ATIS-1000019.2007(R2012)

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

Printed in the United States of America.

(R2012)

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].

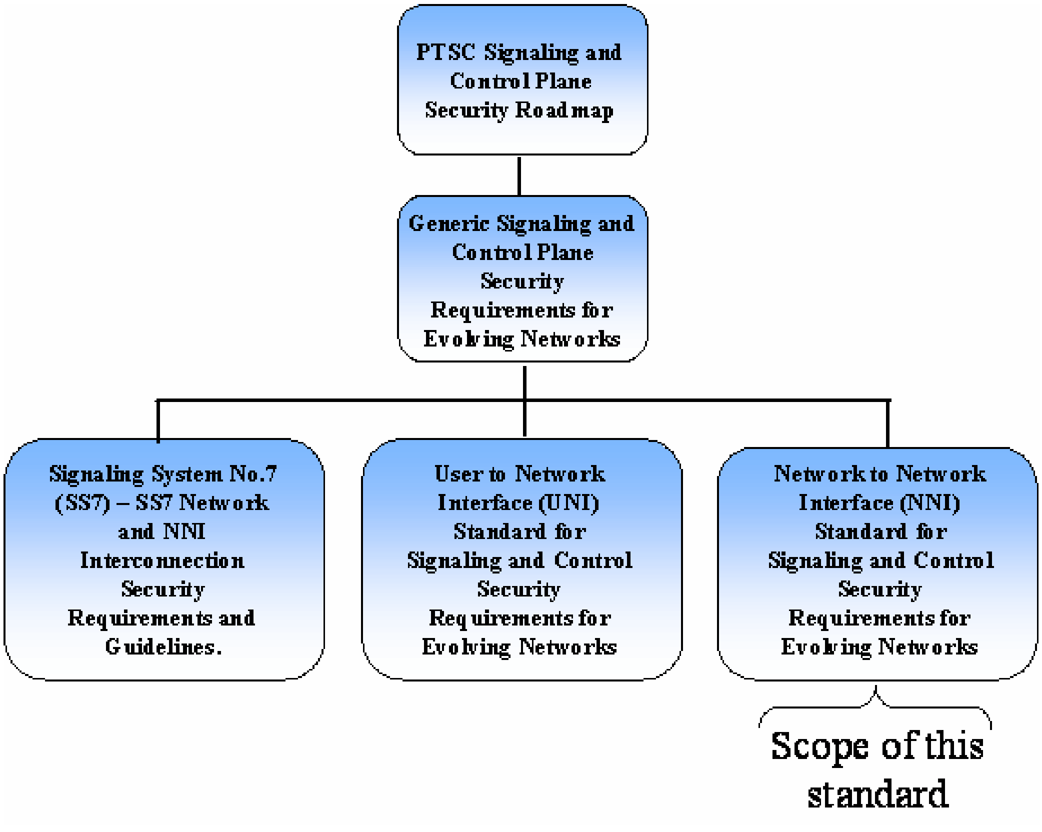
PTSC Signaling and Control Plane Security Roadmap
Generic Signaling and Control Plane Security Requirements for Evolving Networks
Signaling System No.7 (SS7) – SS7 Network and NNI Interconnection Security Requirements and Guidelines.
User to Network Interface (UNI) Standard for Signaling and Control Security Requirements for Evolving Networks
Network to Network Interface (NNI) Standard for Signaling and Control Security Requirements for Evolving Networks
Scope of this standard

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

1 INTRODUCTION/EXECUTIVE SUMMARY 1

2 SCOPE, PURPOSE, & RELATED DOCUMENTS 2

2.1 SCOPE 2
2.2. PURPOSE 4
2.3 RELATED DOCUMENTS 4

3 NORMATIVE REFERENCES 4

4 DEFINITIONS & ABBREVIATIONS 5

4.1 DEFINITIONS 5
4.2 ABBREVIATIONS 5

5 REFERENCE SIGNALING & CONTROL NETWORK MODEL 5

6 H.323 SECURITY 6

6.1 GENERAL REQUIREMENTS 8
6.2 ACCESS CONTROL SECURITY DIMENSION 8
6.3 AUTHENTICATION SECURITY DIMENSION 9
6.4 NON-REPUDIATION SECURITY DIMENSION 9
6.5 DATA CONFIDENTIALITY SECURITY DIMENSION 10
6.6. COMMUNICATION SECURITY DIMENSION 10
6.7 DATA INTEGRITY SECURITY DIMENSION 10
6.8 AVAILABILITY SECURITY DIMENSION 10
6.9 PRIVACY SECURITY DIMENSION 10

7 SIP SECURITY 11

7.1 GENERAL REQUIREMENTS 12
7.2 ACCESS CONTROL SECURITY DIMENSION 12
7.3 AUTHENTICATION SECURITY DIMENSION 13
7.4 NON-REPUDIATION SECURITY DIMENSION 13
7.5 DATA CONFIDENTIALITY SECURITY DIMENSION 14
7.6 COMMUNICATION SECURITY DIMENSION 14
7.7 DATA INTEGRITY SECURITY DIMENSION 14
7.8 AVAILABILITY SECURITY DIMENSION 14
7.9 PRIVACY SECURITY DIMENSION 15
7.9.1 Privacy of Personal Data 15
7.9.2 Topology Hiding 15
7.9.3 Spam Protection 15

A ANNEX – H.323 BACKGROUND 16

A.1 H.323 SIGNALING AND CONTROL CHANNELS BACKGROUND 16
A.1.1 H.323 Overview 16
A.1.2 Media Gateways 16
A.1.3 H.323 Signaling Protocols 17
A.2 H.323 MESSAGING SEQUENCE 18
A.3 H SERIES VIDEO CODECS 18
A.4 H.235 SECURITY PROFILES 18
A.5 H.235.1 – BASELINE SECURITY PROFILE 19
A.6 H.235.2 – SIGNATURE SECURITY PROFILE 19
A.7 H.235.3 – HYBRID SECURITY PROFILE 19

B INFORMATIVE REFERENCES 20

TABLE OF FIGURES

FIGURE 1 - SIGNALING AND CONTROL SECURITY DOCUMENTS II
FIGURE 2 - ARCHITECTURAL DIAGRAM OF INTERCONNECTED VOIP/MULTIMEDIA NETWORKS.......... 2
FIGURE 3 - SIGNALING AND CONTROL PLANE SECURITY DOCUMENT SERIES 3
FIGURE 4 - H.323 ARCHITECTURAL MODEL 6
FIGURE 5 - H.323 NETWORK TO H.323 NETWORK INTERFACE 7
FIGURE 6 - SIP NETWORK TO H.323 NETWORK INTERFACE 7
FIGURE 7 - SIP NETWORK TO SIP NETWORK INTERFACE 11
FIGURE 8 - H.323 ARCHITECTURE 16

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.

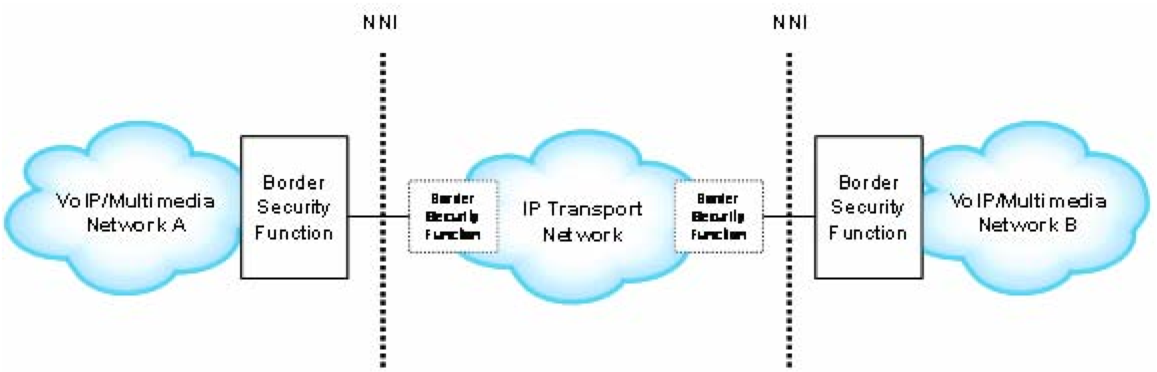

Figure 2 - Architectural Diagram of Interconnected VoIP/Multimedia Networks

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.

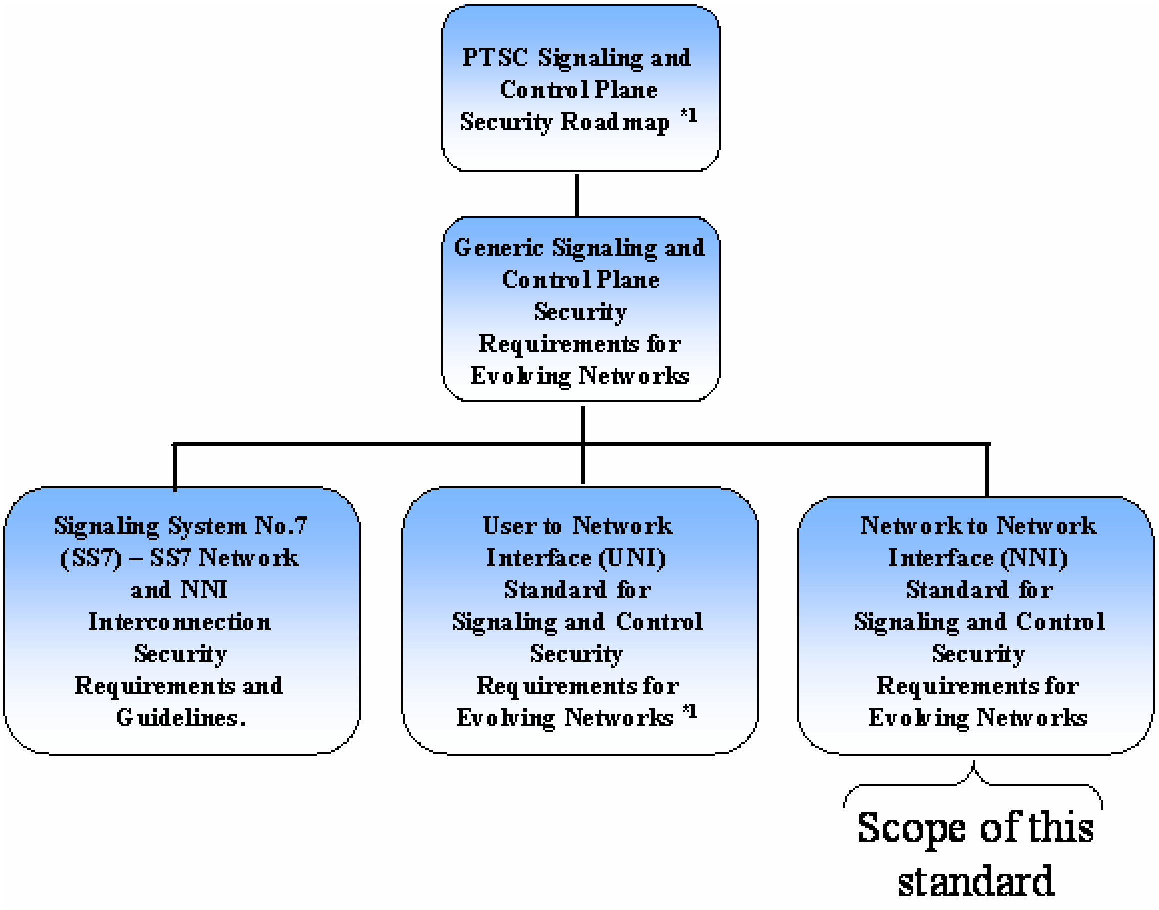
PTSC Signaling and Control Plane Security Roadmap *1
Generic Signaling and Control Plane Security Requirements for Evolving Networks
Signaling System No.7 (SS7) – SS7 Network and NNI Interconnection Security Requirements and Guidelines.
User to Network Interface (UNI) Standard for Signaling and Control Security Requirements for Evolving Networks *1
Network to Network Interface (NNI) Standard for Signaling and Control Security Requirements for Evolving Networks
Scope of this standard

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.

2.2. Purpose

This document provides baseline security requirements to address security for VoP/Multimedia applications using H.323 and SIP.

The purpose of this document is to specify security requirements for the VoP/Multimedia signaling and control plane functions of evolving telecommunications networks, to allow secure interoperability of equipment from multiple vendors by providing signaling and control plane security requirements to carriers and vendors.

2.3 Related Documents

The related signaling and control plane security standards are:

- ATIS-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks*.

3 Normative References

[Generic] ATIS-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks*.[1]

[SIP NNI] ATIS-1000009.2006, *IP Network-to-Network Interface (NNI) Standard for VoIP*.[1]

[H.225] ITU-T Recommendation H.225, *Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems*.[2]

[H.235.0] ITU-T Recommendation H.235.0, *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.[2]

[H.245] ITU-T Recommendation H.245, *Control Protocol for Multimedia Communication*.[2]

[H.323] ITU-T Recommendation H.323, *Packet Based Multimedia Communications Systems*.[2]

[X.805] ITU-T Recommendation X.805, *Security Architecture for Systems Providing End-to-End Communications*.[2]

[RFC 3261] IETF RFC 3261, *SIP: Session Initiation Protocol, Internet Engineering Task Force*.[3]

[RFC 3323] IETF RFC 3323, *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.

[RFC 4301] IETF RFC 4301, *Security Architecture for the Internet Protocol*.

[RFC 4346] IETF RFC 4346, *The Transport Layer Security (TLS) Protocol, Version 1.1*.

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

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

[3] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

4 DEFINITIONS & ABBREVIATIONS

4.1 Definitions

Common definitions used in this specification are given in [Generic].

4.1.1 Network Edge Entity: The optional combination of communication party and network element where the NNI is implemented.

4.1.2 Border Security Function: A set of security functions to enables secure communication to occur across the network to network interface.

4.2 Abbreviations

Common abbreviations used in this specification are given in [Generic].

ACL	Access Control List
BSF	Border Security Function
DoS	Denial of Service
NAT	Network Address Translation
NNI	Network to Network Interface
RAS	Registration, Admission, Status

5 REFERENCE SIGNALING & CONTROL NETWORK MODEL

As discussed in [Generic], this document uses the framework and architecture proposed in ITU-T Recommendation X.805. The Security Architectural Model presented in [X.805] consists of three architectural components:

1. *Security Planes* (End User Plane, Signaling and Control Plane, and Management Plane);
2. *Security Layers* (Applications Security, Network Services Security and Infrastructure Security); and
3. *Security Dimensions* (Access Control, Authentication, Non-repudiation/Audit Logging, Data Confidentiality and Privacy, Data Integrity, Availability).

This standard is related to the ITU-T Recommendation X.805 model in the following manner:

1. *Security Planes Addressed*: Signaling and Control Plane Only.
2. *Security Layers Addressed*: Applications Security only (H.323 and SIP).
3. *Security Dimensions Addressed*: All.

6 H.323 SECURITY

[H.323]is the ITU Recommendation for the setup and control of packet telephony and multimedia.

The following requirements address the NNI security for general areas of H.323 Voice over IP applications including:

- Connection Establishment (Registration, Admission, Status)
- Signaling/Call Control

Within [H.323], other signaling and control standards are referenced:

- ***ITU-T Recommendation H.225***, *Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems.*
  - H.225 includes the Registration, Admission, Status (RAS) channel for communications between endpoints and the gatekeeper.
- ***ITU-T Recommendation H.245***, *Control Protocol for Multimedia Communication.*

The H.323 network architectural model is shown in Figure 4. See Reference [H.323] for more information on the H.323 architecture, including H.323 definitions. Figure 5 illustrates the H.323 network to H.323 network interface. Figure 6 illustrates the SIP network to H.323 network interface.

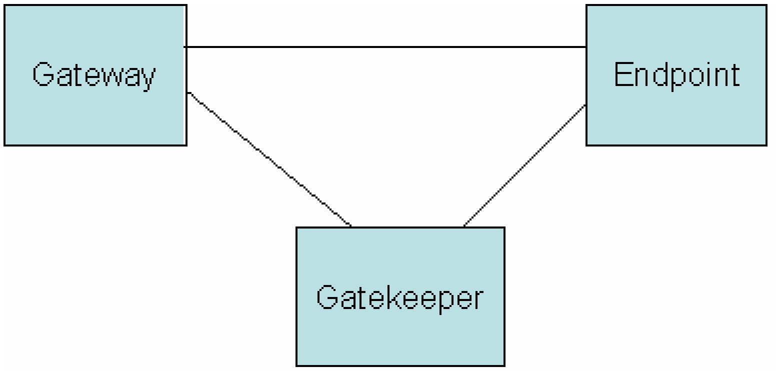

Figure 4 - H.323 Architectural Model

NOTE -- Solid Line Indicates Signaling Relationship.

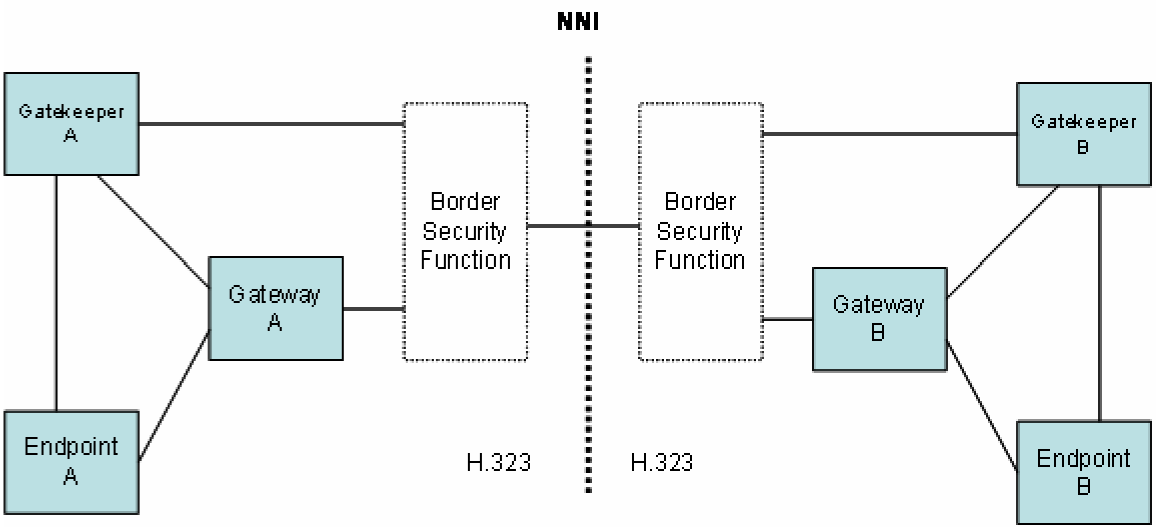

Figure 5 - H.323 Network to H.323 Network Interface

NOTE 1 -- Solid Line Indicates Signaling Relationship.
NOTE 2 -- The Border Security Function is not an H.323 defined entity.

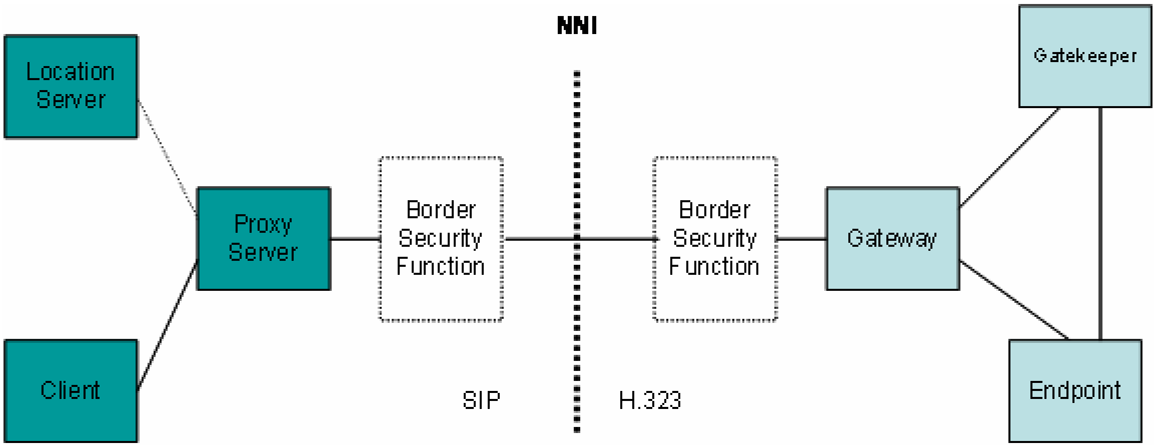

Figure 6 - SIP Network to H.323 Network Interface

NOTE 1 -- Solid Line Indicates Signaling Relationship.
NOTE 2 -- The Border Security Function is not an H.323 or SIP defined entity.

6.1 General Requirements

REQ-SEC-NNI-00100	Mechanisms for authentication and confidentiality based on IPsec and/or TLS shall be provided at a minimum for all Connection Establishment and Signaling/Call Control exchanges between network peer entities across the NNI. If NAT is implemented across the NNI and IPsec is used, said IPsec mechanisms must work in the presence of NAT.

NOTE -- See [H.235] for information on H.323 IPsec and TLS security profiles. Reference [ITU-T H.235]. Refer to [Generic] for IPsec and TLS Protocol Requirements.

6.2 Access Control Security Dimension

REQ-SEC-NNI-00200	Some means shall be used to restrict/grant access to specific network entities across the NNI interface.

NOTE -- Access Control Lists (ACLs) may be used to provide access control.

REQ-SEC-NNI-00300	Some means shall be used to allow or reject specific types of information entering a network across the NNI.

NOTE -- Firewall mechanisms may be used to allow or reject specific information entering a network across the NNI. For example, firewall mechanisms may be used to reject all but SIP and/or H.323 signaling and media plane and other desired information from entering a network across the NNI.

REQ-SEC-NNI-00400	Means to detect and log unauthorized access attempts to the network at the NNI shall be supported and used.

NOTE -- A system configurable threshold may be set for the number of unauthorized access attempts beyond which a system alarm will be generated, logged, and reported to a management system.

6.3 Authentication Security Dimension

REQ-SEC-NNI-00500	There shall be a secure (mutually authenticated) mode of communication established between network entities implementing the border security function (BSF) across the NNI before they exchange call connection messages with either: ♦ TLS; or ♦ IPsec.

REQ-SEC-NNI-00600	Mutual authentication mechanisms across the NNI shall include at least one of the following: 1. Non-clear-text passwords. 2. Digital authenticators. 3. Digital signatures.

REQ-SEC-NNI-00700	Signaling traffic must include an element in the signaling data or message that enables the receiving network to verify the authenticity of the message. For example, authentication mechanisms within the IPsec and/or TLS protocols may be used for data or message authentication across the NNI.

REQ-SEC-NNI-00800	It shall be possible to independently assign an authentication mechanism or algorithm (as specified in the H.245 OpenLogical Channel message) to each independent media channel.

6.4 Non-Repudiation Security Dimension

REQ-SEC-NNI-00900	The capability for unauthorized access attempts at the NNI to be logged and reported to a management system shall be provided.

NOTE -- A system configurable threshold may be set for the number of unauthorized access attempts beyond which a system alarm will be generated, logged, and reported to a management system.

REQ-SEC-NNI-01000	The capability to identify unauthorized H.323 signaling packets at the NNI and to log and report these to a management system shall be provided.

NOTE -- A system configurable threshold may be set for the number of unauthorized H.323 signaling packets beyond which a system alarm will be generated, logged, and reported to a management system.

6.5 Data Confidentiality Security Dimension

REQ-SEC-NNI-01100	The negotiated security mechanism (see requirement REQ-SEC-NNI-00100) across the NNI shall be supported to provide confidentiality of signaling data (e.g., H.323 aliases, phone numbers, network addresses, and call accounting information) to protect the signaling data from unauthorized access or observation.

6.6. Communication Security Dimension

No additional requirements to address the Communication Security dimension have been identified beyond those specified in the Authentication Security (see 6.3) and Data Integrity (see 6.7) dimensions.

6.7 Data Integrity Security Dimension

REQ-SEC-NNI-01200	The negotiated security mechanism (see requirement REQ-SEC-NNI-00100) across the NNI shall be used to provide signaling data integrity.

6.8 Availability Security Dimension

As a best practice guideline, interconnected networks should implement mechanisms to detect and mitigate H.323 DoS attacks directed both from the host to the foreign networks and in the opposite direction (i.e., attacks across the NNI). For example, network entities implementing the BSF should support capabilities to detect and prevent DoS attack. Mechanisms may differ depending on the attack direction. Both application layer flooding attacks and malformed packet attacks should be mitigated by the DoS protection mechanisms.

6.9 Privacy Security Dimension

It is necessary to be able to hide internal network addresses and topology from viewing and discovery from the NNI in order to enhance security. For example, attackers accessing a network from the NNI should not be able see internal IP addresses of call servers and other VoIP/Multimedia network elements.

REQ-SEC-NNI-01300	Network edge entities shall be capable of supporting network address translation (NAT) functions in order to hide internal network topology, if internal network resources use private IP addressing schemes.

7 SIP SECURITY

Session Initiation Protocol (SIP) is a control protocol for multimedia over packet networks including telephony, conferencing, and instant messaging. The SIP protocol initiates call/session setup, authentication and other call features within an IP domain. The SIP protocol is specified in IETF RFC-3261.

The following requirements address the security for the following two general areas of SIP Voice over IP applications across the NNI interface:

- Session Establishment; and
- Signaling/Call Control.

Figure 7 shows the SIP network to SIP network interface. More information on SIP network architecture, including SIP definitions, can be found in [RFC 3261]. ATIS-1000009.2006 specifies the IP Network-to-Network Interface (NNI) for VoIP between carriers using SIP. [SIP NNI].

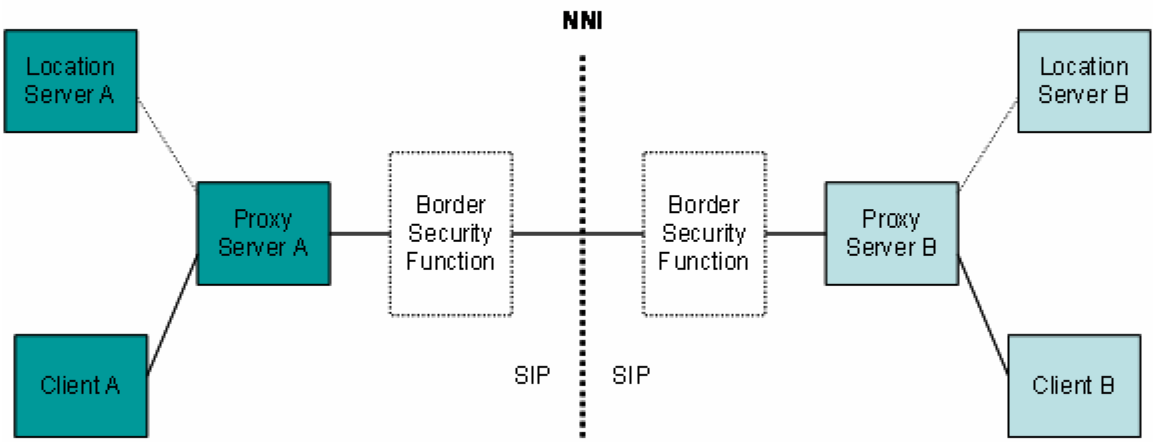

Figure 7 - SIP Network to SIP Network Interface

NOTE -- Solid Line IndicatesSignaling Relationship

7.1 General Requirements

REQ-SEC-NNI-01400	Mechanisms for authentication and confidentiality based on IPsec and/or TLS shall be provided at a minimum for all Connection Establishment and Signaling/Call Control exchanges between network peer entities across the NNI. If NAT is implemented across the NNI and IPsec is used, said IPsec mechanisms must work in the presence of NAT.

Refer to ATIS-1000007.2006 for IPsec and TLS Protocol Requirements.

7.2 Access Control Security Dimension

REQ-SEC-NNI-01500	Some means shall be used to restrict/grant access to specific network entities across the NNI interface.

NOTE -- Access Control Lists (ACLs) may be used to provide SIP Authorization/Access Control.

REQ-SEC-NNI-01600	Some means shall be used to allow or reject specific types of information entering a network across the NNI.

NOTE -- Firewall mechanisms may be used to allow or reject specific information entering a network across the NNI. For example, firewall mechanisms may be used to reject all but SIP and/or H.323 signaling and media plane and other desired information from entering a network across the NNI.

REQ-SEC-NNI-01700	Means to detect and log unauthorized access attempts to the network at the NNI shall be supported and used.

NOTE -- A system configurable threshold may be set for the number of unauthorized access attempts beyond which a system alarm will be generated, logged, and reported to a management system.

7.3 Authentication Security Dimension

REQ-SEC-NNI-01800	There shall be a secure (mutually authenticated) mode of communication established between network entities implementing the BSF across the NNI before they exchange call connection messages with either: ♦ TLS; or ♦ IPsec.

REQ-SEC-NNI-01900	Mutual authentication mechanisms across the NNI shall include at least one of the following: 1. Non-clear-text passwords. 2. Digital authenticators. 3. Digital signatures.

REQ-SEC-NNI-02000	Signaling traffic must include an element in the signaling data or message that enables the receiving network to verify the authenticity of the message. For example, authentication mechanisms within the IPsec and/or TLS protocols may be used for data or message authentication across the NNI.

7.4 Non-Repudiation Security Dimension

REQ-SEC-NNI-02100	The capability for unauthorized access attempts at the NNI to be logged and reported to a management system shall be provided.

NOTE -- A system configurable threshold may be set for the number of unauthorized access attempts beyond which a system alarm will be generated, logged, and reported to a management system.

REQ-SEC-NNI-02200	The capability to identify unauthorized SIP signaling packets at the NNI and to log and report these to a management system shall be provided.

NOTE -- A system configurable threshold may be set for the number of unauthorized SIP signaling packets beyond which a system alarm will be generated, logged, and reported to a management system.

7.5 Data Confidentiality Security Dimension

REQ-SEC-NNI-02300	The negotiated security mechanism (see requirement REQ-SEC-NNI-01400) across the NNI shall be supported to provide confidentiality of signaling data (e.g., phone numbers, network addresses, and call accounting information) to protect the signaling data from unauthorized access or observation.

7.6 Communication Security Dimension

No additional requirements to address the Communication Security dimension have been identified beyond those specified in the Authentication Security (see 7.3) and Data Integrity (see 7.7) dimensions.

7.7 Data Integrity Security Dimension

REQ-SEC-NNI-02400	The negotiated security mechanism (see requirement REQ-SEC-NNI-01400) across the NNI shall be used to provide signaling data integrity.

7.8 Availability Security Dimension

As a best practice guideline, interconnected networks should implement mechanisms to detect and mitigate SIP DoS attacks directed both from the host to the foreign networks and in the opposite direction (i.e., attacks across the NNI). For example, network entities implementing the BSF should support capabilities to detect and prevent DoS attacks. Mechanisms may differ depending on the attack direction. Both application layer flooding attacks and malformed packet attacks should be mitigated by the DoS protection mechanisms.

7.9 Privacy Security Dimension

7.9.1 Privacy of Personal Data

Endpoints and communication parties can obscure some personal data in signaling packets or use network service, as described in IETF RFC-3323.

REQ-SEC-NNI-02500	Network edge entity shall be able to support processing and delivery over NNI of the signaling packets which have the following data obscured as per reference [RFC 3323]: ♦ Identity of the communication party. ♦ Exact location of the communication party.

NOTE -- Compliance with this requirement should not stop a network edge entity from having a policy in place that would prevent endpoints from being anonymous or using anonymity services in the host network.

7.9.2 Topology Hiding

It is necessary to hide internal network addresses and topology from viewing and discovery from the NNI in order to enhance security. For example, attackers accessing a network from the NNI should not be able see internal IP addresses of call servers and other VoIP/Multimedia network elements.

REQ-SEC-NNI-02600	Network edge entities shall be capable of supporting network address translation (NAT) functions to hide internal network topology, if internal network resources use private IP addressing schemes.

7.9.3 Spam Protection

This document does not include any requirements to counter spam -- e.g., VoIP call spam, instant messaging spam, and presence spam. This subject is for further study.

Annex A
(informative)

A ANNEX – H.323 BACKGROUND

A.1 H.323 Signaling and Control Channels Background

A.1.1 H.323 Overview

H.323 is a international protocol, published by the ITU, that supports interoperability between differing vendor implementations of telephony and multimedia products across IP-based networks. H.323 entities provide real-time audio, video, and/or data communications. Support for audio is mandatory, while support for data and video is optional.

A.1.2 Media Gateways

The primary components of an H.323 network include: endpoints, gateways, gatekeepers, and MCUs (Multipoint Control Units). *Endpoints* (telephones, softphones, IVRs, voicemail, video cameras, etc.) are the devices typically used by end-users in the normal use of the system. *Gateways* (gateways and controllers) handle signaling and media transport, and typically serve as the interface to other types of networks such as ISDN, PSTN, and or other H.323 systems. Gateways which focus primarily on converting between IP and other forms of media (such as PSTN) are termed *Media Gateways*. *Gatekeepers* are the logical entity with which endpoints register and are administered. They also manage call setup, teardown, and status and can assist in address resolution. *MCUs* are designed to support multi-party conferencing.

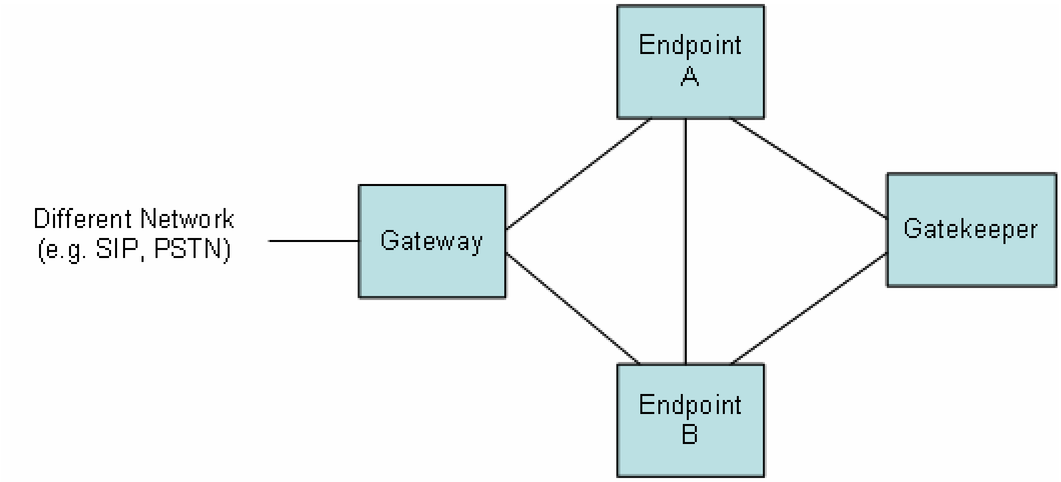

Figure 8 - H.323 Architecture

NOTE -- Solid Line Indicates Signaling Relationship.

A.1.3 H.323 Signaling Protocols

H.323 allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of call setup and negotiating procedures and basic data-transport methods -- the most common in VoIP applications being H.225.0, H.235, H.245, H.248, and the Q.900 signaling series. In addition, for VoIP communications H.323 specifies a group of audio codecs -- the G.700 series. The following is an overview of these major protocols.

- **H.225** describes standards for Call Signaling Protocols (CSPs) and Media Stream Packetization. H.225/Q.931 call signaling is used to initiate connections between H.323 endpoints, over which the real-time data can be transported. H.225 messages are in binary ASN.1 PER (Packed Encoding Rules) format. The signaling channel is opened between an endpoint-gateway, a gateway-gateway, or gateway-gatekeeper prior to the establishment of any other channels. Although the H.225.0 signaling channel may be implemented on top of UDP, all entities must support signaling over TCP port 1720. H.225 also defines messages used for endpoint-gatekeeper and gatekeeper-gatekeeper communication -- this part of H.225 is known as "RAS" (Registration, Admission, Status), and, unlike CSPs, runs over UDP.
- **Q.931** is originally a Layer 3 protocol of ISDN. A subset of this standard is used in H.323 in the primary call signaling channel. It carries PER-encoded H.225 call signaling messages as a payload.
- **H.235** recommends an assortment of messages, procedures, structures and algorithms for securing signaling, control, and multimedia communications under the H.323 architecture.
- **H.245** describes a set of call control protocols. After a connection has been set up via the call signaling procedure, H.245 messages (there are many of these) are used to resolve the call media type, to exchange terminal capabilities, and to establish the media flow before the call can be established. H.245 messages also manage call parameters after call establishment. H.245 messages are encoded in ASN.1 PER syntax. The messages carried include notification of terminal capabilities, and commands to open and close logical channels. The H.245 control channel is permanently open, unlike the media channels.
- **H.248** is the international standard for media gateway control. H.248 addresses the relationship between the Media Gateway (MG), which converts circuit-switched voice to packet-based voice (the MG handles the media), and the Media Gateway Controller (or softswitch), which dictates the service logic of that traffic -- that is, it manages call signaling and other non-media-related functions
- **Other protocols** are also defined within the H.323 standard. These include, but are not limited to: the H.260 series, the H.450-series, the H.460 series, the T.120 series, T.140, and the H.320 series.

Abstract Syntax Notation One (ASN.1) is commonly misunderstood. It is not a programming language, but it is a flexible notation that allows one to define a variety of data types. ASN.1 encoding rules are sets of rules used to transform data specified in the ASN.1 language into a standard format that can be decoded on any system that has a decoder based on the same set of rules. The H.323 protocol family is compiled into a wire-line protocol using Packed Encoding Rules (PER). PER is a compact binary encoding that is used on limited-bandwidth networks. It is designed to optimize the use of bandwidth, but the tradeoff is complexity: decoding PER PDUs (protocol data units) has lead to problems due to a number of factors including issues with octet alignment, integer precision, and unconstrained character strings.

A.2 H.323 Messaging sequence

H.323 signaling exchanges typically are routed via the gatekeeper or directly between the participants as chosen by the gatekeeper. Media exchanges are normally directly routed between the participants of a call.

Normally, the first message components used to initiate an H.323 exchange are Gatekeeper Discovery packets. Establishing a call between two endpoints requires two TCP connections between the endpoints: one for call setup (Q.931/H.225 messages), and one for capabilities exchange and call control (H.245 messages). First, an endpoint initiates an H.225/Q931 exchange on a TCP well-known port (TCP 1720) with another endpoint. Successful completion of the "call" results in an end-to-end reliable channel supporting H.245 messaging.

H.245 negotiations usually take place on a separate channel from the one used for H.225 exchanges, but newer applications support tunneling of H.245 PDUs in the H.225 signaling channel. There is no well-known port for H.245. The H.245 transport address is always passed in a call-signaling message. The media channels (those used to transport voice and video) are similarly dynamically-allocated. As an aside, this use of dynamic ports makes it difficult to implement security policy on firewalls, NAT, and traffic shaping.

H.323 data communications utilizes both TCP and UDP. TCP ensures reliable transport for control signals and data, because these signals must be received in proper order and cannot be lost. UDP is used for audio and video streams, which are time-sensitive but are not as sensitive to an occasional dropped packet. Consequently, the H.225 call signaling channel and the H.245 control channel typically run over TCP, while audio, video, and RAS channel exchanges rely on UDP for transport.

A.3 H Series Video Codecs

H series video codec standards, such as H.263 (and H.263s successor H.264), support video compression (coding) for video-conferencing and video-telephony applications. A number of video coding standards exist, each of which is designed for a particular type of application -- for example, JPEG for still images, MPEG2 for digital television and H.261 for ISDN video conferencing. H.263 and H.264 are aimed particularly at video coding for low bit rates (typically 20-30kbps). The H.263 and H.264 standards specify the requirements for video encoders and decoders, and the format and content of the encoded stream.

H.263 and H.264 are part of the SERIES H Audiovisual and Multimedia Systems specifications. H.263 utilizes ITU-T Recommendation H.245 Control protocol as does H.323. As such, the signaling and control channel security requirements are identical to those specified for H.323.

A.4 H.235 Security Profiles

H.235 describes various security profiles for H.323 networks. H.235 allows many different options including the use of TLS and IPsec for security. Profiles are defined in H.235 as follows:

- **H.235.1** – Shared secrets and keyed hashes.
- **H.235.2** – Digital signatures on every message.
- **H.235.3** – Digital signatures and shared secret establishment on first handshake, afterwards keyed hash.

A.5 H.235.1 – Baseline Security Profile

The Baseline Security Profile relies on symmetric techniques. Shared secrets are used to provide authentication and/or message integrity. The supported scenarios for this profile are endpoint to gatekeeper, gatekeeper to gatekeeper, and endpoint to endpoint. For the profile, the gatekeeper-routed signaling (hop-by-hop security) is favored. Using it for the direct call model is generally possible but limited, due to the fact that a shared secret has to be established between the parties that want to communicate before the actual communication takes place. This might be possible in smaller environments but will lead to huge administrative effort in larger environments.

A.6 H.235.2 – Signature Security Profile

The Signature Security Profile relies on asymmetric techniques. Certificates and digital signatures are used to provide authentication and message integrity. The signature security profile mandates the gatekeeper-routed model. Other call models are for further study. Since this profile relies on a public key infrastructure rather than on pre-established shared secrets it scales for larger, global environments. In addition to the Baseline Security Profile, it provides non-repudiation.

A.7 H.235.3 – Hybrid Security Profile

The Hybrid Security Profile relies on asymmetric and symmetric techniques. It can be seen as a combination of the Baseline and the Signature Security Profile. Certificates and digital signatures are used to provide authentication and message integrity (as in the Signature Security Profile) for the first handshake between two entities. During this handshake a shared secret is established that will be used further on in the same way described for the Baseline Security Profile. The hybrid security profile mandates the gatekeeper-routed model. Other call models are open for further study. Since this profile relies on a public key infrastructure rather than on pre-established shared secrets it scales for larger, global environments.

Other potentially applicable H.235-based security procedures for NNI security are specified in ITU-T Recommendations H.235.4, H.235.5, H.235.6, H.235.7, H.235.8 and H.235.9.

Annex B
(informative)

B INFORMATIVE REFERENCES

ATIS-0300276.2008, *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*.[1]

ITU-T H.225.0, *Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications System*s.[2]

ITU-T Recommendation H.248.1, *Gateway Control Protocol Version 2*. (Signaling standard developed jointly by the ITU-T and IETF and published as H.248 and RFC3525 respectively).[2]

ITU-T H.245, *Control Protocol for Multimedia Communications*.[2]

ITU-T H.460.22, *Negotiation of Security Protocols to Protect H.225.0 Call Signaling Message*.[2]

IETF RFC 2402, *IP Authentication Header*.[3]

IETF RFC 2406, *IP Encapsulating Security Payload (ESP)*.[3]

IETF RFC 2409, *The Internet Key Exchange (IKE)*.[3]

IETF RFC 2960, *Stream Control Transmission Protocol*.[3]

IETF RFC 3309, *Stream Control Transmission Protocol (SCTP) Checksum Change*.[3]

IETF RFC 3554, *On the Use of Stream Control Transmission Protocol (SCTP) with IPsec*.[3]