ATIS-0100001.2004(R2013)

User Plane Security Guidelines and 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-0100001.2004(R2013), *User Plane Security Guidelines and Requirements for ETS*

Is an American National Standard developed by the **ATIS Network Performance, Reliability and Quality of Service Committee (PRQC)**.

Published by

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

Printed in the United States of America.

ATIS-0100001.2004
(R2013)

American National Standard for Telecommunications

USER PLANE SECURITY GUIDELINES AND REQUIREMENTS FOR ETS

Secretariat

Alliance for Telecommunications Industry Solutions

Approved October 22, 2004

American National Standards Institute, Inc.

Abstract

This Standard provides a set of user plane security guidelines and requirements for Emergency Telecommunications Services (ETS) over IP networks. The scope is intended to address security as it relates to user plane performance, reliability, and availability of ETS. ETS does not include E-911.

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 carriers, customers, and manufacturers. The Network Performance, Reliability, and Quality of Service Committee (PRQC) develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. PRQC also develops and recommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

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, PRQC Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

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

R. Wohlert, PRQC Chair
N. Seitz, PRQC Vice-Chair
S. Carioti, ATIS Disciplines
S. Barclay, ATIS Secretariat
C. Underkoffler, ATIS Chief Editor
A. Webster and A. Nguyen, PRQC Technical Editors

Organization Represented	Name of Representative
Alcatel USA Inc.	Ken Biholar
ASTRI	Jacky Chow
AT&T	Percy Tarapore Charles A. Dvorak (Alt.)
BellSouth Telecommunications	Archie McCain David M. Brady (Alt.)
C.S.I Telecommunications	Michael S. Newman Thomas G. Croda (Alt.)
Defense Info. Systems Agency	Chris Fitzgerald
Ericsson Incorporated	Mustafa Kocaturk Susana Sabater-Maroto (Alt.)
Harris Corporation	Marlis Humphrey
Intelsat	Mark T. Neibert
Lucent Technologies	Stuart O. Goldman
National Communications System	An Nguyen Jean Trakinat (Alt.)
NTIA	Neal B. Seitz

Organization Represented	Name of Representative
Nortel Networks	Oscar Avellaneda Joseph A . Zebarth (Alt.)
Qwest	Michael Fargano David Clark (Alt.)
SBC Communications, Inc.	Randolph Wohlert Pierre Costa (Alt.)
Siemens Info & Comm Ntwks, Inc.	Suhas S. Gandhi David E. Francisco (Alt.)
Sprint Corporation	Mark L. Jones
Telcordia Technologies	Spilios Makris Cliff Halevi (Alt.)
Tellabs Operations, Inc.	William A. Walker Kevin Stodola (Alt.)
Verizon Communications	John Colombo Wendy Pugh (Alt.)

The Security Task Force Subcommittee, which was responsible for the development of this document, had the following members:

O. Avellaneda
C. Bailey
J. Bennett
J. Colombo
C. Dvorak
R. Holley
F. Kaudel
P. Kimbrough
J. Lankford
S. Makris
A. McCain
A. Nguyen
R. Paterson
N. Seitz
P. Tarapore
A. Thiessen
K. Trahan
J. Trakinat
A. Webster
R. Wohlert
W. Wycoff
J. Zebarth

TABLE OF CONTENTS

TABLE OF TABLES

(R2013)

American National Standard for Telecommunications –

User Plane Security Guidelines and Requirements for ETS

1 Scope, Purpose, & Application

1.1 Scope

This Standard provides guidelines and requirements for security aspects of ETS communications relevant to the user plane. The user plane consists of those aspects related to the user and includes what is called the bearer plane. Security of the other planes in the telecommunications network model (i.e., the signaling and control plane, and the management plane) is not within the scope of this Standard. Non-traceability and the impacts on performance of security for ETS are also outside the scope of this document and may be addressed in future documents.

1.2 Purpose

The purpose of this Standard is to provide security guidelines and requirements relating to ETS communications. What is needed is a consistent set of recommended security guidelines and requirements for the ETS as they relate to user plane performance, reliability, and availability of IP-based networks. The guidelines and requirements provided are specific to ETS, but may be applicable to other communications services provided over IP networks. In addition, security guidelines for the signaling and control plane and the management plane are also needed, but are not addressed in this document.

1.3 Application

This Standard applies to the user plane security mechanisms necessary for the implementation and maintenance of secure and reliable ETS communications. This Standard provides guidelines and requirements regarding cryptographic standards that should be used, but does not specify particular products that may implement these cryptographic standards. It should be noted that certain FIPS Standards will be required in applications contracted by the U.S. Government (e.g., AES, HMAC-SHA).

2 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.

[1] Federal Information Processing Standards Publication 197, *Announcing the Advanced Encryption Standard (AES)*, November 26, 2001.[1]

[2] FIPS 198 March 2002, *The Keyed-Hash Message Authentication Code (HMAC)*.[1]

[1] This document is available from the National Institute of Standards and Technology (NIST) at < http://csrc.nist.gov/publications/fips/ >.

[3] FIPS 180-2 August 2002, *Secure Hash Standard (SHS)*.[1]

NOTE - Informative references for this standard appear in Annex B.

3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS

3.1 Definitions

3.1.1 Authorization: (1) An *authorization* is a right or a permission that is granted to a system entity to access a system resource. (2) An *authorization process* is a procedure for granting such rights. (3) To *authorize* means to grant such a right or permission. [10]

3.1.2 Authentication: The process of verifying an identity claimed by or for a system entity.

An *authentication process* consists of two steps:

1. *Identification step*: Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)

2. *Verification step*: Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

(See: "relationship between data integrity service and authentication services" under Data Integrity Service. [10])

3.1.3 Authentication Service: A security service that verifies an identity claimed by or for an entity. (See: *authentication*.) In a network, there are two general forms of authentication service: data origin authentication service and peer entity authentication service. [10]

3.1.4 Data Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (i.e., to any unauthorized system entity). [11]

3.1.5 Data Confidentiality Service: A security service that protects data against unauthorized disclosure. (See: *data confidentiality*.) [10]

3.1.6 Data Integrity: The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. (See: *data integrity service*.) [10]

3.1.7 Data Integrity Service: A security service that protects against unauthorized changes to data -- including both intentional change or destruction and accidental change or loss -- by ensuring that changes to data are detectable.

A data integrity service can only detect a change and report it to an appropriate system entity; changes cannot be prevented unless the system is perfect (error-free) and no malicious user has access. However, a system that offers data integrity service might also attempt to correct and recover from changes.

Relationship between data integrity service and authentication services: Although data integrity service is defined separately from data origin authentication service and peer entity authentication service, it is closely related to them. Authentication services depend, by definition, on companion data integrity services. Data origin authentication service provides verification that the identity of the original source of a received data unit is as claimed; there can be no such verification if the data unit has been altered. Peer entity authentication service provides verification that the identity of a peer entity in a current association is as claimed; there can be no such verification if the claimed identity has been altered. [10]

3.1.8 Emergency Telecommunications Service: A telecommunications service offering available on public communications networks that facilitates the work of authorized emergency personnel in times of disaster, national emergency, or for executive/governmental communications relating to National Security/Emergency Preparedness (NS/EP).

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ATIS	Alliance for Telecommunications Industry Solutions
EPA	Environmental Protection Agency
ETS	Emergency Telecommunications Service
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
GETS	Government Emergency Telecommunications Service
HAZMAT	Hazardous Materials
HMAC	Keyed-Hash Message Authentication Code
NS/EP	National Security / Emergency Preparedness
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
WPS	Wireless Priority Service

4 BASIC GUIDELINES FOR SECURITY AND CRYPTOGRAPHIC MECHANISMS AND THEIR IMPLEMENTATION

1. Wherever possible, security protocols will be open source and standardized.
2. Where encryption is used, AES (in its current FIPS equivalent) will be utilized wherever it applies.
3. Where encryption is used for integrity, HMAC (SHA-1) will be used.
4. Simplicity, reliability, and wide-spread implementability will be valued over the inclusion of a plethora of options.
5. Security mechanisms for ETS communications (other than AES and HMAC-SHA1) will be reviewed by qualified security/cryptographic experts before selection. The selected mechanisms (beyond those already provided in the public network) should be implemented by qualified security/cryptographic experts.

It should be noted that certain FIPS Standards will be required in applications contracted by the U.S. Government (e.g., AES, HMAC-SHA).

5 SECURITY LEVELS FOR ETS COMMUNICATIONS

In developing security guidelines for ETS, it is useful to ascertain the level of security that is needed for a particular ETS communication. It is recognized that different users of this service will require differing levels of security. While authentication is needed in all cases, some cases may not need data confidentiality. In Annex A, 5 levels (1 is highest) of emergency users/priorities are listed in Table A.1. Annex A also offers descriptive scenarios to further clarify the distinctions between the different levels. These levels are supported in the Wireless Priority Service[2]. It is expected that the number of priority levels might be different for other networks (e.g., the Internet). Because they are already part of an existing ETS, the 5 levels defined in Annex A are used to delineate the different levels of security needed for an ETS communication. Even though some network types (e.g., the Internet) may only offer one priority level for ETS communications, the network may provide different security mechanisms to different classes of users. From a user-plane perspective, security will be end-to-end.

6 SECURITY REQUIREMENTS FOR ETS COMMUNICATIONS

6.1 Authentication Requirements

ETS users must be able to be authenticated by at least one method. Ideally, at least two authentication mechanisms should be supported: one that will be available on any user's equipment (generic) and one that will require a specialized piece of user equipment (hardware specific). Once authenticated, the call or session could in some way be labeled as an ETS communication to facilitate ETS handling. Other methods for providing security without labels may be possible. Any call/session entering an ETS enabled network with an ETS label (e.g., from the PSTN) will be authorized by default if it is from a trusted network and the call/session will receive the appropriate priority treatment in the network. *Trusted networks* are networks that are trusted at the level of security needed for the particular communication session. The recognition of trusted networks will be accomplished in the signaling and control plane and is for further study. For networks that are not *trusted*, one or more of the authentication methods described below will be used.

The behavior of ETS labels (if used) on international networks is not part of this Standard. This important topic is for further study.

6.1.1 Generic Authentication

Generic authentication of calls/sessions originating on an ETS enabled access network, if offered, will be available to an ETS user on any given user's equipment. This might be accomplished, for example, by calling a special number and entering a PIN, or accessing a special website and downloading an applet that prompts for a username and password. If a PIN is used, the length should be at least twelve[3] characters (numerals and/or letters). For the generic authentication, no special hardware is required nor is any special hardware expected to be in the communications equipment. The intent of this method is that authentication can be accomplished using access to the public network using common consumer premises equipment.

[2] See < http://wps.ncs.gov/ > for more information.

[3] Twelve numerals are used in the current GETS system. ETS must have at least that level of security. This level of security is considered the lowest acceptable level.

The recognition of ETS enabled networks and how ETS communications will be established across one or more network sections that are not ETS-enabled are for further study and will probably be addressed in the signaling and control plane.

6.1.2 Hardware Specific Authentication

Hardware specific methods of authentication may be dependent upon the ETS users' equipment. This authentication will only be available on particular pieces of equipment (e.g., phones, computers, etc.), and may additionally require a smartcard, and/or biometrics, and/or a PIN.

6.2 Authorization Requirements

An authenticated ETS user will be authorized to receive special handling of his/her communications consistent with that user's priority level. The authorization level determination usually takes place during the authentication process. The authorization level will determine, among other things, the kind of security required for that call/session (i.e., the level of confidentiality and integrity validation needed).

6.3 Data Confidentiality Requirements

Authenticated ETS users authorized at certain levels will have their communications encrypted. The required method will incorporate the AES in its current FIPS equivalent using a minimum 256-bit key [8]. The encryption for data confidentiality will be done by the user equipment.

6.4 Data Integrity Requirements

Authenticated ETS users authorized at certain levels will have their non-realtime (i.e., other than interactive voice and video) communications checked for data integrity. The required method will incorporate the HMAC-SHA-256 in its current FIPS equivalent. Security for signaling and control is not addressed in this Standard.

Annex A
(informative)

A Priorities for NS/EP Users

This Annex defines 5 levels (1 is highest) of emergency users or priorities and offers descriptive scenarios to further clarify the distinctions. These levels will be used in the classification of ETS users regarding their security needs. These levels are supported in the Wireless Priority Service. It is expected that the number of priority levels might be different for other networks. For example, some applications may provide 5 levels of priority and security at the access to the network but may support only 1 (or even 0) levels of priority over certain network portions (e.g., backbone networks).

Table A.1 - Priorities for NS/EP Users

Priority Level	Responsibility	Qualifying Criteria
1	Executive Leadership and Policy Makers	Users who qualify for the Executive Leadership and Policy Makers priority will be assigned Priority 1. A limited number of PLMN technicians who are essential to restoring the PLMN networks shall also receive this highest priority treatment. Wireless carrier may assign Priority 1 to its technicians with operational responsibilities.
2	Disaster Response / Military Command and Control	Users who qualify for the Disaster Response/Military Command and Control priority will be assigned Priority 2. Individuals eligible for Priority 2 include personnel key to managing the initial response to an emergency at the local, State, regional, and Federal levels. Personnel selected for this priority should be responsible for ensuring the viability or reconstruction of the basic infrastructure in an emergency area. In addition, personnel essential to the continuity of government and national security functions (e.g., conducting international affairs and intelligence activities) are included.
3	Public Health, Safety, and Law Enforcement Command	Users who qualify for the Public Health, Safety, and Law Enforcement Command priority will be assigned Priority 3. Eligible for this priority are individuals who direct operations critical to life, property, and maintenance of law and order immediately following an event.
4	Public Services / Utilities and Public Welfare	Users who qualify for the Public Services/Utilities and Public Welfare priority will be assigned Priority 4. Eligible for this priority are those users whose responsibilities include managing public works and utility infrastructure damage assessment and restoration efforts and transportation to accomplish emergency response activities.
5	Disaster Recovery	Users who qualify for the Disaster Recovery priority will be assigned Priority 5. Eligible for this priority are those individuals responsible for managing a variety of recovery operations after the initial response has been accomplished.

Table 1 is taken from an informative annex of a 3GPP draft Technical Report, 3GPP TR 22.9050 V6.2.0 (2003-03) of the 3rd Generation Partnership Project, *Technical Specification Group Services and System Aspects, Priority Service feasibility study, Release 6, GSM.*

The following subsections offer illustrative examples of the 5 levels.

A.1 Level 1 Executive Leadership and Policy Makers

In the aftermath of a devastating earthquake in San Francisco, the U.S. President, at an undisclosed location, needs to telephone the Vice President, who is also at an undisclosed location. The substance of the discussion and the identities of the participants must be cloaked in the strictest confidentiality.

A.2 Level 2 Disaster Response/Military Command and Control

A huge multi-megawatt power station is incapacitated by a series of upstream accidents and a resulting overload. Bringing it back online successfully requires the coordination of several regional power company facilities. Initial communications among these entities is done over the PSTN using Level 2 priority. If the PSTN congestion increases, the communication is done using WPS. Drawings of the power grid and the sequence of switches to be thrown are encrypted and sent over the Internet.

A.3 Level 3 Public Health, Safety, and Law Enforcement Command

When a tractor-trailer capsizes on the Interstate and spills chemicals onto most lanes of traffic, HAZMAT officials require access to cell phone resources. If there is a danger of explosion, the nearest firefighters will need to be summoned. Officials at FEMA need to assist in coordinating the removal of the hazard. Officials at EPA need to assist in cleanup. Local highway police need to assist in untangling the traffic jam and rerouting new traffic away from the spill. In some cases, the public network needs to be accessed to provide information and coordination between the various public safety entities. Priority access is vital if the local bandwidth is congested with concerned citizens and news gathering personnel. Encryption may be desired.

A.4 Level 4 Public Services/Utilities and Public Welfare

A flash flood has caused devastation of property, has injured several persons, and has destroyed telephone lines in a mountain region of Idaho. The call for coordinated public safety assistance was initiated by the Governor via Level 1 communications over the PSTN. The summoned public safety workers and rescue teams converged on the area from several neighboring jurisdictions. Using Project 25 radios, the individual teams can micro-coordinate their own specific rescue efforts, but their Project 25 radios do not provide the necessary interoperability to communicate with teams from other jurisdictions. By using WPS, the widely spaced teams are able to communicate with each other to coordinate large-scale rescue activities. Video transmission to the state office of emergency coordinators, to the Governor’s office, and to the Idaho Department of Transportation provides much needed information about further dangers that were triggered by the flood and that may pose a threat. Vital information is communicated about particular road repairs needed and about egress of injured or endangered people. Encryption is probably not needed.

A.5 Level 5 Disaster Recovery

In a series of non-manmade catastrophes (an earthquake followed by a tidal wave), communications (PSTN and cell facilities) on a long stretch of California are wiped out. After the serious dangers have been addressed and all victims have been moved to safety, the utility workers arrive on the scene. They use radio, wireless, and satellite communications to coordinate their efforts in restoration of power and telecommunications services. As service is restored, these workers receive priority at Level 5 to access the location of damaged cell towers and the utility workers are able to engage in the exchange of video images (maps) on their notebook computers to mark off areas of severest landline and power-line damage and to indicate assigned territories for repair work. Encryption is probably not needed.

Annex B
(informative)

B INFORMATIVE REFERENCES

[4] T1.276-2003, *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*.[4]

[5] ITU-T Recommendation E.106, *Description of an International Emergency Preference Scheme*.[5]

[6] Draft ITU-T Recommendation F.706, *Service Description for an International Emergency Multimedia Service (IEMS)*.[3]

[7] T1.TR.79-2003 *Overview of Standards in Support of Emergency Telecommunications Service (ETS)*.[2]

[8] Ferguson, N and Schneier, B., *Practical Cryptography*, Wiley Publishing, Inc., 2003.

[9] Anderson, R., *Security Engineering*, John Wiley and Sons, 2001.

[10] Shirey, R., *Internet Security Glossary*, RFC 2828, May 2000.

[11] ISO/IEC 7498-2, *Information Processing Systems--Open Systems Interconnection Reference Model---Part 2: Security Architecture*.[6]

[12] Kaufman, C., Perlman, R., and Speciner, M., *Network Security, Private Communication in a Public World*, 2nd Edition, Prentice Hall, 2002.

[13] Carlberg, K., Desourdis Jr., R., Polk, J., and Brown, I., *Preferential Emergency Communications, From Telecommunications to the Internet*, Kluwer Academic Publishers, 2003.

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

[5] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[6] This document is available from the International Electrotechnical Commission. < http://www.iec.ch/webstore/shop_entry.htm >