ATIS-1000025.2013

USER TO NETWORK INTERFACE (UNI) STANDARD FOR SIGNALING AND CONTROL SECURITY REQUIREMENTS FOR EVOLVING VOP/MULTIMEDIA NETWORKS

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-1000025.2013, *User to Network Interface (UNI) Standard for Signaling and Control Security Requirements for Evolving VoP/Multimedia Networks*

Is an American National Standard developed by the **Security (SEC) Subcommittee** under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

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

ATIS-1000025.2013

(Revision of ATIS-1000025.2008)

American National Standard for Telecommunications

User to Network Interface (UNI) Standard for Signaling and Control Security Requirements for Evolving VoP/Multimedia Networks

Alliance for Telecommunications Industry Solutions

Approved May 6, 2013

American National Standards Institute, Inc.

Abstract

This standard 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 standards as shown in Figure 1. This standard provides security requirements for VoP and Multimedia signaling and control services that cross the User to Network Interfaces (UNI).

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 Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

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

M. Dolly, PTSC Chair (AT&T)

V. Shaikh, PTSC Vice-Chair (Applied Communications Sciences)

W. Downum, PTSC SEC Chair (Ericsson)

Z. Zeltsan, PTSC SEC Vice-Chair (Alcatel-Lucent)

W. Downum, Technical Editor (Ericsson)

C. Underkoffler, ATIS Chief Editor

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

Table of Contents

Table of Figures

American National Standard on –

User to Network Interface (UNI) Standard for Signaling and Control Security Requirements 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 user to network interface (UNI) 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 an overlay network that provides point to point facilities segregated from those 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. With the evolving telecommunications networks, however, signaling and control traffic is often combined with end-user traffic on the same IP transport facility. 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 and can be affected by user plane traffic.

This standard 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 standards as shown in Figure 1. This standard provides security requirements for VoP and Multimedia signaling and control services that cross the User to Network Interfaces (UNI).

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

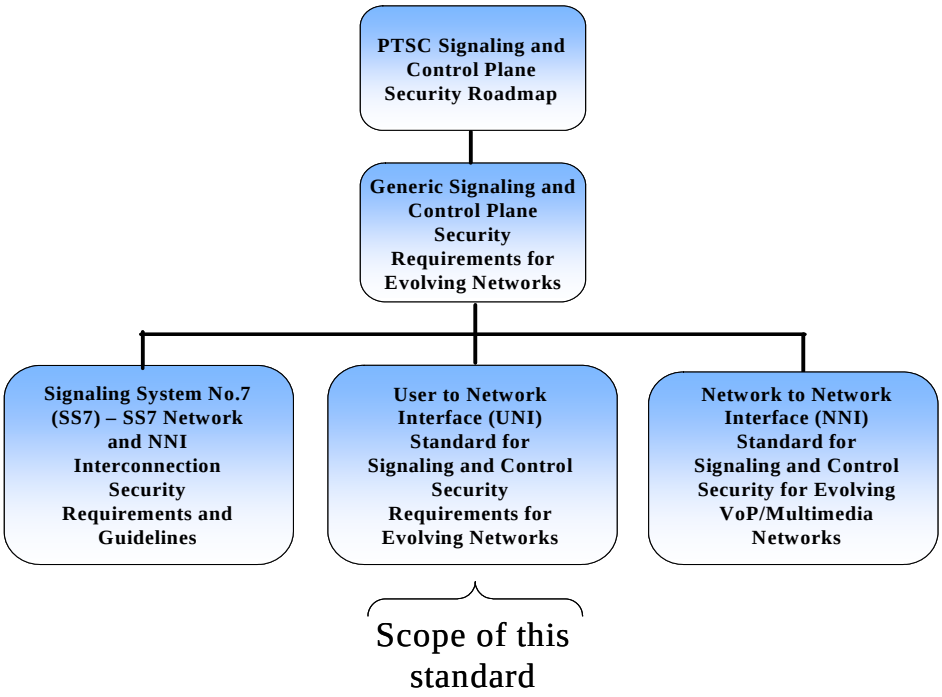

Figure 1: Signaling and Control Plane Security Standards

2 Scope, Purpose, & Application

2.1 Scope

The scope of this standard is to define the User to Network Interface Signaling Security requirements. The standard addresses security requirements for voice over packet and multimedia security, including:

- SIP Signaling. [RFC 3261]
- H.323: Packet-based multimedia communications systems. [ITU-T H.323]
    - H.225: Call signaling protocols and media stream packetization for packet-based multimedia communication systems. H.225 includes the RAS: Registration, Admission, Status protocol. [ITU-T H.225.0]
    - H.245: Control protocol for multimedia communication. [ITU-T H.245]

This standard 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), Asynchronous Transfer Mode (ATM), and Internet Protocol (IP) transport mechanisms. The security requirements given in this standard apply to service provider networks and may also be applicable to individual company single location and corporate enterprise multi-location networks.

This standard takes the following into consideration:

- Network operators may not always have complete control with respect to which terminal the user uses to connect to the network, and thereby its capabilities with respect to security may not be known.
- The user may use a separate access provider network.
- There may be differences in security depending on the access technology used to connect the user to the network.

This standard concerns the user to network interface (UNI) of evolving networks. For this standard, the UNI is defined as the interface between a VoP/multimedia end user device or terminal and the network that provides service to the device or terminal.

Management and Bearer Plane Security issues are outside the scope of this standard.

As illustrated in Figure 1, this standard is part of a series of related signaling and control plane security standards.

2.2 Purpose

The purpose of this standard is to specify baseline security requirements for signaling and control plane functions of evolving telecommunications networks that use H.323 and SIP protocols. The intent of this standard is to provide signaling and control plane security requirements which may be used by carriers and vendors to allow secure interoperability of multi-vendor end-user devices and networks. This standard provides a minimal set of security requirements as well as general security guidance.

2.3 Related Standards

The related signaling and control plane security standards in this suite include:

- ATIS-1000024, *US Standard for Signaling Security – Security Roadmap*.
- ATIS-1000007.2006 (R2011), *Generic Signaling and Control Plane Security Requirements for Evolving Networks*.
- ATIS-1000019.2007 (R2012), *Network-to-Network Interface (NNI) Standard for Signaling and Control Security Requirements for Evolving VoP and Multimedia Networks*. .
- ATIS-1000012.2006 (R2011), *Signaling System No.7 (SS7) – SS7 Network and NNI Interconnection Security Requirements and Guidelines*.

3 Normative 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.

[Generic] ATIS-1000007.2006 (R2011), *Generic Signaling and Control Plane Security Requirements for Evolving Networks*.[1]

[SIP NNI] ATIS-1000019.2007 (R2012), *Network-to-Network Interface (NNI) Standard for Signaling and Control Security Requirements for Evolving VoP and Multimedia Networks*.[2]

[ATIS-0100014] ATIS-0100014, *Information and Communications Security for NGN Converged Services IP Networks and Infrastructure*.[3]

[ATIS-1000012] ATIS-1000012.2006 (R2011), *Signaling System No.7 (SS7) – SS7 Network and NNI Interconnection Security Requirements and Guidelines*.[4]

---

[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/product.aspx?id=25488 >.

[2] 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/product.aspx?id=26098 >.

[3] 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/product.aspx?id=25562 >.

[ATIS-1000024] ATIS-1000024, *US Standard for Signaling Security – Security Roadmap*.[5]

[RFC 3261] *SIP: Session Initiation Protocol, Internet Engineering Task Force*, June 2002.
<http://www.ietf.org/rfc/rfc3261.txt?number=3261>.
As updated by [RFC 3265], [RFC 3853], [RFC 4320], [RFC 4916], [RFC 5393], [RFC 5621], [RFC 5626], [RFC 5630], [RFC 5922], [RFC 5954], [RFC 6026], [RFC 6141], [RFC 6665].

[RFC 3265] *Session Initiation Protocol (SIP)-Specific Event Notification*, July 2002.
< http://www.ietf.org/rfc/rfc3265.txt?number=3265 >.

[RFC 3853] *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)*, July 2004.
< http://www.ietf.org/rfc/rfc3853.txt?number=3853 >.

[RFC 4320] *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction*, January 2006.
< http://www.ietf.org/rfc/rfc4320.txt?number=4320 >.

[RFC 4916] *Connected Identity in the Session Initiation Protocol (SIP)*, June 2007.
< http://www.ietf.org/rfc/rfc4916.txt?number=4916 >.

[RFC 5393] *Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies*, December 2008.
< http://www.ietf.org/rfc/rfc5393.txt?number=5393 >.

[RFC 5621] *Message Body Handling in the Session Initiation Protocol (SIP)*, September 2009.
< http://www.ietf.org/rfc/rfc5621.txt?number=5621 >.

[RFC 5626] *Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)*, October 2009.
< http://www.ietf.org/rfc/rfc5626.txt?number=5626 >.

[RFC 5630] *The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)*, October 2009.
< http://www.ietf.org/rfc/rfc5630.txt?number=5630 >.

[RFC 5922] *Domain Certificates in the Session Initiation Protocol (SIP)*, June 2010.
< http://www.ietf.org/rfc/rfc5922.txt?number=5922 >.

[RFC 5954] *Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261*, August 2010.
< http://www.ietf.org/rfc/rfc5954.txt?number=5954 >.

[RFC 6026] *Correct Transaction Handling for 2xx Responses to Session Initiation Protocol (SIP) INVITE Requests*, September 2010.
< http://www.ietf.org/rfc/rfc6026.txt?number=6026 >.

[RFC 6141] *Re-INVITE and Target-Refresh Request Handling in the Session Initiation Protocol (SIP)*, March 2011.
< http://www.ietf.org/rfc/rfc6141.txt?number=6141 >.

---

[4] 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/product.aspx?id=25487 >.

[5] 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/product.aspx?id=25008 >.

[RFC 6665] *SIP-Specific Event Notification*, July 2012.
< http://www.ietf.org/rfc/rfc6665.txt?number=6665 >.

[ITU-T X.805] ITU-T SG17 Draft Recommendation X.805, *Security Architecture for Systems Providing End-to-End Communications*, (10/03).[6]

[ITU-T H.323] ITU-T Recommendation H.323 v7, *Packet-based multimedia communications systems*, (12/2009).[6]

[ITU-T H.235] ITU-T Recommendation H.235.x, *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*, (2005).[6]

[RFC 3323] *A Privacy Mechanism for the Session Initiation Protocol (SIP)*, Internet Engineering Task Force, November 2002.
< http://www.ietf.org/rfc/rfc3323.txt?number=3323 >

[RFC 4301] *Security Architecture for the Internet Protocol*, Internet Engineering Task Force, December 2005.
< http://www.ietf.org/rfc/rfc4301.txt?number=4301 >
As updated by [RFC 6040].

[RFC 6040] *Tunnelling of Explicit Congestion Notification*, November 2010.
< http://www.ietf.org/rfc/rfc6040.txt?number=6040 >

[RFC 5246] *The Transport Layer Security (TLS) Protocol Version 1*.
< http://www.ietf.org/rfc/rfc5246.txt?number=5246 >
As updated by [RFC 5746], [RFC 5878], [RFC 6176].

[RFC 5746] *Transport Layer Security (TLS) Renegotiation Indication Extension*, February 2010.
< http://www.ietf.org/rfc/rfc5746.txt?number=5746 >

[RFC 5878] *Transport Layer Security (TLS) Authorization Extensions*, May 2010.
< http://www.ietf.org/rfc/rfc5878.txt?number=5878 >

[RFC 6176] *Prohibiting Secure Sockets Layer (SSL) Version 2.0*, March 2011.
< http://www.ietf.org/rfc/rfc6176.txt?number=6176 >

[ITU-T H.323] ITU-T Recommendation H.323, *Packet Based Multimedia Communications Systems*, , July 2006.[6]

4 Definitions

Common definitions used in this specification are given in ATIS-1000007.2006 (R2011), *Generic Signaling and Control Plane Security Requirements for Evolving Networks* Standard [Generic].

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

5 Abbreviations & Acronyms

Common abbreviations used in this specification are given in ATIS-1000007.2006. [Generic].

In addition this standard uses the following abbreviations:

ACL	Access Control List
NAT	Network Address Translation
RAS	Registration, Admission, Status
CRV	Call Reference Value
UA	User Agent

6 Reference Signaling & Control Network Model

As discussed in ATIS-1000007.2006 (R2011), this standard uses the framework and architecture proposed in ITU-T Recommendation X.805. The Security Architectural Model presented in ITU-T Recommendation 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).
3. Security Dimensions (Access Control, Authentication, Non-repudiation, Data Confidentiality, Communications, Data Integrity, Availability, and Privacy).

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.

Figure 3 illustrates SIP signaling interfaces:

- I1 is the interface between two SIP User Agents (UAs).
- I2 is the interface between a SIP UA and SIP proxy.
- I3 is the interface between two SIP proxies.

This standard addresses interface I2 only.

NOTE: The SIP Element may be a SIP Registrar, SIP Proxy, Back to Back UA (B2BUA), or a UA.

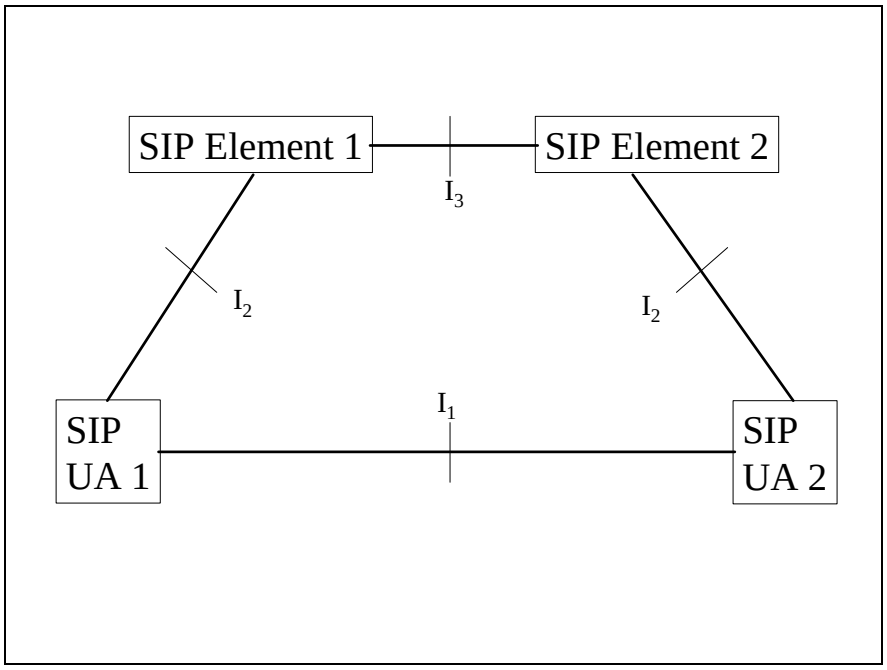

Figure 2: SIP Reference Model

7 UNI Signaling Security Requirements

7.1 SIP

Session Initiation Protocol (SIP) is a control protocol used to support multimedia services over packet networks including services such as 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 and the SIP family of RFCs.

7.1.1 General Requirements

<REQ-SEC-UNI-00100>

Mechanisms for authentication shall be provided for all Connection Establishment and Signaling/Call Control exchanges between user agents (UAs) and SIP Proxy and other SIP Network Elements across the UNI.

<End of REQ-SEC-UNI-00100>

<CR-SEC-UNI-00200>

If data integrity is provided across the UNI, then the mechanism shall be based on Ipsec or TLS. The mechanism shall be provided for all Connection Establishment and Signaling/Call Control exchanges between user agents (Uas) and SIP Proxy and other SIP Network Elements across the UNI.

<End of CR-SEC-UNI-00200>

<CR-SEC-UNI-00300>

If data confidentiality is provided across the UNI, then the mechanism shall be based on Ipsec or TLS. The mechanism shall be provided for all Connection Establishment and Signaling/Call Control exchanges between user agents (Uas) and SIP Proxy and other SIP Network Elements across the UNI.

<End of CR-SEC-UNI-00300>

<CR-SEC-UNI-00400>

If NAT functionality is implemented across the UNI and Ipsec is used, then Ipsec mechanisms shall work in the presence of this NAT functionality.

<End of CR-SEC-UNI-00400>

NOTE: Refer to ATIS-1000007.2006 (R2011) for IPsec and TLS Protocol Requirements [Generic].

Different access technologies used to connect the user to the network may have different inherent security levels. For example, a DSL line from a service provider connecting a single residential SIP user to a proxy server within the service provider's domain may have a similar level of security for the user to network connection as a traditional phone connection. However, a service provider connecting a SIP user via a wireless access technology without air interface security enabled may be less secure than a traditional phone connection. As such, it is strongly recommended that all end user terminals connecting to networks via any access technology use IPsec or TLS security mechanisms to secure the signaling channels as recommended in CR-SEC-UNI-00200 and CR-SEC-UNI-00300. However, as it may be difficult to guarantee all end users have end user devices with IPsec or TLS capabilities, and some service providers may wish to allow such end users to connect to their networks, the use of IPsec or TLS is left as a conditional requirement whereby the choice is left to individual service provider policy.

7.1.2 Access Control Security Dimension

<REQ-SEC-UNI-00500>

Some means on the network side of the UNI shall be used to restrict/grant access to specific UAs on the customer side of the UNI.

<End of REQ-SEC-UNI-00500>

NOTE: Access Control Lists (ACLs) may be used to provide SIP Authorization/Access Control; however, when using DHCP to obtain IP addresses, ACLs should not be used due to changing IP addresses.

<REQ-SEC-UNI-00600>

Means to detect and log unauthorized access attempts to the network at the UNI shall be supported.

<End of REQ-SEC-UNI-00600>

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.

7.1.3 Authentication Security Dimension

<REQ-SEC-UNI-00700>

The terminal equipment shall be authenticated by the network across the UNI before call connection messages are exchanged.

<End of REQ-SEC-UNI-00700>

NOTE: If IPsec or TLS protocols are used, authentication mechanisms within these protocols may be used to provide authentication of the terminal equipment.

NOTE: Authentication of the network by the terminal equipment is not currently a requirement.

<REQ-SEC-UNI-00800>

Authentication mechanisms across the UNI shall make use of at least one of the following:

1. **Non-clear-text passwords.**

2. **Digital authenticators.**
3. **Digital signatures.**

<End of REQ-SEC-UNI-00800>

<REQ-SEC-UNI-00900>

Signaling traffic from the terminal shall include an element in the signaling data or message that enables the receiving network to verify the authenticity of the message.

<End of REQ-SEC-UNI-00900>

NOTE: If IPsec or TLS protocols are used, authentication mechanisms within these protocols may be used to provide data or message authenticity across the UNI.

<REQ-SEC-UNI-01000>

Each SIP User Agent (for example, those found in access Endpoints such as terminals, Gateways, IP Phones, or Soft Clients) shall register with the Network Provider VoP registration functional entity, as per RFC3261.

<End of REQ-SEC-UNI-01000>

<REQ-SEC-UNI-01100>

SIP registration is required for service to be authorized. Each SIP Endpoint shall register with the Network Provider VoP registration functional entity, as per RFC 3261.

<End of REQ-SEC-UNI-01100>

NOTE: Access will be denied to non-registered end points.

<REQ-SEC-UNI-01200>

Each called and calling User Agent Endpoint shall be identified by a unique URI.

<End of REQ-SEC-UNI-01200>

7.1.4 Non-Repudiation Security Dimension

<REQ-SEC-UNI-01300>

The capability for authorized access attempts at the UNI to be logged and reported to a management system shall be provided.

<End of REQ-SEC-UNI-01300>

<REQ-SEC-UNI-01400>

The capability for unauthorized access attempts at the UNI to be logged and reported to a management system shall be provided.

<End of REQ-SEC-UNI-01400>

NOTE: Access attempts which fail authentication are defined as unauthorized access attempts.

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-UNI-01500>

The capability to identify unauthorized SIP signaling packets at the UNI and to log and report these to a management system shall be provided

<End of REQ-SEC-UNI-01500>

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.

7.1.5 Data Confidentiality Security Dimension

<CR-SEC-UNI-01600>

Confidentiality functions within the security mechanism (see requirement CR-SEC-UNI-00300) across the UNI may 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.

<End of CR-SEC-UNI-01600>

7.1.6 Communication Security Dimension

No additional requirements to address the Communication Security dimension have been identified beyond those specified in the Authentication Security (section 7.1.3) and Data Integrity (section 7.1.7) dimensions in this standard.

7.1.7 Data Integrity Security Dimension

<CR-SEC-UNI-01700>

Data integrity functions within the security mechanism (see requirement CR-SEC-UNI-00200) across the UNI may be supported to provide data integrity of signaling data (e.g., phone numbers, network addresses, and call accounting information) to protect the signaling data from unauthorized modification.

<End of CR-SEC-UNI-01700>

7.1.8 Availability Security Dimension

As a best practice, network entities communicating across the UNI should implement mechanisms to detect and mitigate IP DoS attacks. Both application layer flooding attacks, network layer flooding attacks, and malformed packet attacks should be mitigated by the DoS protection mechanisms.

Attacks directly against SIP are not necessarily required to break or disable the service entirely. Where SIP relies upon ancillary services (such as DNS, RSVP, SNMP, and others), attacks against these underlying infrastructure services should also be mitigated by security and DoS protection mechanisms.

7.1.9 Privacy Security Dimension

<REQ-SEC-UNI-01800>

User Agents and Proxy network elements shall be able to support processing and delivery of signaling packets over the UNI which have the following data obscured, as per [RFC3323]:

- **Identity of the communication party.**
- **Exact location of the communication party.**

<End of REQ-SEC-UNI-01800>

NOTE: Endpoints and communication parties can obscure some personal data in signaling packets or use network service, as described in [RFC3323].

NOTE: REQ-SEC-UNI-01800 is in addition to other security requirements specified in this standard (e.g., encryption), because some signaling links may be outside a service provider's span of control.

NOTE: Compliance with this requirement should not prevent a Proxy network element from applying a local policy that would prevent Endpoints from being anonymous.

NOTE: Calling party presentation restriction (privacy) needs to be honored by the network and not relayed to the Endpoint over the UNI.

<REQ-SEC-UNI-01900>

Access to information – such as alias translation database information, phone numbers, network addresses, and call accounting information – shall be restricted by an access control mechanism.

<End of REQ-SEC-UNI-01900>

7.2 H.323

H.323 (Packet-based multimedia communications systems) is the ITU Recommendation for the setup and control of packet telephony and multimedia. [ITU-T H.323]

The following requirements address the UNI 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*.
    - o 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*.

H.323 network architectural models used in this document are shown in Figure 3 and Figure 4, with the network side of the UNI on the left of each figure. Figure 3 shows a solution where the Gatekeeper is within the Carrier Network. Figure 4 shows a solution where a Gatekeeper is provided on the user side of the UNI. See [ITU-T H.323] for more information on the H.323 architecture, including H.323 definitions. See also ITU-T Recommendation H.235, *H.323 security - Framework for security in H-series (H.323 and other H.245-based) multimedia systems* [ITU-T H.235].

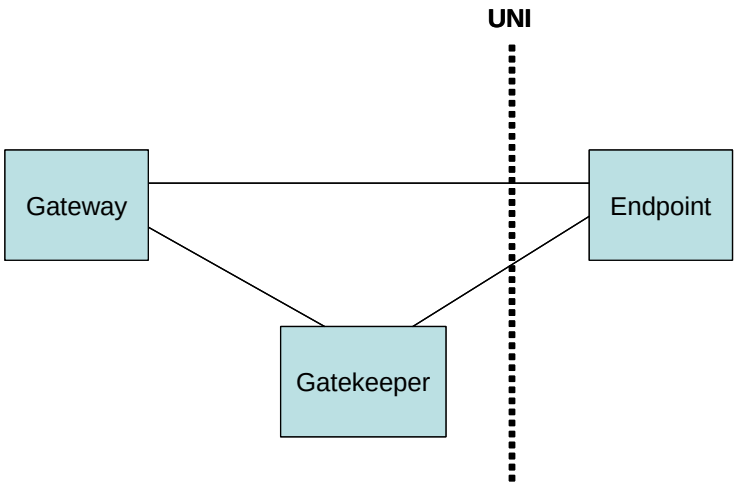

Figure 3: H.323 Architectural Model #1

NOTE: Solid Line Indicates Signaling Relationship.

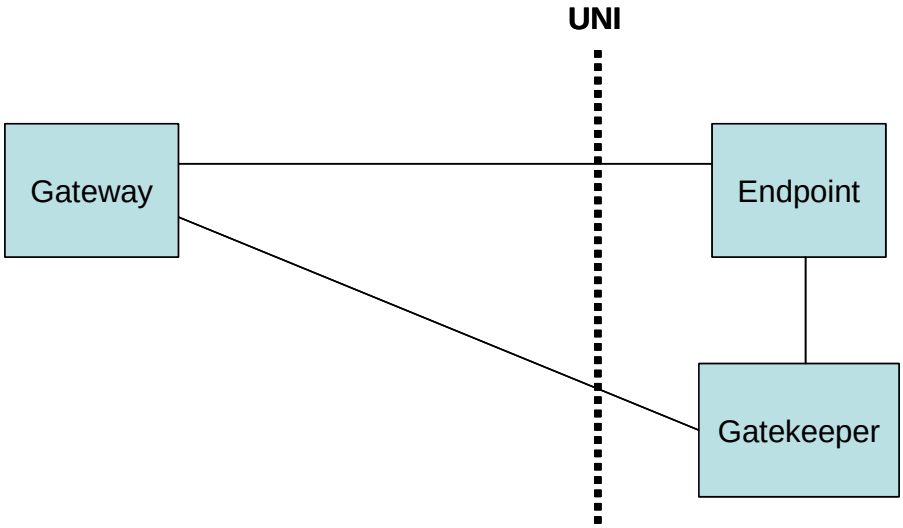

Figure 4: H.323 Architectural Model #2

NOTE: Solid Line Indicates Signaling Relationship.

NOTE: There may be a Session Border Controller at the UNI.

7.2.1 General Requirements

<REQ-SEC-UNI-02000>

Mechanisms for authentication shall be provided for all Connection Establishment and Signaling/Call Control exchanges between Endpoints and Gatekeepers, Endpoints and Gateways, and Gateways and Gatekeepers.

<End of REQ-SEC-UNI-02000>

<CR-SEC-UNI-02100>

If data integrity is provided across the UNI, then the mechanism shall be based on IPsec or TLS. The mechanism shall be provided for all Connection Establishment and Signaling/Call Control exchanges between Endpoints and Gatekeepers, Gateways and other H.323 Network Elements across the UNI.

<End of CR-SEC-UNI-02100>

<CR-SEC-UNI-02200>

If data confidentiality is provided across the UNI, then the mechanism shall be based on IPsec or TLS. The mechanism shall be provided for all Connection Establishment and Signaling/Call Control exchanges between Endpoints and Gatekeepers, Endpoints and Gateways, and Gateways and Gatekeepers.

<End of CR-SEC-UNI-02200>

<CR-SEC-UNI-02300>

If NAT functionality is implemented across the UNI and IPsec is used, then IPsec mechanisms shall work in the presence of this NAT functionality.

<End of CR-SEC-UNI-02300>

NOTE: Refer to ATIS-1000007.2006 (R2011) for IPsec and TLS Protocol Requirements [Generic].

7.2.2 Access Control Security Dimension

<REQ-SEC-UNI-02400>

Some means shall be used to restrict/grant access to specific Endpoints, on the customer side of the UNI, across the UNI interface.

<End of REQ-SEC-UNI-02400>

NOTE: Access Control Lists (ACLs) may be used to provide H.323 Authorization/Access Control; however, when using DHCP to obtain IP addresses, ACLs should not be used due to changing IP addresses.

<REQ-SEC-UNI-02500>

Means to detect and log unauthorized access attempts to the network at the UNI shall be supported.

<End of REQ-SEC-UNI-02500>

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.

7.2.3 Authentication

<REQ-SEC-UNI-02600>

Endpoints shall be authenticated by the network across the UNI before call connection messages are exchanged.

<End of REQ-SEC-UNI-02600>

NOTE: If IPsec or TLS protocols are used, authentication mechanisms within these protocols may be used to provide authentication of the Endpoints.

<REQ-SEC-UNI-02700>

Authentication mechanisms across the UNI shall make use of at least one of the following:

1. **Non-clear-text passwords.**
2. **Digital authenticators.**
3. **Digital signatures.**

<End of REQ-SEC-UNI-02700>

<REQ-SEC-UNI-02800>

Signaling traffic from the Endpoints and Gatekeeper (if on the user side of the UNI) shall include an element in the signaling data or message that enables the receiving network to verify the authenticity of the message.

<End of REQ-SEC-UNI-02800>

NOTE: If IPsec or TLS protocols are used, authentication mechanisms within these protocols may be used to provide data or message authenticity across the UNI.

<REQ-SEC-UNI-02900>

Each Endpoint – e.g., terminal, IP Phone, or Soft Client – shall register with the H.323 Gatekeeper functional entity.

<End of REQ-SEC-UNI-02900>

<REQ-SEC-UNI-03000>

Each Gatekeeper on the user side of the UNI shall register with the Network Provider.

<End of REQ-SEC-UNI-03000>

<REQ-SEC-UNI-03100>

Each Endpoint registered with the appropriate Gatekeeper shall have a unique H.323 alias.

<End of REQ-SEC-UNI-03100>

<REQ-SEC-UNI-03200>

Each Endpoint registered with the appropriate Gatekeeper shall have a unique Call Reference Value (CRV).

<End of REQ-SEC-UNI-03200>

<REQ- SEC-UNI-03300>

The CRV and the H.323 alias shall be associated to identify each Endpoint.

<End of REQ- SEC-UNI-03300>

7.2.4 Non-repudiation Security Dimension

<REQ-SEC-UNI-03400>

The capability for authorized access attempts at the UNI to be logged and reported to a management system shall be provided.

<End of REQ-SEC-UNI-03400>

<REQ-SEC-UNI-03500>

The capability for unauthorized access attempts at the UNI to be logged and reported to a management system shall be provided.

<End of REQ-SEC-UNI-03500>

NOTE: Access attempts which fail authentication are defined as unauthorized access attempts.

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-UNI-03600>

The capability to identify unauthorized H.323 signaling packets at the UNI and to log and report these to a management system shall be provided

<End of REQ-SEC-UNI-03600>

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.

7.2.5 Data Confidentiality Security Dimension

<CR-SEC-UNI-03700>

Confidentiality functions within the security mechanism (see requirement CR-SEC-UNI-02200) across the UNI may 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.

<End of CR-SEC-UNI-03700>

7.2.6 Communication Security Dimension

No additional requirements to address the Communication Security dimension have been identified beyond those specified in the Authentication Security (section 7.2.3) and Data Integrity (section 7.2.7) dimensions in this standard.

7.2.7 Data Integrity Security Dimension

<CR-SEC-UNI-03800>

Data integrity functions within the security mechanism (see requirement CR-SEC-UNI-02100) across the UNI may be supported to provide data integrity of signaling data (e.g., phone numbers, network addresses, and call accounting information) to protect the signaling data from unauthorized modification.

<End of CR-SEC-UNI-03800>

7.2.8 Availability Security Dimension

As a best practice, network entities communicating across the UNI should implement mechanisms to detect and mitigate H.323 DoS attacks. Both application layer flooding attacks, network layer flooding attacks, and malformed packet attacks should be mitigated by the DoS protection mechanisms.

Attacks directly against H.323 are not necessarily required to break or disable the service entirely. Where H.323 relies upon ancillary services (such as DNS, RSVP, SNMP, and others), attacks against these underlying infrastructure services should also be mitigated by security and DoS protection mechanisms.

7.2.9 Privacy Security Dimension

<REQ-SEC-UNI-03900>

Access to information – such as alias translation database information, phone numbers, network addresses, and call accounting information – shall be restricted by an authentication mechanism.

<End of REQ-SEC-UNI-03900>

Annex A
(informative)

A References

[ITU-T H.248] ITU-T Recommendation H.248.1 v3, *Gateway Control Protocol Version 2*, (2005).[6]
(Signaling standard developed jointly by the ITU-T and IETF and published as H.248 and RFC3525 respectively).

[ATIS-0300276] ATIS-0300276.2008, *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*.[7]

[ITU-T H.225.0] ITU-T Recommendation H.225.0 v7, *Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems,* (2009).[6]

[ITU-T H.245] ITU-T Recommendation H.245 v16, *Control Protocol for Multimedia Communications*, (2011).[6]

[ITU-T H.460.22] ITU-T Recommendation H.460.22, *Negotiation of Security Protocols to Protect H.225.0 Call Signaling Message with Corrigendum 1* (2008).[6]

[RFC 4960] *Stream Control Transmission Protocol*, September 2007.
< http://www.ietf.org/rfc/rfc4960.txt?number=4960 >
As updated by [RFC 6096], [RFC 6335].

[RFC 6096] *Stream Control Transmission Protocol (SCTP) Chunk Flags Registration*, January 2011.
< http://www.ietf.org/rfc/rfc6096.txt?number=6096 >

[RFC 6335] *Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry*, August 2011.
< http://www.ietf.org/rfc/rfc6335.txt?number=6335 >

[RFC 3554] *On the Use of Stream Control Transmission Protocol (SCTP) with IPsec*, July 2003.
< http://www.ietf.org/rfc/rfc3554.txt?number=3554 >

[RFC 5996] *Internet Key Exchange (IKE) Version 2 (IKEv2)*, September 2010.
< http://www.ietf.org/rfc/rfc5996.txt?number=5996 >
As updated by [RCF 5998].

[RCF 5998] *An Extension for EAP-Only Authentication in IKEv2*, September 2010.
< http://www.ietf.org/rfc/rfc5998.txt?number=5998 >

[RFC 4303] *IP Encapsulating Security Payload (ESP)*, December 2005.
< http://www.ietf.org/rfc/rfc4303.txt?number=4303 >

[7] 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/product.aspx?id=25578 >.

[RFC 4835] *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*, April 2007.

< http://www.ietf.org/rfc/rfc4835.txt?number=4835 >