ATIS-1000060.2014 (R2019)

Emergency Telecommunications Service (ETS): Long Term Evolution (LTE) Access Network Security Requirements for National Security/Emergency Network (NGN) Priority Services

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 standard.

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-1000060.2014(R2019), *Emergency Telecommunications Service (ETS): Long Term Evolution (LET) Access Network Security Requirements for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services*

Is an American National Standard developed by the **Cybersecurity (CSEC)** 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-1000060.2014(R2019)

American National Standard for Telecommunications

Emergency Telecommunications Service (ETS): Long Term Evolution (LTE) Access Network Security Requirements for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services

Alliance for Telecommunications Industry Solutions

Approved **November 10, 2014**

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 requirements for the security protection of NS/EP NGN-PS in LTE Access Networks.

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.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, 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 of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair [AT&T]

V. Shaikh, PTSC Vice-Chair [Applied Communication Sciences]

M Geller, PTSC-CSEC Chair [Cisco]

R. Singh, PTSC-CSEC Vice-Chair [Applied Communication Sciences]

M. Ghassemzadeh, Technical Editor [Applied Communication Sciences]

R. Singh, Technical Editor [Applied Communication Sciences]

The Cybersecurity [CSEC] Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

American National Standard on –

Emergency Telecommunications Service (ETS): Long Term Evolution (LTE) Access Network Security Requirements for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services

1 Scope, Purpose, & Application

This document defines a minimum set of security requirements for the National Security and Emergency Preparedness (NS/EP) Next Generation Network Priority Services (NGN-PS) within the context of Long Term Evolution (LTE) access networks. They include requirements on the LTE functions, components and interfaces and their interworking with the Circuit Switched (CS) technologies that Service Providers expect to use for voice communications[1] in the initial LTE deployments.

The purpose of this document is to provide a minimum set of security requirements for the security protection of NS/EP NGN-PS in LTE Access Networks. The requirements address the protection of the LTE priority features, capabilities, and procedures. Specifically, they address the problem of securing the advance priority features and special priority handling (referred to here, collectively, simply as special handling) that NS/EP NGN-PS messages will require as they transit the LTE Access Network[2] in support of priority communications. Without protection of the LTE special handling to provide priority treatment for NS/EP NGN-PS, the needs of the NS/EP community to respond effectively to crises could be hampered. The requirements focus on security protection against attacks that would compromise the integrity and availability of the LTE Access Network advance priority and special handing features. The requirements also address confidentiality protection of the Service User's private and sensitive information. This information, which might include location information or data that could reveal the user's identity, must be protected while it is in transit across the network and while it is being stored on various network entities.

The scope of this document includes (1) integrity and availability protection of the LTE advance priority features and the special handling functions and capabilities, including the scheduling mechanisms, (2) integrity and availability of NS/EP communications on the LTE Access Network segment, and (3) confidentiality protection of sensitive and private Service User data. The scope includes secure state transitions and mobility within a LTE provider domain; and security for transport of signaling and user data over LTE interfaces, the Management Plane, Supporting IP Services, and Circuit Switch Fallback (CSFB) Signaling for interworking with Universal Mobile Telecommunications System (UMTS) and Code Division Multiple Access (CDMA) Single Carrier Radio Transmission Technology (1xRTT).

The scope is restricted to security of NS/EP NGN-PS (i.e., NGN Government Emergency Telecommunications Services and Wireless Priority Services, abbreviated as GETS and WPS, respectively) as defined in [ATIS-1000057] that are specific to the LTE access network. The scope of this document is limited to priority voice services for non-roaming scenarios.

Figure 1-1 illustrates the approach used to define and organize the security requirements that address protection of NS/EP NGN-PS for the LTE Access Network. In this document, the LTE Access Network as defined in [3GPP TS 23.002] consists of the:

[1] NGN Service Providers have elected to reuse CS technology rather than an IMS solution for their initial voice communications solution. The 3GPP specification [TS 23.272] covers circuit switch fallback (CS-FB).

[2] This refers specifically to traversal over various LTE interfaces in order to securely establish bearer channels needed for priority communications.