ATIS-1000019.2007(S2017)

Network to Network Interface (NNI) Standard for Signaling and Control Security for Evolving VoP Multimedia Networks

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 and Forums, 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, Connected Vehicle, 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 < 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.

ATIS-1000019.2007(R2012), *Network to Network Interface (NNI) Standard for Signaling and Control Security for Evolving VoP Multimedia Networks*

Is an American National Standard developed by the **Signaling, 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

Copyright © 2012 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < http://www.atis.org >.

Printed in the United States of America.

(S2017)
ATIS-1000019.2007

American National Standard for Telecommunications

NETWORK TO NETWORK INTERFACE (NNI) STANDARD FOR SIGNALING AND CONTROL SECURITY FOR EVOLVING VOP MULTIMEDIA NETWORKS

Secretariat

Alliance for Telecommunications Industry Solutions

Approved March 1, 2007

American National Standards Institute, Inc.

Abstract

This document specifies Voice over Packet and Multimedia signaling and control plane security requirements for evolving 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 carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) -- formerly T1S1 -- 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.

This document specifies Voice over Packet and Multimedia signaling and control plane security requirements for evolving networks. This standard is part of a suite of signaling and control security documents as shown in Figure 1. This standard provides security requirements for VoP and Multimedia signaling and control services that cross the Network to Network Interfaces (NNI).

This standard is in alignment with ITU-T Recommendation X.805 [X.805].

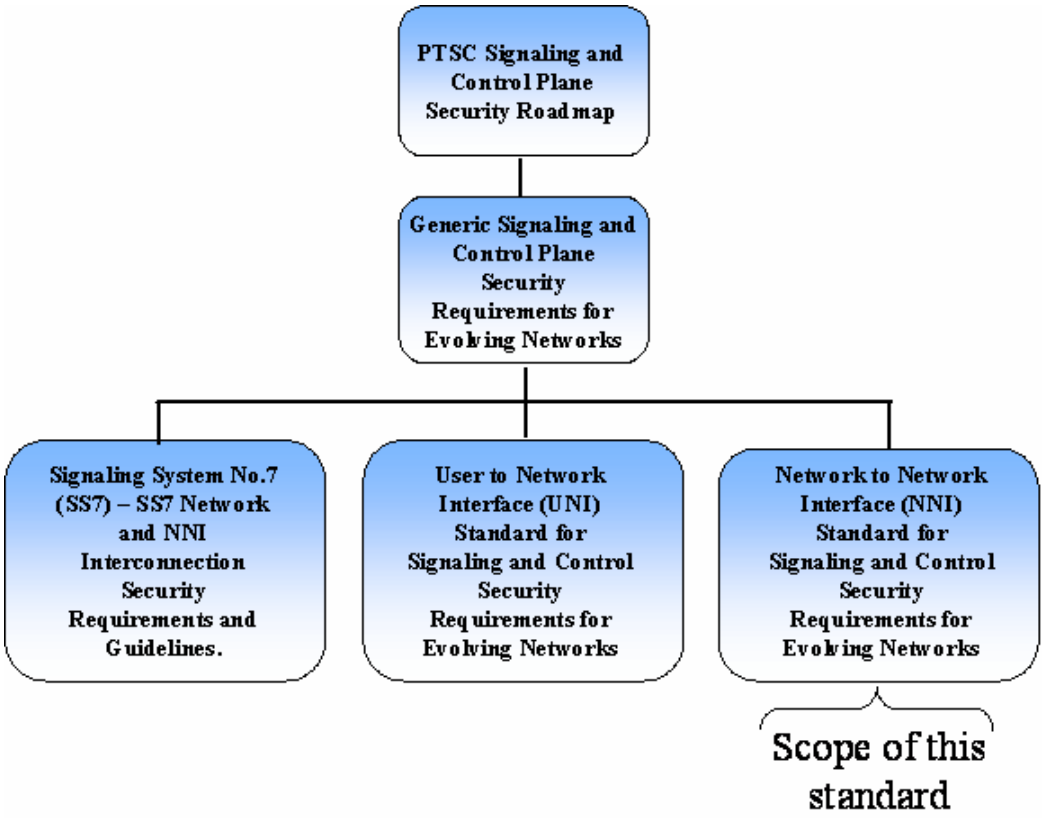

Figure 1 - Signaling and Control Security Documents

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC Secretariat, 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 members:

B. Hall, PTSC Chair
J. Zebarth, PTSC Vice-Chair
C. Underkoffler, ATIS Chief Editor
M. Lee, PTSC Technical Editor

Organization Represented	Name of Representative
AcmePacket	Kevin Klett
Alcatel USA Inc.	Ken Biholar
AT&T	Bob Hall George Stanek (Alt)
Avivi Systems	Esmeralda Swartz
BellSouth Telecommunications	Rick McNealy
Cingular Wireless LLC	Don Zelmer Marc Grant (Alt)
Cisco Systems	Rajiv Kapoor Chip Sharp (Alt)
Department of Defense	Chris Fitzgerald Ryan Kuseki (Alt)
Embarq Corporation	John M. Heinz Bill L. Wiley (Alt)
Ericsson Incorporated	Susana Sabater-Maroto Stephen Hayes (Alt)
ETRI	Shin-Gak Kang Wook Hyun (Alt)
FBI ESTS	Marybeth Paglino Edward Ignacio (Alt)
Hewlett-Packard	Steve Mills
Intel Corporation	Walt Brown
Intelsat	Mark T. Neibert
Intrado	Christian Militeau Robert Sherry (Alt)
Lucent Technologies	Stuart O. Goldman
Microsoft Corporation	Wendy Fong

Organization Represented	Name of Representative
National Communications Systems	Nicholas Andre Carol-Lyn Taylor (Alt)
NEC Corporation of America	Milorad Cvijetic
NeuStar	Peggy Rehm Tom McGarry (Alt)
Nokia Telecommunications Inc.	Joyabrata Mukherjee Ed Ehrlich (Alt)
Nortel	Joseph A. Zebarth
PSEP Canada	Sim Simanis Gary Hutchinson (Alt)
Qwest	Steve Showell Michael Fargano (Alt)
Siemens Communications, Inc.	Ron Franks David E. Francisco (Alt)
Sprint Corporation	Mark L. Jones
SS8 Networks Inc.	Cemal Dikmen Scott Coleman (Alt)
Telcordia Technologies	Wesley Downum Cliff Halevi (Alt)
Tellabs Operations, Inc.	William A. Walker
Tridea Works	Selvan Rengasami Ken Coon (Alt)
VeriSign, Inc.	Anthony Rutkowski
Verizon Communications	Thomas Helmes Dave Morris (Alt)

The Security (SEC) Subcommittee was responsible for the development of this document.

TABLE OF CONTENTS

TABLE OF FIGURES

American National Standard for Telecommunications –

Network to Network Interface (NNI) Standard for Signaling and Control Security for Evolving VoP Multimedia Networks

1 INTRODUCTION/EXECUTIVE SUMMARY

Many security threats exist to the signaling and control plane of telecommunications networks. In addition, new security threats to the signaling and control plane are being introduced as the network evolves. The purpose of this standard is to provide network to network interface (NNI) signaling and control plane security requirements for Voice and Multimedia over packet in evolving telecommunications networks.

In some telecommunications networks, signaling and control traffic is transmitted on a separate network from that carrying the service provider's end-user traffic. In these networks, security threats to the signaling and control plane are isolated from any malicious activity on the end-user plane. However, with the evolving telecommunications networks, signaling and control traffic is often combined with end-user traffic on a single network. Combining traffic in this manner minimizes costs by requiring only a single integrated network infrastructure; however, new security challenges are introduced. Threats in the end-user plane now become threats to the signaling and control plane since the signaling and control plane becomes more accessible to the multitude of end-users.

Connections between carrier VoIP networks have been made via TDM or analogue mechanisms. Using TDM or analogue techniques isolates VoIP networks from each other and circumvents many interoperability issues, but it also adds unnecessary service limitations, cost, and complexity. It also degrades VoIP quality, as multiple TDM to IP transcoding hops increase latency and can add distortion. These undesirable effects undermine service quality and the potential to deliver voice, video, and other real-time communication services over a cost-effective converged infrastructure. To realize the full benefits of VoIP, networks must be able to be connected directly at the IP level without converting to TDM.

To enable direct IP connection between carrier networks, stringent security mechanisms must be in place at the network to network interface to ensure the networks are not vulnerable to attack. These security mechanisms help allow desired IP telephony traffic to enter the network while blocking intruders and attacks in a controlled manner to protect internal network resources.

To ensure a secure network to network interface, a concept that is useful is that of a *Border Security Function (BSF)*. The BSF is a set of security functions to enables secure communication to occur across the network to network interface. The security functions included in the BSF may be distributed into various network elements such as Call Servers or Soft Switches, or the security functions may be included in stand alone network elements such as a Session Border Controller (SBC). Implementation topology recommendations for the BSF are beyond the scope of this document. Other non-security related functions may also included at the NNI such as signaling translation and QoS policy enforcement; however, such non-security related functions are beyond the scope of this document.

A diagram of two interconnected networks is given below in Figure 2. The BSF security functions may include, but are not limited to:

- Access control mechanisms to allow only desired peer networks to access a network across the NNI.
- Authentication mechanisms to ensure the identity of signaling plane peer entities communicating across the NNI, and data origin authentication of signaling messages being sent across the NNI.
- Non-repudiation services for signaling messages being sent across the NNI.
- Data confidentiality services for signaling plane information being sent across the NNI to ensure it cannot be viewed by unauthorized parties.
- Security of communication across the NNI interface.
- Data integrity services for signaling plane information being sent across the NNI to ensure that it cannot be modified by unauthorized parties.
- Security services to enhance availability; for example to protect networks from denial of service attacks at the NNI.
- Security services, to ensure privacy of sensitive data and internal network topologies.

In Figure 2, an IP Transport Network is shown for completeness between different VoIP/Multimedia Networks. IP Transport Networks may or may not implement their own Border Security Function depending on particular IP Transport Network security policy. For simplicity, subsequent diagrams in this document do not show the IP transport network.

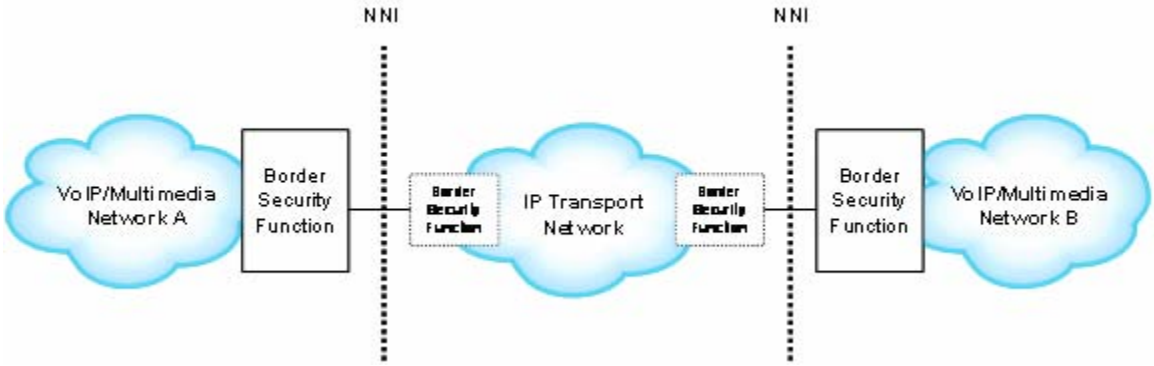

Figure 2 - Architectural Diagram of Interconnected VoIP/Multimedia Networks

2 SCOPE, PURPOSE, & RELATED DOCUMENTS

2.1 Scope

This document addresses VoP/Multimedia signaling and control plane security requirements of evolving telecommunications networks. Evolving telecommunications networks often combine legacy telecommunication facilities with new technologies such as Wireless (air interface), ATM, and Internet

Protocol transport mechanisms. The security requirements given in this document apply to service provider networks and may also be applicable to individual company corporate enterprise networks.

The scope of this document is specifically security requirements for the Network to Network Interface (NNI) between similar or dissimilar VoP/Multimedia networks.

As illustrated in Figure 3, this document is part of a series of related signaling and control plane security standards.

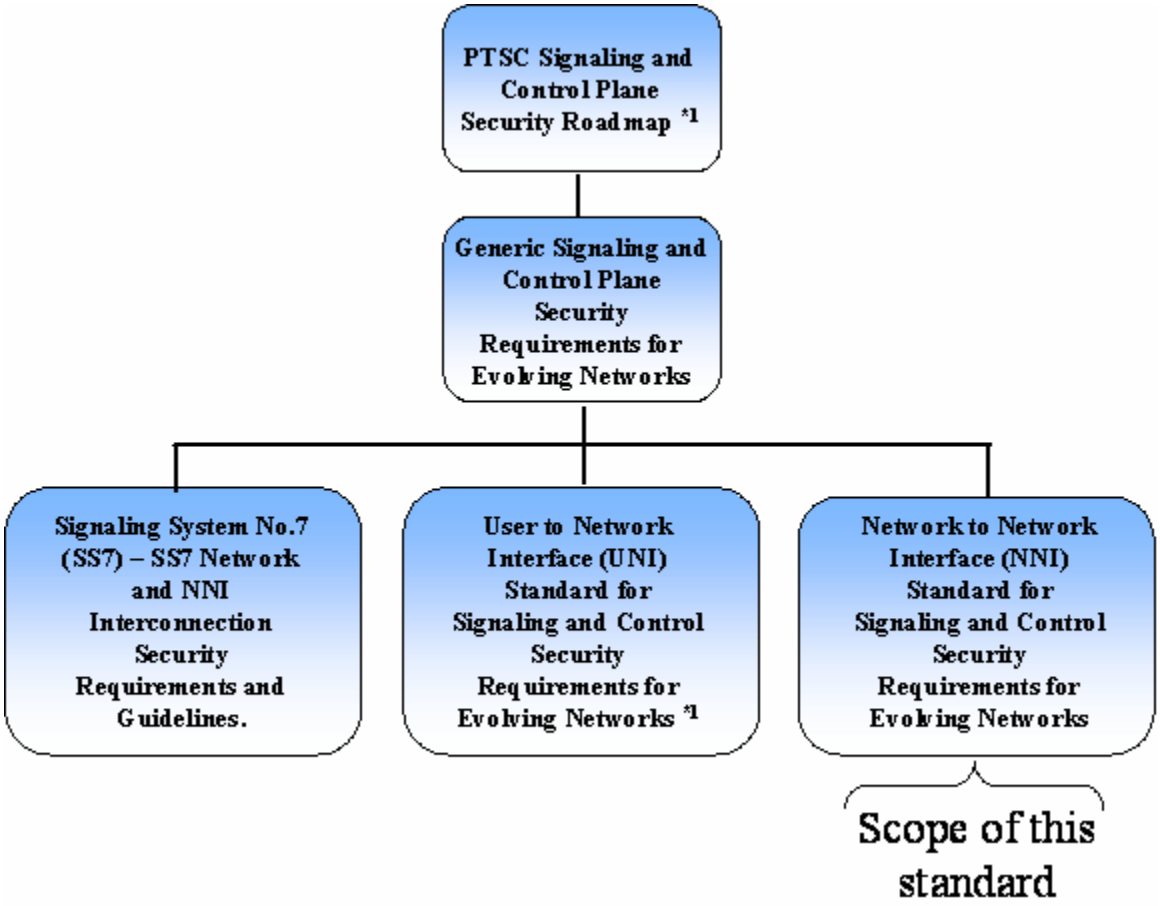

Figure 3 - Signaling and Control Plane Security Document Series

*1 *Proposed*

This document aligns with the organization and framework provided by ITU-T Recommendation X.805, *Security Architecture for Systems Providing End-to-End Communications*. [X.805], and existing security standards are referenced and specified as appropriate.

NOTE -- Endpoints for example user terminal to user terminal peer to peer signaling across the NNI is not within the scope of this document.