a PIN at the application layer. However, the Service Provider does not authenticate itself to the user except to provide the expected prompts and service logic. Similarly, for GETS-FC the subscribed UE does not authenticate the Service Provider except for the case of 4G technologies such as Evolved Packet System/Long Term Evolution (EPS/LTE). Capabilities to allow the Priority Services User to identify and authenticate the Service Provider would minimize risks associated with imposter Service Providers (e.g., threat of an attacker inserting fake access network equipment masquerading as a legitimate Service Provider).

O-5. It is desirable that the Service Provider provide capabilities for the Priority Services User to identify and authenticate the Service Provider.

The ability of the Priority Services User to verify that it is attached to a legitimate Service Provider home core network, serving, or visiting network and obtain NGN Priority Services from a legitimate Service Provider would provide protection against attackers masquerading as a legitimate Service Provider.

NOTE: This objective may be changed to a requirement after further study. Specifically, this objective may have to be a requirement for NGN Priority Services applications beyond voice.

NOTE: Specific measures or capabilities that could be used are for further study. For example, a simple mutual authentication procedure performed by having a user-specific audio selection played after the user submits a PIN or having the voice used to prompt for the Directory Number (DN) be the user's own voice.

6 Network-to-Network Interface

6.1 Authentication

6.1.1 Mutual Authentication of Service Provider

End-to-end communication for NGN Priority Services may involve multiple network segments and administrative domains (e.g., originating access network, NGN PS Service Provider network, intermediate network, terminating access network). When receiving NGN Priority Services traffic, the Service Provider is required to verify the validity and authorization of the source (e.g., network) of the received traffic. When handing off NGN Priority Services traffic, the Service Provider is required to verify the validity and authorization of the entity to which it is handing off the NGN traffic (e.g., network). Presently, security trust relationships for interconnection are verifiable only through direct physical interconnection between two interconnected networks.

R-9. Service Providers shall mutually authenticate each other when exchanging (i.e., handing off or receiving) NGN Priority Services traffic. This includes any NGN Priority Services signaling or media traffic exchanges between two Service Providers across NNI interconnection.

This may be accomplished through verification of direct physical interconnections and SLAs.

There is no dynamic means to verify the integrity of priority information received from remote networks[14] in real time. A network receiving NGN Priority Services traffic and control signaling in the post authentication and authorization phase has to trust that the sending network is presenting a legitimate NGN Priority Services call or session. In the case of an intermediate network handing off to a terminating network, the chain of trust may extend further back to the originating network. Dynamic real-time capabilities to mutually authenticate Service Providers and validate the integrity of priority information are needed to prevent illegitimate entities masquerading, forging, or misrepresenting legitimate Service Providers.

NOTE: Dynamic means to authenticate interconnected networks and remote network and verify the integrity of priority information are for further study. The intention here is not authentication on a per call/session basis. The intention is to introduce the notion of mechanisms to do authentication on an as-needed basis or periodically.

6.2 Access Control

Access control at the NNI refers to the capability of the receiving network to accept or reject specific traffic inbound from a neighboring network and to restrict access to resources within the network by entities outside the network.

In the first case, the requirement for access control stems from the recognition that the IP-based NGN bears all traffic within the same network (unlike the PSN, in which media traffic and signaling traffic traverse two distinct networks). Therefore, the network needs a capability to reject incoming traffic that does not meet mutually-agreed upon policy, such as signaling traffic based on protocols it does not recognize. It may also need a capability to reject specific messages within a signaling stream. Finally, it may need a capability to reject specific protocols that the network architects, engineers, or security architects deem unwanted.

[14] Two networks that are not directly connected are considered remote.

In the second case, the network needs a capability to control access to resources (e.g., databases) that it manages, preventing entities outside the network from accessing such resources unless those entities are given specific permission (or conversely, allowing all access except to specific entities).

The following requirements address these two needs and the added need to detect all access attempts and record them in a security audit log. Though a security logging mechanism capable of logging all security events such as access control violations is mandated for information systems and network devices (as a requirement to the equipment vendor), it is understood that the Service Provider can configure the logging mechanism to record only those access control events that it deems important according to its security policy (or to other criteria). The Service Provider can therefore log all access attempts or log only those attempts that violate its access control policy. While the Service Provider might recognize that it is important that both successful events and unsuccessful events be recorded, should they be needed for subsequent investigation or security analysis following a security breach or event, it must base its decision to include all or only a subset of those events for reasons that have to do with resources, costs, or other factors.

R-10. The Service Provider shall establish rules and enforce access control measures to protect against unauthorized communications across the NNIs. Specifically, the SPs should only allow communications to traverse the NNI between NEs that have been identified and pre-authorized (e.g., through SLAs).

R-11. When receiving NGN Priority Services signaling traffic from another service provider, the Service Provider shall verify the trust relationships between itself and the service provider from which it receives the traffic.

R-12. When receiving NGN Priority Services media traffic from another service provider, the Service Provider shall verify the trust relationships of the service provider from which it receives NGN Priority Services traffic.

R-13. When handing off NGN Priority Services signaling traffic to another service provider, the Service Provider shall verify the trust relationships of the service provider to which it hands off NGN Priority Services traffic.

R-14. When handing off NGN Priority Services media traffic to another service provider, the Service Provider shall verify the trust relationships of the service provider to which it hands NGN Priority Services traffic.

The Service Provider is required to detect and log successful and unsuccessful attempts to access the network at the NNIs, as discussed in 10.1.5.3

6.3 Integrity

End-to-end communication for NGN PS may involve multiple network segments and administrative domains (e.g., originating access network, NGN PS provider network, intermediate networks, terminating access network). This clause provides requirements related to the security protection of network interconnection interfaces and inter-network communications (i.e., inter-domain). Inter-network NGN PS communications have to be protected against interception, corruption, and manipulation.

R-15. The Service Provider shall protect the integrity of all inter-network NGN PS signaling traffic crossing NNIs.

R-16. The Service Provider shall protect the integrity of all inter-network NGN PS media traffic crossing NNIs.

Actions that could be taken to protect the integrity of signaling and media traffic include, but are not limited to:

a) Physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures).
b) Cryptographic protection.
c) Establishment and enforcement of appropriate integrity requirements defined in Service Level

Agreements.
d) Monitoring integrity of NNIs configurations.

6.4 Confidentiality

The Service Provider is required to protect NGN PS communications against unauthorized access. Media streams (e.g., voice) have to be protected against unauthorized access because eavesdropping on NGN PS media streams could reveal sensitive security information (i.e., conveyed in the media communication). Similarly, signaling information has to be protected from eavesdropping to reduce the chance of signaling traffic analysis revealing sensitive information having a potential for misuse (e.g., calling patterns, location information, and identity of Priority Services Users).

While confidentiality protection is often associated with cryptographic mechanisms, the requirements in this clause to provide confidentiality protection of NGN PS are not intended to imply that cryptographic must be used in all scenarios or for all NGN PS end-to-end traffic flows. The intent of the requirements of this clause is that the service provider must provide and implement the necessary measures to ensure that NGN PS communications are protected from eavesdropping. This means that each segment of an NGN PS communication (both signaling and media) should be examined as the communication traverses the network (i.e., untrusted, trusted but vulnerable, and trusted) to determine the appropriate mechanisms to be used to provide confidentiality protection, as mandated by a security policy. For example, it might be possible to provide confidentiality protection through the use of physical and the associated operation means in specific segments of a network (i.e., trusted segment) as follows:

- Physical means, such as dedicated facilities, provide confidentiality by placing PS traffic on a given physical connection, and restricting the access to that connection to only the parties whose data traverses the connection. Physical security at the endpoints in the form of restricted-access Network Elements (NEs) supplement the physical protection of confidential information by ensuring that unauthorized access at the endpoints cannot be obtained. If the endpoints and the physical path over which confidential PS traffic travels have adequate physical protection, then confidentiality requirements can be met without resorting to cryptography.
- SLAs can provide confidentially by specifying the manner in which PS traffic will be handled by the Service Providers in a peering environment. For instance, if the NEs that handle NGN PS traffic belong to cooperating Service Providers who have established SLAs that specify an approved level of confidentiality by virtue of their enforcement of the SLA, then requirements for confidentiality can be met without cryptography.

In certain network segments, the nature of the security risk or trust scenario (e.g., untrusted IP transport network segment) might rule out all but cryptographic mechanisms as only means to provide confidentiality protection. Therefore, when physical security and the associated operational measures, or other means, cannot mitigate confidentiality risks, cryptographic means would be needed. An example of such a scenario is when a NGN PS communication is traversing an untrusted portion of the network. In this context, *untrusted* refers to the situation in which NGN PS traffic passes through an untrusted zone, as defined in Annex A or a situation in which NGN PS traffic passes across physical or logical facilities, NEs, or provider environments in which no enforced security policy exists or can be relied upon.

R-17. The Service Provider shall protect the confidentiality of all inter-network NGN PS signaling crossing NNIs.

R-18. The Service Provider shall protect the confidentiality of all inter-network NGN PS media traffic crossing NNIs.

Actions that could be taken to protect the confidentiality of signaling and media traffic include, but are not limited to:

(a) Physical security measures (e.g., physical protection of network elements, transmission medium, and facilities, and enforcement of appropriate access control measures).
(b) Cryptographic protection.
(c) Establishment and enforcement of appropriate confidentiality requirements defined in Service Level

Agreements.

7 User-to-Network Interface

The User-to-Network Interface (UNI) is the point of separation between a carrier‘s facilities and the service user’s installation, at which both the technical interface and the division of operational responsibility are established. The UNI has two common “flavors”: the interface between an enterprise customer network (e.g., an IP-based Private Branch Exchange, or PBX) and the public carrier network, or the interface between the service user and a public carrier network. There are two broad types of endpoints:

1. An individual UE, such as SIP phones and analog telephone adapters.
2. An aggregate UE, such as IP PBXs.

When considering the threat spectrum and modes of attack against an NGN, it is reasonable to assume that the number of attacks entering a given network across the UNI exceeds the number entering from a peer network across an NNI or ANI/SNI. It follows that the security requirements for UNI-based security must address a significant portion of the threat spectrum, and must be implementable with reasonable effort. The security measures must address signaling and control thoroughly, since the control plane offers the most damaging avenue of attack. They must also address the protection of media, since confidentiality and integrity of media data can be considered important during a crisis situation or for high priority PS Users. Therefore, the requirements that specify the security measures and mechanisms that must be in place at the UNI must address both signaling and, selectively, media. Furthermore, since individual UE endpoints interact with the network differently than aggregate UE endpoints, the UNI requirements need to address both kinds of UE endpoints. An example of why this is so can be found in the fact that an IP PBX can register the individual UE endpoints within its private enterprise IP network or perform an implicit registration of all UE endpoints within the enterprise as an implicit private registration set, which is not a point of concern for individual UE endpoints.

As in other clauses of this report, the security requirements for the UNI are grouped under the umbrella of the basic security functions: authentication, authorization, access control, integrity, and confidentiality (availability is handled separately). The requirements within each of those groupings address both the signaling and media aspects of the UNI.

7.1 Authentication

Prior to allowing a UE to connect to the access network, the access node must verify the authenticity of the UE, to reduce the likelihood of malicious or unauthorized network intrusions via the access network. In addition, the signaling node (the Proxy Call Session Control Function, or P-CSCF, in IMS) must authenticate the UE prior to establishing services requested by the UE. This two-step authentication is necessary to verify that the UE is authorized at both the access level and the service level. The need for two-step authentication is particularly evident when the access level and the service level capabilities are being offered by two distinct service providers, since the service level provider will have no way, in general, to gain authentication information about the UE from the access level provider unless an IdM infrastructure is implemented to provide authentication assurance transparent to the Priority Services User.

R-19. The Service Provider shall identify and authenticate the UE at the access node prior to establishing a communications path between the UE and the access network (i.e., before a service request is permitted).

R-20. The Service Provider shall identify and authenticate the UE at the core IMS network signaling node (e.g., P-CSCF) prior to providing services to the UE.

In cases where the service user, such as a Priority Services user, needs assurances of the authenticity of the service provider, it is desirable to give the networks the capability to authenticate themselves to the UE just as the

UE authenticates itself to them. The access and signaling networks should therefore be given the capability to negotiate mutual authentication with the UE.

7.2 Access Control

Access control at the UNI refers to the capability of the access network to accept or reject specific traffic inbound from a UE and to restrict UE access to resources within the network. The access node needs to support mechanisms that allow it to control inbound traffic and restrict access to network resources. The following requirements address these two needs and the added need to monitor and record all access events (e.g., failed attempts, successful accesses). The events to be monitored can be specified (by policy, for example), but the capability to log all attempts should be mandated, with the understanding that the logging mechanisms can be configured to record only those access control events that are deemed important according to policy or other criteria.

R-21. The Service Provider shall monitor and screen UNI traffic to protect against unauthorized and harmful content entering the network at UNIs.

R-22. The Service Provider shall establish rules and enforce access control measures to prevent unauthorized access to network elements and systems supporting NGN Priority Services via UNIs.

The Service Provider is required to detect and log successful and unsuccessful attempts to access the network at the UNIs, as discussed in 10.1.5.3.

7.3 Integrity

End-to-end communication for NGN PS may involve multiple network segments and administrative domains (e.g., originating access network, NGN PS provider network, intermediate networks, terminating access network). This clause provides requirements related to the security protection of Priority Services User and network interconnection interfaces. Priority Services User and network interconnection is between the originating/terminating access network and signaling/service control networks. NGN PS communications have to be protected against interception, corruption and manipulation.

R-23. The Service Provider shall protect the integrity of all NGN PS related signaling crossing UNIs.

R-24. The Service Provider shall protect the integrity of Priority Services User UE and access network signaling as the prerequisite for the NGN PS signaling.

R-25. The Service Provider shall protect the integrity of all NGN PS media crossing UNIs between the Priority Services User UE and the transport network.

R-26. The Service Provider shall protect the integrity of all NGN User Plane (media) traffic crossing UNIs between the Priority Services User UE and the cellular access network (air interface).

Actions that could be taken to protect the integrity of signaling and media traffic include, but are not limited to:

(a) Physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures).
(b) Cryptographic protection.
(c) Establishment and enforcement of appropriate integrity requirements defined in Service Level Agreements that include integrity requirements and objectives.
(d) Monitoring integrity of UNIs configurations.

7.4 Confidentiality

As stated in 6.4, the Service Provider is required to protect NGN PS communications against unauthorized access. Media streams (e.g., voice) have to be protected against unauthorized access because eavesdropping on NGN PS media streams could reveal sensitive security information (i.e., conveyed in the media communication). Similarly, signaling information has to be protected from eavesdropping to reduce the chance of signaling traffic analysis revealing sensitive information having a potential for misuse (e.g., calling patterns, location information, and identity of Priority Services Users). The Service Provider is required to protect NGN PS communications against unauthorized access. Media streams (e.g., voice) have to be protected against unauthorized access because eavesdropping on NGN PS media streams could reveal sensitive security information (i.e., conveyed in the media communication).

R-27. The Service Provider shall protect the confidentiality of all NGN PS signaling crossing UNIs between the Priority Services User and the core network.

R-28. The Service Provider shall protect the confidentiality of signaling traffic between the Priority Services User UE and the access network as the prerequisite for the NGN PS signaling.

R-29. The Service Provider shall protect the confidentiality of all NGN PS media traffic crossing UNIs between the Priority Services User and the transport network.

R-30. The Service Provider shall protect the confidentiality of all User Plane (media) traffic crossing UNIs between the Priority Services User UE and the cellular access network (air interface).

Actions that could be taken to protect the confidentiality of signaling and media traffic include, but are not limited to:

(a) Physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures).
(b) Cryptographic protection.
(c) Establishment and enforcement of appropriate confidentiality requirements defined in Service Level Agreements.

7.5 Data Communications Between Authorized Government Agency & Service Provider

There will be data communications between the Authorized Government Agency (currently the OEC) and the Service Providers to exchange updates to NGN PS authorization information. In particular, this pertains to the NGN PS GETS Credentials database. Not all Service Providers will support the NGN PS Credentials database; some who do not may forward calls for authorization to one who does, and others who do not may arrange for authorization access by contracting with a Service Provider or 3rd-party that does support the database. The database generally contains NGN PS GETS Credentials (e.g., GETS PIN), and for each credential, the approved NS/EP NGN-PS service privileges, including Service User's priority level.

The following requirements pertain to the security protection of data communications between the Authorized Government Agency (currently the OEC) and the Service Providers (e.g., data communications to update NGN PS GETS Credentials database).

7.5.1 Authentication

R-31. Subject to mutual agreement with the OEC, the Service Provider and the OEC shall mutually authenticate each other for data communications that support NGN PS (e.g., data communications to update NGN PS GETS Credentials database).

7.5.2 Access Control

R-32. Subject to mutual agreement with the OEC, the Service Provider and the OEC shall establish rules and enforce access control measures to protect against unauthorized communications between the OEC and the Service Provider.

7.5.3 Integrity

R-33. Subject to mutual agreement with the OEC, the Service Provider and the OEC shall protect the integrity of data communications (e.g., data communications to update NGN PS GETS Credentials database) between the OEC and the Service Provider.

7.5.4 Confidentiality

R-34. Subject to mutual agreement with the OEC, the Service Provider and the OEC shall protect the confidentiality of data communications (e.g., data communications to update NGN PS GETS Credentials database) between the OEC and the Service Provider.

8 Application/Server-to-Network Interface

NOTE: Reference to "3rd-party" in this clause refers only to entities with which the Service Provider has a relationship.

8.1 Authentication

Actions to support recognized NGN Priority Services may involve multiple network segments and administrative domains (e.g., originating access network, NGN Priority Services Provider network, Content Partner Network, or 3rd-party Application Provider Network). Content Partner Networks communicate with the NGN Priority Services Provider through an SNI, which usually uses non-session-based protocols (e.g., Internet protocols such as HTTP) to exchange both signaling and media information. An Application Program Interface (API) is primarily used for session-based signaling exchanges between a 3rd-party application provider and the NGN Priority Services Provider to provide value-added services and to enhance NGN Priority Services service logic within the NGN Priority Services Provider Network.

When receiving requests for NGN Priority Services, the Service Provider should verify the validity and authorization of the source of the requests. When returning the output of an NGN Priority Services application, the Service Provider should verify the validity and authorization of the Content Partner network or 3rd-party Application Provider to which it is handing off the output. Where today, security trust relationships for such interactions might be assumed, the potential sensitivity of NGN-based Priority Services applications might necessitate an active effort to verify trust.

R-35. The Service Provider and the 3rd-party Application/Content Provider shall mutually authenticate each other when exchanging (i.e., handing off or receiving) NGN Priority Services traffic. This includes any NGN Priority Services signaling or media traffic exchanges crossing application-to-network interface (ANI) and server-to-network (SNI) interconnections.

NOTE: This requirement is not intended to imply authentication on a per call/session basis. The intention is to perform authentication on an as-needed basis or periodically.

This may be accomplished through verification of direct physical interconnections and SLAs.

There is no dynamic means to verify the integrity of priority information received from remote networks[15] in real time. A network receiving NGN Priority Services traffic and control signaling in the post authentication and

[15] Two networks that are not directly connected are considered remote.

authorization phase has to trust that the sending network is presenting a legitimate NGN Priority Services call or session. In the case of an intermediate network handing off to a terminating network, the chain of trust may extend further back to the originating network. Dynamic real-time capabilities to mutually authenticate Service Providers or Application/Content Providers and validate the integrity of priority information is needed to prevent illegitimate entities masquerading, forging, or misrepresenting legitimate Service Providers or Application/Content Providers.

NOTE: Dynamic means to authenticate interconnected networks and remote network and verify the integrity of priority information are for further study.

8.2 Access Control

Access control at the ANI/SNI refers to the capability of the receiving network to accept or reject specific traffic inbound from a neighboring network and to restrict access to resources within the network by entities outside the network.

In the first case, the requirement for access control stems from the recognition that the IP-based NGN bears all traffic within the same network (unlike the PSN, in which media traffic and signaling traffic traverse two distinct networks). Therefore, the network needs a capability to reject incoming traffic that does not meet mutually-agreed upon policy, such as signaling traffic based on protocols it does not recognize. It may also need a capability to reject specific messages within a signaling stream. Finally, it may need a capability to reject specific protocols that the network architects, engineers, or security architects deem unwanted.

In the second case, the network needs a capability to control access to resources (e.g., databases) that it stewards, preventing entities outside the network from accessing such resources unless those entities are given specific permission (or conversely, allowing all access except to specific entities).

The following requirements address these two needs and the added need to monitor and record all access attempts. It should be noted that such monitoring can be configured (by policy, for instance) to log all access attempts or to log only those attempts that violate the access control policy. The *capability* to log all attempts should therefore be mandated (as a requirement to the equipment vendor), with an understanding that the Service Provider will configure the logging mechanisms to record only those access control events that are deemed important according to its security policy or to other criteria.

R-36. The Service Provider shall monitor and screen traffic to protect against unauthorized and harmful content entering the network at ANI/SNIs.

R-37. The Service Provider shall establish rules and enforce access control measures to prevent unauthorized access to network elements and systems supporting NGN Priority Services via ANI/NNIs.

R-38. When receiving NGN Priority Services signaling traffic from a 3rd-party Application/Content Provider, the Service Provider shall verify the trust relationship of the service provider from which it is receiving the NGN Priority Services traffic.

R-39. When receiving NGN Priority Services media traffic from a 3rd-party Application/Content Provider, the Service Provider shall verify the trust relationship of the service provider from which it is receiving the NGN Priority Services traffic.

R-40. When handing off NGN Priority Services signaling traffic to a 3rd-party Application/Content Provider, the Service Provider shall verify the trust relationship of the 3rd-party Application/Content Provider to which it is handing off the NGN Priority Services traffic.

R-41. When handing off NGN Priority Services media traffic to a 3rd-party Application/Content Provider, the Service Provider shall verify the trust relationship of the 3rd-party Application/Content Provider to which it is handing off the NGN Priority Services traffic.

The Service Provider is required to detect and log successful and unsuccessful attempts to access the network at the ANI/SNIs, as discussed in 10.1.5.3.

8.3 Integrity

End-to-end communication for NGN PS may involve multiple network segments and administrative domains (e.g., originating access network, NGN PS provider network, intermediate networks, terminating access network). This clause provides requirements related to the security protection of network interconnection interfaces and inter-network communications (i.e., inter-domain). Inter-network NGN PS communications have to be protected against interception, corruption, and manipulation.

R-42. The Service Provider shall protect the integrity of all inter-network NGN PS signaling crossing ANIs and SNIs.

R-43. The Service Provider shall protect the integrity of all inter-network NGN PS media traffic crossing ANIs and SNIs.

Actions that could be taken to protect the integrity of signaling and media traffic include, but are not limited to:

(a) Physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures).
(b) Cryptographic protection.
(c) Establishment and enforcement of appropriate integrity requirements defined in Service Level Agreements that include integrity requirements and objectives.
(d) Monitoring integrity of ANIs and SNIs configurations.

8.4 Confidentiality

As stated in 6.4, the Service Provider is required to protect NGN PS communications against unauthorized access. Media streams (e.g., voice) have to be protected against unauthorized access because eavesdropping on NGN PS media streams could reveal sensitive security information (i.e., conveyed in the media communication). Similarly, signaling information has to be protected from eavesdropping to reduce the chance of signaling traffic analysis revealing sensitive information having a potential for misuse (e.g., calling patterns, location information, and identity of Priority Services Users). The Service Provider is required to protect NGN PS communications against unauthorized access. Media streams (e.g., voice) have to be protected against unauthorized access because eavesdropping on NGN PS media streams could reveal sensitive security information (i.e., conveyed in the media communication).

R-44. The Service Provider shall protect the confidentiality of all inter-network NGN PS signaling crossing ANIs and SNIs.

R-45. The Service Provider shall protect the confidentiality of all inter-network NGN PS media traffic crossing ANIs and SNIs.

Actions that could be taken to protect the confidentiality of signaling and media traffic include, but are not limited to:

(a) Physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures).
(b) Cryptographic protection.
(c) Establishment and enforcement of appropriate confidentiality requirements defined in Service Level Agreements.

9 Intra-network Communications

Intra-network communications consists of the messages exchanged by network entities within the Service Provider's network and administrative *domain*[16]. As such, much of the communication traffic is *de facto* partially

[16] The term *domain* is defined in clause 4.

protected by its containment within the Service Provider's service centers (e.g., data centers). In these circumstances, the physical media and Network Elements (NEs) are housed within the service center and thus protected from unauthorized access. This protected environment can be thought of as a large "trusted environment" which consists of trusted security zones that offer protection by combining natural barriers (i.e., the building itself and perimeter defenses) with special security precautions that will be discussed later.

Outside the trusted zone but still considered highly trusted are those network entities that stand at the border of the trusted zone, providing access points to other networks or to customers. These NEs populate a "trusted but vulnerable zone" that, due to their location or exposure, are susceptible to some form of attack. NEs in this zone may be physically inside or outside the service center and may communicate both with trusted entities inside the trusted zone and with other entities outside the Service Provider's network. Border control devices are typical of devices in this zone, as are other devices such as remote Service Provider equipment (e.g., radio cell sites).

A third zone – the "untrusted zone" – completes the picture. This zone consists of NEs and devices belonging to peer networks, customer networks, or other NGN provider networks. Devices in this zone might not be under the Service Provider's control and so cannot be fully protected by the Service Provider's security policies and security mechanisms.

The zone model (see [ITU Y.2701] for details) is a convenient conceptualization that helps in the determination of how much and what kinds of security protection are needed for a given network entity or communications path; it is not a scale to evaluate the innate security of the entity, for such does not exist in general. It is important to note, for instance, that devices inside the trusted zone are not automatically secure, per se; only that the security mechanisms and policies needed to protect them may be different from those needed to protect entities in the trusted-but-vulnerable zone. Because intra-network communications consists of traffic that either stays within the trusted zone or traverses one or more zone boundaries, the zone model provides a basis for applying security protection to the network entities that enable those communications.

9.1 Authentication

NE-to-NE communication within the trusted zone does not require that the communicating entities authenticate one another. However, communications between entities inside the trusted zone with any entity in either of the other zones requires that the communicating devices authenticate one another. For trusted-to-untrusted zone communications the reason is clear; neither of the communicating entities can trust one another, and each must therefore be able to authenticate itself to the other if requested to do so.

Similarly, NEs in the trusted-but-vulnerable zone (i.e., border NEs) must authenticate devices in the untrusted zone before they begin to exchange either media or signaling traffic.

R-46. The Service Provider shall establish and enforce rules for each NGN NE in its Trusted zone to authenticate NGN NEs within other Trusted zones prior to establishing a communications path to those NEs.

R-47. The Service Provider shall establish and enforce rules for each NE in a trusted-but-vulnerable zone to authenticate any NEs prior to establishing a communications path to those NEs.

Examples of NEs in the trusted-but-vulnerable zone are the Session Border Controller, and the radio control NEs or cell sites (e.g., NodeB/eNodeB).

These requirements also apply when traffic is exchanged between two different technologies managed by the same administrative domain (intra-domain).

9.2 Access Control

Given that the NGN is a highly complex structure consisting of many overlay networks, the Service Providers need to establish and enforce access control rules to protect against compromises from occurring within the network.

R-48. The Service Provider shall monitor and screen traffic to protect against unauthorized and harmful content being propagated through intra-network communications.

R-49. The Service Provider shall establish rules and enforce access control measures to prevent unauthorized access to network elements and systems supporting NGN Priority Services.

9.3 Integrity

Intra-network NGN PS communications need to be protected against corruption, manipulation, and interception. To provide integrity protection requires that specific measures be applied to secure the signaling and media on a hop-by-hop basis.

R-50. The Service Provider shall protect the integrity of all intra-network NGN PS signaling including any in-band signaling and control (e.g., voice prompt and PIN collection).

R-51. The Service Provider shall protect the integrity of all intra-network signaling and control including any admission and policy control procedures (e.g., Diameter signaling) used to support NGN Priority Services.

R-52. The Service Provider shall protect the integrity of intra-network NGN Priority Services media traffic.

NOTE: Intra-network NGN PS traffic between access network backhaul NEs or between backhaul access network NEs and Packet Core NEs carrying NGN PS traffic will require cryptographic protection.

Actions that could be taken to protect the integrity of signaling and media traffic include, but are not limited to:

(a) Physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures).
(b) Cryptographic protection.
(c) Monitoring integrity of internal network configurations and relationships.

9.4 Confidentiality

Current 3GPP IMS standards do not mandate the use of cryptographic confidentiality protection at the IP layer or above on any signaling or media streams in the IMS core network. Use of cryptographic confidentiality protection within the IMS core network is left as a Service Provider decision, for practical reasons. For business reasons and to meet customer needs for privacy, the Service Provider needs to protect NGN PS communications against unauthorized access. Media streams (e.g., voice) have to be protected against eavesdropping because such unauthorized access on NGN PS media streams could reveal sensitive security information contained in the communication. Also, the signaling between IMS core network elements needs to be protected against unauthorized access because eavesdropping on the signaling of NGN PS calls/session could reveal information about the Priority Services User identity, location, and service usage, which need to be confidential for certain NS/EP users.

R-53. The Service Provider shall protect the confidentiality of all intra-network NGN PS signaling, including any in-band signaling and control (e.g., voice prompt and PIN collection).

R-54. The Service Provider shall protect the confidentiality of all intra-network signaling and control including any admission and policy control procedures (e.g., Diameter signaling) that support NGN Priority Services.

NOTE: Intra-network traffic between access network backhaul NEs or between backhaul access network NEs and Packet Core NEs carrying NGN PS traffic will require cryptographic protection.

R-55. The Service Provider shall protect the confidentiality of all intra-network NGN Priority Services media traffic.

Actions that could be taken to protect the confidentiality of signaling and media traffic include, but are not limited to:

(a) Physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures).
(b) Cryptographic protection.

NOTE: Intra-network traffic between access network backhaul NEs or between backhaul access network NEs and Packet Core NEs carrying NGN PS traffic will require cryptographic protection.

NOTE: The need for network-based, cryptographic confidentiality protection should be assessed on a service-by-service basis for all future NS/EP services. Beyond voice, NS/EP priority data services may present a greater need for cryptographic confidentiality protection. Unlike voice services where a user can choose whether or not to communicate certain information, users may not be able to precisely control all the information that is exchanged on a data link between devices. Certain new services provided by the network, such as NS/EP priority multi-party video conferencing, may have to support cryptographic confidentiality because it may not be possible to add it at the service user devices. In other cases, application layer security provided by endpoint devices using secure session technology, such as Transport Layer Security, may be sufficient.

10 Security for the Management Plane

The management plane supports the fault, configuration, accounting, performance, and security (FCAPS) functions. The network carrying the traffic for these activities may be in-band or out-of-band with respect to the service provider's user traffic and is normally referred to as the "management network". The security of the management plane is concerned with the protection of the management network and the related operations, administration, maintenance, and provisioning (OAM&P) functions of the network elements, transmission facilities, back-office systems (operations support systems, business support systems, customer care systems), and data centers.

Security of NGN PS depends on the security of the management network and associated systems and platforms (S&P) used to carry out management functions. This clause focuses on requirements for the security of the management plane for the support of NGN Priority Service.

The integrity and availability of NGN PS depends on the security of the S&Ps. The focus of this clause, then, is to offer a set of requirements common to all S&Ps used to support NGN PS, with an additional set that applies to specific kinds of platforms or systems. The purpose of this clause is to provide S&P related security requirements to prevent compromise to NGN PS from occurring via the S&Ps.

The security requirements in this clause are applicable to all S&Ps that are directly or indirectly used to support NGN PS. S&Ps operate within the network (e.g., NEs) and tangential to the network as support entities (e.g., Operations Support Systems, or OSSs).

The term "administrator" is used in this clause to refer to an individual (e.g., Service Provider employee, craft personnel, contractor, or other worker) authorized for accessing S&Ps for Operations, Administration, and Maintenance (OA&M) purposes. "Administrative User" is used here in place of the more common term "user" to avoid the possibility of confusion with service users – that is, callers, subscribers, PS Users, etc.

Roles and access control privileges assigned to individual administrators for OA&M purposes are governed by the Service Provider privilege management policy. Specifically, the privilege management policy dictates actions individual administrators are authorized to perform. The term "privileged user" is used in this clause to refer to administrator whose privileges on a system or platform exceed those of the average administrator. Security administrators and system administrators might be examples of privileged users.

The term "PS S&P" is used in this clause to refer to Service Provider systems or platforms that host functions such as applications and databases that directly support Priority Services, and that indirectly support NGN PS functions (e.g., routers handling priority routing). The term is merely a convenient label and is not meant to imply special manufacture or special purpose (although some PS S&Ps might, in fact, be special-purpose devices).

10.1 Management Plane Security Requirements

One area of major concern for network technologies is the potential vulnerability of the management network over which Operations, Administration, Maintenance, and Provisioning (OAM&P) traffic passes. The management network that connects management systems and network nodes may cover a wide geographic area. It may be accessible from remote terminals, workstations, and laptop devices. In addition, the management network may be linked to other networks, which may themselves be accessible through public networks posing certain security risks. The integrity, confidentiality, and availability of NGN Priority Services depend on the security of the management communications.

This clause addresses management plane security requirements that are to be applied to all S&Ps that support NGN Priority Services.

R-56. The Service Provider shall ensure that S&Ps supporting NGN Priority Services meet all requirements defined in ATIS-0300276, *OAM&P – Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane* [ATIS-0300276].

Some additional security requirements are also needed by specific S&Ps to address stronger or special-case requirements that result from those S&Ps' PS-specific function within the network, their need to protect data or resources of a particular nature, or other criteria.

The remainder of this clause addresses security requirements in the areas of authorization, authentication, access control, integrity, and confidentiality. Unless otherwise noted, the requirements in this clause apply to all systems and platforms. Those requirements that address the security of a specific platform or systems type (e.g., OSS, NE) will designate the platform or system to which it refers.

In the case of NE-specific requirements, the requirements address NE security rather than imposing any constraints on the Functional Element (FE) groupings packaged into a Network Element that provides explicit NGN Priority Services functions or support functions for NGN Priority Services. These NEs may belong to an access network, packet core, or the IMS core performing signaling and user plane functions.

10.1.1 Identification

Identification refers to the process by which a system recognizes the administrators who are accessing it. Identification is handled through the use of an *identifier* – a unique, auditable representation of the identity of an individual administrator within the system or platform. Generic security requirements imposed on each S&P demand that they support the creation and administration of unambiguous identifiers (commonly called *userids*) to uniquely identify administrators, and that only authorized persons be allowed to access the S&P.

R-57. The Service Provider shall have a policy for unique identification of individual administrators. This includes policy for the lifecycle management of administrator identity information.

R-58. The Service Provider shall provide and use mechanisms that uniquely identify individual administrators (e.g., the creation of accounts based on a unique userid) who require access to S&Ps supporting NGN Priority Service.

10.1.2 Authentication

Authentication is the process of verifying the claimed identity of an administrator who is attempting to access an S&P. Authentication works hand-in-hand with identification of the administrator. Authentication involves validating the authenticity of the identity of an administrator by verifying multiple identifiers and attributes associated with the administrator. The Service Provider must assess the risks associated with the consequences of authentication errors to determine the appropriate level of assurance in an administrator's identity. Authentication errors with potentially worse consequences require higher levels of assurance (i.e., dependent on the assigned privileges or actions that can be taken by the administrator). Authentication in carrier class networks demands that S&Ps be able to support a variety of authentication mechanisms that enable a range of objectives to be met. For example,

passwords may be suitable for some conditions; dial or dial-back mechanisms may suffice for others; smart cards, digital certificates, or biometrics may be needed where strong authentication is required. In some cases, there may be a need for multiple mechanisms.

R-59. The Service Provider shall define and enforce policy to govern the level of assurance (i.e., degree of confidence) required for authentication of administrators who require access to S&Ps supporting NGN Priority Services. This includes establishing rules for using specific authentication mechanisms based on the risks associated with the consequences of authentication errors and actions that can be taken by the administrator.

R-60. The Service Provider shall authenticate the identity of individual administrators prior to giving them access to S&Ps that support NGN Priority Services.

S&Ps are not required to use passwords as credentials to authenticate administrators, though that is historically the most common method of authentication. Other methods include smart cards, cryptographic authentication, and biometrics, which provide stronger authentication than passwords. Almost all authentication methods require that the machine hosting the account holder store the authentication information (e.g., password, biometric data), which means that they must provide protection to those data. While technically, this protection falls under data integrity, it is discussed here because the data in question are specific to authentication.

R-61. The Service Provider shall protect stored authentication data from unauthorized access, manipulation, and corruption on S&Ps supporting NGN Priority Services.

R-62. The Service Provider shall protect the confidentiality of the authentication information exchanges between administrators and S&Ps supporting NGN Priority Services.

R-63. The Service Provider shall protect the integrity of the information exchanges between administrators and S&Ps supporting NGN Priority Services.

R-64. The Service Provider shall protect the authentication mechanisms of S&Ps supporting NGN Priority Services against attacks (e.g., message replay and denial of service attacks) that would compromise their integrity and availability. This includes using capabilities to minimize capture and stolen credentials (e.g., suppression of clear-text password display).

10.1.3 Authorization & Privilege Management

Authentication on its own is not sufficient in determining what the authenticated administrator is authorized to do once access is granted. Authentication must be combined with authorization and privilege management mechanisms and approaches to provide access control to S&Ps. One example is the assignment of roles and privileges to administrators for role-based access control (RBAC) to S&P management interfaces for OA&M purposes and to reduce the risk from insider threats. Authorization or privilege can be viewed as an assigned attribute to the identity of an administrator. Depending on the security policy of the Service Provider, the authorization privileges assigned to an administrator could be validated though the authentication process.

R-65. The Service Provider shall have a policy to govern the assignment and the management of individual administrator's roles and privileges for role-based access control to S&Ps supporting NGN Priority Services. This includes policy for the lifecycle management of role and privilege assignments to individual administrators.

R-66. The Service Provider shall enforce and manage role-based access control of individual administrators of S&Ps supporting NGN Priority Services.

R-67. The Service Provider shall verify privileges of individual administrators on S&Ps supporting NGN Priority Services prior to allowing the individual administrator to perform any function or action.

R-68. The Service Provider shall protect the integrity of privilege management data for S&Ps supporting NGN Priority Services.

10.1.4 Access Control

Access control is a general term that refers to the capability of the S&P to limit access to itself and to the resources under its control, granting access to those who are authorized to access it or its resources, and denying access to all others. The general concept is that access decisions are made based on the authentication of the administrator and privilege verification. Two kinds of access control are recognized in this report: system access control and data access control. Each is defined and discussed separately, below.

R-69. The Service Provider shall apply access control to all ports and interfaces of an S&P that support NGN Priority Services and that accept operations-related command inputs. This includes ports that provide direct, dial-up, and data communications network access.

R-70. The Service Provider shall not allow any session to be established via a port on an S&P that supports NGN Priority Services that is not designated to accept operations-related command inputs.

R-71. The Service Provider shall end a session by means of a secure (i.e., uninterruptible) log-off procedure on S&Ps that support NGN Priority Services. The session shall be terminated immediately if it is interrupted due to causes such as timeout, power failure, link disconnection, or other unexpected failures.

"Secure logoff" means that when an account holder ends his session, the S&P insures that it logs the account holder off, closes any applications associated with the account holder's session, and clears scratchpad data areas and other temporary data associated with the session. Secure logoff avoids a situation in which another person who sits down at the workstation after the account holder has logged off gains unauthorized access to any data or applications the account holder had used during the session.

10.1.4.1 System Access Control

System access control consists of security measures to prevent unauthorized access to network elements and systems. The Service Provider needs to support and implement system access control measures to counter threats associated with unauthorized access to network elements and systems supporting NGN Priority Services.

R-72. The Service Provider shall have a policy to prevent unauthorized access to S&Ps that are supporting NGN Priority Services.

R-73. The Service Provider shall protect against unauthorized access to S&Ps that are supporting NGN Priority Services.

R-74. The Service Provider shall identify, authenticate, and authorize administrators and remote systems before giving them access to S&Ps supporting NGN Priority Services. Only authorized administrators and remote systems shall be granted system access.

In supporting the above requirements, the following should also be considered:

1. To reduce the dangers of unauthorized persons accessing the S&P by guessing the credentials of administrators (e.g., userid and passwords), the S&P should support a capability to temporarily suspend or degrade the logon process for a given administrative userid.
2. S&Ps should also have the capability to implement a Service Provider policy for dealing with attempted intrusions. Having the system suspend the logon process for that userid until an administrator intervenes, or until a specified period of time has elapsed, are examples of such policies.
3. S&Ps should be able to end an account holder's session if the account holder fails to interact with the S&P within a certain period of time, usually a few minutes. The S&P should display a blank screen or some screen saver, lock the account, and require that the administrator authenticate himself before the S&P will resume his session.
4. S&Ps should be able to disable an account if the account holder fails to establish a session with the S&P within a certain period of time, that period being determined by the Service Provider.

In order that privileged functions such as security administration are carried out only by authorized persons, the S&Ps supporting NGN Priority Services must be able to distinguish between privileged administrators (e.g., "super users") and other administrators. Being able to make this distinction allows the S&P to control access to privileged actions such as creating and revoking accounts, altering the operation of the system's security features, and other sensitive activities. Furthermore, the S&P should be able to restrict privileged user access to specific ports or IP addresses to reduce the danger of privileged actions being invoked by unauthorized persons.

10.1.4.2 Data Access Control

10.1.4.2.1 Data and Resource Protection

Once an administrator has obtained access to an S&P supporting NGN Priority Services, his access is governed by security mechanisms that prevent unrestricted access to resources such as files, databases, functions, and command sets. The S&P must provide an access control mechanism to manage access to its resources (e.g., data, functions), granting access to administrators who are authorized to access them while denying access to all others.

R-75. The Service Provider shall protect against unauthorized access to NGN Priority Services data and resources [i.e., the Service Provider shall permit only authorized administrators to access NGN Priority Services data and resources (e.g., files, command sets, software) on S&Ps supporting NGN Priority Services].

R-76. The Service Provider shall protect the integrity of the access control mechanisms and all associated data (e.g., files, command sets, and software) on S&Ps supporting NGN Priority Services.

10.1.4.2.2 Database Partitioning

There are functional databases to support the different NGN PS calling methods. The PIN database, for instance, contains a user PIN, a service user priority level, and various calling privileges for each user of GETS-AN and GETS-NT services. The Translation database contains the routing number for each GETS-NT and GETS-PDN. In addition, there is also off-line data that link a PIN to specific individuals and their contact information. The need to maintain the integrity of this information is sufficiently high to warrant special rules that prevent a single administrator from having access to all of these data resources, to reduce or remove the threat of insider tampering.

From a risk mitigation perspective, it is desirable to not grant any individual administrator access to all NGN PS databases or all NGN PS data. In addition, if a single individual is entitled to access both NGN PS and non-PS information, it may be preferable to assign two accounts with separate privileges to mitigate the threat of a single compromised account providing access to all.

R-77. The Service Provider shall establish and enforce rules to prevent any single individual administrator from having access and management control (e.g., alteration) privileges for all NGN PS databases and all NGN PS data.

This can be achieved in different ways, depending upon the service architecture.

(a) If the NGN PS databases are housed in separate physical systems, system access controls can be used to prevent the same individual from being an administrator on both systems (Clause 10.1.4.1 addresses system access control).
(b) If the NGN PS databases are logically implemented in a single physical database, database access controls can be used to limit access to individual data elements by administrator (Clause 10.1.4.2 addresses data access control).
(c) If an NGN PS database is implemented as part of a database that serves other purposes, partitioning (i.e., separation of access) should be in place between NGN PS data and other database information.

10.1.5 System & Data Integrity

System integrity deals with consistency and reliability issues associated with the network elements, systems, functions, and software resources. Data integrity is the property that data has not been altered or destroyed in an unauthorized manner. Data integrity services within the S&P provide protection against data being altered or destroyed in an unauthorized manner.

10.1.5.1 S&P Integrity

Network elements supporting NGN Priority Services must provide integrity protection. This protection extends to any NGN Priority Services databases (e.g., PIN authentication database). The systems, procedures, data, and personnel who support and maintain the NGN Priority Services master databases must be secured, trusted, and monitored.

R-78. The Service Provider shall protect the integrity of all network elements supporting NGN Priority Services. This includes integrity protection of the IMS Core network elements, NGN Priority Services Application Servers, NGN Priority Services PIN databases, and any other network element that supports NGN Priority Services.

Actions that could be taken to protect the integrity of systems include, but are not limited to:

(a) Physical security (i.e., secure facility) measures.
(b) Enforcement of stringent access control rules to management interfaces providing access to the configured parameters and data.
(c) Appropriate monitoring of system integrity and configuration integrity.
(d) System hardening (e.g., disabling unused ports, secure remote access).

10.1.5.2 NGN Priority Services Data Integrity

NGN Priority Services specific data will be stored, hosted, or configured on certain S&Ps. For example, it is assumed that the HSS or the NGN Priority Services Application Server is the central repository for subscriber-related information. The HSS stores all of the static and dynamic information for a PS user. It keeps a master list of features and services associated with a user, and also the location and means of access to the user. It provides user profile information, either directly or via servers. Specifically for NGN Priority Services, it is assumed that NGN Priority Services specific data will be stored in the HSS, NGN Priority Services Application Servers, and NGN Priority Services PIN database. The stored NGN Priority Services data must be provided with integrity protection to prevent any corruption or manipulation of the data impacting the integrity or availability of NGN Priority Services.

R-79. The Service Provider shall protect the integrity of NGN Priority Services provisioned data. This includes any NGN Priority Services specific data, such as GETS-FC subscription data, that is provisioned in the HSS, Priority Services Application Server, Priority Services PIN databases, IP address resolution databases, IP routing databases, or in any other S&P or database.

R-80. The Service Provider shall protect the integrity of backup and archived NGN Priority Services data.

R-81. The Service Provider shall protect the integrity of any data distribution, transmission, updates or changes, and any offline data associated with NGN Priority Service.

Actions that could be taken to protect the NGN PS data integrity include, but are not limited to:

(a) Physical security measures.
(b) Enforcement of stringent access control rules to management interfaces providing access to the configured parameters and data.
(c) Appropriate monitoring.
(d) Cryptographic protection.

10.1.5.3 Accountability – Security Logging

10.1.5.3.1 S&P

The capability for the system to record the actions of administrators is a critical part of the system's security defenses. This logging of actions by administrators provides a history that can be used to trace problems, track privilege abuse and misuse of the system, provide evidence in legal proceedings, and deter attempts to misuse the system and its resources.

R-82. The Service Provider shall generate and maintain security logs of successful and unsuccessful attempts to administratively access S&Ps supporting NGN Priority Service.

R-83. For administrative access to S&Ps supporting NGN Priority Services, the Service Provider shall capture and record all activities (e.g., additions, changes, and removal of accounts; changes to the access authorizations of account holders).

R-84. The Service Provider shall, on S&Ps supporting NGN Priority Services, generate a security log of significant security-related events that captures information sufficient for after-the-fact investigation.

R-85. The Service Provider shall protect the security log data from unauthorized access (i.e., security log must be accessible only to users who have been assigned roles having privileges to access security logging data).

R-86. The Service Provider shall protect the security logging mechanism and its controls from unauthorized access.

R-87. The Service Provider shall protect the integrity of the security logging mechanism and its controls.

R-88. The Service Provider shall log any alteration (e.g., enabling or disabling of logging functions) to the operation of the security logging mechanism of S&Ps supporting NGN Priority Service.

The security logging mechanism should at least be able to record events that suggest attempted impropriety, as these events can suggest imminent danger to the host system or ongoing attempts to attack the host system. In supporting the above requirements, the following default security log records should be considered:

(a) Unauthorized access attempts against sensitive resources or data.
(b) Attempts to alter the S&P's operational status.
(c) Attempts to alter the configuration or function of security mechanisms.
(d) Attempts to alter the system clock.
(e) Invalid logon attempts.
(f) All privileged user actions.
(g) Events considered by the S&P manufacturer to be security relevant.

The security logging mechanism should be robust enough to permit the privileged user (in this case, the Security Administrator) to configure and control the types of events to be recorded in the log. This may include disabling the default recording of certain events if, for example, those events are not deemed important to security personnel. Examples of such events are disabling of valid logons and the creation and deletion of some resources such as temporary files. All changes to the configuration of the logging mechanism should be logged (e.g., it should not be possible to make changes to its configuration without those changes being logged).

10.1.5.3.2 Network Access

Logging of successful and unsuccessful access to the network through external interfaces and network connectivity is necessary to provide a history that can be used to trace problems, track abuse and misuse, provide evidence in legal proceedings, and deter attempts to misuse the system and its resources.

R-89. The Service Provider shall log all successful and unsuccessful attempts to access the network at the NNIs.

R-90. The Service Provider shall log all successful and unsuccessful attempts to access the network at the UNIs.

R-91. The Service Provider shall log all successful and unsuccessful attempts to access the network at the ANIs and SNIs.

10.1.5.4 Configurable Parameters & Default Values

There are many security threats related to the management of configurable parameters and defaults values set by vendors and equipment suppliers. For example, the default values of various configurable parameters, as delivered by the vendor, have to be adjusted to meet the local requirements. The configurable parameters must be properly assigned and kept up to date so they can function satisfactorily. The human administrator must be appropriately authorized to perform the security administration.

R-92. The Service Provider is required to establish and enforce rules for the administration of configurable parameters and default values in the context of supporting NGN Priority Services applications. Access control measures shall be implemented and enforced so that the execution of these functions is reserved only for the authorized administrator (i.e., all other users shall be denied this permission).

10.1.5.5 NGN Priority Services Congestion & Admission Control Mechanisms

This clause includes requirements for the security protection of the management related aspects of NGN Priority Services related congestion control mechanisms (e.g., throttling or other mechanisms used by the carriers).

Mechanisms to throttle NGN PS call/session requests are defined to control NGN PS call/session volume at the user-network interface (i.e., P-CSCF) and at the Interconnection Border Control Function (IBCF) for IP interconnection. The throttling and admission control mechanisms must be protected against integrity compromises affecting NGN PS integrity and availability. Specifically, adequate security management controls must be employed to protect the configurable throttling parameters including the monitoring and auditing of configured parameters.

R-93. The Service Provider shall protect the integrity of throttling and admission control mechanisms. This includes integrity protection of the configured parameters and data associated with the throttling and admission control mechanisms.

Actions that could be taken to protect the NGN PS data integrity include, but are not limited to:

1. Physical security measures.
2. Enforcement of stringent access control rules to management interfaces providing access to the configured parameters and data.
3. Appropriate monitoring and auditing of configured parameters and data.

10.1.6 Data Confidentiality

The confidentiality of data stored or used by an S&P must be maintained when disclosure of that data could affect PS or its authorized users, as in the case of NEs that store PS subscriber PIN information, Personally Identifiable Information (PII), or sensitive PS application-based data. The confidentially of sensitive information should be maintained while it is stored within the S&P and when it is in transit across the network. In both cases, mechanisms must be supported and used to enforce data confidentiality.

R-94. The Service Provider shall protect sensitive NGN Priority Services provisioned or stored data on S&Ps (e.g., subscription data) from unauthorized disclosure (e.g., protection from unauthorized insiders). This includes any sensitive offline data associated with NGN Priority Services. Sensitive data includes NGN Priority Services subscription information,

usage records, and other logged information.

R-95. The Service Provider shall protect transmitted sensitive NGN Priority Services information (e.g., data in messages sent across the network for distribution, updates or changes, associated with the NGN Priority Service) from unauthorized disclosure.

R-96. The Service Provider shall provide confidentiality protection to Personally Identifiable Information (PII) of Priority Services Users. PII includes the identity and any associated attributes (e.g., privileges, location, and usage patterns) of a Priority Services User.

Actions that could be taken to protect the data confidentiality and PII protection include, but are not limited to:

(a) Physical security measures

(b) Enforcing security measures to prevent data exposure to unauthorized entities

(c) Enforcement of stringent access control rules to management interfaces providing access to the configured parameters and data

(d) Measures to limit data to the minimum needed by individuals (i.e., administrators).

(e) Compartmenting Priority Services User PII access in shared systems and applications.

(f) Cryptographic protection.

10.1.7 Management Communications

It is recognized that the Service Provider may provide management communications via a variety of different management protocols such as Transaction Language 1 (TL1), Simple Network Management Protocol (SNMP), Common Management Information Protocol (CMIP), or Extensible Markup Language (XML) within the management plane; however, the following requirements apply regardless of which particular protocol is used.

R-97. The Service Provider shall establish and enforce methods for managed and managing entities supporting NGN Priority Services to uniquely identify all entities (person, system, software module) that participate in management exchanges.

R-98. Service Provider shall protect the integrity of identifiers used for management exchanges.

R-99. The Service Provide shall establish and enforce rules for the authentication and access control methods used for remote access to managed entities supporting NGN Priority Services.

R-100. The Service Provider shall protect network management transactions related to NGN Priority Services using two-way peer entity authentication at association setup time.

R-101. The Service Provider shall protect the integrity of network management communications supporting NGN Priority Services.

R-102. The Service Provider shall protect the confidentiality of management network communications supporting NGN Priority Services.

R-103. The Service Provider shall provide non-repudiation methods for network management communications supporting NGN Priority Services.

Note that these requirements implicitly forbid the use of SNMPv1 and SNMPv2 because those versions do not support a secure method of authentication, relying instead on the so-called community string, a character string that is not protected in transit and is, for all intents, simply an identifier rather than an authenticator. SNMPv3 does support a secure authentication.

11 IP Transport Network Security

The transport stratum of NGNs typically employs a variety of IP routers, Ethernet switches, and supporting databases. NGN PS depends on the integrity and availability of the IP transport network and routing infrastructure (e.g., Border Gateway Protocol version 4). This includes the integrity of the IP transport network elements and the IP services (e.g., IP routing, name and address resolution, time synchronization, and other services) utilized in providing priority treatment to support NGN PS.

In order to meet the requirements defined in the other clauses for integrity, confidentiality, and availability protection of NGN PS application services, the Service Provider is expected to implement appropriate security measures in the IP transport and routing network infrastructure.

This clause is not intended to dictate how the Service Providers secure their IP transport network and routing infrastructure. Instead, the focus of this clause is to define requirements that are specific to NGN PS in the context of preventing impacts to NGN PS application services from occurring via compromises to the IP transport and routing infrastructure.

11.1 Intra-Network IP Transport

11.1.1 General

"Intra-network" refers to communications between elements within the same Service Provider's network. The security of the following aspects of IP transport is important for NGN Priority Services:

- *Routing*; e.g., Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System.
- *Forwarding*; e.g., Multiprotocol Label Switching (MPLS).
- *Priority Mechanisms*, since this has special significance for NGN PS.
- *Supporting IP services*; e.g., Domain Name System (DNS).

In addition to the forwarding of each packet to the next appropriate hop, IP routers are responsible for applying priority rules to incoming traffic. Some methods of traffic prioritization, such as DiffServ, use packet marking to tag each packet with a priority. The IP router reads the priority of each packet and then processes it accordingly. In other methods, a router applies priority based on the logical path, tunnel, or interface on which a packet arrives. It is important that the functional capabilities and network resources used in the IP transport network to provide priority treatment and support NGN Priority Services applications services be given sufficient security protection. This should include implementation of architectural and physical design measures in the IP transport network to be resistant to security attacks (e.g., design of sub-networks to limit exposure to external IP networks and designs to ensure that internal Virtual Private Networks (VPNs) are not exposed to external networks). It should also include sound security practices for configuration and operation of IP transport network elements (e.g., measures to ensure that unused IP ports are disabled and management IP ports are physically separate from those that handle packet transfer).

R-104. The Service Provider shall protect the IP transport network elements (e.g., IP routers, Ethernet switches, and MPLS nodes), functions, and capabilities (e.g., priority functions) from intrusions (e.g., interception, hijacking, and replay) that would compromise the authenticity, integrity, confidentiality, and availability of NGN Priority Services, in accordance with commercially-available security best practices

R-105. The Service Provider shall protect the integrity of the IP traffic priority mechanisms, functional capabilities, and accompanying protocol data (e.g., DiffServ code points) employed to support NGN Priority Services.

NOTE: This includes integrity protection of any NGN Priority Services related configured data or parameters in the IP transport network.

11.1.2 Routing Functions & Protocols

IP transport networks typically employ a variety of routing functions and protocols for intra-network transport (e.g., Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) for IP routing; the Label Distribution Protocol (LDP) to support forwarding by MPLS; and DNS for domain name and address resolution). NGN PS depends on the integrity and availability of the IP routing functions, protocols and supporting databases (e.g., DNS) employed in supporting the application services. Specifically, integrity and availability of DNS is critical to NGN Priority Services. Integrity of IP address assignments via Dynamic Host Configuration Protocol (DHCP) and static IP assignment is also important. For example, compromise of DHCP could lead to DNS availability impacts. Therefore, appropriate security measures are need to prevent integrity and availability impacts to NGN Priority Services from occurring via compromises to the IP routing functions, protocols and routing databases (e.g., DNS) used to support the NGN Priority Services. Given the critical nature of DNS in supporting the routing for application services in general including NGN Priority Services, it is a primary target for cyber attacks. Service Providers are expected to take appropriate security measures for integrity and availability protection. DNS Security (DNS-SEC) could be used to provide integrity of data exchange between network elements and DNS.

R-106. The Service Provider shall provide security protection in accordance with commercially-available security best practices to the IP routing functions and protocols, and IP routing databases that support NGN Priority Services. This includes:

(a) Service Provider implementation of appropriate security capabilities to prevent integrity or availability impacts to NGN Priority Services from occurring via compromises to IP routing functions and protocols.

(b) Service Provider use of appropriate security capabilities to minimize integrity or availability impacts to NGN Priority Services from occurring via compromises to any IP address resolution and routing databases, such as those supporting DNS and OSPF, used within the Service Provider's network. Specifically, integrity and availability protection is required to DNS systems and data utilized for NGN Priority Services support. This includes integrity and availability protection of data updates (e.g., any updates through Internet).

(c) Service Provider implementation of security capabilities to provide integrity protection to any NGN Priority Services related configured data or parameters in IP address resolution and IP routing databases.

There are no stipulations made in regards to how the Service Provider meets the requirements defined in this clause. Actions that could be taken to protect the confidentiality of media traffic include, but are not limited to:

1. Physical security measures (e.g., physical protection of IP network elements, transmission medium, and facilities), and enforcement of appropriate access control measures).
2. Cryptographic protection of IP network control and routing protocols.
3. Use of appropriate monitoring and intrusion detection and prevention tools.
4. Implementation of appropriate IP network security best practices.
5. Implementing appropriate operational measures to detect and fix IP network vulnerabilities.

11.1.3 Use of Encryption

Unique markings are used at the IP transport layers to differentiate NGN Priority Services signaling and media traffic from ordinary traffic. Such markings may include a unique Class of Service (COS) value or Virtual Local Area Network (VLAN) identifier at layer 2, and a unique Differentiated Services Code Point (DSCP) or Multiprotocol Label Switching (MPLS) identifier at layer 3.

When Internet Protocol Security (IPsec) tunnel mode encryption is used in VPNs, the entire IP packet is encrypted or authenticated. It is then encapsulated into a new IP packet with a new IP header. According to [IETF RFC 2474 and RFC 2475] copying the inner DSCP to the outer IPSec header is optional. When encryption (e.g., IPsec) is used in the network for NGN Priority Services traffic, it is important that the DSCP values from the inner header be copied to the IPsec tunnel header to preserve the information and allow the egress nodes to provide priority treatment.

The following requirement is applicable when IPsec tunnels are used for NGN Priority Services:

R-107. The Service Provider shall establish and enforce rules to populate and protect the integrity of priority information (e.g., DSCP values) when IPsec tunnels are used for NGN Priority Services traffic. Specifically, rules on how the DSCP values from the inner header is populated in the IPsec tunnel header at the IPsec ingress point shall be established and enforced to allow priority treatment between the ingress and egress IPsec points.

NOTE: Further study is needed to determine whether a similar requirement is needed regarding encryption at the link layer.

11.2 Inter-network IP Transport

11.2.1 General

Inter-network NGN Priority Services depend on the integrity and availability IP interconnection between Service Providers. To meet the requirements defined in the other clauses for integrity, confidentiality, and availability protection of NGN Priority Services, the Service Provider is expected to support and implement appropriate security measures to prevent impacts to NGN Priority Services integrity, confidentiality, and availability from occurring through compromises to the IP network interconnections.

The security of IP interconnections between Service Providers will depend on factors such as architecture, physical connectivity, and service level agreements. For example, there are different security implications depending on whether the IP interconnection used to support NGN Priority Services is based on the following scenarios as depicted in Figure 4.

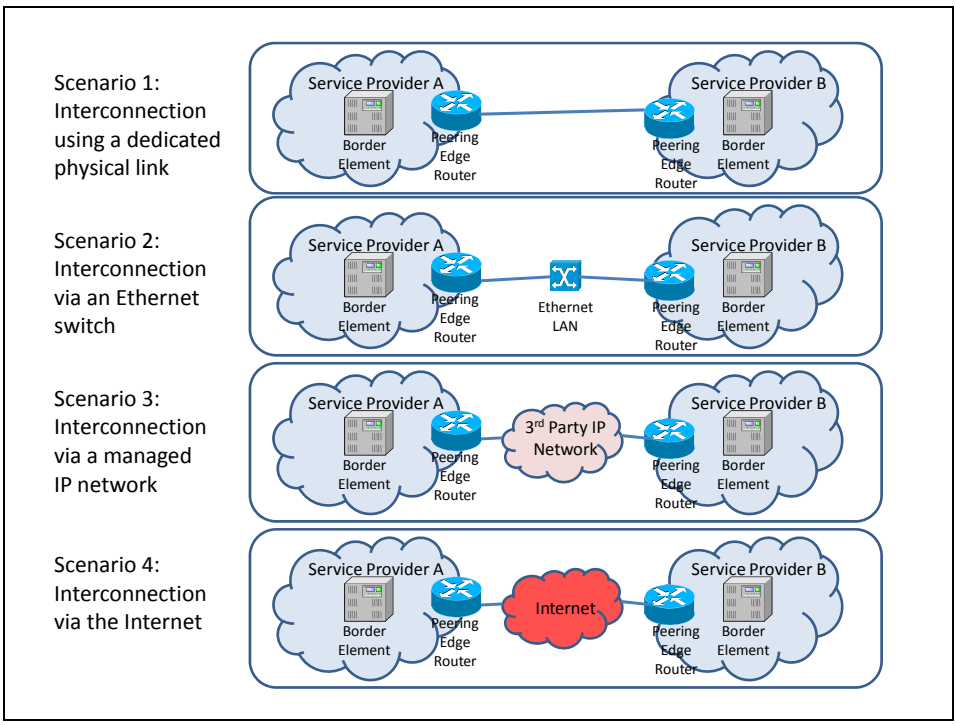

Figure 4 – IP Network Interconnection Scenarios

There are no stipulations or restrictions being made in this document as to the IP interconnection being used to support NGN Priority Services. The general objective is that it is incumbent on the Service Providers to support and implement appropriate security measures to protect IP network interconnection and prevent impacts to NGN Priority Services from occurring through compromises of IP network interconnection.

R-108. The Service Provider shall protect the IP transport network between two interconnected

Services Providers from intrusions (e.g., interception, hijacking, and replay) that would compromise the authenticity, integrity, confidentiality, and availability of NGN Priority Services in accordance with commercially-available security best practices.

To meet this requirement, the Service Provider should establish and enforce rules to protect the IP transport network interconnection between Services Providers, and document the rules in SLAs.

R-109. The Service Provider shall protect the integrity of the IP traffic priority mechanisms, functional capabilities and the accompanying protocol data (e.g., DiffServ code points) employed to support NGN Priority Services over IP network interconnection between two Service Providers.

NOTE: This includes integrity protection of any NGN Priority Services related configured data or parameters relate to the IP interconnection as well as any mapping that is involved (e.g., mapping of DiffServ code points based on the scheme being used in the individual interconnection Service Provider).

In addition, when NGN PS traffic traverses an untrusted IP network, the following conditional requirements apply:

CR-1. If NGN PS signaling is traversing an untrusted IP transport network segment (e.g., 3rd-party IP transport), the Service Provider shall use encryption (e.g., IPsec) for integrity and confidentiality protection.

CR-2. If NGN PS media is traversing an untrusted IP transport network segment (e.g., 3rd-Party IP transport), the Service Provider shall use encryption (e.g., IPsec) for integrity and confidentiality protection.

11.2.2 Routing Functions & Protocols

The effectiveness of NGN Priority Services, as well as the broader VoIP services, depends critically on the address resolution and routing protocols. In particular, DNS and the BGPv4 routing protocol are fundamental to the transport of traffic across the Internet. The BGPv4 routing mechanism is subject to a number of well-known attacks resulting in prefix "blackholing," traffic redirection, traffic subversion, or creation of routing instability. [Nordstrom] These attacks are more likely when Scenario 3 or especially Scenario 4 of Figure 4 are used. It is anticipated that the Service Provider will adjust the protection mechanisms to match the level of vulnerability.

O-6. It is desirable that the Service Provider provide security protection in accordance with commercially-available security best practices to the IP routing functions and protocols that support internetwork NGN Priority Services. This includes:

(a) Service Provider implementation of appropriate security capabilities to minimize integrity and availability impacts to NGN Priority Services via compromises to any IP routing functions and protocols (e.g., BGPv4) employed for the IP interconnection between two Service Providers.

(b) Service Provider use of appropriate security capabilities to minimize integrity and availability impacts to NGN Priority Services via compromises to any IP address resolution and IP routing databases, such as those supporting DNS and BGPv4, used on the IP interconnection between two Service Providers. Specifically, integrity and availability protection is required to any DNS systems and data utilized for NGN Priority Services support across the IP interconnection between two Service Providers. This includes integrity and availability protection of any data updates.

It also includes Service Provider implementation of security capabilities to provide integrity protection to any NGN Priority Services related configured data or parameters in IP address resolution databases and the IP routing databases employed for the IP interconnection between two Service Providers (see R-79).

There are no stipulations made in regards to how the interconnected Service Provider meets the requirements defined in O-6. Actions that could be taken to protect the confidentiality of media traffic include, but are not limited to:

1. Physical security measures (e.g., physical protection of IP network elements, transmission medium and facilities), and enforcement of appropriate access control measures).
2. Cryptographic protection of IP network control and routing protocols.
3. Use of appropriate monitoring and intrusion detection and prevention tools.
4. Implementation of appropriate IP network security best practices.
5. Implementation of appropriate operational measures to detect and fix IP network vulnerabilities.

In addition, when internetwork NGN PS signaling and media traffic traverse an untrusted IP network, the following conditional requirements apply:

CR-3. If inter-network NGN PS signaling between two interconnected Service Providers is traversing an untrusted IP transport network segment (e.g., 3rd-party IP transport or Internet), the Service Providers shall use encryption (e.g., IPsec) for integrity and confidentiality protection.

CR-4. If inter-network NGN PS media between two interconnected Service Providers is traversing an untrusted IP transport network segment (e.g., 3rd-party IP transport or Internet), the Service Providers shall use encryption (e.g., IPsec) for integrity and confidentiality protection.

11.2.3 Use of Encryption

As discussed in 4.6, the use of security mechanisms (e.g., encryption) shall not interfere or obscure information for priority treatment mechanisms.

The following requirement is applicable when IPsec tunnels are used for internetwork NGN Priority Services traffic (i.e., crossing NNIs, ANIs, and SNIs):

R-110. The Service Providers shall establish and enforce rules to populate and protect the integrity of priority information (e.g., DSCP values) when IPsec tunnels are used for internetwork NGN Priority Services traffic.

Specifically, rules on how the DSCP values from the inner header is populated in the IPsec tunnel header at the IPsec ingress point shall be established in SLAs and enforced to allow priority treatment the between ingress and egress IPsec points.

NOTE: Further study is needed to determine whether a similar requirement is needed regarding encryption at the link layer.

12 Management of Security for NGN Priority Services

To provide a well-ordered and consistent security stance, Service Providers need a comprehensive process to manage the design, implementation, and operation of security solutions, measures, practices, tools, and capabilities that must be adopted and implemented to ensure the security of NGN Priority Services in the evolving NGN environment. This clause provides objectives and requirements that relate to the overall management of NGN Priority Services security.

12.1 General Objectives & Requirements

There are many different security services, functions, capabilities, and measures that need to be coordinated and administered in the Service Provider network. One broad area pertains to the management of a security infrastructure that spans different network elements, sites and locations, interconnections, technologies, vendor products and implementations, and perhaps more. For example, the operational activities to implement the

security measures, practices, tools, and capabilities that protect NGN Priority Services would touch the various components and layers of the Service Provider network (e.g., signaling, management, user planes) and involve coordination between the different organizations involved in the daily operations of the Service Provider's network. It is important to have a documented plan for general security administration that supports NGN Priority Services.

R-111. The Service Provider is required to have defined plans for security management in support of NGN Priority Services. These plans shall include security administration and coordination within the Service Provider domain and across domains for interconnection and inter-network services.

The security management plan shall include (but not be limited to) the following:

(a) *Security Risk Assessment*: Processes and procedures for asset, threat, and vulnerability analysis pertaining to NGN Priority Services.

(b) *Security Solution (Security Architecture)*: Security architecture design, establishing security policy, and specifications of solutions to mitigate the identified threats pertaining to NGN Priority Services.

(c) *Security Solution Implementation*: Physical implementation and deployment of the necessary security solutions and measures for NGN Priority Services protection.

(d) *Security Operations*: The ongoing operations of the security solutions and measures for NGN Priority Services protection.

O-7. It is desirable that the Service Provider be able to demonstrate to the OEC the adequacy of the security administration processes that provide security protection of NGN PS applications.

R-112. The Service Provider is required to protect documented security administration processes from unauthorized disclosure. This includes, but is not limited to:

(a) Security measures that prevent unauthorized access to documented administration procedures by both intruders and insiders.

(b) Integrity and confidentiality protection of documented and administration procedures.

O-8. It is desirable that the Service Provider monitor and review the overall security management process continuously for improvement.

O-9. It is desirable that security management applicable to NGN Priority Services be structured and linked with the broader security administration processes of the Service Provider.

12.2 Risk Assessment

It is critical that a security risk assessment be performed periodically and when changes, new technologies, services, or applications are introduced to the Service Provider network, to determine security risks to NGN Priority Services. It is possible that changes that are not directly associated with NGN Priority Services could have an effect on it, and a risk assessment is a vital step in ruling out that possibility.

R-113. The Service Provider shall establish and implement a process to provide security risk assessments for NGN Priority Services. It is required that the security risk assessment cover all aspects of NGN Priority Services including the signaling, user, and management planes.

R-114. A security risk assessment shall be performed when changes, new technologies, services, or applications are introduced to the Service Provider network, to determine security risks to NGN Priority Services.

O-10. It is desirable that the Service Provider implement mitigation solutions for any discovered vulnerabilities to NGN PS.

It is desirable that the Service Provider share relevant information about NGN Priority Services security risks, as appropriate, with the OEC on an ongoing basis.

The first step in conducting a network security risk assessment is to define the environment across which the review applies – for example, identifying the assets that support NGN Priority Services.

Once the assets have been identified, the second step is to conduct a Threat Analysis for the assets. Threats refer to the ways in which the asset may be compromised, and are important for determining the kind of security that should be applied to protect any particular asset.

The final step is to perform an analysis of the level of exposure each asset has to exploitation. This is known as a Vulnerability Analysis. It involves identifying the implemented security controls, assessing their effectiveness, and determining how well they mitigate weaknesses and address non-compliance to industry practices and established security criteria.

Taken together, these three analyses (Asset Analysis, Threat Analysis, and Vulnerability Analysis) comprise the recommended Risk Assessment.

12.3 Security Architecture & Solutions

The security architecture and solution addresses the establishment of security policy, security architecture design, and the specification of solutions to mitigate identified threats to NGN Priority Services. The architecture and security solutions are based on the Service Provider's security policies and procedures, and the results of the risk assessment; and provide the foundation for the security requirements that the security solution must meet.

The general assumption is that the security of NGN Priority Services depends on the broader security architecture and solutions designed by the Service Provider for their general NGN Infrastructure protection. However, it is important that the Service Provider identify any specific or supplemental measures that are needed for NGN Priority Services protection, given the unique and critical nature of NGN Priority Services.

12.3.1 Security Policies

The technical means (e.g., security tools and capabilities) for securing the underlying NGN supporting NGN Priority Services, along with the security services themselves, have to be supported by security policies in order to be effective.

A well-written and effectively implemented policy provides direction for protecting critical assets associated with the support of NGN Priority Services. Appropriate security policies are needed for setting rules for the expected behavior of employees (e.g., of system administrators, and security personnel), for authorizing security personnel to carry out necessary actions, for defining the consequences of security violations, and for tracking compliance with regulations and legislation.

A fundamental part of the framework is to establish and document comprehensive and consistent security policies and procedures for the NGN.

R-115. The Service Provider is required to have a security management process to establish and document security policies applicable to the security protection of NGN Priority Services.

The following are some general topics that should be addressed when developing and establishing security policies for NGN Priority Services:

- Policy for access to network elements and operations systems (e.g., management interfaces) supporting NGN Priority Services
- Policy for physical access to NGN provider sites, facilities, and buildings hosting network elements and equipment that support NGN Priority Services
- Policy for access to sensitive and confidential data that support NGN Priority Service
- Remote access and Wireless Local Area Network (WLAN) access policies within the NGN provider sites that support NGN Priority Service
- Policy governing change management processes for applying network configuration changes and for

problem resolution in the context of NGN Priority Services security

- Policy for regular review of existing security policies in order to address the latest threats.
- Policy for incident response and repair procedures as well as a schedule to update the procedures to address the latest threats.
- Rules and responsibilities for each person involved in network security and describe how each person is expected to work with other security personnel regarding NGN Priority Services security.
- Methods to disseminate security information regarding NGN Priority Services security effectively to the appropriate personnel.
- Policy to perform a security risk assessment of the NGN network in support of NGN Priority Services.
- Methods to independently audit the compliance of the Service Provider's organization to the security policies applicable to NGN Priority Services security protection.
- Methods and procedures to address problems created by security breaches.
- Policies to impose appropriate security controls on external contractors, consultants, and temporary staff who have access to NGN network systems that support NGN Priority Services.
- Policies to impose appropriate security controls to manage outsourced services and systems that indirectly or directly support NGN Priority Services.

12.3.2 Security Architecture Design

NGN Priority Services security depends on the overall security architecture design implemented by the Service Provider to protect its NGN infrastructure and supported application services. The Service Provider security architecture is viewed as the blueprint for an organized, well-defined description of the necessary security services, their interactions, and their placement within the distributed components of the network infrastructure. As such, it serves to structure the engineering and deployment of the actual software and hardware (e.g., intrusion detection systems) that will implement the security controls. It also promotes an understanding of the responsibilities and interrelations of the various human, physical, and logical components of the security infrastructure.

O-11. It is desirable that the Service Provider include appropriate measures for the security protection of NGN Priority Services in the overall security architecture. This should include specific designs as needed for security protection of assets and resources associated with the support of NGN Priority Services.

One of the overarching principles when designing a secure system is *defense in depth* which combines multiple security measures to create a layered protection that will protect systems even when one layer of security fails.

R-116. The Service Provider is required to implement a security architecture based on industry best practices and that has design features appropriate for the protection of NGN Priority Services integrity, confidentiality, and availability. The security architecture shall include multiple security measures to create a layered protection that will protect systems even when one layer of security is breached.

Figure 5 shows an example of a security architecture based on the general concept of layered security protection for a core network. The figure shows three defensive zones:

- The outer zone interconnects the access network, other networks, and 3rd-party application providers with proxy servers via Security Gateways (SEGs). SEGs are network elements that provide Session Border Controller (SBC), Data Border Function (DBF), Firewall, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS) functions and capabilities.
- The middle zone interconnects proxy servers with call control functions (e.g., I-CSCF, S-CSCF). This zone serves as a buffer between critical network elements in the NGN that should have no external exposure (i.e., network elements in the inner zone).
- The inner zone protects critical network elements (e.g., HSS,) and databases storing sensitive and private information (e.g., NGN Priority Services subscriber information databases).
- The Service Provider should take appropriate measures to ensure that the assets used to support NGN Priority Services are themselves well protected by the security architecture.

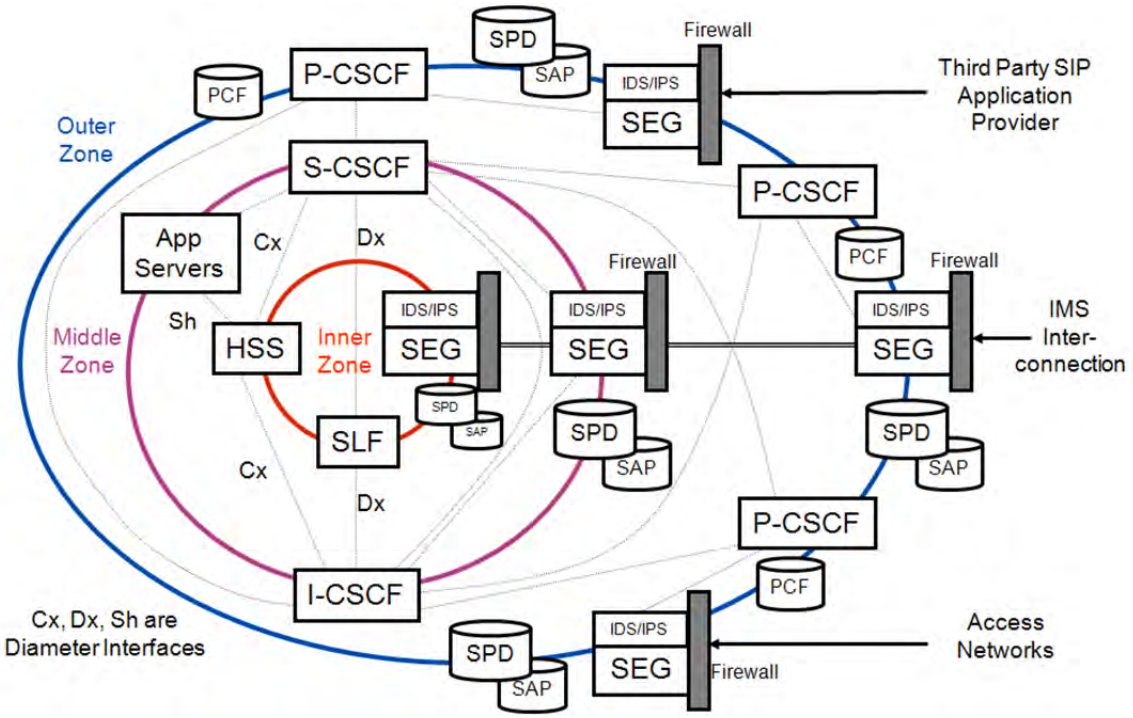

Figure 5 – Example Security Architecture for Core Network

The example outlined above is consistent with the general trust model defined in [ATIS-1000029].

12.4 Security Operations

12.4.1 Organizational Structure, Roles, & Responsibility

A complicating factor in many security problems lies in a lack of a holistic view of security within an organization and a corresponding lack of clearly defined roles and responsibilities across the organizational structure. In many cases, no single organization has an end-to-end comprehensive view of how security measures are developed, designed, implemented, and managed within the NGN and its related environment (i.e., the network elements, the supporting OSSs and management systems including the interconnection communication data network, outsourced managed environments, existing and new service applications, and supplier access).

In the event of a serious NGN Priority Services security incident, fragmented security management could present serious, but avoidable, impediments to isolating and mitigating adverse effects in a timely manner.

O-12. It is desirable that the Service Provider provide a security management organizational structure having an end-to-end comprehensive view of how security measures are developed, designed, implemented, and managed for NGN priority Services in the NGN and the interrelated environment.

NOTE: This Objective may be changed into a Requirement at some future date.

R-117. The Service Provider organizational structure shall have clearly defined roles and responsibilities for the management of NGN Priority Services security.

Roles and responsibilities should be clearly defined to coordinate policy enforcement, security risk assessment, security incident reporting functions, and SLAs with specifically designated organizational Single Points of Contact (SPOCs) who coordinate their own organizations' resources that support NGN Priority Services.

12.4.2 Security Training & Awareness

Lack of security awareness can lead to unsafe practices and ambivalence towards the security measures that are in effect, which could lead to compromises of NGN Priority Services.

O-13. It is desirable that the Service Provider establish and implement an effective training and awareness program directed towards NGN Priority Services security protection.

The first step toward implementing an effective security awareness program is to identify the target audience and then prepare material that is appropriate for their functional expertise and job responsibilities. Depending on the target audience, one or more methods of fostering security awareness may be used. For some users, in-depth security training on various topics may be periodically required. For others, a general awareness program, bolstered with periodic supplementary materials or reminders, will be all that is required.

12.4.3 Management of Insider Threats

An individual (e.g., an employee, contractor, or other worker) may be able to gain unauthorized management access or misuse their management access to network elements and systems supporting NGN Priority Services such as databases, application servers, P-CSCF and HSS. Example attacks that can be perpetrated using unauthorized management access include:

- Altering administrable service options.
- Disabling security reporting mechanisms.
- Modifying service logic.
- Introducing rogue processes or malicious code onto the underlying platform.
- Changing or altering user subscriptions and profiles.

R-118. The Service Provider shall establish and implement security processes to minimize insider threats to NGN Priority Services.

Example mitigation methods that could be considered include:

- Authentication controls, role-based privileging, separation of functions, and secure access methods for remote, console, craft, and automated system access.
- Logging of security events related to NGN management actions.
- Compartmenting of NGN Priority Services information, applications, and access to shared systems and applications.
- Auditing of configured data in NGN network elements and databases (e.g., subscriptions profiles in HSS) for recording and exposure of unauthorized changes.

12.4.4 Collaboration for Cyber Security Information Exchange

Service Providers should establish collaborative relationships with partners for sharing information about cyber security events (including real-time exchange of information during cyber security attacks). An exchange of information about cyber security incidents can provide mutual benefits and can be used to anticipate threats to NGN Priority Services placing the Service Provider in a situation to provide effective countermeasures.

O-14. It is desirable that the Service Provider establish and implement management and operational processes sufficient to provide collaborative relationships for sharing and exchanging information about cyber security events. The processes should take into

consideration analysis functions to make the information useful as input into security actions and countermeasures to protect NGN Priority Services.

Refer to the following ITU-T Recommendations for information about cyber security information exchange:

- [ITU-T X.1500], *Overview of cybersecurity information exchange (CYBEX)*
- [ITU-T X.1520], Common vulnerabilities and exposures (CVE)
- [ITU-T X.1521], *Common vulnerability scoring system*
- [ITU-T X.1570], *Discovery mechanisms in the exchange of cybersecurity information.*

12.4.5 Management of Incident Response & Recovery from Security Events

Availability of NGN Priority Services depends on the operational procedures in place for recovery and service restoration from security events. It is critical that these procedures be clearly defined, documented, and implemented. This includes the necessary policies and practices for service recovery and restoration within a Service Provider domain and across domains for interconnection and inter-network services. Protection of the operational procedure documentation and implementation from intruders and insider threats is necessary.

R-119. The Service Provider is required to have a documented Incident Response and Recovery plan describing the policies; management; and operational steps, processes, and procedures for service recovery and restoration from security events. This includes the necessary policies and practices for service recovery and restoration within the Service Provider domain and across domains for interconnection and inter-network services.

R-120. The Service Provider is required to protect documented management and operational procedures for service recovery and restoration for security events. This includes, but is not limited to:

(a) Security processes to prevent unauthorized access to documented management and operational procedures from both intruders and insiders.

(b) Integrity and confidentiality protection of documented management and operational procedures.

12.4.6 Management of Supply Chain

Public networks supporting NGN PS will be constructed of equipment from a multi-national vendor base. Each vendor relies upon a supplier community that consists of its tier 1 and 2 suppliers, at minimum. Tier 1 and 2 suppliers in turn obtain technology from smaller companies. The supply chain continues all the way down to the manufacturers of the most fundamental components in network equipment. Each of these suppliers may design, develop, and manufacture their products in worldwide locations in many countries. The Service Provider must establish and implement security measures to minimize supply chain threats that could compromise NGN Priority Services integrity, confidentiality, and availability.

R-121. The Service Provider is required to establish and enforce rules for supply chain management of security risks and threats.

R-122. The Service Provider shall be able to provide a plan for supplier chain management to the OEC that shows its enforcement of rules and practices that minimize supplier chain risks.

13 Availability

13.1 Introduction

Availability is a measure of the percentage of time that a service system is in its operational state. Availability is a characteristic that is relevant to both reliability and security. In the context of security, availability is used to define security capabilities to ensure that system assets are available, working as intended, and service is not denied to

authorized users. It is also associated with the applicable operational measures to restore disrupted operations and services in a timely manner as a result of security events (e.g., security compromise or breach).

[ATIS-0100004], *Availability and Restorability Aspects of Emergency Telecommunications Service (ETS)*, provides the following definitions for availability and reliability:

- *Availability*: A measure or calculation of how much time a system, subsystem, or service component is functioning properly.
- *Reliability*: The probability that a service system will perform its purpose adequately as specified for the period of time.

The original set of White House NS/EP functional requirements provided in Table 1includes the following general requirements related to the reliability, survivability, and availability of NGN PS:

- *Restorability*: Should a disruption occur, services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
- *Survivability/Endurability*: Services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or man-made disaster up to and including nuclear war.
- *Reliability/Availability*: Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

This clause provides objectives and requirements for reliability, survivability, and availability in the context of NGN PS security.

> NOTE: The scope of this clause is limited to the security aspects of reliability, survivability, and availability. Requirements and objectives for NGN PS reliability and availability performance in terms of quantitative measures are not within the scope of this document.

13.2 General Objectives

NGN PS must be highly available. Availability objectives for ETS are provided in [ATIS-0100004], *Availability and Restorability Aspects of Emergency Telecommunications Service (ETS)*. It is assumed that service availability for NGN PS will be specified in the SLAs between the OEC/DHS and the Service Providers. It is also assumed that service availability for NGN PS across Service Provider networks will be addressed in the bi-lateral SLAs between interconnected Service Provider networks. Refer to [ATIS-0100016], *End-to-End Service Availability: General Definition*, and [ATIS-0100026], *A Methodology for Design of End-to-End Network Reliability for Proactive Network Reliability Planning*, for information on end-to-end availability.

Availability measures the percentage of time the service system is in its operational state. To ensure high availability of NGN PS, failures of each service system (support NGN PS) must be kept small, and service recovery must be expeditious (once there is an outage or failure). For the perspective of this document, failures as a result of security compromises should be taken into account in the overall availability planning and design for NGN PS.

The following are general objectives for NGN PS availability in the context of security:

O-15. It is desirable that Service Providers take into account potential failures due to security events in the planning and design for the overall service availability of NGN PS within the Service Provider network. This includes measures for expeditious recovery from failures due to security events.

O-16. It is desirable that the Service Providers take into account potential failures due to security events affecting inter-network interconnections in the overall planning and design for end-to-end service availability of NGN PS (i.e., NGN PS calls/sessions traversing multiple Service Provider networks). This includes measures for expeditious recovery from failures due to security events.

NOTE: Further study is needed to determine whether these two objectives can be modified and upgraded to requirements having conditions or consequences that can be verified.

13.3 Protection from Service Degradation

NGN PS must be protected against security threats potentially affecting performance factors such as quality of service (QoS) and quality of experience (QoE) on NGN PS calls/sessions. For example, security compromises that reduce or degrade the audio quality of a NGN PS call/session without a failure of the call/session.

R-123. The Service Provider shall provide protection against attacks that would compromise NGN PS performance objectives, in accordance with commercially-available security best practices.

13.4 Availability Protection

13.4.1 Denial of Service

A denial of service (DoS) attack is an incident in which users are deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service (DDoS), large numbers of compromised systems (sometimes called a *botnet*) attack a single target.

NGN PS must be protected against DoS, DDoS, and other types of attacks that could affect NGN PS availability. This includes protection against attacks affecting NGN PS availability for individual Priority Services Users, a group of Priority Services Users, Priority Services Users in a specific location or site (e.g., Government Agency enterprise network site), Priority Services User in a targeted geographic or regional area, or NGN PS as a whole.

R-124. The Service Provider shall protect the availability of NGN Priority Services (e.g., protection against DoS, DDoS, and other types of attacks impacting NGN PS availability) in accordance with commercially-available security best practices. This shall include protection against DoS, DDoS, and other types of attacks affecting NGN PS availability for individual Priority Services Users, a group of Priority Services Users, Priority Services Users in a specific location or site (e.g., Government Agency enterprise network site), Priority Services User in a targeted geographic or regional area, or NGN PS as a whole.

Actions that may be taken to protect the availability of NGN Priority Services include, but are limited to:

(a) Use of admission control and throttling mechanisms.
(b) Use of DoS and DDoS mitigation tools and functions.
(c) Use of Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS).
(d) Use of Security Monitoring Tools (e.g., Deep Packet Inspection).
(e) Use of Situational Awareness Tools.

R-125. The Service Provider's use of security tools and capabilities for availability protection (e.g., DoS and DDoS mechanisms) shall include appropriate measures to prevent unintended denial of legitimate NGN PS calls/sessions (e.g., blocking or preventing an legitimate NGN PS call/session from completing or the discard of legitimate NGN PS packets).

13.4.2 Resource Exhaustion

Resource exhaustion is a result of events that cause network resources to become overtaxed to the point of no longer handling their workload with acceptable performance. Two potential causes of resource exhaustion that could affect NGN Priority Services are traffic redirection and recursive looping attacks.

13.4.2.1 Traffic Redirection

Traffic redirection is a situation in which network traffic is redirected from its intended destination to a targeted termination point with a malicious intent of a flooding attack. For example, the traffic from a particular destination engineered to regularly handle a large call volume (as, say, a toll-free service center) could be redirected to a targeted point that is not engineered to handle a large call volume, resulting in a flooding attack.

Traffic redirection attacks launched by insiders through unauthorized manipulation of network resources (e.g., routing databases) can be mitigated through access control and authentication mechanisms that restrict access to only authorized persons such as administrators. Clause 10 defines authentication and access control requirements for the management plane that address this threat for both insider and outsider attacks.

Network resources that provide NGN PS could be exhausted through the redirection of non-PS traffic to a GETS-AN or GETS-NT. In particular, redirection of 800/toll-free numbers that receive a significant amount of traffic to a GETS-AN or GETS-NT number to flood it needs to be prevented.

The Service Provider must establish appropriate rules to prevent redirection of redirection of non-PS traffic to GETS-ANs and GETS-NTs.

R-126. The Service Provider shall establish and enforce rules to prevent unauthorized, malicious or unintended redirection of 8YY/toll-free service to a GETS-AN or GETS-NT.

Actions that could be taken to protect against redirection of 8YY/toll-free service to a GETS-AN or GETS-NT include, but are not limited to:

a) Monitoring of traffic volume to GETS-AN and GETS-NT (see clause 10).
b) Management of Insider Threats (see clause 8).
c) Provisioning system controls to prevent redirected 8YY/toll-free to GETS-AN or GETS-NT.

13.4.2.2 Recursive Looping

Recursive looping can occur when a call/session is forwarded repeatedly through a small group of destinations each of which, instead of terminating the call, forwards it to the next destination, with the last one forwarding it back to the first. Recursive looping attacks could congest parts of the network, and even involve more than one Service Provider network in the process.

Recursive looping attacks initiated by insiders through unauthorized manipulation of network resources can be mitigated with access control and authentication mechanisms that restrict access to translation databases and other resources to authorized personnel. The authentication and access control requirements defined in clause 8 for the management plane address this threat for insider and outsider attacks that rely on incursions into the Service Provider's Operations Support Systems.

Recursive looping attacks that rely on misuse of call forwarding are more difficult to address since there is no way to anticipate them or detect them in their early stages. The fact that they can be carried out without the attacker accessing network resources (other than UEs) complicates the matter further. Preventative measures that can detect and disallow tight recursion loops involving only two devices can prevent amateurish attacks but have no effect on more serious attacks involving three or more destinations, particularly looping attacks that span multiple service providers' networks.

13.5 Diversity & Redundancy for Survivability

Electrical, physical, and geographical diversity and redundancy are needed for the network to survive a variety of uncontrollable perils, such as natural disasters, man-made events, equipment failure, cable cuts, and security attacks on the network. Inadequate diversity and redundancy of critical NGN PS equipment and connecting facilities can result in the unavailability of NGN PS as a result of security related events (e.g., security attacks).

R-127. The Service Provider is required to establish and enforce rules for diversity management that enable the network to survive security attacks.

R-128. The Service Provider diversity management plan shall establish rules to survive security

attacks and compromises affecting availability of network elements, functions, and resources supporting NGN PS.

R-129. The Service Provider diversity management plan shall establish and enforce rules for electrical diversity, physical diversity, and geographical diversity that enable the network to survive security attacks and compromises that would affect availability of network elements, functions, and resources supporting NGN PS.

R-130. The Service Provider diversity management plan shall establish and enforce rules for redundancy of network elements, components, and systems that enable the network to survive security attacks and compromises that would affect availability of network elements, functions and resources supporting NGN PS.

R-131. The Service Provider diversity management plan shall indicate how diversity and redundancy rules and policies are enforced and audited for compliance.

R-132. The Service Provider shall be able to provide a plan for diversity management to the OEC that shows its enforcement of rules and practices.

13.6 Security Monitoring at NGN PS Specific Equipment

Security monitoring tools and throttling mechanisms could be implemented at NGN PS specific network elements (e.g., the NGN PS application servers) to detect DoS, abuse, and intrusions.

R-133. The Service Provider shall use security monitoring tools at network elements (NGN PS application server, NGN PS PIN database, and the HSS) that authenticate Priority Services Users and authorize NGN PS calls/sessions, to detect fraud, abuse, and intrusion.

NOTE: Specific requirements for security monitoring are for further study.

The NGN PS application server represents a central architecture point where most NGN PS traffic, except possibly for GETS-FC calls, will arrive for processing. The NGN PS application server, for instance, could maintain a tally over a windowed interval of the number of calls/sessions allowed for each PIN. If the call/session volume exceeds a preset limit for a PIN over that interval, call/session requests can be rejected with an announcement to the user indicating the reason for rejection. Because the window moves in time, users that were previously blocked from initiating NGN PS calls/sessions will automatically be reinstated. Tracking call requests by PIN at the NGN PS application server may make it easier to detect and stop attacks that are distributed across different interfaces and points of ingress. Furthermore, actions to block suspected abuse might be more precisely applied at NGN PS application servers.

R-134. The Service Provider shall monitor PIN usage to protect against fraud and abuse.

PIN usage may be monitored: (a) for simultaneous usage; and (b) against a prearranged maximum.

NOTE: Further study of specific additional requirements to monitor PIN usage including imposing a limitation on the number of calls/session allowed to a PIN is needed, and checking for simultaneous usage.

R-135. The Service Provider shall monitor the usage from NGN Priority Services Subscribed UEs to protect against fraud and abuse.

NOTE: Specific additional requirements to monitor the usage from NGN Priority Services Subscribed UEs, including checking for simultaneous usage are for further study.

O-17. It is desirable that the Service Provider provide a report to the OEC when fraud or abuse of NGN PS is detected.

NOTE: Further study is needed to define requirements addressing actions to be taken by the Service Provider when fraud or abuse is detected for NGN PS (e.g., should PIN or subscription be blocked).

14 Bibliography

The following are informative references; at the time of publication, the editions indicated were valid. All standards are subject to revision, and parties are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[b-TMF GB917] TMforum GB917, *SLA Management Handbook*, Release 3.1. April 25, 2012.

[GR-815], Telcordia Technologies, Inc. March 2002. *Generic Requirements for Network Element/Network System (NE/NS) Security, Issue 2*. GR-815 CORE.

[Nordstrom]. Ola Nordstrom and Constantinos Dovroli. “Beware of BGP Attacks.” *ACM SIGCOMM Computer Communications Review*, Volume 34, Number 2: April 2004.

[Telecom 1996], U.S. Congress. House. *Telecommunications Act of 1996*. 104th Cong., 2d sess., 1996. File s652.

[TR-835], Telcordia*. OTGR – Operations Application Messages – Network Element and Network System Security Administration Messages, Issue 3*. Telcordia TR-NWT-000835. Telcordia Technologies. January 1993.

Annex A
(informative)

A Example Service Level Agreement (SLA) Template for NS/EP NGN-PS Security

As noted in clause 13.2:

- It is assumed that service availability for NGN-PS will be specified in the Service Level Agreements (SLAs) between the OEC/DHS and the Service Providers.
- It is also assumed that service availability for NGN-PS across Service Provider networks will be addressed in the bi-lateral SLAs between interconnected Service Provider networks.

The purpose of this Annex is to provide an example of an SLA template that may be used to add content pertaining to the security of NGN PS to the overall SLAs referenced above. In order to set the proper context for understanding the template, some general SLA concepts are first reviewed.

Note that SLAs may also be used between the Service Provider and a 3rd-party Application/Content Provider; however, these are not specifically addressed within this Annex.

A. 1 General SLA Concepts

According to the TeleManagement Forum GB917, *SLA Management Handbook*, a Service Level Agreement (SLA) is an element of a formal, negotiated commercial contract between two parties, i.e., a Service Provider (SP) and a Service Customer (SC). In the simplest case, an SP plays an SP role and an SC plays an SC role. However, more complex scenarios may also be defined. For the purposes of this document, the scenarios of interest are depicted below.

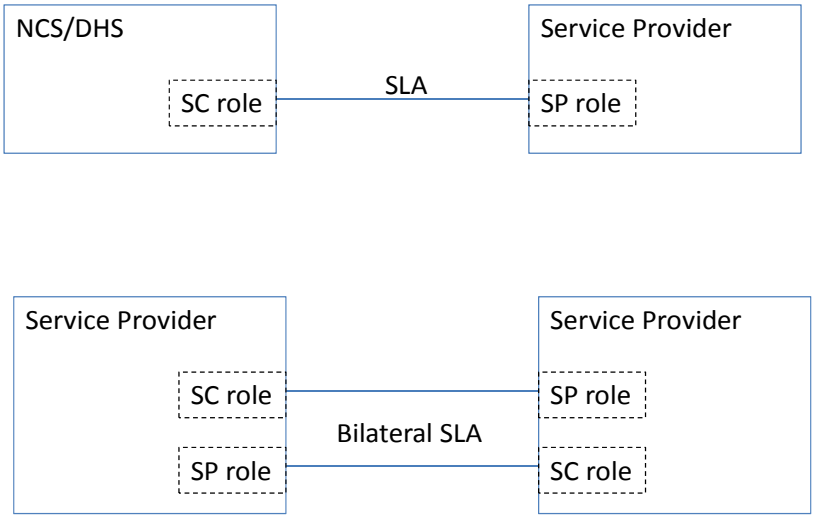

Figure A.1 - SLA Scenario Schematic

ITU-T Recommendation M.3342, *Guidelines for the definition of SLA representation templates*, provides several general SLA templates that are intended to be filled out by both parties involved in an SLA – i.e., they are to be filled out from the perspective of the SC role and the also the perspective of the SP role.

A.1.1 Overview of the M.3342 SLA Templates

Guidelines for the Definitions of SLA Representation Templates (GDSRT), as defined by ITU-T M.3342, are the instructional explanations about how SLA content of a specific service can be organized and represented. GDSRT provides the format of each proforma that may be involved in SLA representation templates, the structures about how SLA content is organized, which proformas to select in order to form a complete set of templates for a specific service, and the instructions about how the proformas can be filled in. On the basis of the guidelines, specific representation templates for a specific service can be developed accordingly. Based on the SLA Representation Templates, the SLA negotiation between SCs and SPs can be carried out, and the agreed results can be captured in the SLA representation templates, thus forming a practical SLA instance.

All SLAs should utilize the proformas for “Service Identification” and “SLA Profile”. The “SLA Profile” proforma provides a summary and list of all the proformas (tables) that are used in a specific SLA, and the indexes for them.

Figure A.2/M.3342 gives the basic composition of SLA contents, regardless of the services provided. Generally, the content of an SLA includes four parts as illustrated below.

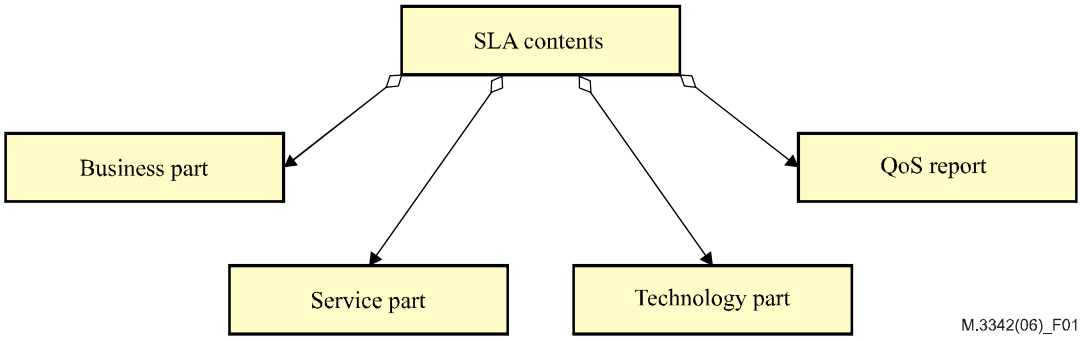

Figure A.2 - Basic Composition of SLA Content (per 1/M.3342)

A brief description of each part is provided below:

1) *Business part:*

This part describes the general business information and business procedures related to the service provided by the SP to the SC. It may describe items such as:

- Points of Contact;
- Terms and Conditions;
- Service Center;
- Change Procedures;
- Service Violations and Remedies;
- Tariffs and Billing; and
- Service Termination.

2) *Service part:*

This part describes the detailed information about the service provided to the SC. It includes negotiated items such as:

- Services Provided; and
- Service Level.

3) *Technology part:*

This part gives the detailed information about items such as:

- QoS Parameters;

- Supporting Equipments;
- System Design Information;
- SP Backup and Disaster Recovery Mechanisms; and
- Network and Delivery Upgrades.

4) *QoS report:*

This part includes the QoS report information provided to the SC and the SP in order to evaluate service level negotiated in the SLA and covers items such as:

- Monitoring and Reporting.

A.2 Special Considerations for Network-to-Network Interface

This clause identifies examples of security information to be mutually agreed by each Service Provider and documented within an SLA for NGN PS Security across the Network-to-Network Interface.

The following tables identify relevant security information from clause 6 of the main body of this document that should be addressed in the SLAs.

Table A.1 - NGN PS Authentication at NNI" proforma

Functional Requirement	Mechanism Used	Conditions	Reference
Authenticate adjacent Service Provider when handing off NGN Priority Services signaling traffic	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-9
Authenticate adjacent Service Provider when handing off NGN Priority Services media traffic	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-9
Authenticate adjacent Service Provider when receiving NGN Priority Services signaling traffic	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-9
Authenticate adjacent Service Provider when receiving NGN Priority Services media traffic	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-9

Table A.2 - NGN PS Access Control at NNI" proforma

Functional Requirement	Mechanism Used	Conditions	Reference
Identification of external NEs	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-10
Pre-authorization of external NEs	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-10
Verify trust relationship with service provider upon receipt of NGN Priority Services signaling traffic	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-11
Verify trust relationship with service provider upon receipt of NGN Priority Services media traffic	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-12
Verify trust relationship with service provider upon hand off of NGN Priority Services signaling traffic	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-13
Verify trust relationship with service provider upon hand off of NGN Priority Services media traffic	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-14

Table A.3 - "NGN PS Integrity at NNI" proforma

Functional Requirement	Mechanism Used	Conditions	Reference
Integrity protection of NGN PS signaling	*Identify and document mechanism to be used (e.g., physical protection and/or cryptographic protection)*	*Describe associated conditions and/or constraints*	R-15
Integrity protection of NGN PS media traffic	*Identify and document mechanism to be used (e.g., physical protection and/or cryptographic protection)*	*Describe associated conditions and/or constraints*	R-16

Table A.4 - NGN PS Confidentiality at NNI" proforma

Functional Requirement	Mechanism Used	Conditions	Reference
Confidentiality protection of NGN PS signaling	*Identify and document mechanism to be used (e.g., cryptographic protection)*	*Describe associated conditions and/or constraints*	R-17
Confidentiality protection of NGN PS media traffic	*Identify and document mechanism to be used (e.g., cryptographic protection)*	*Describe associated conditions and/or constraints*	R-18

A.3 Special Considerations for Internetwork IP Transport

This clause identifies examples of security type information to be mutually agreed and documented within an SLA by each Service Provider involved in internetwork IP transport for NGN PS Security.

As stated in clause 9.2, the security of IP interconnections between Service Providers will depend on factors such as architecture, physical connectivity, and SLAs. The SLA contents themselves will also depend on architecture as shown below.

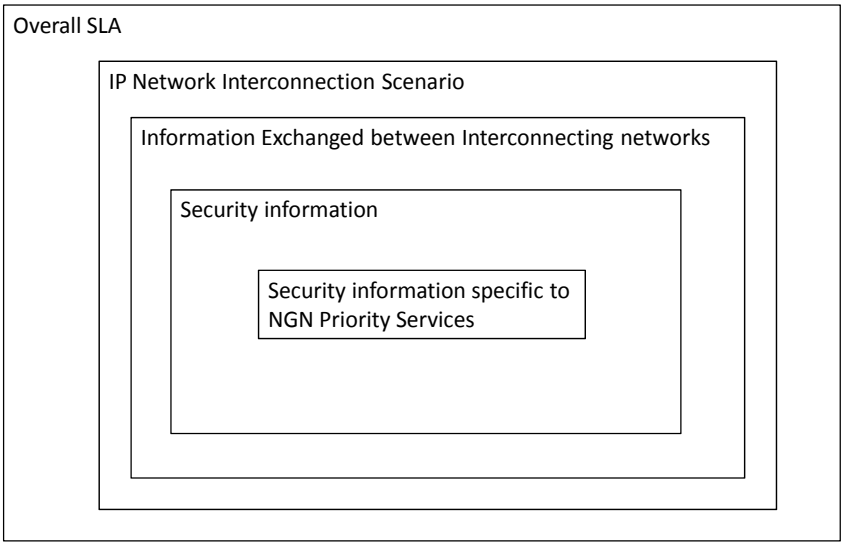

Figure A.3 - SLA Content Structure

Looking from the SLA perspective, the overall SLA will require each Service Provider to identify and agree upon which type of interconnection they will use (Figure A.3 provides some choices for IP Network Interconnection Scenarios). Based on the type of interconnection scenario specified, a particular set of information will need to be exchanged between the interconnecting networks. This includes information such as transport, service-specific application layer, network node identities, configuration, billing, and security. A subset of the security information specified within the SLA will need to address the specific security needs of NGN PS. These needs are specified by O-6 within clause 11.2.

The following tables identify relevant security information from clause 11.2 of the main body of this document that should be addressed in the SLAs.

Table A.5 - NGN PS Security for Internetwork IP Transport" proforma

Functional Requirement	Mechanism Used	Conditions	Reference
Intrusion protection of IP transport network	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-108
Integrity protection of IP traffic priority mechanisms	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-109
Integrity protection of functional capabilities	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-109
Integrity of protection of accompanying protocol data	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-109

Table A.6 - NGN PS Security for IP routing functions and protocols" proforma

Functional Requirement	Mechanism Used	Conditions	Reference
Protect against compromises to IP routing functions and protocols	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	O-6a
Protect against compromises to IP address resolution databases	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	O-6b
Protect against compromises to IP routing databases	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	O-6b

Table A.7 - NGN PS Security for IPsec tunnels" proforma

Functional Requirement	Mechanism Used	Conditions	Reference
Integrity protection of priority information	*Identify and document mechanism to be used*	*Describe associated conditions and/or constraints*	R-110

A.4 NGN-PS Security Templates

This clause identifies examples of security type information to be mutually agreed by each party (i.e., between SC role and SP role as described in clause A.1) and documented within an SLA for NGN PS Security.

The following tables identify relevant security information that may be used to supplement the SLA templates defined by ITU-T M.3342.

A.4.1 Proforma for "NGN PS Security Point of Contact"

A specific point of contact should be identified for NGN PS Security concerns.

Table A.8 - "NGN PS Security Point of Contact" proforma[17]

	Service Customer	Service Provider
Responsibility		
Name of Contact		
Work Title*		
Description*		
Telephone Numbers		
Fax Numbers*		
E-mail Addresses*		
Postal Addresses*		
Additional Information*		

Where:

- *Responsibility*: This field is used to specify what the contact person is responsible for, and the possible values to be filled in this field are "Technical matter" and "Administrative matter". Based on the contact person's actually responsibility, the allowed values can also be extended.
- *Name of Contact*: The full name of the contact person for this Service.
- *Work Title*: The work title for the contact person. This field can be left empty.
- *Description*: The short description of the scope or the responsibility of the contact person. This field can be left empty.
- *Telephone Numbers*: The contact telephone number of the contact person. At least one number is specified. It is recommended that both the office telephone number and the mobile numbers be filled in this field, in case of an emergency.
- *Fax Numbers*: The contact fax number of the contact person. If there are more than one fax number (e.g., one for backup purposes), they can also be filled in this field. This field can also be left empty if there are no contact fax numbers.
- *E-mail Addresses*: The contact e-mail addresses of the contact person. If there is more than one e-mail address (e.g., one for backup purposes), they can also be filled in this field. This field can also be left empty if there are no contact e-mail addresses for this person.
- *Postal Addresses*: The postal address of the contact person (including the postal code information). If there is more than one postal address (e.g., one for backup purposes), they can also be filled in this field. This field can also be left empty if there are no contact postal addresses.
- *Additional Information*: This field is reserved for extensions, and can be used to specify any other additional information that is related to this contact person. This field can be left empty.

  NOTE – The information of the SC contact person should be filled in the corresponding "Service Customer" column, and the information of the SP contact person should be filled in the corresponding "Service Provider" column.

[17] This table is based on Table 3/M.3342 – The "Points of Contact" proforma.

A.4.2 Proformas for "NGN PS Security Parameters"

NOTE- Measurement of NGN PS Security parameters is not currently required, but rather is an area for further investigation.

[ATIS-0100036], *Media Plane Performance Security Impairments for Evolving VoIP/Multimedia Networks*, discusses media plane performance security impairments and their impact on QoS. It also asserts the following:

Using a standard approach for QoS measurement would be beneficial for NGN NS/EP.

Given that QoS degradations may occur from a variety of sources, and given that one of those sources is security impairments, it would be beneficial to also have a standard approach for NGN PS Security measurement.

The "NGN PS Security Parameters" related proformas include the following three parts: the "NGN PS Security Metrics" proforma, the "NGN PS Security Key Performance Indicator (KPI) Definition" proforma, and the " NGN PS Security Key Quality Indicator (KQI) Definition" proforma.

The structure of the "NGN PS Security Metrics" proforma is shown in Table A.9:

Table A.9 - "NGN PS Security Metrics" proforma[18]

Technology Dependency						
QoS Parameter Area						
Parameter ID	**Parameter Name**	**Value Range**	**Value Units**	**Qualifier**	**Definition Reference**	**SC Check**

Where:

- *Technology Dependency*: This indicates whether the QoS metrics in this table is technology dependent or independent.
- *QoS Parameter Area*: This indicates which area this QoS Parameter is dealing with. The possible categories to be filled in this field can be "Network Performance Metrics", "Traffic Metrics" and "Service Metrics".
- *Parameter ID*: It is assigned for each Parameter for reference and identification purpose.
- *Parameter Name*: This is field is used to specify the full name and the abbreviation of the specified QoS Parameter.
- *Value Range*: This field can be filled with the agreed value range (it can be negotiated between the SC and the SP, or the SC can select the value range from a list that SP provides), indicating the possible values that the QoS parameter should be in the range in order to be conformed to the agreed service level.
- *Value Units*: This indicates the units that are used by this parameter. When no units are used for this QoS parameter (such as a ratio), this field is filled with "--", indicating "not applicable".
- *Qualifier*: This indicates whether this QoS Parameter is mandatory, optional or conditional for this service.
- *Definition Reference*: This field should be filled in the index for the detailed definitions that can be found somewhere in Table 13 or 14.
- *SC Check*: This field should be filled in by the SC, indicating whether the SC wants this QoS Parameter to be included the SLA or not. When the "Qualifier" field is filled with "mandatory", this field is filled with "--", indicating "not applicable", which means that there is no need for the SC to specify. If the "Qualifier" field is filled with "optional", the SC can specify in this field whether this QoS parameter is required for this service or not, using "√" or "X".

[18] This table is based on Table 12/M.3342 – The "QoS Metrics" proforma.

The structure of the “NGN PS Security KPI Definition” proforma is shown in Table A.10.

Table A.10 - NGN PS Security KPI Definition” proforma[19]

Index	KPI ID	KPI Name	Source*	Definition*
NOTE – Either “Source” or “Definition” field can be optional, but at least one of them should be filled.				

Where:

- *Index*: This field is used for reference purpose, and it can be used by other table items to locate this QoS Parameter.
- *KPI ID*: The Identifier assigned for each KPI.
- *KPI Name*: This field is used to specify the full name and the abbreviation of the specified KPI.
- *Source*: This field can be used to fill in the information about which Recommendation or specification the KPI is defined in. If the KPI is new, and cannot be found in any specifications, this field can be filled with “--”, indicating “not applicable”.
- *Definition*: This field can be used to provide the detailed definition about the KPI. It can be captured from the Recommendation or specification where this KPI is defined in. This field can be left empty if the source field is filled, and the source can be publicly accessed. When no definitions can be found in any specifications, the KPI definition is provided.

The structure of the “NGN PS Security KQI Definition” proforma is shown in Table A.11.

Table A.11 - –”NGN PS KQI Definition” proforma[20]

Index	KQI ID	KQI Name	Source*	Included KPI List		Definition*
				KPI ID	KPI Name	
NOTE – Either “Source” or “Definition” field can be optional, but at least one of them should be filled.						

Where:

- *Index*: This field is used for reference purposes, and it can be used by other table items to locate this QoS Parameter.
- *KQI ID*: It is assigned for each KQI for reference and identification purposes.
- *KQI Name*: This field is used to specify the full name and the abbreviation of the specified KQI.
- *Source*: This field can be used to provide information about the source that defines the KQI. If the KQI is new, and cannot be found in any Recommendation or specification, this field is filled with “--”, indicating “not applicable”.

[19] This table is based on Table 13/M.3342 – The “KPI Definition” proforma.

[20] This table is based on Table 14/M.3342 – The “KQI Definition” proforma.

- *Definition*: This field can be used to provide the detailed definition about the KQI. It can be captured from the Recommendation or specification where this KQI is defined. This field can be left empty if the source field is filled, and the source can be publicly accessed. When no definitions can be found in any specifications, the KQI definition is provided.

A.4.3 Proforma for "NGN PS Security Design Information"

The structure of the "NGN PS Security Design Information" proforma is shown in Table A.12.

Table A.12 - NGN PS Security Design Information" proforma[21]

General System Design*	
Routing Details*	
SC Access for Design Information*	
Configuration Techniques*	
Scalability Design*	
Additional Information*	

Where:

- *General System Design*: A description of how the system design will meet the following types of criteria: the absence of common failure points, the redundancy level required, alternative routing of facilities, transmission media restrictions, and restrictions on services that may be provided by other parties. This field can be left empty.
- *Routing Details*: A description of transmission media routing details that may be required along with a requirement that the routing and/or the media will not be changed without prior discussion and agreement. This field can be left empty.
- *SC Access for Design Information*: Description of the process whereby the SC may access the design information for periodic review or to review modifications. This field can be left empty.
- *Configuration Techniques*: Specification of the techniques to be used for recording configuration and for configuration change control. This field can be left empty.
- *Scalability Design*: A description of how the system design meets the stated scalability requirements. This field can be left empty.
- *Additional Information*: This field is reserved for extensions, and can be used to specify any other additional information that is related to the design of the service infrastructure. This field can be left empty.

A.4.4 Proforma for "NGN PS Security Recovery Mechanisms"

The structure of the "NGN PS Security Recovery Mechanisms" proforma is shown in Table A.13.

[21] This table is based on Table 17/M.3342 – The "System Design Information" proforma.

Table A.13 - "NGN PS Security Recovery Mechanisms" proforma[22]

Backup Procedures*	
System Redundancy*	
Recovery Parameters*	
SP Disaster Recovery Priority*	
SC Support*	
Additional Information*	

Where:

- *Backup Procedures*: Description of the procedures for data and application backups. This field can be left empty.
- *System Redundancy*: Description of the service delivery system redundancy. This field can be left empty.
- *Recovery Parameters*: Description of recovery parameters – i.e., how quickly can data be restored. This field can be left empty.
- *SP Disaster Recovery Priority*: Description of the priority and process for SP disaster recovery. This field can be left empty.
- *SC Support*: Description of the SC support required to assist with disaster recovery. This field can be left empty.
- *Additional Information*: This field is reserved for extensions, and can be used to specify any other additional information that is related to the backup and recovery mechanisms. This field can be left empty.

A.4.5 Proforma for "NGN PS Security Report"

The structure of the "NGN PS Security Report" proforma is shown in Table A.14.

Table A. 14 - "NGN PS Security Report" proforma[23]

Content of Reports	
Reporting Frequency	
Report Delivery Mechanism	
Ad hoc Support*	
Time Points and Intervals	
Report Presentation	
Monitoring Approach*	
Detecting Mechanisms*	
SC Auditing Process*	
Performance Assessment*	
Additional Information*	

Where:

- *Content of Reports*: Specifications of the content of performance reports.
- *Reporting Frequency*: Specifications of the frequency of performance reports.

[22] This table is based on Table 18/M.3342 – The "SP Backup and Recovery Mechanisms" proforma.
[23] This table is based on Table 20/M.3342 – The "QoS Report" proforma.

- *Report Delivery Mechanism*: Specification of the performance report delivery mechanism – e.g., e-mail, postal delivery, electronic retrieval, report distribution lists, and the number of copies.
- *Ad hoc Support*: Specification of ad hoc reporting support. This field can be left empty.
- *Time Points and Intervals*: Definitions of the time points or intervals associated with performance events, and data aggregation intervals.
- *Report Presentation*: Specifications of the method for performance report data presentation – e.g., tables histograms, charts, etc.
- *Monitoring Approach*: Specification of the approach and extent to which the SP will monitor all necessary services -*- e.g., network devices, circuits, services and applications, to prevent service unavailability. This field can be left empty.
- *Detecting Mechanisms*: Description of the mechanisms and processes the SP will use to detect and track downtime. This field can be left empty.
- *SC Auditing Process*: Description of the process that the SC may use to audit the SP's tracking and reporting mechanisms. This field can be left empty.
- *Performance Assessment*: Specification of when and how SC service monitoring data will be used to assess service performance. This field can be left empty.
- *Additional Information*: This field is reserved for extensions, and can be used to specify any other additional information that is related to QoS reporting. This field can be left empty.