ATIS-1000655.2001(R2011)

Signalling System Number 7 (SS7) – Upper Layer Security Capability

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 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 vis
< http://www.atis.org >.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the 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 OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF FEES RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith.

ATIS-1000655.2001(R2011), *Signalling System Number 7 (SS7) – Upper Layer Security Capability*

Is an American National Standard developed by 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-1000655.2001 (R2011)

(formerly T1.655-2001)

American National Standard for Telecommunications

Signalling System Number 7 (SS7) – Upper Layer Security Capability

Secretariat

Alliance for Telecommunications Industry Solutions

Approved March 13, 2001

American National Standards Institute, Inc.

Abstract

This standard describes the Security network capability, which allows an end user service in an originating Signaling Point (SP) to invoke various security functions in the originating and/or destination SP. The Security capability can be used for identification and authentication of the communicating entities; it also provides information that supports resource access control, system access control, and encryption and decryption functions.

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.

This document is entitled the *American National Standard for Telecommunications – Signalling System Number 7 (SS7) – Upper Layer Security Capability*. It is based on the Generic Upper Layer Security (GULS) functions described in *Information Technology - Open Systems Interconnection Upper Layers Security Model*, ISO/IEC IS 10745, June 1993. This standard is the result of work by members of the T1S1.3 Working Group on U.S. Standards for Common Channel Signalling. This revision to the standard includes the KeyExchange parameter, associated procedures and informative annexes E and F, giving examples of exchanging encryption keys. Descriptions of parameters now included in T1.114-2000 have been removed.

This standard is intended for use in conjunction with *American National Standard for Telecommunications – Signalling System Number 7 (SS7) – Transaction Capabilities Application Part (TCAP),* T1.114-2000.

Future control of this document will reside with Accredited Standards Committee on Telecommunications, T1. This control of additions to the specification, such as ongoing protocol evolution, new applications, and operational requirements, will permit compatibility among U. S. networks. Such additions will be incorporated in an orderly manner with due consideration to the ITU-T layered model principles, conventions, and functional boundaries.

Suggestions for improvement of this standard will be welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, 1200 G Street NW, Suite 500, Washington, D.C. 20005.

This standard was processed and approved for submittal to ANSI by the Accredited Standards Committee on Telecommunications, T1. Committee approval of this standard does not necessarily imply that all committee members voted for its approval. At the time it approved this standard, the T1 Committee had the following members:

E.R. Hapeman, T1 Chair
W.R. Zeuch, T1 Vice-Chair
J.A. Crandall, T1 Director
S.M. Carioti, T1 Disciplines
S.D. Barclay, T1 Secretary
C.A. Underkoffler, T1 Chief Editor
W.B. Downum, T1S1 Technical Editor

EXCHANGE CARRIERS

Organization Represented	Name of Representative
AT&T Wireless Services, Inc.	Peter Musgrove
Bell Atlantic	Josephine Gallagher James F. Baskin (Alt.)
BellSouth Telecommunications Inc.	Malcolm Threlkeld, Jr. John Spencer (Alt.)
Covad Communications Co.	Ron Marquardt David Rosenstein (Alt.)
GTE Telephone Operations	Thomas Deaton Gary E. McAninch (Alt.)
NorthPoint Communications, Inc.	Mark Peden Mike Borsetti (Alt.)
Qwest	James L. Eitel Richard Prince (Alt.)
Rhythms	Rand Kennedy David Reilly (Alt.)
Rogers Wireless Inc.	Edward O'Leary Peter Oldfield (Alt.)
SBC Communications, Inc.	C.C. Bailey John E. Roquet (Alt.)
Sprint – Local Telecom. Division	Leroy D. Kellogg
US Telecom Association (USTA)	Paul Hart Donald G. Bender (Alt.)

GENERAL INTEREST

Organization Represented	Name of Representative
Aerial Communications	George P. Lynch Rob Rowe (Alt.)
AT&T Broadband	Paul Hughes Jim Dahl (Alt.)
BellSouth Cellular Corp.	Don Zelmer Andy Clegg (Alt.)
BOPS Inc.	Ali S. Sadri, PhD
CSI Telecommunications	Michael S. Newman William J. Buckley (Alt.)
Catapult Communication	Katya Gircus Nancy Gayed (Alt.)
Defense Information Systems Agency	Don Choi
Golden Bridge Technology Inc.	Kourosh Parsa Karin Zickermann (Alt.)
Microcell Connexions	Venkatesh Sampath Andrew Chow (Alt.)
National Communications System	Nicholas Andre F. McClelland (Alt.)
NTIA	Neal B. Seitz
Pacific Bell Wireless	David Williams Randolph Wohlert (Alt.)
Rural Utilities Service	Orren E. Cameron III Norberto Esteves (Alt.)
Telcordia Technologies	Rick Harrison Cliff Halevi (Alt.)
Voicestream Wireless Corp.	Gary K. Jones Mark Younge (Alt.)

INTEREXCHANGE CARRIERS

Organization Represented	Name of Representative
AT&T	Boris S. Lebovits Rick Canaday (Alt
Bell Canada	P. Norman Smith
General Communication, Inc.	Derek L. Welton C.R. Baugh, Ph.D. (Alt.)
Lockheed Martin Global Telecom	Mark T. Neibert Prakash Chitre (Alt.)
Sprint – Long Distance Division	Thomas G. Croda James Lord (Alt.)
WorldCom	Yi-Shang Shen J. Martin Carroll (Alt.)

MANUFACTURERS

Organization Represented	Name of Representative
3COM	Fred Lucas Richard L. Stuart (Alt.)
ADC Telecommunications Inc.	Mike Rude
Airspan Communications Corp.	Douglas M. McCallister Chris Rogers (Alt.)
Alcatel USA Inc.	Ken Biholar Roz Sahakian (Alt.)
Aware, Inc.	Marcos Tzannes William Mey (Alt.)
Broadcom Corporation	David C. Jones Aidan C. Fourie (Alt.)
Centillium Communications, Inc.	Dr. Syed Abbas Guozhu Long (Alt.)
Cisco Systems, Inc.	John McDonough Chip Sharpe (Alt.)
Conexant Systems, Inc.	Quentin C. Cassen
Copper Mountain Networks	Joseph D. Markee John Reister (Alt.)
ECI Telecom Inc.	Ron Murphy Todd Poole (Alt.)
Elastic Networks, Inc.	Patrick H. Stanley, P.E. Jack Terry (Alt.)
Ericsson Inc.	Linda Troy Stephen Hayes (Alt.)
Excelsus Technologies Inc.	Frederick Kiko Don Robert House (Alt.)
Fujitsu America Inc.	Kenneth T. Coit Hirohiko Yamamoto (Alt.)
General Datacomm Inc.	Fred Cronin Mike McLoughlin (Alt.)
Globespan Semiconductor, Inc.	Massimo Sorbara Clete Gardenhour (Alt.)
Harris Corp.	Marlis Humphrey Tony Harb (Alt.)
Hekimian Laboratories	William H. Duncan
Hewlett-Packard	Karen Higginbottom
Hughes Network Systems, Inc.	Dr. Leonard Golding Enrique Laborde (Alt.)
Lucent Technologies	Dave R. Andersen Greg Ratta (Alt.)
Marconi Communications	Mark Scott David K. Brown (Alt.)
Mayan Networks	Farooq Raza Kevin W. Williams (Alt.)
Megaxess, Inc.	John Boal Mihnea Nemes (Alt.)

Organization Represented	Name of Representative
Mitel Corp.	Silvana Rodrigues Kelvin Steeden (Alt.)
Motorola Inc.	Syed Niaz Dan Grossman (Alt.)
NEC America Inc.	Donovan Nak Hajime Koto (Alt.)
Next Level Communications	Sabit Say Jeffrey Weber (Alt.)
Nokia Telecommunications Inc.	Chris Wallace Walt Tamminen (Alt.)
Nortel Networks	Mel N. Woinsky Ed Eckert (Alt.)
OKI America Inc.	Henri Suyderhoud Hisao Fujikawa (Alt.)
Paradyne Corp.	Richard K. Smith Phil Kyees (Alt.)
PMC-Sierra, Inc.	Winston Mok Terence Lau (Alt.)
Qualcomm Inc.	Mark Epstein Ed Tiedemann (Alt.)

Organization Represented	Name of Representative
Siemens Information & Communications Networks, Inc.	David E. Francisco Jim Stanco (Alt.)
ST Microelectronics	Jean-J Raynal Roy Harvey (Alt.)
Symmetricom Inc.	Tony Pilarinos Don Skipwith (Alt.)
Telecommunications Techniques	Michael Lewis Jerry Gentile (Alt.)
Tellabs Operations, Inc.	Corey Parollini Tom Rarick (Alt.)
Tellium, Inc.	Krishna Ba[illegible] Ph.D. Siegfried Gie[illegible] (Alt.)
Texas Instruments	Jam[illegible] T. Carlo Pete Cr[illegible]w, Ph.D. (Alt.)
TranSwitch Corp.	[illegible]ender Vij [illegible]win Soltysiak (Alt.)
Westell Technologies, Inc.	Guy Cerulli Tariq Amjed (Alt.)

At the time it approved this standard, Technical Subcommittee T1S1 on Services, Architectures & Signalling, which is responsible for the development of this standard, had the following members:

B. Hall, T1S1 Chair
G. Ratta, T1S1 Vice Chair

Organization Represented	Name of Representative
ADC Telecommunications Inc.	Sal Morlando Paul Krischlunas (Alt.)
Alcatel USA Inc.	Jeff Copley
AT&T	Doris S[illegible] Lebovits John K[illegible]elic[illegible] (Alt.)
AT&T Broadband	Soha[illegible] Grewal Jim Dahl
Bell Atlantic	[illegible]ana Shillingburg Michael Brusca (Alt.)
Bell Canada	Stewart Patch P. Norman Smith (Alt.)
BellSouth Telecommunications Inc.	Robert V. Epley David Whitney (Alt.)
CSI Telecommunications	Michael S. Newman William J. Buckley (Alt.)
Cisco Systems	Dan Greene Sue Geyer (Alt.)
Compaq Computer Corp.	John L. Schantz Anantha Ramu (Alt.)

Organization Represented	Name of Representative
Defense Information Systems Agency	Don Choi Ralph Liguori (Alt.)
Ericsson Incorporated	Linda Troy
Fujitsu America Inc.	Doug Hunt Kenneth T. Coit (Alt.)
General Datacomm Inc.	Mike McLoughlin
GTE Telephone Operations	Michael Collison John Rollins (Alt.)
Harris Corporation	Marlis Humphrey Tony Harb (Alt.)
Hekimian Laboratories	William H. Duncan
Hewlett-Packard	James G. Baker
ICG Communications	Thomas Tardy Kenneth Frederick (Alt.)
Illuminet	Kenn Moisey
Inet Technologies Inc.	Mart Nurmet Said Saadeh (Alt.)
LG Sansys, Inc.	Hee Joung Lee Mark Hosford (Alt.)

Organization Represented	Name of Representative
Lockheed Martin Global Telecom	Mark T. Neibert Andy Gallant (Alt.)
Lucent Technologies	Robert B. Waller Greg Ratta (Alt.)
Mayan Networks	Farooq Raza Santu Muller (Alt.)
Megaxess, Inc.	John Boal Mihnea Nemes (Alt.)
National Communications System	Nicholas Andre Dale Barr (Alt.)
NEC America Incorporated	Kuei Y. Kou Donovan Nak (Alt.)
Nokia Telecommunications Inc.	Jean-Luc Bouthhemy Walt Tamminen (Alt.)
Nortel Networks	Mel N. Woinsky Lewis C. Robart (Alt.)
OKI America Incorporated	Henri Suyderhoud Hisao Fujikawa (Alt.)
Oresis Communications, Inc.	Michael R. Zeug George Shenoda (Alt.)
Paradyne Corporation	Richard K. Smith Phil Keyes (Alt.)

Organization Represented	Name of Representative
Qwest	Steve Showell James L. Eitel
Rhythms	Rand Kennedy David Reilly (Alt.)
SBC Communications, Inc.	B.S. Sambasivan Clifton Campbell (Alt.)
Siemens Information and Communication Networks, Inc.	David LaMaster Ron Franks (Alt.)
Sprint – Long Distance Division	James Lord Albert D. Du Re[illegible] (Al[illegible]
Telcordia Technologies	Selvan Renga[illegible]mi Wesley Do[illegible]num (Alt.)
Tellabs Operations, Inc.	Jim Orn[illegible] Mike Wurst[illegible]lt.)
Tellium, Inc.	K[illegible]a Bala, PhD Sieg[illegible]d Giebl (Alt.)
US Telecom Association (US[illegible]	[illegible]aul Johnson Donald G. Bender (Alt.)
Voicestream Wireless Cor[illegible]	Albert H. Yuhan, Ph.D. Gary K. Jones (Alt.)
WorldCom	Yatendra Pathak Bernard Ku (Alt.)

Sub Working Group T1S1.3 (Network Capabilities), which developed this standard, had the following active participants:

Wesley Downum, T1S1.3 Chair
Rich Hemmeter, T1S1.3 Network Capabilities Co[illegible]

Jeff Copley	Ceylan Lennon	Dana Shillingburg
Ranga Dendi	Stewart Patch	Ray P. Singh
Stuart Goldman	Yatendra Pathak	Rajendra P. Udeshi
William H. Krall	Kraig Sanders	Scott Wilson

Table of Contents

Table of Figures

Table of Tables

American National Standard
for Telecommunications –

Signalling System Number 7 (SS7) – Upper Layer Security Capability

1 Scope, Purpose, and Application

The Security capability allows an end user service in the originating Signalling Point (SP) to invoke various security functions in the originating and/or destination SP. The Security capability can be used for identification and authentication of the communicating entities. It also provides information that supports resource access control, system access control, and encryption and decryption functions. The Security capability may be invoked by a variety of services. The end user will interact with an end user service which may invoke the Security capability. Note that the specific end user service that invokes Security is not within the scope of this capability description. The Security capability is not visible to the end user, but allows an end user service to take place. Thus, there is a "layering" of services and capabilities. The specification of the different security functions (e.g., identification, authentication, encryption) may be determined by the service or the Signalling point. The information exchange model and information element model for the Security network capability are based on the standards in the Reference section of this description.

A security policy is a statement of the rules that are to be enforced regarding the accessibility of data items and processing functions to entities within the network. In order to state the policy in a meaningful way, it is necessary to mention the threats that the policy is intended to prevent. Informative Annex B provides a threat analysis and security policy overview for Signalling System Number 7 (SS7).

Informative Annex C provides an overview of basic security functions and operation.

2 Normative References

The following standards contain provisions that, 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 standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

T1.114-2000, *Telecommunications - Signalling System No. 7 (SS7) - Transaction Capabilities.*[1]

ANSI X3.92-1981, *American National Standard Data Encryption Algorithm*.[2]

ANSI X9.9-1986, *Financial Institution Message Authentication*.[2]

CCITT Recommendation X.208-1988, *Specification of Abstract Syntax Notation One (ASN.1)*. [3]

---

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

[2] This document is available from the InterNational Committee for Information Technology Standards (INCITS). < http://www.techstreet.com/ncitsgate.html >