ATIS-0300276.2008(s2022)

OPERATIONS, ADMINISTRATION, MAINTENANCE, AND PROVISIONING SECURITY REQUIREMENTS FOR THE PUBLIC TELECOMMUNICATIONS NETWORK: A BASELINE OF SECURITY REQUIREMENTS FOR THE MANAGEMENT PLANE

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Networked Car, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), 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). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit < http://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 OF MERCHANTABILITY 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, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS 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.

ATIS-0300276.2008(S2022), *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*
Is an American National Standard developed by the **Architectures Interfaces and Protocols (AIP) Subcommittee** under the **ATIS Telecom Management and Operations Committee (TMOC)**.

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

Printed in the United States of America.

ATIS-0300276.2008(S2022)

American National Standard for Telecommunications

Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

Alliance for Telecommunications Industry Solutions

Approved August 4, 2008

American National Standards Institute, Inc.

Abstract

This standard contains a set of baseline security requirements for the management plane. The requirements outlined in this standard allow equipment/system suppliers, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure.

Foreword

The information contained in this foreword is not part of this American National Standard (ANS) and has not been processed in accordance with the American National Standards Institute's requirements for an ANS. As such, the 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.

Executive Orders and Presidential directives and commissions previously identified eight infrastructures as critical national assets necessary for the defense and economic security of the United States, with Telecommunications as being one of these critical infrastructures. The President's National Security Telecommunications Advisory Committee Network Security Information Exchange (NSIE) and Government NSIE established a Security Requirements Working Group (SRWG) to examine the security requirements for controlling access to the public switched network, in particular with respect to the emerging next generation network. In the telecommunications industry, this access incorporates operation, administration, maintenance, and provisioning for network elements and various supporting systems and databases (i.e., operational support system).

Members of the SRWG, from a cross-section of telecommunications carriers and vendors, developed an initial list of security requirements that would allow vendors, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure. This initial list of security requirements was submitted as a contribution to ATIS/Committee-T1/T1M1 (now ATIS/TMOC) for consideration as a standard and this work evolved into ANS T1.276 (2003). A supplement to ANS T1.276 (2003) was issued as ATIS-0300276.a.2005. The current 2008 release of this standard is a revision of T1.276 (2003). This revision reflects the evolution of the network towards being IP based, updates the cryptography requirements as a result of advances in the technology, and also incorporates the revisions proposed by supplement (ATIS-0300276.a.2005). Additionally, the standard describes its relationship to its international derivative (ITU-T Recommendation M.3016.x series).

Although the requirements in this standard employ telecommunications terms and formats, the underlying principles should apply equally to the management of computing elements in other infrastructures. Other infrastructures may wish to modify and apply these recommendations as appropriate to their respective infrastructure.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Telecom Management and Operations Committee (TMOC) develops operations, administration, maintenance and provisioning standards, and other documentation related to Operations Support System (OSS) and Network Element (NE) functions and interfaces for communications networks - with an emphasis on standards development related to U.S.A. communication networks in coordination with the development of international standards.

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, TMOC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, TMOC, which was responsible for its development, had the following roster:

L. Garbarini, TMOC Chair (Alcatel-Lucent)
M. Fargano, TMOC Vice Chair (Qwest)
C. Underkoffler, ATIS Chief Editor
H.H. Lam, TE (Alcatel-Lucent)
M. Lee, TE (Nortel)

The **IP** Subcommittee was responsible for the development of this document.

Table of Contents

Table of Tables

Table of Figures

American National Standard
for Telecommunications –

Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

Introduction

This standard contains a set of baseline security requirements for the management plane. The requirements outlined in this standard allow equipment/system suppliers, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure. Although the present baseline represents the current understanding of the state of the art, technologies will advance and conditions will change. To be successful, this standard shall evolve as conditions warrant. This standard is intended as a foundation. Service providers may include unique requirements to meet specific needs over and above those in this baseline.

1 Scope, Purpose, and Application

In some telecommunications networks, management traffic is often transmitted on a separate network from that carrying the service provider's end-user traffic. In these networks, security threats to the management plane are completely isolated from any malicious activity on the end-user plane. The management plane is relatively easy to secure because access to this plane is restricted to known administrators, and traffic is restricted to known management activities. However, in some cases management traffic is combined on a single network with the service provider's end-user traffic. Combining traffic in this manner minimizes costs by requiring only a single integrated network infrastructure; however, many new security challenges are introduced. Threats in the end-user plane now become threats to the management and control planes. The management plane now becomes accessible to the multitude of end-users, and many types of malicious activities become possible. The purpose of this standard is to recommend minimum baseline security mechanisms to help mitigate security risks in the management of telecommunications networks.

To provide a complete end-to-end solution, all security measures (e.g., access control, authentication) should be applied to each type of network activity (i.e., management plane activity, control plane activity, and end user plane activity) for the network infrastructure, network services, and network applications. This standard focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the network infrastructure. As such, the standard addresses only one aspect of an overall end-to-end security solution, but may be used as a starting point for subsequent standards addressing the security of “control” and “end user” planes, as appropriate.

The requirements in this standard are applicable to NEs and MSs to be deployed in the future. For NEs in the network that do not meet all the mandatory security requirements, the overall security requirements at the network architecture design should be supported. This standard addresses security for NE, MS, and element management system (EMS) equipment, and does not specifically address security for other