ATIS-1000024

US STANDARD FOR SIGNALING SECURITY – SECURITY ROADMAP

TECHNICAL REPORT

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 250 companies actively formulate standards in ATIS' 18 Committees, covering issues including: IPTV, Service Oriented Networks, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, and Billing and Operational Support. In addition, numerous Incubators, Focus and Exploratory Groups address emerging industry priorities including "Green", IP Downloadable Security, Next Generation Carrier Interconnect, IPv6 and Convergence.

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). For more information, please visit < http://www.atis.org >.

ATIS-1000024, *US Standard for Signaling Security – Security Roadmap*

Is an ATIS 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-1000024

Technical Report on

US STANDARD FOR SIGNALING SECURITY – SECURITY ROADMAP

Alliance for Telecommunications Industry Solutions

Approved September 16, 2008

Abstract

This Standard provides a roadmap for the suite of signaling and control plane security standards that includes ATIS-1000007.2006, ATIS-1000019.2007, ATIS-1000012.2006, and ATIS-1000025.2008. The suite of standards under the umbrella of this roadmap provides requirements covering generic signaling and control security, network-to-network signaling and control security, user-to-network signaling and control security, and Signalling System #7 security.

FOREWORD

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.

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. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

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.

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

TABLE OF CONTENTS

TABLE OF FIGURES

US Standard for Signaling Security – Security Roadmap

0 INTRODUCTION/EXECUTIVE SUMMARY

This Technical Report provides a roadmap of the following set of signaling and control plane security standards developed by the PTSC:

1. ATIS-1000007.2006, *Generic Signaling and Control Plane Security for Evolving Networks*.
2. ATIS-1000019.2007, *Network to Network (NNI) Standard for Signaling and Control Security for Evolving VoP Multimedia Networks*.
3. ATIS-1000012.2006, *Signaling Systems No. 7 (SS7) - SS7 - Network and NNI Interconnection Security Requirements and Guidelines*.
4. ATIS-1000025.2008, *US Standard for Signaling Security – UNI Access and Signaling Standard*.

As the PTSC develops additional security standards, this document may be updated.

1 SCOPE, PURPOSE, & APPLICATION

1.1 Scope

This document provides a roadmap to the following set of security standards developed by the PTSC:

1. ATIS-1000007.2006, *Generic Signaling and Control Plane Security for Evolving Networks*.
2. ATIS-1000019.2007, *Network to Network (NNI) Standard for Signaling and Control Security for Evolving VoP Multimedia Networks*.
3. ATIS-1000012.2006, *Signaling Systems No. 7 (SS7) - SS7 - Network and NNI Interconnection Security Requirements and Guidelines*.
4. ATIS-1000025.2008, *US Standard for Signaling Security – UNI Access and Signaling Standard*.

The set of standards included in this series focuses on signaling and control plane security for evolving networks including the Next Generation Network (NGN).

1.2 Security Reference Model

In general, a telecommunications network consists of three communications planes: 1) the user plane; 2) the management plane; and 3) the control plane, as illustrated in Figure 1 and as described in ATIS-1000007.2006, *Generic Signaling and Control Plane Security for Evolving Networks* [1].

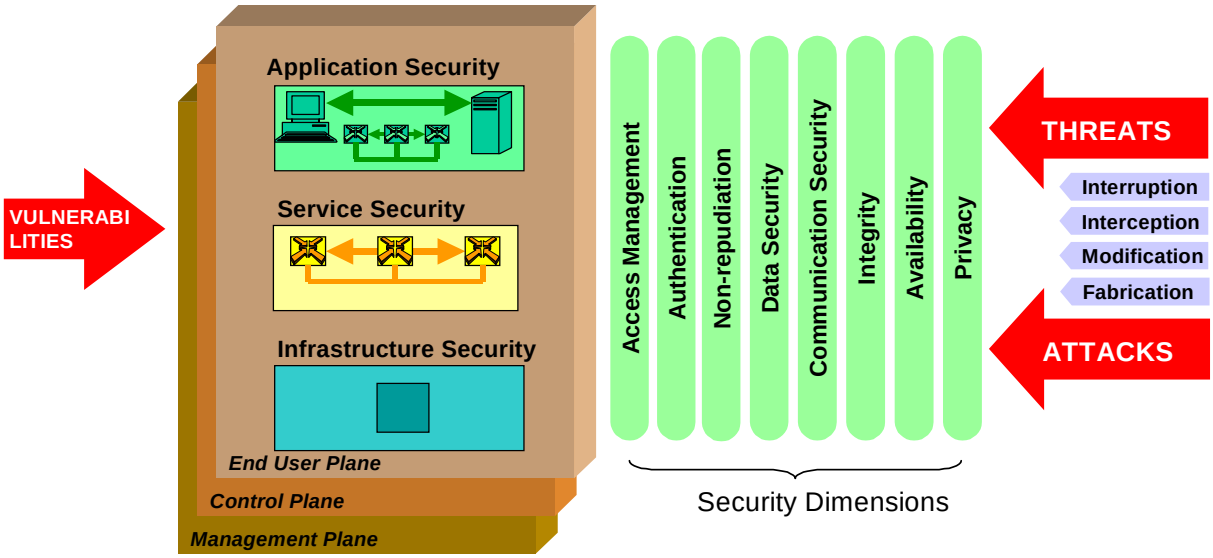

Figure 1 - Security Reference Model

The standards included in this series focus on signaling and control plane security for evolving networks including the Next Generation Network (NGN). The requirements provided in this series of standards should be treated as a minimum set of security requirements for signaling and control plane interconnection interfaces. Network providers and security administers are encouraged to take additional measures beyond those specified in these standards.

Security of the user (bearer) and management planes are not within the scope of this series of standards. It is important that security measures be supported and implemented to protect all network assets including the signaling and control, user (bearer), and management planes. These signaling and control plane security standards are intended to be used together with the other security standards and best practices specified by other ATIS committee (e.g., TMOC and PRQC) and other relevant standards development organizations (e.g., ITU-T and IETF) as applicable. It should be noted that there is the possibility of interrelationships between the various planes. Additional non-normative information on this and other security topics can be found in ATIS-0100014, *Information and Communications Security for NGN Converged Services IP Networks and Infrastructure*.

2 REFERENCES

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

[2] ATIS-1000019.2007, *Network to Network (NNI) Standard for Signaling and Control Security for Evolving VoP Multimedia Networks*.[1]

[3] ATIS-1000012.2006, *Signaling Systems No. 7 (SS7) - SS7 - Network and NNI Interconnection Security Requirements and Guidelines*.[1]

[4] ATIS-1000025.2008, *US Standard for Signaling Security – UNI Access and Signaling Standard*.[1]

3 DEFINITIONS

3.1 Security: The process of minimizing the vulnerabilities of assets and resources, or the result of this process.

3.2 Security Administrator: An authority (a person or a group of people) responsible for enforcing the security policy for a security domain.

4 ABBREVIATIONS, ACRONYMS, & SYMBOLS

ATIS	Alliance for Telecommunications Industry Solutions
ITU-T	International Telecommunications Union – Telecommunications Sector
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	IP Security
IKE	Internet Key Exchange
NRIC	Network Reliability Interoperability Council
NGN	Next Generation Network
NNI	Network to Network Interface
PRQC	Network Performance, Reliability, and Quality of Service Committee
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee
TMOC	Telecom Management and Operations Committee
TLS	Transport Layer Security
SIP	Session Initiation Protocol
SG	Signaling Gateway
SS7	Signaling Systems No. 7

[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 >

UNI	User to Network Interface
VOP	Voice Over Packet

5 General Methodology

The general methodology is to specify requirements, conditional requirements, and objectives for security of the control and signaling network. In addition, best practices and guidelines to minimize security risks are specified. Requirements, Conditional Requirements, and Objectives are testable. Recommendations and best practices that are not testable are considered as guidelines and are not numbered. Requirements, Conditional Requirements, and Objectives are numbered in increments of 100.

The Requirements, Conditional Requirements, and Objectives are highlighted in "tags" to facilitate requirements traceability. Each tag in the series of the security related documents has a label containing a unique number (e.g., <REQ-SEC-00900>) where the alpha characters (e.g., REQ-SEC) identify the type of requirement (e.g., REQ) and the document (e.g., SEC), and the numeric characters (e.g., 00900) identify the specific requirement.

The following terminology is used in this series of signaling and control plane security standards:

- **Requirement**: Feature or function that is necessary to meet the needs of a service provider. Failure to meet a requirement may cause application or service restrictions, result in improper functioning of the product, or hinder operations. A requirement is identified by the letters "**REQ-SEC**".
- **Conditional Requirement**: Feature or function that is needed by some, but not all, service providers and, as such, is left for the individual service providers to choose. A conditional requirement is identified by the letters "**CR-SEC**".
- **Objective**: Feature or function that is desirable and may be required by a service provider. An Objective represents a goal to be achieved. An Objective may be reclassified as a Requirement at some future date. An objective is identified by the letters "**O-SEC**" and includes the words it is desirable or it is an objective.

6 Signaling and Control Plane Security Roadmap

Figure 2 shows a high level organization of the signaling and control plane security standards described in this document.

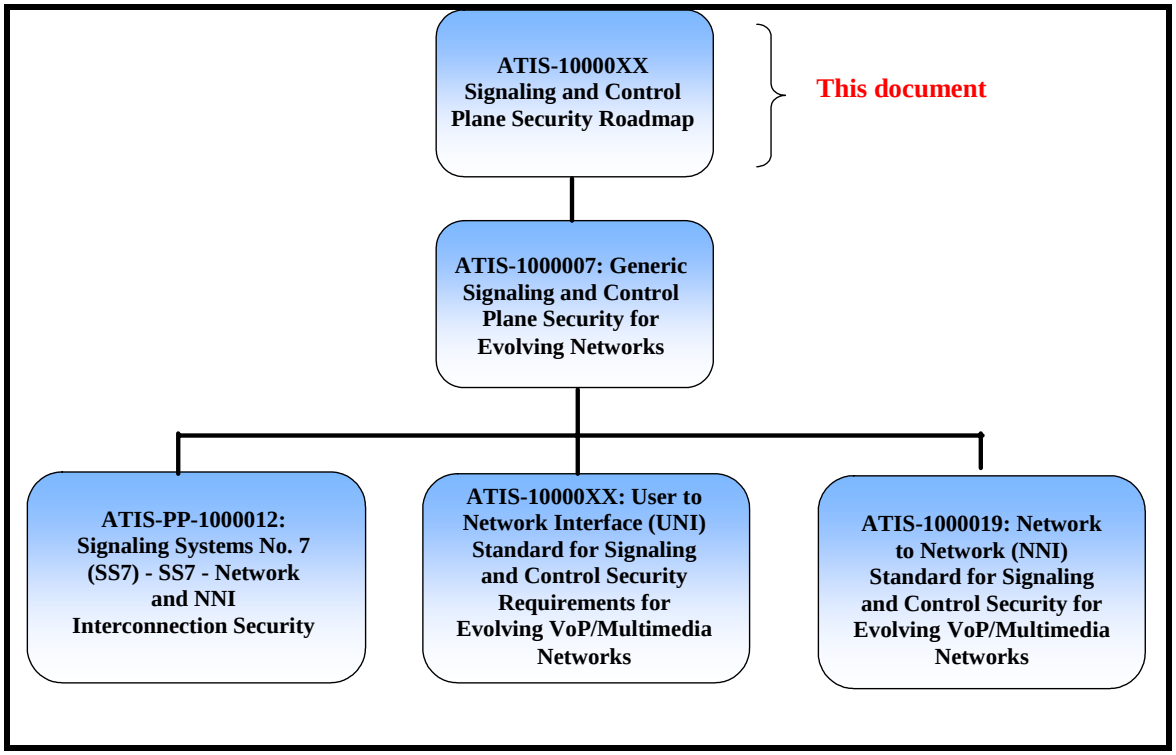

Figure 2 - Signaling and Control Plane Security Road Map

6.1 ATIS-1000007.2006, Generic Signaling and Control Plane Security for Evolving Networks

6.2.1 Scope of ATIS-1000007.2006

ATIS-1000007.2006 [1] addresses generic signaling and control plane security aspects of evolving telecommunications networks and is based on ITU-T Recommendation X.800, *Security Architecture for Open Systems Interconnection for CCITT Applications*, and Recommendation X.805, *Security Architecture for Systems Providing End-to-End Communications*. It provides generic signaling and control plane security requirements and a general security framework for evolving telecommunications networks. The concepts presented in this standard are intended for use by the other related standards which deal with specific signaling and control security areas.

6.2.2 Organization of ATIS-1000007.2006

1	INTRODUCTION, SCOPE, PURPOSE, & APPLICATION
1.1	INTRODUCTION
1.2	SCOPE
1.3	PURPOSE
1.4	RELATED DOCUMENTS
2	NORMATIVE REFERENCES
3	DEFINITIONS

8.3.11	IKE Implementation Oakley groups
8.3.12	IKE Support of Perfect Forward Secrecy
8.3.13	Random number generators for IPsec/IKE
8.4	TLS PROTOCOL REQUIREMENTS
8.4.1	TLS Encryption Algorithms
8.4.2	TLS Authentication Algorithms
8.4.3	Key Exchange Algorithms for TLS
8.4.4	Ciphersuites for TLS
8.4.5	Use of X.509 Certificates in TLS
8.4.6	TLS Authentication
8.4.7	Random number generators for TLS
A	SIGNALING & CONTROL PLANE – SECURITY BEST PRACTICES
A.1	FIREWALLS
A.2	OPERATING SYSTEM HARDENING
A.3	VULNERABILITY ASSESSMENT
A.4	INTRUSION DETECTION SYSTEMS
B	REFERENCES

6.3 ATIS-1000012.2006, Signaling Systems No. 7 (SS7) – SS7 Network and NNI Interconnection Security Requirements and Guidelines

6.3.1 Scope of ATIS-1000012.2006

ATIS-1000012.2006 [3] addresses Signaling System No.7 (SS7) Network security, and SS7 network interconnection security. This includes security of an SS7 network interconnection to a multimedia signaling and control network such as SIP network and H.323 network. Specifically, this standard provides security requirements and guidelines to minimize security risks to the SS7 network and its interconnections.

6.3.2 Organization of ATIS-1000012.2006

0	INTRODUCTION
1	SCOPE, PURPOSE, & APPLICATION
1.1	SCOPE
1.2	PURPOSE
1.3	REQUIREMENTS, OBJECTIVES AND GUIDELINES
1.4	SECURITY THREATS
2	NORMATIVE REFERENCES
3	DEFINITIONS, ACRONYMS, & ABBREVIATIONS
3.1	DEFINITIONS
3.2	ACRONYMS & ABBREVIATIONS
4	SS7 SIGNALING NETWORK SECURITY NEEDS & SECURITY ARCHITECTURE
4.1	TRADITIONAL SS7 NETWORK
4.1.1	Overview

9.2.4.3	Data Confidentiality
9.2.4.4	Privacy
9.2.4.5	Data Integrity
9.2.4.6	Availability
9.2.5	Application Layer
9.2.5.1	Data Confidentiality
9.3	TRADITIONAL SS7 NETWORK TO IP-BASED SIGNALING NETWORK INTERCONNECTION
9.3.1	SS7 and IP-based Signaling Network Interconnection Via SG Providing Transport Protocol Interworking
9.3.1.1	Reference Architecture
9.3.1.2	General Requirements and Guidelines
9.3.1.2.1	Network Design
9.3.1.2.2	Security Plan, Policy and Practices
9.3.1.2.3	Network Reliability Interoperability Council (NRIC) Best Practices
9.3.1.2.4	Documentation & Specification Safeguard
9.3.1.3	Infrastructure Layer
9.3.1.3.1	Access and Authentication Control
9.3.1.3.1.1	Network Element Access
9.3.1.3.1.2	Physical Security
9.3.1.3.2	Availability
9.3.1.3.2.1	Security Arrangements and Diversity/Redundancy
9.3.1.4	Network Services Layer
9.3.1.4.1	Access and Authentication
9.3.1.4.1.1	SS7 Message Screening
9.3.1.4.1.2	MTP Layer Screening
9.3.1.4.1.3	SCCP Layer Screening
9.3.1.4.1.4	ISUP Layer Screening
9.3.1.4.1.5	TCAP Layer Screening
9.3.1.4.1.6	Packet Screening
9.3.1.4.1.6.1	IP Layer Screening
9.3.1.4.1.6.2	Transport Layer Screening (SCTP)
9.3.1.4.1.6.3	Adaptation Layer (SUA, M3UA, M2UA and M2PA) Screening
9.3.1.4.2	Message Monitoring Capabilities
9.3.1.4.2	Data Confidentiality
9.3.1.4.3	Privacy
9.3.1.4.4	Data Integrity
9.3.1.4.5	Availability
9.3.2	SS7 Network Interconnection to IP-based Signaling Network Via SG/PSTN Gateway Node Providing Call Control Protocol Interworking.
9.3.2.1	General Requirements
9.3.2.1.1	Network Design
9.3.2.1.2	Security Plan, Policy, & Practices
9.3.2.1.3	Network Reliability Interoperability Council (NRIC) Best Practices
9.3.2.1.4	Documentation and Specification Safeguard
9.3.2.2	Infrastructure Layer
9.3.2.2.1	Access and Authentication Control
9.3.2.2.1.1	Network Element Access
9.3.2.2.1.2	Physical Security
9.3.2.2.2	Availability
9.3.2.2.2.1	Security Arrangements and Diversity/Redundancy

9.3.2.3	Network Services Layer
9.3.2.3.1	Access and Authentication
9.3.2.3.1.1	SS7 Message Screening
9.3.2.3.1.2	MTP Layer Screening
9.3.2.3.1.3	SCCP Layer Screening
9.3.2.3.1.4	ISUP Layer Screening
9.3.2.3.1.5	TCAP Layer Screening
9.3.2.3.1.6	Packet Network Screening
9.3.2.3.1.6.1	IP Layer Screening
9.3.2.3.1.6.2	Transport Layer Screening (SCTP, TCP and UDP)
9.3.2.3.1.6.3	SIP Screening
9.3.2.3.2	Message Monitoring Capabilities
9.3.2.3.3	Data Confidentiality
9.3.2.3.4	Privacy
A	INFORMATIVE REFERENCES

6.4 ATIS-1000019.2007, Network to Network (NNI) Standard for Signaling and Control Security for Evolving VoP/Multimedia Networks

6.4.1 Scope of ATIS-1000019.2007

ATIS-1000019.2007 [2] addresses VoP/Multimedia signaling and control plane security requirements of evolving telecommunications networks. Specifically, the scope of this standard includes security requirements for the Network to Network Interface (NNI) between similar or dissimilar VoP/Multimedia networks.

6.4.2 Organization of ATIS-1000019.2007

1	INTRODUCTION/EXECUTIVE SUMMARY
2	SCOPE, PURPOSE, & RELATED DOCUMENTS
2.1	SCOPE
2.2.	PURPOSE
2.3	RELATED DOCUMENTS
3	NORMATIVE REFERENCES
4	DEFINITIONS & ABBREVIATIONS
4.1	DEFINITIONS
4.2	ABBREVIATIONS
5	REFERENCE SIGNALING & CONTROL NETWORK MODEL
6	H.323 SECURITY
6.1	GENERAL REQUIREMENTS
6.2	ACCESS CONTROL SECURITY DIMENSION
6.3	AUTHENTICATION SECURITY DIMENSION
6.4	NON-REPUDIATION SECURITY DIMENSION
6.5	DATA CONFIDENTIALITY SECURITY DIMENSION
6.6.	COMMUNICATION SECURITY DIMENSION
6.7	DATA INTEGRITY SECURITY DIMENSION

6.8	AVAILABILITY SECURITY DIMENSION
6.9	PRIVACY SECURITY DIMENSION
7	SIP SECURITY
7.1	GENERAL REQUIREMENTS
7.2	ACCESS CONTROL SECURITY DIMENSION
7.3	AUTHENTICATION SECURITY DIMENSION
7.4	NON-REPUDIATION SECURITY DIMENSION
7.5	DATA CONFIDENTIALITY SECURITY DIMENSION
7.6	COMMUNICATION SECURITY DIMENSION
7.7	DATA INTEGRITY SECURITY DIMENSION
7.8	AVAILABILITY SECURITY DIMENSION
7.9	PRIVACY SECURITY DIMENSION
7.9.1	Privacy of Personal Data
7.9.2	Topology Hiding
7.9.3	Spam Protection
A	ANNEX – H.323 BACKGROUND
A.1	H.323 SIGNALING AND CONTROL CHANNELS BACKGROUND
A.1.1	H.323 Overview
A.1.2	Media Gateways
A.1.3	H.323 Signaling Protocols
A.2	H.323 MESSAGING SEQUENCE
A.3	H SERIES VIDEO CODECS
A.4	H.235 SECURITY PROFILES
A.5	H.235.1 – BASELINE SECURITY PROFILE
A.6	H.235.2 – SIGNATURE SECURITY PROFILE
A.7	H.235.3 – HYBRID SECURITY PROFILE
B	INFORMATIVE REFERENCES

6.5 ATIS-1000025.2008, US Standard for Signaling Security – UNI Access and Signaling Standard

6.5.1 Scope of ATIS-1000025.2008

ATIS-1000025.2008 [4] addresses security of the User-to-Network Interface (UNI) of evolving networks. The UNI is defined as an interface between VoP/multimedia end user device or terminal and the network providing service or attachment to the device or terminal.

6.5.2 Organization of ATIS-1000025.2008

1	INTRODUCTION/EXECUTIVE SUMMARY
2	SCOPE, PURPOSE AND APPLICATION
2.1	SCOPE
2.2	PURPOSE
2.3	RELATED STANDARDS