ATIS-1000055.2013 (R2018)

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 >.

ATIS-1000055.2013(R2018), *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(R2018)

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

Table of Figures

Table of Tables

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.

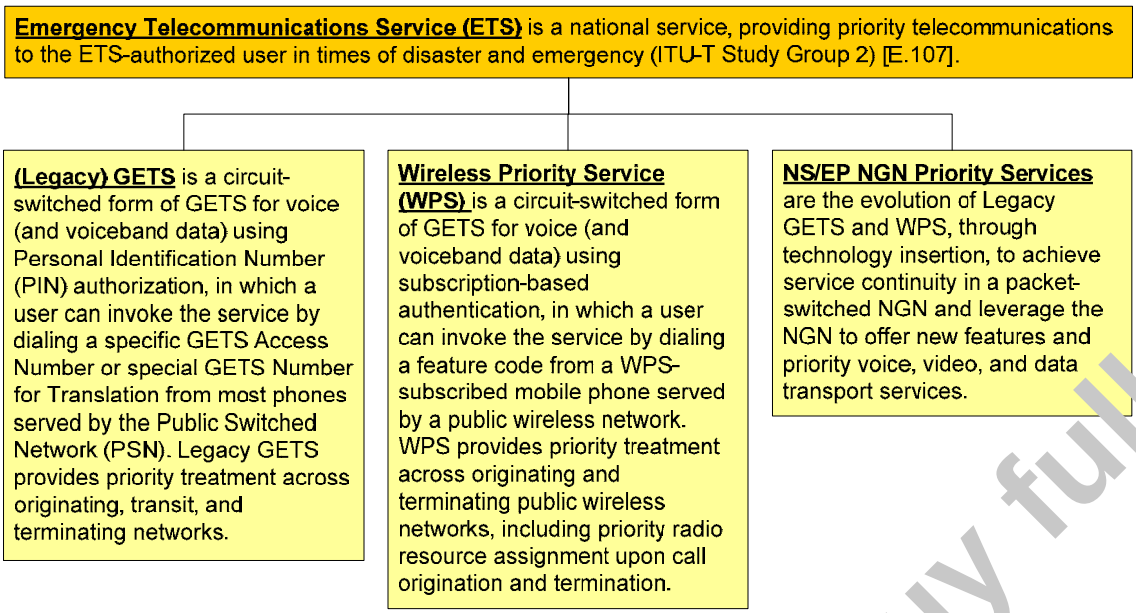

Figure 1 - Relationship of Concepts and Terms

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.
- *Design 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.