ATIS-1000012.2006

SIGNALING SYSTEM NO.7 (SS7) – SS7 NETWORK AND NNI INTERCONNECTION SECURITY REQUIREMENTS AND GUIDELINES

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' 20 Committees, covering issues including: IPTV, Service Oriented Networks, Home Networking, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, 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 >.

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 ANY SUM 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-1000012.2006, *Signaling System No.7 (SS7) – SS7 Network and NNI Interconnection Security Requirements and Guidelines*

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

Printed in the United States of America.

ATIS-1000012.2006

American National Standard for Telecommunications

SIGNALING SYSTEM NO.7 (SS7) - SS7 NETWORK AND NNI INTERCONNECTION SECURITY REQUIREMENTS AND GUIDELINES

Secretariat

Alliance for Telecommunications Industry Solutions

Approved November 8, 2006

American National Standards Institute, Inc.

Abstract

This document provides security requirements and guidelines for Signaling System No.7 (SS7) network and its network interconnections.

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 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.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, Packet Technologies and Systems Committee (PTSC) Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, Packet Technologies and Systems Committee, which is responsible for the development of this Standard, had the following members:

B. Hall, PTSC Chair
J. Zebarth, PTSC Vice-Chair
S. Carioti, ATIS Disciplines
S. Barclay, ATIS Secretariat
C. Underkoffler, ATIS Chief Editor
R. Singh, PTSC Technical Editor

Organization Represented	Name of Representative
AcmePacket	Kevin Klett
Alcatel USA Inc.	Ken Biholar
AT&T	Bob Hall George Stanek (Alt)
BellSouth Telecommunications	Rick McNealy
C.S.I. Telecommunications	Michael S. Newman Thomas G. Croda (Alt)
Cingular Wireless LLC	Don Zelmer Marc Grant (Alt)
Cisco Systems	Rajiv Kappor Mike Hammer (Alt)
Department of Defense	Chris Fitzgerald Ryan Kuseski (Alt)
Ericsson Incorporated	Susana Sabater-Maroto Stephen Hayes (Alt)
FBI ESTS	Marybeth Paglino Edward Ignacio (Alt)
Harris Corporation	Marlis Humphrey
Hewlett-Packard	Steve Mills
Intelsat	Mark T. Neibert
Intrado	Christian Militeau Robert Sherry (Alt)

Organization Represented	Name of Representative
Lucent Technologies	Stuart O. Goldman
Microsoft Corporation	Wendy Fong
National Communications System	Nicholas Andre Carol-Lyn Taylor (Alt)
Nokia Telecommunications Inc.	Joyabrata Mukherjee Ed Ehrlich (Alt)
Qwest	Steve Showell Michael Fargano
Siemens Communications, Inc.	Rob Franks David E. Francisco (Alt)
Sprint LTD	John M. Heinz Bill L. Wiley (Alt)
Sprint Nextel	Mark L. Jones
Telcordia Technologies	Wesley Downum Cliff Halevi (Alt)
Tellabs Operations, Inc.	William A. Walker
Tridea Works	Greg Ratta
Verisgin, Inc.	Anthony M. Rutkowski
Verizon Communications	Thomas Helmes Dave Morris (Alt)

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

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

American National Standard for Telecommunications –

Signaling System No.7 (SS7) – SS7 Network and NNI Interconnection Security Requirements and Guidelines

0 INTRODUCTION

The national telecommunications network is evolving into an environment consisting of multiple interconnected network types based on different transport technologies and signaling protocols/architectures. Specifically, it is evolving from a closed environment to include converged network segments (e.g., Next Generation and Voice Over Packet Networks) using common transport for User Network Interface (UNI) control, Network-to-Network Interface (NNI) control and bearer traffic (e.g., Voice over IP services). Also, direct or indirect connectivity to the public Internet is possible (e.g., interconnection to service providers offering voice services over the public Internet). Survivability of the national telecommunications network against malicious attacks will require coordination of security mitigation measures among the different interconnected networks. This standard identifies basic requirements and guidelines to minimize security risks to the SS7 network and its interconnections. This document is based on current understanding of the applicable technologies and operations environment. However, to be successful, this document must continue to evolve as changes in the technologies and operations conditions warrant. Service providers and their vendors may use this document as a foundation and include other network specific requirements to meet specific security needs over and beyond those described in this document.

1 SCOPE, PURPOSE, & APPLICATION

1.1 Scope

This document is part of a suite of signaling and control security standards. Figure 1 illustrates the relationships among these standards. The scope of this document is a Signaling System No.7 (SS7) Network, and SS7 network interconnections. This includes interconnection to other SS7 networks and to multimedia signaling and control networks such as SIP and H.323 networks. Specifically, this document provides security requirements and guidelines for a Signaling System No.7 (SS7) network and its network interconnections.

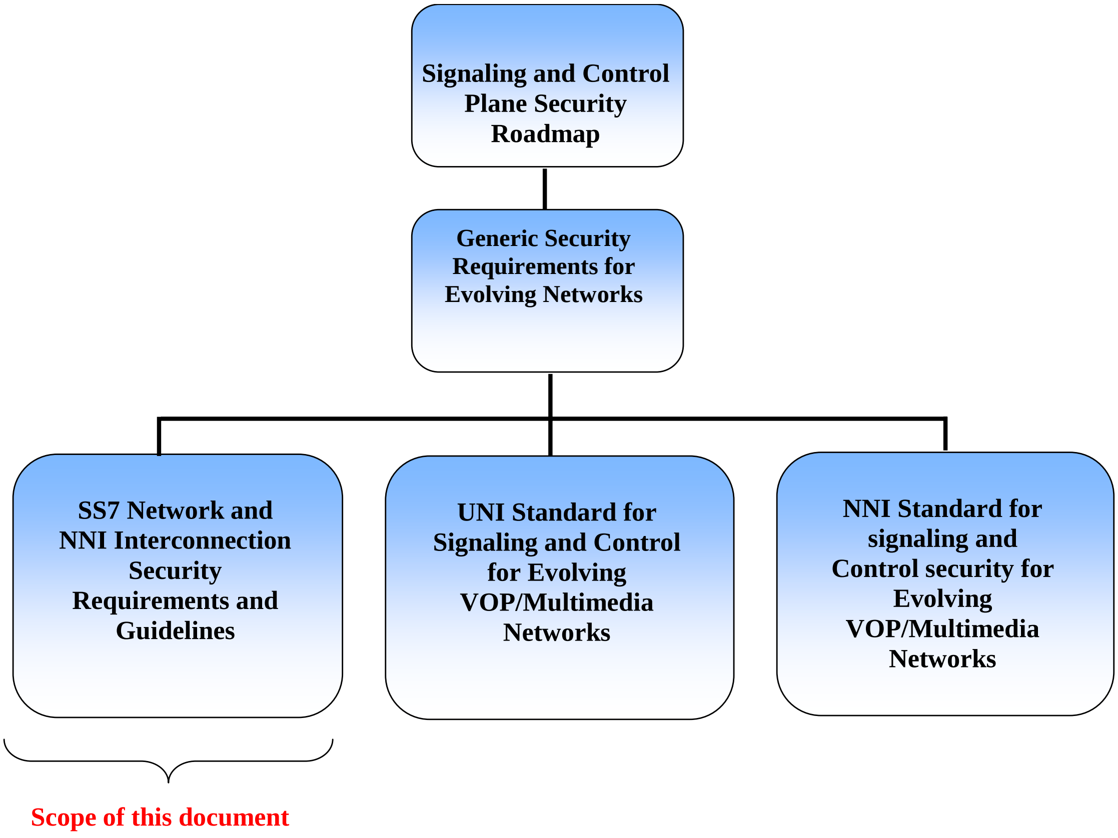
Signaling and Control Plane Security Roadmap
Generic Security Requirements for Evolving Networks
SS7 Network and NNI Interconnection Security Requirements and Guidelines
UNI Standard for Signaling and Control for Evolving VOP/Multimedia Networks
NNI Standard for signaling and Control security for Evolving VOP/Multimedia Networks
Scope of this document

Figure 1 – Scope and relationship with other documents

The traditional SS7 network uses the ISDN User Part (ISUP) call control protocol over a Message Transfer Part (MTP) transport network consisting of dedicated MTP2 or Signaling ATM Adaptation Layer (SAAL) signaling links. This document provides:

- Security requirements and guidelines for SS7 networks including the supported application protocols and services.
- Security requirements and guidelines regarding interconnection of an SS7 network to other SS7 networks and other signaling network types (e.g., H.323 and SIP).
- Security requirements and guidelines related to SS7 network interactions with the management plane (i.e., management networks) and user plane (i.e., bearer networks).

1.2 Purpose

The main purpose of this document is to provide guidance and recommendations to network providers and equipment manufacturers in areas of network security. It is also intended to guide industry groups to develop and specify the necessary protocol capabilities or enhancements for security.

1.3 Requirements, Objectives and Guidelines

The content of this standard is specified in the form of Requirements, Objectives and Guidelines as defined in ATIS-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks* [1].

1.4 Security Threats

A threat is defined as a potential violation of security. The SS7 signaling network must be protected from the possibility of deliberate or accidental actions or conditions that may lead to a compromise of security. There are many types of threats. The following are examples of general categories of security threats derived from T1.233-2004 [6] and X.800 [7]:

1.4.1 Unauthorized Access: This threat includes unauthorized access to systems and resources within systems such as data and software systems. Specifically, for SS7, this includes unauthorized access to the SS7 network, its resources, and SS7 services/protocols. Once unauthorized access is gained, damage could be done to disrupt normal operation. Sensitive and valuable information could be lost, modified, or disclosed that may ultimately jeopardize the operation of the SS7 network in addition to the services supported.

1.4.2 Masquerade: This threat involves pretense by an entity to be a different entity in order to gain access to information or to acquire additional privileges to use resources. For example, the pretense by one network entity sending signaling messages to a second network entity while pretending to be another network entity, thereby bypassing restrictions that would prohibit the requested exchange of information or resource usage.

1.4.3 Integrity of Information: This threat involves the fabrication, manipulation, or modification of information residing in systems as well as information in transit. For example, specifically for SS7, this involves manipulation or modification of the information in SS7 signaling messages.

1.4.4 Confidentiality of Information: This threat involves the observation of information by an unauthorized entity. Illegitimate access to the information could involve capturing messages in transit or unauthorized access to information in systems. For example, specifically for SS7, this may involve observation of MTP network management messages or private information (such as personal identification number) in signaling messages. If the transfer of information is not protected, if instead, the information travels across virtually open networks in clear-text, then it can be "seen" and understood by unauthorized parties with access to the open networks. An alternative to protecting the transfer of the information is to protect the information itself in such a way that even if it is intercepted, it is unreadable or unusable by any unauthorized party.

1.4.5 Denial of service: This threat involves one entity preventing other entities from performing their service functions. For example, this may involve denial of access to a database via corruption of the access function within the database, or denial of all SS7 communication by flooding a specific network element, the entire SS7 network, or a portion of the SS7 network. The threat of flooding involves the fabrication of extra traffic preventing or delaying others entities from using the network element or the SS7 network.

1.4.6 Non-Repudiation: This threat involves a communicating party denying its participation in all or part of a communication in which it did participate. For example, specifically for SS7, one network may incorrectly deny that one of its network elements sent signaling messages received by the threatened network element.

2 Normative References

The following standard contains provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the edition indicated was valid. All standards are subject to revision, and the parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below.

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

[2] T1.110-1999 (R2005), *Signalling System Number 7 (SS7) – General Information.*[1]

[3] ATIS-1000111.2005, *Signalling System No.7 (SS7) – Message Transfer Part.*[1]

[4] T1.655-2001 (R2006), *Upper Layer Security Network Capability.*[1]

[5] T1.233-2004, *Security Framework for Telecommunications Management Network (TMN) Interfaces.*[1]

[6] ITU-T Recommendation X.800, *Security Architecture for Open System Interconnection for CCITT Applications.*[2]

3 Definitions, Acronyms, & Abbreviations

3.1 Definitions

3.1.1 Closed Network Environment: A network or set of interconnected networks that provide transport only for a limited domain of applications and network elements.

> NOTE: A closed SS7 network is characterized by SS7 signaling network facilities and SS7 signaling traffic that are separated from other signaling/control traffic, from bearer network signaling/control traffic, and from bearer traffic (e.g., end user access). In addition, the SS7 signaling network is separated from management networks and traffic (i.e., from facilities and traffic related to maintenance and operations access).

3.1.2 Open Network Environment: A network environment that is not closed.

> NOTE: That is, access to the network transport is open to applications or network elements that are parts of different network domains. An example of an open network environment is an SS7 network passing SS7 messages over the public Internet. An open network interconnected with an otherwise-closed network forms an open network.

3.3 Traditional SS7 Network: An SS7 network using the ISDN User Part (ISUP), Transaction Capabilities Application Part (TCAP), and Signaling Connection Control Part (SCCP) over a Message Transfer Part (MTP) transport network deployed on dedicated MTP2 or Signaling ATM Adaptation Layer (SAAL) signaling links in a closed network environment.

[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/ >

3.2 Acronyms & Abbreviations

ACM	Address Complete Message
AIN	Advanced Intelligent Network
ANSI	American National Standards Institute
ATIS	Alliance for Telecommunications Industry Solutions
AS	Application Server
B-ISUP	Broadband ISDN User Part
CdPA	Called Party Address
CgPA	Calling Party Address
COA	Changer Over Acknowledgement
COO	Change Over Order
DCS	Digital Cross-connect System
DPC	Destination Point Code
DSL	Digital Subscriber Loop
DS1	Digital System 1
DS3	Digital System 3
GTT	Global Title Translation
IAM	Initial Address Message
IN	Intelligent Network
IP	Internet Protocol
IPsec	IP Security
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LNP	Local Number Portability
MGC	Media Gateway Controller
MSU	Message Signal Unit
MTP	Message Transfer Part
MTP3	Message Transfer Part Layer 3
MTP2	Message Transfer Part Layer 2
MTP1	Message Transfer Part Layer 1
M2PA	MTP2 Peer-to-Peer Adaptation
M2UA	MTP2 User Adaptation
M3UA	MTP3 User Adaptation
NE/NS	Network Element/Network System
NGN	Next Generation Network
NNI	Network to Network Interface
NRIC	Network Reliability Interoperability Council
OPC	Originating Point Code
OMAP	Operations, Maintenance, and Administration Part
SAAL	Signalling ATM Adaptation Layer

SCP	Service Control Point
SCCP	Signalling Connection Control Part
SCTP	Stream Control Transmission Protocol
SEP	Signalling End Point
SG	Signalling Gateway
SI	Service Indicator
SIO	Service Information Octet
SIP	Session Initiation Protocol
SPC	Signalling Point Code
SUA	SCCP User Adaptation
SSN	Subsystem Number
SSP	Service Switching Point
SS7	Signalling System No.7
STP	Signalling Transfer Point
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
UDP	User Datagram Protocol
UDT	Unit Data Transfer
UNI	User to Network Interface
TC	Transaction Capabilities
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TFC	Transfer Control
TFP	Transfer Prohibited
TFR	Transfer Restricted
VOP	Voice Over Packet
VoIP	Voice over IP
XUDT	Extended Unit Data Transfer

4 SS7 Signaling Network Security Needs & Security Architecture

This clause recommends security requirements and planning guidelines to assist network providers/administrators and their vendors in protecting the SS7 network and the supported services. The concepts and requirements described in this clause are extended to address the inter-network environment in clause 9.

4.1 Traditional SS7 Network

4.1.1 Overview

A Traditional SS7 Network in the context of this document is defined by its use of the Message Transfer Part Layer 3 (MTP3) protocol as the network layer transport protocol and conventional Message

Transfer Part Level 2 (MTP2) or Signaling ATM Adaptation Part (SAAL) signaling links over dedicated facilities. Specifically, a traditional SS7 network, in the context of this document, is identified by the use of the following SS7 protocols in a closed network environment;

- *Application Protocols* – Integrated Services Digital Network User Part (ISUP) and Transaction Capabilities Application Part (TCAP).
- *Network Transport Layer Protocols* – Message Transfer Part Level 3 (MTP3) or Signaling Connection Control Part over Message Transfer Part Level 3 (SCCP/MTP3).
- *Link Layer Protocols* – Message Transfer Part Level 2 (MTP2) or Signaling ATM Adaptation Layer (SAAL).

A closed SS7 environment is defined by, but is not limited by, the following characteristics:

- Use of conventional SS7 links (MTP2 or SAAL) deployed over dedicated facilities.
- Network design to isolate/separate SS7 network and SS7 traffic from other control signaling network types and signaling traffic (e.g., access signaling network/access signaling traffic).
- Network design to isolate/separate SS7 network and SS7 traffic from the bearer network and bearer traffic (i.e., user traffic).
- Network design to isolate/separate SS7 network and SS7 traffic from management/maintenance networks and management/maintenance traffic.

4.1.2 Functional Architecture

Architectures, structures and configurations of traditional SS7 networks are specified in T1.110-1999 (R2005) [2] and ATIS-1000111.2005 [3]. An example functional architecture of a traditional SS7 network is shown in Figure 2.

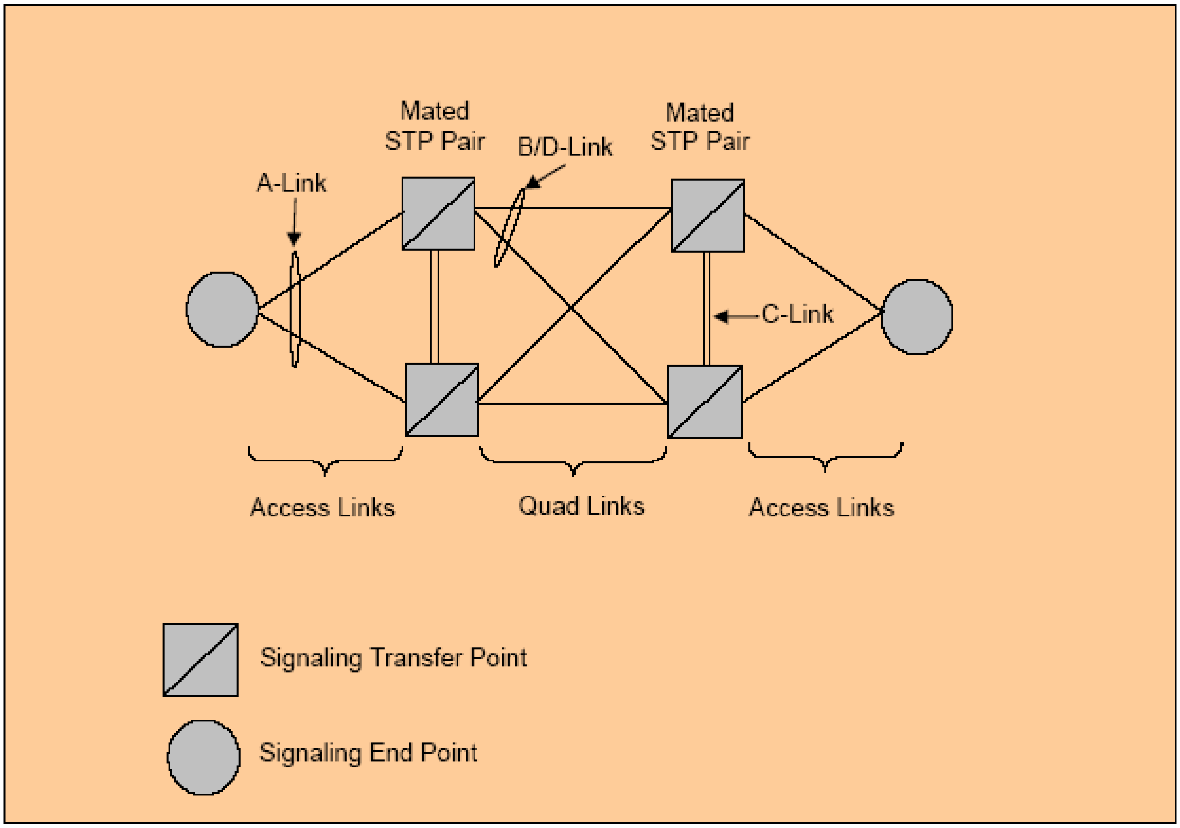

Figure 2 - Example Traditional SS7 Network Architecture

From a security perspective, the objective is to protect the availability and integrity of the SS7 network and its supported application services. This involves continuous security planning, development and implementation of mitigation services, and planning and implementation of security practices/processes to protect the SS7 network and its individual Network Elements (signaling links, STPs, SEPs, etc.) and supported application services. Specifically, hardware and software systems, components, and protocol interfaces of SS7 network elements must be safeguarded so that their intended functions and services are not compromised intentionally or unintentionally.

4.1.3 SS7 Protocols and Fundamental Security Needs

4.1.3.1 Traditional SS7 Protocol Stack

The protocol architecture of the traditional SS7 network is specified in T1.110-1999 (R2005) [2] and is illustrated in Figure 3. From a security perspective, the objective is to protect the individual SS7 protocols and interfaces so that the functions and services are not compromised.

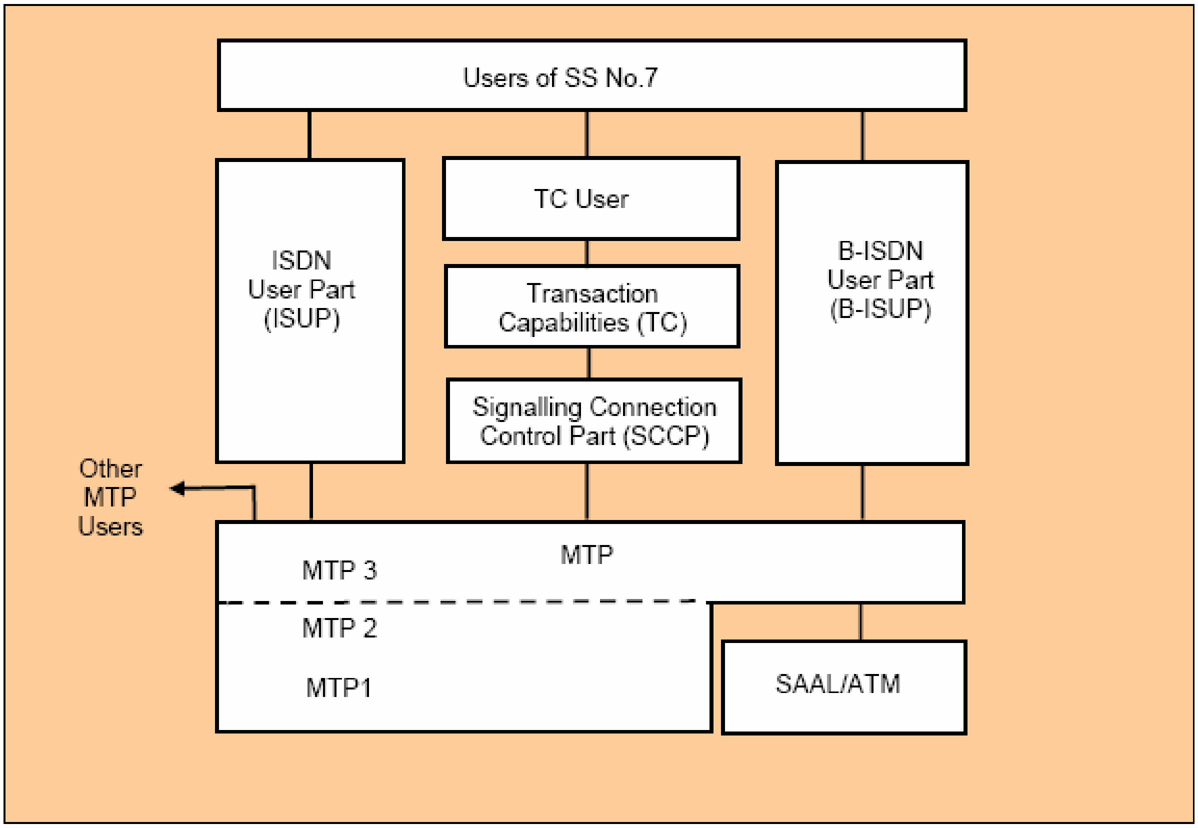

Figure 3 - Traditional SS7 Network Protocol Architecture

4.1.3.2 Fundamental Security Needs

The fundamental challenge for SS7 security is to assure data transfer between two communicating SS7 entities without any external intrusion. Table 1 identifies the resulting security needs of each individual SS7 application or network layer protocol.

NOTE: In Table 1, protection against message insertion includes protection against insertion of individual messages and protection against Denial of Service attacks.

Table 1 - Fundamental Security Needs of SS7 Application and Network Layers Protocols

SS7 Protocol	Fundamental Security Needs
MTP3 Header	Protection against alteration and manipulation. Protection against observation by unauthorized entities.
MTP3 Management Messages	Protection against message insertion and deletion. Protection against mis-sequencing. Protection against alteration and manipulation. Protection against observation by unauthorized entities.
SCCP Header	Protection against alteration and manipulation. Protection against observation by unauthorized entities.
SCCP Management Messages	Protection against message insertion and deletion. Protection against mis-sequencing. Protection against alteration and manipulation. Protection against observation by unauthorized entities.
ISUP Call Set-up Messages	Protection against message insertion and deletion. Protection against mis-sequencing. Protection against alteration and manipulation. Protection against observation by unauthorized entities.
ISUP Management Messages	Protection against message insertion and deletion. Protection against mis-sequencing. Protection against alteration and manipulation. Protection against observation by unauthorized entities.
TCAP Application Messages	Protection against message insertion and deletion. Protection against mis-sequencing. Protection against alteration and manipulation. Protection against observation by unauthorized entities.
TCAP Management Messages	Protection against message insertion and deletion. Protection against mis-sequencing. Protection against alteration and manipulation. Protection against observation by unauthorized entities.

4.2 Security Architecture and Methodology

This document uses the Security Architecture and the Methodology defined in ATIS-1000007.2006 [1] to specify requirements and guidelines to protect the SS7 signaling network from security threats. This involves security measures to protect the following SS7 entities:

1. The SS7 signaling network infrastructure consisting of the SS7 network elements and the SCCP/MTP transport network. Specifically, this includes the SS7 Signaling End Points (e.g., Switches and Service Control Points), the Signaling Transfer Points (STPs) and the signaling links (e.g., MTP2 and SAAL links) including the transport facilities.

2. The SS7 application protocols. This includes the ISUP call control application protocol and the Transaction Capabilities Application Protocol (TCAP) application protocol.
3. Services supported by the SS7 applications (e.g., POTS, ISDN, AIN, LNP, etc.).

The Security Architecture defined in ATIS-1000007.2006 [1] consists of three Security Layers;

1. Infrastructure
2. Network Services
3. Applications.

The Methodology involves applying the following security dimensions defined in detail in ATIS-1000007.2006 [1]:

1. Access Control
2. Authentication
3. Non-repudiation
4. Data Confidentiality
5. Communication Security
6. Data Integrity
7. Availability
8. Privacy

The requirements and guidelines specified in this document are organized based on the Security Layers defined in ATIS-1000007.2006 [1] as follows:

Application of Security Architecture and Methodology to the SS7 Network	
Security Layer	Security Layer Descriptions
Infrastructure Security Layer	Transmission facilitates and network elements (e.g., SS7 Links, Switches, SCPs, and STPs)
Network Services Security Layer	Network transport layer services and protocols (e.g., MTP and SCCP)
Application Security Layer	Application protocols and application services. This includes, traditional SS7 application protocols (ISUP, TCAP and OMAP), and application services supported by these protocols (e.g., POTS, IN and LNP).

5 GENERAL REQUIREMENTS & GUIDELINES

5.1 Network Design

The design and maintenance of an SS7 network, and security practices must be based on the security needs listed in Table 1. Regardless of the network architecture, underlying transport network type, transport/link layer protocols, and network environment, it is essential that the fundamental security needs identified in Table 1 be met during exchange of SS7 messages. It is recommended that each SS7 network provider, administrator, and vendor develop and implement specific security capabilities and practices to achieve the fundamental security needs identified in Table 1 when planning, designing, and deploying SS7 networks. This includes;

- Specific network architecture/topology designs to minimize security risks.
- Specific solutions for administration, operations, and maintenance of the SS7 network, SS7 network elements, SS7 hardware and software systems and components to minimize security risks.
- Specific vendor designs and implementation of SS7 products and protocol solutions to minimize security risks.
- Continuous evaluation and adjustment of security plans, practices, and processes and solutions as network conditions changes.

The SS7 transport network must be designed to minimize the possibility of external intrusion between two communicating SS7 entities. The following requirements are applicable when planning, designing, and implementing the SS7 network:

<REQ-SEC-SS7-00100>

The signaling association between two communicating SS7 entities shall be protected against intrusions resulting in the alteration or manipulation of the header fields or of the content of the SS7 messages.

<end of REQ-SEC-SS7– 00100>

<REQ-SEC-SS7-00200>

The signaling association between two communicating SS7 entities shall be protected against intrusions resulting in insertion, deletion, or replay of SS7 messages.

<end of REQ-SEC-SS7 00200>

<REQ-SEC-SS7-00300>

The signaling association between two communicating SS7 entities shall be protected against intrusions resulting in unrecoverable mis-sequencing of SS7 messages.

<end of REQ-SEC-SS7 00300>

<REQ-SEC-SS7-00400>

The signaling association between two communicating SS7 entities shall be protected against observation of the exchanged SS7 messages by unauthorized entities (i.e., parties other than those authorized by the participating service providers).

<end of REQ-SEC-SS7-00400>

<REQ-SEC-SS7-00500>

The signaling association between two communicating signaling entities shall be implemented to allow participating service providers to use security tools to inspect exchanged SS7 messages.

<end of REQ-SEC-SS7-00500>

5.2 Security Plan, Policy & Practices

It is recommended that each SS7 network provider and administrator develop and implement a security plan. The security plan should address the entire SS7 network. Specifically, as a best practice, it is recommended that SS7 network providers and administrators define and implement security plans that include (but are not limited to) the following considerations:

- Identification of, SS7 resources, services, and capabilities to be protected.
- Enumeration of the threats associated with each asset, resource, service, or capability to be protected.
- Establishment of a security policy regarding each identified SS7 resource, service, and capability to be protected.
- Implementation of specific measures to protect each SS7 resource, service, or capability.
- Periodic review of security policies and measures.
- Implementation of processes to educate and train network personnel to "think security."

5.3 Network Reliability Interoperability Council (NRIC) Best Practices

Recommended best practices for network reliability and security are constantly being reviewed and updated by the Network Reliability Interoperability Council (NRIC). Many of the NRIC best practices are applicable to SS7. It is recommended that SS7 network providers, administrators, and vendors implement SS7 applicable NRIC best practices.

5.4 Documents and Specification Safeguard

It is recommended that each SS7 network provider and administrator develop and implement processes and practices to identify and protect proprietary and sensitive SS7 information (e.g., information that can be used in a malicious manner). Such processes and practices include, but are not limited to, the following:

- Identifying and safeguarding proprietary information (e.g., SS7 network element specifications, documents, and information regarding network architecture and routing specifications).
- Identifying and safeguarding dissemination of sensitive information (e.g., preventing unauthorized entities from correlating a Signaling Point Code with the identification and location of an SS7 node).
- Processes and practices to routinely review and filter sensitive information associated with the SS7 network and SS7 network elements that are disseminated publicly (e.g., on web sites).

5.5 Management Plane Security

Refer to T1.233-2004 [5] and ATIS-0300276.2008 for management plane security requirements.

5.6 Security Management System

The traditional SS7 network was not specifically designed to interface to a Security Management System. However, as signaling network evolves to include NGN signaling and hybrid infrastructures interfacing to a Security Management System may be necessary based on the network provider's solution for security management. Refer to ATIS-0300074, *Guidelines and Requirements for Security Management Systems*, for information on security management systems.

6 INFRASTRUCTURE LAYER

6.1 Access Control

6.1.1 SS7 Network Element Access

The SS7 network consists of multiple physical network elements (e.g., STPs, SSPs, and databases) that are comprised of hardware and firmware that are capable of hosting multiple software facilities. Also, a network provider's operating environment involves operating the SS7 network in conjunction with other networks (e.g., transport, operations, and bearer networks) in a coordinated manner to provide communications services to their customers. SS7 network elements and components (e.g., hardware and software systems) may be operated, managed, maintained, and administered on an individual basis or through centralized management/operations systems and networks. Specific security features and mitigation mechanisms are needed to control access to SS7 systems and resources (both hardware and software).

<REQ-SEC-SS7-00600>

Specific security features and mitigation mechanisms shall be implemented to control access (i.e., authorized network administration personnel) to the SS7 network and Network Elements, including hardware, and software and components. Specifically, this shall include, but not necessarily be limited to, security features and mitigation service for the following regarding access:

- ♦ Identification
- ♦ Authentication
- ♦ Confidentiality
- ♦ Security Auditing (security logs)
- ♦ Security Administration Control
- ♦ Non-Repudiation

<end of REQ-SEC-SS7-00600>

Refer to Telcordia Technologies GR-815-CORE, *Generic Requirements for Network Element/Network System (NE/NS) Security*, for additional information.

6.1.2 SS7 Network Design

It is easier to manage security risks in closed networks. It is recommended that the traditional SS7 network be deployed in a closed network environment. Specifically, each component of the SS7 network should be deployed in an environment dedicated to SS7 signaling, with dedicated resources, physically and logically separate from all other networking aspects. Specifically, the SS7 network and SS7 traffic should, at a minimum, be isolated from the following:

- Other signaling networks (e.g., user-to-network access signaling).
- The bearer network and user traffic.
- The operations and management/maintenance network and traffic.
- The data network and traffic.

The transport network for the traditional SS7 network shall be designed based on the conventional protocol stack specified in T1.110-1999 (R2005) [2] and ATIS-1000111.2005 [3] using only conventional SS7 signaling links. Unauthorized access to SS7 signaling is minimized by using dedicated facilities and resources for SS7 links.

<REQ-SEC-SS7-00700>

MTP2 and SAAL links shall be deployed over dedicated link and transmission facilities.

<end of REQ-SEC-SS7-00700>

6.1.3 Physical Security

Protection of the physical components and facilities of the SS7 network is paramount. Specifically, it is necessary that security procedures and processes be implemented to prevent unauthorized access to the physical components and facilities associated with the SS7 network.

It is recommended that procedures and processes be implemented to prevent unauthorized access to the physical components and facilities associated with the SS7 network. Specifically, this includes, but is not limited to the following:

- Access to locations (e.g., central office buildings) containing SS7 network elements.
- Access to any physical component of SS7 link facilities.
- Access to any physical components, systems and interface devices of SS7 network elements.
- Access to any operations, administration and maintenance interfaces or devices of SS7 network elements (maintenance channel, input/output and MOC terminals, etc.).

6.2 Availability

6.2.1 Security Arrangements and Diversity/Redundancy

Clause 5.5 of Chapter T1.111.6 of ATIS-1000111.2005 [3] specifies MTP security arrangement requirements for traditional SS7 networks. For the traditional SS7 network, security arrangements are mainly formed by redundancy in conjunction with the MTP3 changeover procedure. Network design using redundancy and the MTP3 changeover procedure is used to achieve availability objectives.

Note that these network arrangement requirements are primarily designed to address accidental or incidental SS7 network overload. Although SS7 network management controls, redundancy, and the MTP3 changeover procedure will all mitigate the impact of a Denial of Service attack, defense against that threat is provided primarily by maintaining the SS7 network as a closed network.

> **<REQ-SEC-SS7-00800>**
>
> SS7 networks shall support the security arrangement requirements specified in Clause 5.5 of Chapter T1.111.6 of ATIS-1000111.2005 [3]. Specifically, the requirements for security arrangements for components of the signaling network and for signaling arrangements shall be supported
>
> **<end of REQ-SEC-SS7-00800>**.

T1.111.6 recommends improving availability of signaling routes within a signaling network by replicating signaling links, signaling paths, and signaling routes. Design of robust networks with redundancy and diversity is not only necessary to meet availability objectives, it is critical for network security.

<REQ-SEC-SS7-00900>

SS7 network shall be designed so that replicated SS7 network elements are deployed in diverse geographical locations. Specifically:

- ♦ Mated pairs of STPs shall be deployed in separate geographical locations so that a common event (e.g., fire, earthquake, etc.) would not affect both STPs in the mated configuration.
- ♦ Mated Databases or Databases in multiple replicate arrangements (i.e., more than two replicated databases) shall be deployed in separate geographical locations so that a common event (e.g., fire, earthquake, etc.) would not affect availability of all the databases in a mated or multiple replicate arrangement, respectively

<end of REQ-SEC-SS7-00900>.

Signaling link and link set diversity planning and implementation is critical for SS7 network security. In general, n-way diversity between two portions of an SS7 network connected by multiple link sets means that no instance of (n-1) or fewer simultaneous failures will cause there to be no available links between the two portions. For SS7 networks, full diversity is the provisioning of physically (physical diversity) and electrically (electrical diversity) separate circuits between signaling nodes. No common systems (including high level DS1 or DS3, or higher multiplexing), cable, sheath, duct, conduit, common building, carrier system, digital cross-connect system or supporting structure (e.g., radio tower, pole line, or conduit) can be used if two circuits are to be completely diverse. Physical diversity requires the provisioning of separate circuits on separate facilities and separate physical paths such that a single failure in one of those facilities or path would not cause the failure of both circuits. In this context, "facilities" include the physical medium, channel banks, multiplexers, distribution frames, DCSs, etc., and "path" refers to ducts, conduits, etc. Electrical diversity is the provisioning of separate circuits with separate powering, fusing, electronics, and timing such that a single failure would not cause the failure of both circuits. Specific diversity objectives have been specified in T1.111.5 based on availability requirements for SS7 networks.

<OBJ-SEC-SS7-00100>

It is recommended that SS7 link sets be deployed with full diversity (both electrical and physical diversity). Specifically, the following minimum signaling link set diversity is recommended:

- 2-way diversity for A-link sets.
- 2-way diversity for C-link sets.
- 3-way diversity for B/D-link sets.

<end of OBJ-SEC-SS7-00100>

Telcordia Technologies GR-82-CORE and GR-905-CORE provide more information regarding SS7 link set diversity.

SS7 network providers should plan and implement an SS7 network specific link diversity management process. The SS7 link diversity management process is intended to plan and provision diverse SS7 links initially and to maintain the diversity on a continuous basis. The SS7 link diversity management process should begin when the link is deployed and should include periodic recertification of the diversity.

It is recommended that each SS7 network provider and administrator develop and implement an SS7 link diversity management process. The process should include periodic and continuous evaluation and maintenance of link sets diversity. The diversity process may include, but is not limited to, the following practices:

- Definition of SS7 network diversity rules and specifications.
- Documentation of diversity guidelines.
- Risk management (cost/benefit).
- Assignment of responsibility and accountability.
- Application of diversity rules and guidelines.
- Tracking and resolving diversity problems.

6.3 Capacity Engineering Guidelines

Survivability and availability of the SS7 network depend on the implementation of appropriate engineering and capacity rules and best practices. SS7 network providers should engineer their networks to account for different types of failure scenarios, in support of the requirements specified in

6.2. For example, a SS7 network provider should engineer the link sets in a combined A-link-set pair such that one link set may carry the traffic of the other in the event of a link set failure or STP failure. In this case, the objective for the normal engineered load on links in the link sets is 40 percent of the link capacity, to assure that the failure-mode occupancy does not exceed 80 percent. Similarly, the link sets in B-or-D link set quad, at a minimum, should be engineered for no more than 40 percent occupancy. With 40 percent occupancy, the load should not exceed 80 percent occupancy when an STP assumes its mate's traffic during a dual failure on the B/D-link quad.

Each network provider should also engineer certain critical B-or-D link set quads to withstand the unavailability of 3 of the 4 link sets in the quad and to accommodate all of the alternate-routed load on the remaining link set. In this case, the normal engineered load on each link set should be set at 20 percent of the link capacity, such that 80 percent occupancy should not be exceeded.

Refer to Chapter T1.111.5 of ATIS-1000111.2005 [3] for descriptions of example failure scenarios.

It is recommended that SS7 capacity/engineering plans and best practices include processes to continuously monitor SS7 link occupancy/utilization and to anticipate the need to expand the capacity of the SS7 network.

GR-82-CORE and GR-905-CORE provide additional information regarding engineering and capacity.

7 NETWORK SERVICES LAYER

7.1 Access and Authentication

7.1.1 SS7 Message Screening

Clause 9.2.4.1.1 describes SS7 message screening requirements and guidelines for network interconnection. It is recommended that the SS7 screening procedures specified in 9.2.4.1.1 also be supported selectively for signaling relations within each network administrator's domain. This will reduce risks of threats originating within the network domain. For internal network screening, it is recommended that each network administrator should:

- Identify all signaling relations within the network domain.
- Establish screening rules for signaling relations within its network domain.
- Establish policies and procedures that apply the screening rules.
- Review and revise the screening rules periodically.

7.2 Data Confidentiality

There is no specific protocol mechanism providing confidentiality of an entire SS7 message. The optional TCAP Upper Layer Security Capability provides confidentiality for the TCAP Component Portion of an SS7 message. In the traditional SS7 network, minimizing the risk of observation of SS7 messages (headers and contents) by unauthorized entities depends on the physical security measures recommended for the infrastructure layer, as described in Clause 6 and on the closed environment of the traditional network. The network administrator should be aware of the confidentiality risks that SS7 messages may be observed in an open environment.

7.3 Privacy

Privacy mechanisms provide protection of certain sensitive information, mostly at the application layer. Assuring privacy may require ensuring data is not observed in transit or when stored. For the SS7 network, the privacy security dimension may be addressed by satisfying the confidentiality security dimension, and ensuring security of the stored data.

7.4 Data Integrity

Data integrity (including assurance of proper message sequencing) for SS7 messages is provided by the MTP2, SAAL, and MTP3 protocols (e.g., error detection and error correction mechanisms).

7.5 Availability

7.5.1 Security Arrangements and Diversity/Redundancy

Security risks to network availability are minimized through design of the infrastructure layer and the use of the MTP3 changeover procedure as specified in 6.2.1.

8 APPLICATION LAYER

8.1 Data Confidentiality

8.1.1 SS7 Upper Layer Security Capability

The upper layer security network capability is specified in T1.655-2001 (R2006) [4]. The capability includes identification, authentication, and confidentiality functions for communicating entities using the SS7 Transaction Capabilities Application Part (TCAP) protocol. T1.655-2001 (R2006) [4] includes a generic mechanism to encrypt components of a TCAP message.

It is recommended that the upper layer security network capability [T1.655-2001 (R2006)] be used to support TCAP application services in environments that require identification, authentication or confidentiality protection. For example, some TCAP services require the confidential exchange of private information such as a calling card number or personal identification number.

<OBJ-SEC-SS7-00200>

It is desirable that SS7 entities supporting TCAP applications that involve the exchange of private information (e.g., calling card number or personal identification number) support the upper layer security network capability specified in T1.655-2001 (R2006) [4]. Specifically, the upper layer security network capability should be used to identify and authenticate peer entities and to encrypt private information in transport network environments that are open.

<end of OBJ-SEC-SS7-00200>

8.2 Privacy

Privacy mechanisms provide protection of certain sensitive information, mostly at the application layer. Assuring privacy may require ensuring data is not observed in transit or when stored. For the SS7 network, the privacy security dimension may be addressed by satisfying the confidentiality security dimension, and ensuring security of the stored data.

9 NETWORK INTERCONNECTION

This clause discusses security requirements and guidelines related to SS7 signaling network interconnections. There are multiple possible interconnection scenarios, variations, and end-to-end combinations. However, this standard does not address all the possible variations. The focus is on security of SS7 network interconnection in a generic manner. Specifically, the scope of this clause is limited to security of the following interconnection cases:

1. Traditional SS7 Network to Traditional SS7 Network Interconnection.
2. Traditional SS7 Network to IP-based Signaling Network (e.g., SIP) Interconnection.

9.1 General Objective and Model for Signaling Network Interconnection Security

The requirements, objectives, and guidelines for SS7 network interconnection are based on the Model for Signaling Network Interconnection Security described in clause 5.6 of ATIS-1000007.2006 [1]. As described in ATIS-1000007.2006 [1], each network is responsible for implementing security protection within its network domain based on security policies and the specific security capabilities supported by the network type (e.g., technology).

9.2 Traditional SS7 Network to Traditional SS7 Network Interconnection

This clause describes requirements and guidelines to minimize security risks for traditional SS7 network interconnection to another traditional SS7 network.

9.2.1 Reference Architecture

The generic reference architecture for traditional SS7 network interconnection is described in Clause 6A.4 (Inter-Network Signaling Network Structure) of Chapter 5 of ATIS-1000111.2005 [3] and is shown in Figure 4.

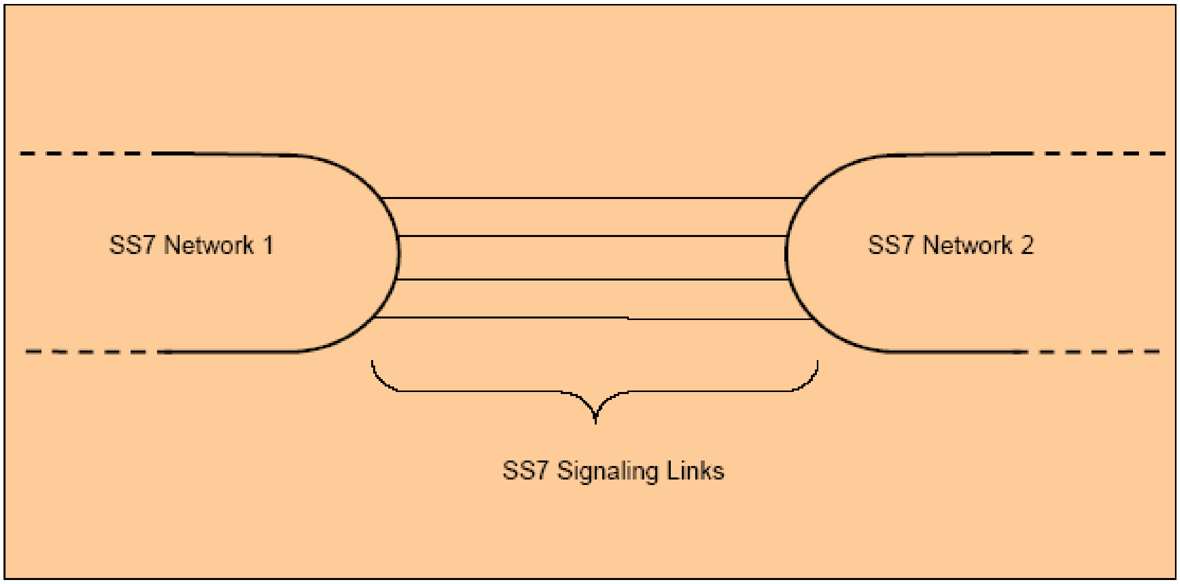

Figure 4 - Generic SS7 Network Interconnection Reference Diagram

As described in Clause 6A.4 of Chapter T1.111.5 of ATIS-1000111.2005 [3], multiple interconnection scenarios are allowed. Signaling end points may be directly interconnected to other signaling end points or to STPs. Direct interconnection between two signaling end points should include screening at the destination signaling end point based on the OPC of the received message. For internetwork interconnection, unless signaling endpoints implement message screening functions, it is recommended that they interconnect through a mated STP pair supporting screening functions rather than interconnecting directly. The recommended interconnection arrangement for a mated STP pair is shown in Figure 5, with the corresponding SS7 protocol relations.

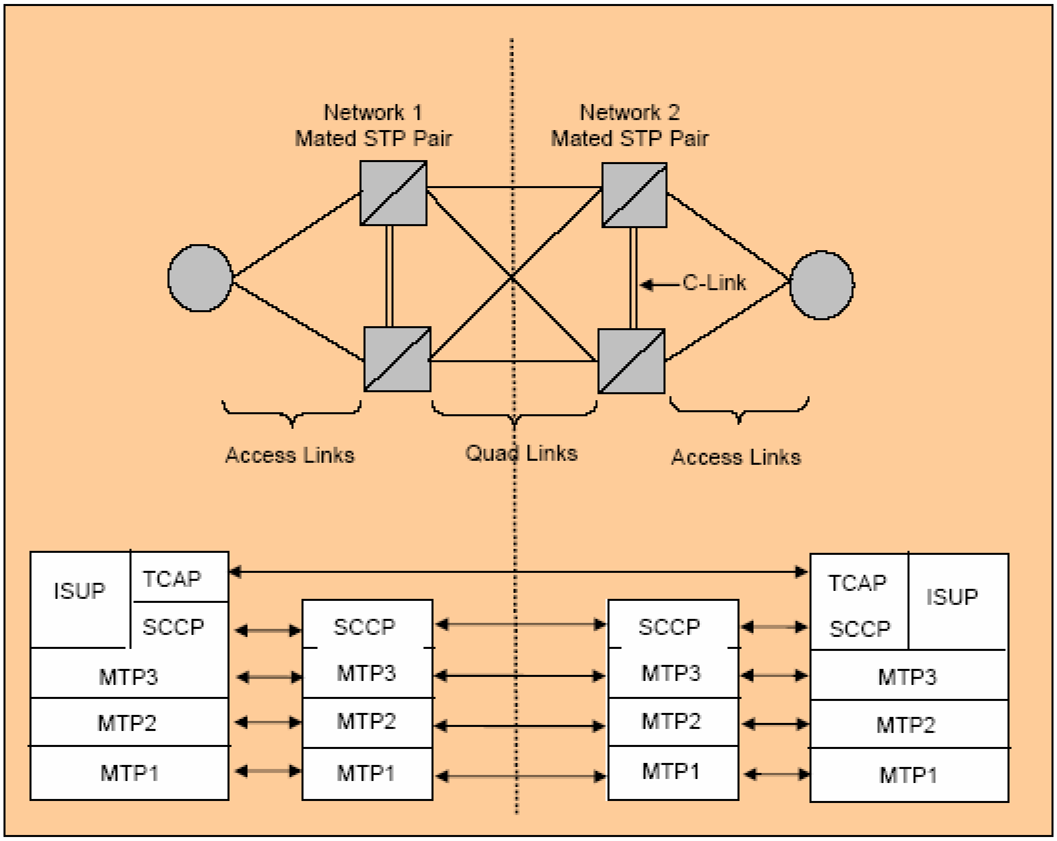

Figure 5 - STP Pair from Network 1 Interconnecting to an STP Pair from Network 2

From a security perspective, the objective is to protect the availability and integrity of the SS7 signaling and the supported services. This involves continuous security planning, development and implementation of security mitigation services, and planning and implementation of security practices/processes to protect the interconnected SS7 network elements and the interconnected interfaces.

9.2.2 General Requirements and Guidelines.

The requirements and guidelines described in Clause 6 are applicable to SS7 network interconnections.

9.2.3 Infrastructure Layer

9.2.3.1 Access and Authentication

The requirements and guidelines described in 6.1 are applicable to SS7 interconnections.

9.2.3.2 Availability

The requirements, objectives and guidelines described in 6.2 are applicable to SS7 network interconnections.

9.2.4 Network Services Layer

9.2.4.1 Access and Authentication

9.2.4.1.1 SS7 Message Screening

Procedures to prevent unauthorized messages on the SS7 network are specified in Clause 8 of chapter T1.111.5 of ATIS-1000111.2005 [3]. These procedures are commonly referred to as gateway screening. *Screening* is a process during which an STP checks the contents of the incoming message and determines whether the message should be accepted or rejected (i.e., whether it is authorized) based on criteria specified by the SS7 network administrator. Historically, it has been assumed that screening is only needed at gateway STPs. However, also supporting screening procedures within a SS7 network domain is necessary to minimize the risks associated with address spoofing or masquerading within a network. Specifically, the screening process allows the SS7 network administrator to control the flow of SS7 messages within an SS7 network. Typically (and as specified in ATIS-1000111.2005 [3]), screening at the STP is focused on lower layer protocol information.

Screening of ISUP and TCAP information is performed at the SS7 application level. For example, an application may make use of the option in T1.655-2001 (R2006) [4] to identify the sender of a TCAP message to determine whether the message is authorized.

Screening functions made available by signaling point manufacturers should be utilized to the fullest extent possible. In addition, network providers should conduct periodic reviews to ensure that screening functions are always active and were not mistakenly deactivated.

<REQ-SEC-SS7-001000>

Procedures to identify unauthorized SS7 messages (i.e. screening procedures) specified in ATIS-1000111.2005, Chapter T1.111.5, clause 8, shall be supported.

<end of REQ-SEC-SS7-001000>

It is recommended that network administrator establish and implement screening rules for each network interconnection. The screening rules should be reviewed periodically and adjusted if necessary.

9.2.4.1.2 MTP Layer Screening

<REQ-SEC-SS7-001100>

Screening procedures shall be supported to verify the validity of Message Signal Units (MSUs), MTP management messages, and parameters. This includes:

- ♦ Verifying that the OPC and DPC are valid and that the OPC is allowed to access the DPC.
- ♦ Verifying validity of MTP management messages and parameters. For a specific MTP management message (e.g., COO, COA, TFP, TFR, TFC, etc.), verify that the originating signaling point is allowed to send it and that the destination signaling point is valid.
- ♦ Verifying the validity of the SIO fields (Service Indicator and Subservice fields).

<end of REQ-SEC-SS7-001100>

<REQ-SEC-SS7-001200>

The following MTP parameters shall be checked during the screening process:

MTP Parameters
Service Information Octet (SIO)
Originating Point Code (OPC)
Destination Point Code (DPC)
Affected Destination (in MTP management messages).
Heading Code (H0 and H1 codes for MTP management messages)

<end of REQ-SEC-SS7-001200>

9.2.4.1.3 SCCP Layer Screening

<REQ-SEC-SS7-001300>

Screening procedures shall be supported to verify the validity of SCCP and SCCP management messages, and SCCP parameters. This includes:

- ♦ Verifying that the Message Type field has a valid value.
- ♦ Verifying whether the originating signaling point is allowed to send the specific message to the destination node.
- ♦ Verifying the validity of the Calling Party Address and Called Party Address.
- ♦ Verifying the validity of parameters in SCCP management messages.

<end of REQ-SEC-SS7-001300>

<REQ-SEC-SS7-001400>

The following SCCP parameters shall be checked during the screening process:

SCCP Parameters
Message Type (e.g., UDT, XUDT)
Calling Party Address (CgPA)
Called Party Address (CdPA) (including Translation Type)
Affected Point Code/Subsystem Number (PC/SSN) in SCCP Management messages

<end of REQ-SEC-SS7-001400>

<REQ-SEC-SS7-001500>

The screening process shall screen SCCP messages and parameters before and after any GTT process.

<end of REQ-SEC-SS7-001500>

9.2.4.1.4 ISUP Screening

<REQ-SEC-SS7-001600>

Screening procedures shall be supported to verify the validity of ISUP messages. This includes:

- Verifying that the Message Type field has a valid value.
- Verifying whether the originating signaling point is allowed to send the specific message to the destination node.

<end of REQ-SECSS7-001600>

<REQ-SEC-SS7-001700>

The following ISUP parameter shall be checked during the screening process:

ISUP Parameter
Message Type (e.g., IAM or ACM)

<end of REQ-SEC-SS7-001700>

9.2.4.1.5 TCAP Screening

<OBJ-SEC-SS7-00300>

It is desirable that the following TCAP information be checked during the screening process:

- TCAP package type (i.e., Unidirectional, Query with Permission, Query without Permission, Response, or Abort).
- Dialogue Portion identification of the sending entity.
- TCAP component type (i.e., Invoke, Return Result, Return Error, or Reject).

<end of OBJ-SEC-SS7-00300>

Application-level screening procedures will include:

- Verifying that a received Terminating Transaction ID refers to a valid transaction.
- Verifying that a received Component ID refers to a valid transaction.
- Verifying that a received operation code is valid in the context of the application.
- Where available, verifying the identified originating application is allowed to send the specific message to the destination application.

9.2.4.2 Message Monitoring

SS7 message screening (described in 9.2.4.1) may not be capable of detecting certain types of intrusion (e.g., message deletion, insertion, and replay). Therefore, each SS7 network provider and administrator should use network specific and implementation specific SS7 message monitoring systems or tools with functions to detect intrusions and attacks that cannot be detected by message screening.

> **<OBJ-SEC-SS7-00400>**
>
> It is recommended that each SS7 network provider and administrators deploy network and implementation specific SS7 monitoring systems or tools capable of detecting attacks or intrusions that cannot be detected by SS7 message screening functions.
>
> **<end of OBJ-SEC-SS7-00400>**

As described in **OBJ-SEC-SS7-00400**, SS7 monitoring solutions are network and implementation specific. Therefore, the specific functions, capabilities, and algorithms for SS7 monitoring systems or tools are not specified in this document. Implementation specific mechanism should be designed to detect attacks and problems (e.g., DoS events, misuse of management messages) through observation and analysis of message patterns (e.g., frequency, contents, message types, etc.). For example, baseline traffic characteristics (norms) can be established and algorithms defined to monitor network traffic. The SS7 message pattern can be compared with the established norms to identify abnormal events. The pattern algorithms could be keyed to the generic SS7 information such as message types (e.g., MTP, SCCP, ISUP, and TCAP message types), information in the message header (e.g., Originating Point Code, Destination Point Code, and Service Indicator), or to detailed application level information (e.g., TCAP and ISUP parameters).

Implementation specific solutions may involve, but are not limited to the following considerations:

- Monitoring at the network level, individual network element level, component or system level, individual protocol level, and at the application/service level.
- Monitoring of generic SS7 information such as message types (e.g., MTP, SCCP, ISU,P or TCAP), address information (e.g., OPC, DPC, and SI), and application level information (ISUP and TCAP parameters) against established norms.
- Monitoring of SS7 traffic volume against established norms**.**

These solutions may be applied globally or may be applied selectively, based on the source of the SS7 traffic.

9.2.4.3 Data Confidentiality

There is no specific protocol mechanism providing confidentiality of an entire SS7 message. The optional TCAP Upper Layer Security Capability provides confidentiality for the TCAP Component Portion of an SS7 message. In the traditional SS7 network, minimizing the risk of observation of SS7 messages (headers and contents) by unauthorized entities depends on the physical security measures recommended for the infrastructure layer, as described in Clause 6, and on the closed environment of the traditional network. The network administrator should be aware of the confidentiality risks that SS7 messages may be observed in an open environment.

9.2.4.4 Privacy

Privacy mechanisms provide protection of certain sensitive information, mostly at the application layer. Assuring privacy may require ensuring data is not observed in transit or when stored. For the SS7 network, the privacy security dimension may be addressed by satisfying the confidentiality security dimension, and ensuring security of the stored data.

9.2.4.5 Data Integrity

Data integrity (including assurance of proper message sequencing) for SS7 messages is provided by the MTP2, SAAL, and MTP3 protocols (e.g., error detection and error correction mechanisms).

9.2.4.6 Availability

The requirements, objectives, and guidelines described in 7.5 are applicable to SS7 network interconnections.

9.2.5 Application Layer

9.2.5.1 Data Confidentiality

The objectives and guidelines described in 8.1 are applicable to SS7 network interconnections.

9.3 Traditional SS7 Network to IP-based Signaling Network Interconnection

This clause discusses traditional SS7 network interconnection to IP-based (e.g., SIP) signaling network. This clause is based on the following assumptions:

- Interconnection to the IP-based signaling network is facilitated by a functional network element -- i.e., a Signaling Gateway (SG) -- providing signaling interworking functions between the two network types.
- The functional SG network element provides a standard SS7 interface to the SS7 network.

There are multiple possible interconnection scenarios, variations and end-to-end combinations (e.g., PSTN/SS7-IP-PSTN/SS7). This standard does not address all the possible variations. The focus is on generic security of the SS7 network to IP-based network interconnection. Specifically, this clause is organized based on two cases that are identified by the protocol interworking at the SG. The two generic cases are described as follows:

1 *SS7 Network Interconnection to IP-based Signaling Network via a SG providing transport protocol interworking*. This generic case represents interconnection architectures where a SG provides

interworking functions between SS7 transport protocols (e.g., SCCP and MTP) and SIGTRAN protocols (e.g., SUA, M3UA, M2PA, M2UA, and SCTP).

2 *SS7 Network Interconnection to IP-based Signaling Network via a SG/PSTN gateway that provides call control protocol interworking*. This generic case represents interconnection architectures where a SG/PSTN network element provides interworking between the SS7 ISUP call control protocol and the IP-based network SIP protocol.

9.3.1 SS7 and IP-based Signaling Network Interconnection Via SG Providing Transport Protocol Interworking

9.3.1.1 Reference Architecture

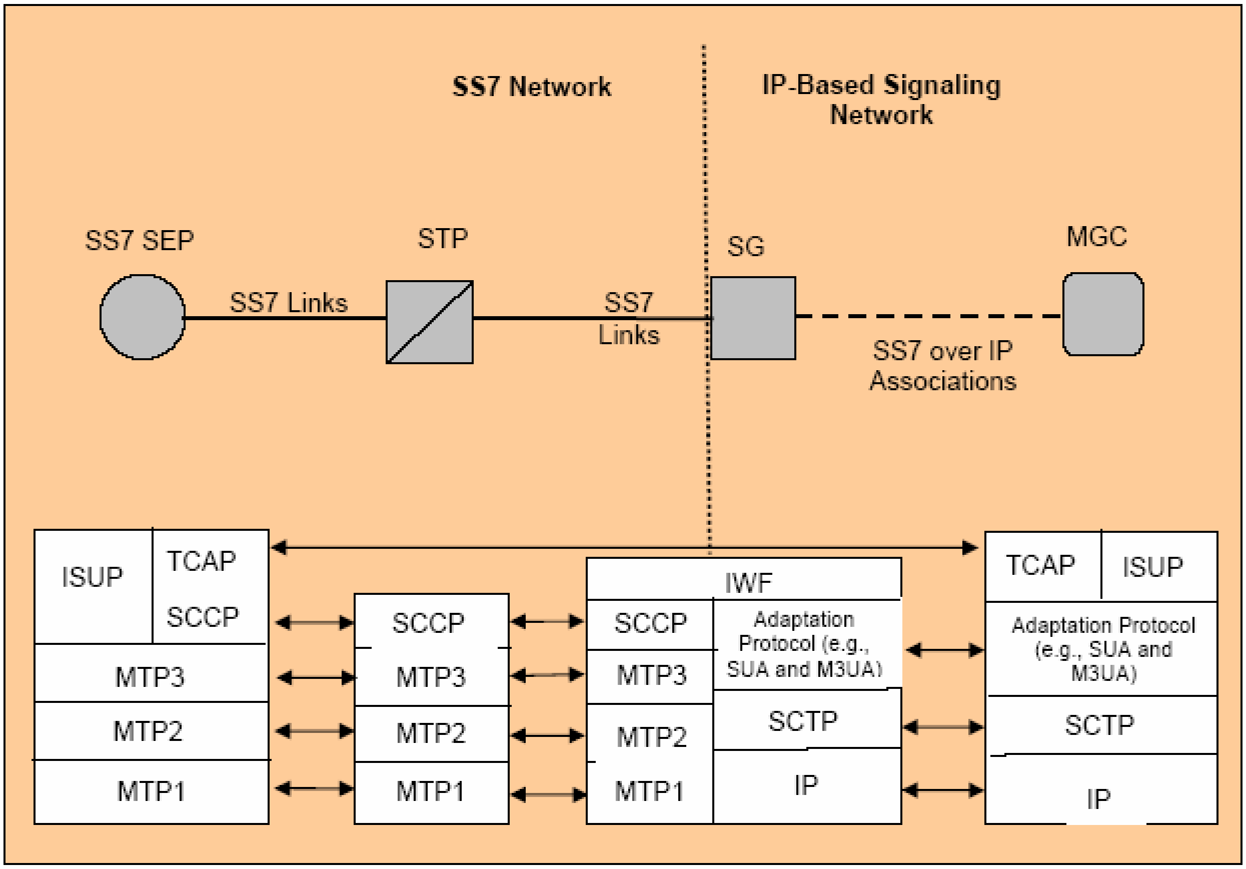

Figure 6 - Reference SS7 and IP-based Signaling Network Interconnection Via SG Providing Transport Protocol Interworking

Figure 6 shows example of a traditional SS7 network interconnecting to an IP-based signaling network via a SG providing transport network protocol interworking. This generic reference model is used to identify the applicable signaling protocols and organize the security requirements in this clause.

From a security perspective, the objective is to protect the availability and integrity of the signaling networks and the supported services and to prevent unauthorized use of the network. This involves continuous security planning, development, and implementation of security mitigation services; and planning and implementation of security practices/processes to protect the interconnected network elements and the interconnected interfaces.

9.3.1.2 General Requirements and Guidelines

9.3.1.2.1 Network Design

The requirements and guidelines described in 5.1 are applicable to SS7 network interconnection to IP-based signaling networks.

9.3.1.2.2 Security Plan, Policy and Practices

The security plan described in 5.2 should include specific rules, policy, and practices for interconnection to IP-based signaling network.

9.3.1.2.3 Network Reliability Interoperability Council (NRIC) Best Practices

NRIC recommended best practices for network reliability and security should be periodically reviewed. Network administrators and vendors should implement NRIC best practices applicable to SS7 network interconnection to IP-based signaling networks.

9.3.1.2.4 Documentation & Specification Safeguard

Guidelines for documentation and specification safeguard described in 5.4 are also applicable to SS7 to IP-based signaling network security.

9.3.1.3 Infrastructure Layer

9.3.1.3.1 Access and Authentication Control

9.3.1.3.1.1 Network Element Access

The guidelines and requirement described in 6.1.1 are applicable to network elements in both network domains, network elements in the SS7 network (e.g., SSPs, STPs and databases), and the interconnected IP-based signaling network (e.g., SGs).

> **<REQ-SEC-SS7-001800>**
>
> The SG shall support security features and mitigation mechanisms for access control as specified in **REQ-SEC-00600**.
>
> **<end of REQ-SEC-SS7-001800>**

9.3.1.3.1.2 Physical Security

Physical security procedures and processes should be implemented to prevent unauthorized access to the physical components and facilities associated with the network interconnection.

It is recommended that procedures and processes be implemented to prevent unauthorized access to the physical components and facilities associated with the SS7 network and the interconnected IP-based signaling network. Specifically, this includes -- but is not limited to -- the following:

- ♦ Access to locations (e.g., central office buildings) containing network elements (e.g., STPs and SGs).
- ♦ Access to any physical component of SS7 link facilities and IP-based network facilities.
- ♦ Access to any physical components, systems, and interface devices of network elements (STPs and SGs).
- ♦ Access to any operations, administration, and maintenance interfaces or devices (maintenance channel, input/output and MOC terminals, etc.) of network elements (e.g., STPs and SGs).

9.3.1.3.2 Availability

9.3.1.3.2.1 Security Arrangements and Diversity/Redundancy

The requirements, objectives, and guidelines described in 6.2 are applicable to SS7 network interconnection to IP-based signaling networks.

<REQ-SEC-SS7-001900>

SS7 network interconnection to IP-based signaling networks shall adhere to the requirements described in 6.2.1.

<end of REQ-SEC-SS7-001900>

<REQ-SEC-SS7-002000>

SS7 network interconnection to IP-based signaling networks shall be designed so that replicated network elements are deployed in diverse geographical locations. Specifically:

- ♦ Mated pairs of STPs shall be deployed in diverse geographical locations so that a common event (e.g., fire, explosion, etc.) would not affect the availability of the interconnection.
- ♦ SGs shall be deployed in diverse geographical locations so that a common event (e.g., fire, explosion, etc.) would not affect the availability of the interconnection.

<end of REQ-SEC-SS7-002000>

It is recommended that the signaling link sets used for interconnection to IP-based signaling network support the diversity objective recommended in **OBJ-SEC-00100**.

The SS7 link diversity management process described in 6.2.1 should be extended to consider the availability of the end-to-end signaling relations. Specifically, it is recommended that equivalent signaling network diversity designs be supported in the IP-based network to allow end-to-end signaling availability. The signaling diversity management process described in 6.2.1 should be include diversity management process and practices for interconnection to IP-based signaling networks. This diversity management process may include:

- Documentation of diversity guidelines for the network interconnection (SS7 side and IP network side).
- Assignment of responsibility and accountability for the network interconnection.
- Tracking and resolving diversity problems.

9.3.1.4 Network Services Layer

9.3.1.4.1 Access and Authentication

9.3.1.4.1.1 SS7 Message Screening

The SS7 message screening requirements and guidelines described in 9.2.4.1.1 are applicable to SS7 network interconnections to IP-based signaling networks.

9.3.1.4.1.2 MTP Layer Screening

<REQ-SEC-SS7-002100>

The SG shall support MTP layer screening as described in 9.2.4.1.2.

<end of REQ-SEC-SS7-002100>

9.3.1.4.1.3 SCCP Layer Screening

<REQ-SEC-SS7-002200>

The SG shall support SCCP layer screening as described in 9.2.4.1.3.

<end of REQ-SEC-SS7-002200>

9.3.1.4.1.4 ISUP Layer Screening

<REQ-SEC-SS7-002300>

The SG shall support ISUP layer screening as described in 9.2.4.1.4.

<end of REQ-SEC-SS7-002300>

9.3.1.4.1.5 TCAP Layer Screening

<OBJ-SEC-SS7-00500>

It is desirable that the SG support TCAP layer screening as described in 9.2.4.1.5.

<end of OBJ-SEC-SS7-00500>

9.3.1.4.1.6 Packet Screening

9.3.1.4.1.6.1 IP Layer Screening

<REQ-SEC-SS7-002400>

The SG shall support screening procedures to verify the validity of signaling packets. This includes:

- Validating the IP address of the originating node (by comparing against a predefined list of authorized IP addressed) indicated in the IP packet.
- Validating the IP address of the destination node (by comparing against a predefined list of IP addresses for the SG).

<end of REQ-SEC-SS7-002400>

9.3.1.4.1.6.2 Transport Layer Screening (SCTP)

<REQ-SEC-SS7-002500>

The SG shall support screening procedures to verify the validity of transport layer protocol (SCTP) address headers. This includes:

- Inspecting and validating the SCTP header, sequence number, and associating these with a valid SCTP association.
- Inspecting and validating the source port number in the SCTP message against predefined rules.
- Inspecting and validating the destination port number in the SCTP message against predefined rules.

<end of REQ-SEC-SS7-002500>

9.3.1.4.1.6.3 Adaptation Layer (SUA, M3UA, M2UA and M2PA) Screening

<REQ-SEC-SS7-002600>

The SG shall support screening procedures to verify the validity of adaptation (SUA, M3UA, M2UA, and M2PA) protocol and management messages, and parameters. This includes:

- Verifying that the adaptation protocol message type is valid.
- Verifying whether the originating signaling point is allowed to send the specific message to the destination node (SG or SS7 node).

- Verifying the validity of the parameters in management messages.

<end of REQ-SEC-SS7-002600>

These procedures may be applied globally or may be applied selectively, based on the source of the traffic. This is true independent of the direction of the traffic (i.e., IP-to-SS7 or SS7-to-IP).

9.3.1.4.2 Message Monitoring Capabilities

For SS7 interconnection to IP-based signaling networks, network providers/administrators should use network specific and implementation specific message monitoring systems or tools with functions to detect intrusions that cannot be detected by screening capabilities -- e.g., message deletion, message insertion and message replay (even if the messages contains valid parameters), and messages in which parameters have been altered.

<REQ-SEC-SS7-002700>

SGs shall support implementation specific monitoring systems or tools capable of detecting attacks or problems through analysis of message patterns (e.g., frequency, contents, message types, etc.) to identify certain threats (e.g., flooding attacks and misuse of management messages).

<end of REQ-SEC-SS7-002700>

Specific functions, capabilities, and algorithms for packet monitoring systems or tools are not specified in this document. Implementation specific mechanism should be designed to detect attacks and problems (e.g., flooding attacks, misuse of management messages) through observation and analysis of packet patterns. For example, baseline traffic characteristics (norms) can be established and algorithms defined to monitor network traffic. The message pattern can be compared with the established norms to identify abnormal events. The pattern algorithms could be keyed to the generic information in the packet message (e.g., IP/port addresses, SCTP header, adaptation protocol address information), or SS7 protocol information (e.g., TCAP and ISUP parameters).

Implementation specific solutions may involve, but are not limited to, the following considerations:

- Monitoring at the network level, individual network element level, component or system level, individual protocol level, and at the application/service level.
- Monitoring of packet level information (IP/port addresses, SCTP addresses, Adaptation protocol address information).
- SS7 protocol address and parameters (e.g., ISUP or TCAP).
- Monitoring of packet traffic volume against established norms.

These solutions may be applied globally or may be applied selectively, based on the source of the traffic.

9.3.1.4.2 Data Confidentiality

The SG shall support at least one IP protocol mechanism (e.g., IPsec) providing confidentiality of the signaled information.

9.3.1.4.3 Privacy

Privacy mechanisms provide protection of certain sensitive information, mostly at the application layer. Assuring privacy may require ensuring data is not observed in transit or when stored. For the SS7 network, the privacy security dimension may be addressed by satisfying the confidentiality security dimension, and ensuring security of the stored data.

9.3.1.4.4 Data Integrity

Data and sequence integrity for SS7 messages in the IP-based signaling network are provided by inherent mechanisms in the SCTP and adaptation protocols (e.g., error detection and error correction mechanisms). Data integrity may also be provided by security mechanisms such as IP Sec or TLS.

9.3.1.4.5 Availability

The requirements, objectives and guidelines described in 7.5 are applicable to SS7 network interconnection to IP-based signaling networks.

> **<REQ-SEC-SS7-002800>**
>
> Each network provider and administrator shall establish and implement network specific plans and best practices for engineering of SGs and IP-based network signaling associations.
>
> **<end of REQ-SEC-SS7-002800>**

> **<REQ-SEC-SS7-002900>**
>
> The SG systems and components message handling capacity shall be engineered to allow for potential failure scenarios without exceeding nominal capacity.
>
> **<end of REQ-SEC-SS7-002900>**

> **<REQ-SEC-SS7-003000>**
>
> The IP-based network signaling associations, virtual links, and virtual link sets shall be engineered to allow for reasonable failure scenarios.
>
> **<end of REQ-SEC-SS7-003000>**

It is recommended that capacity/engineering plans and best practices include processes to continuously monitor the signaling associations and virtual link occupancy (utilization) in the IP-based network.

9.3.2 SS7 Network Interconnection to IP-based Signaling Network Via SG/PSTN Gateway Node Providing Call Control Protocol Interworking.

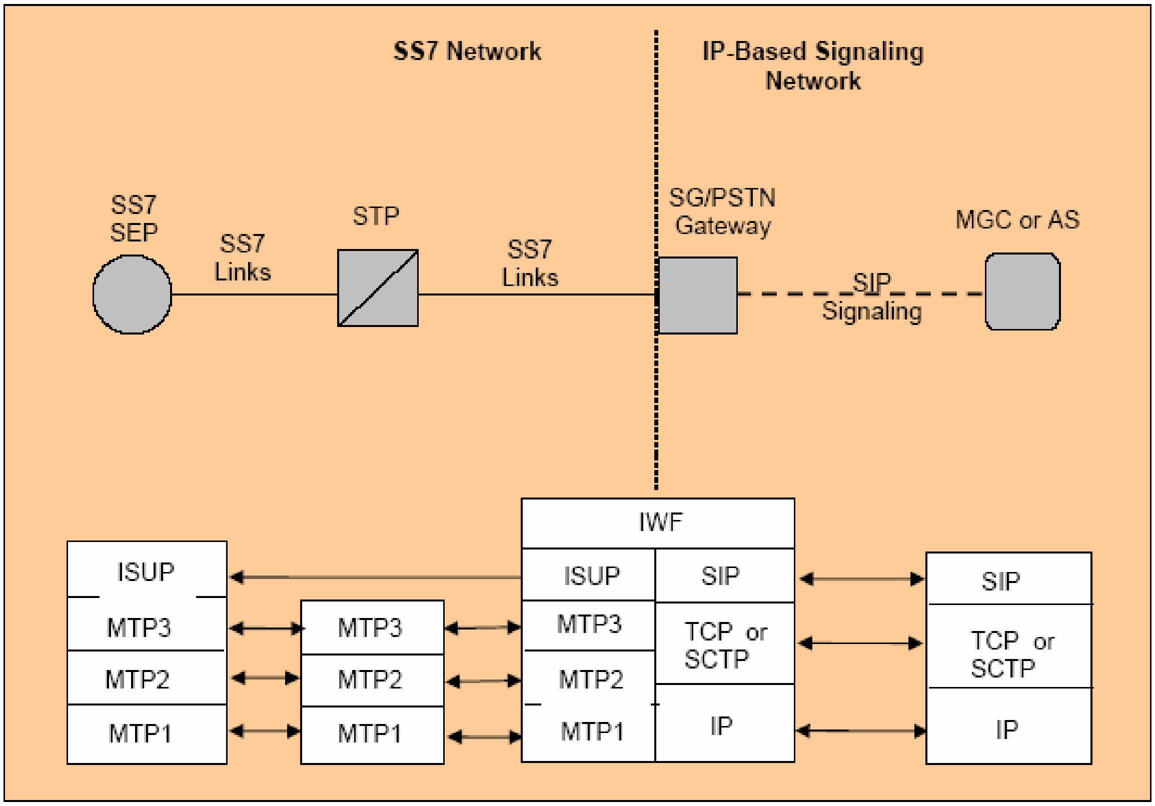

Figure 7 - SS7 Network Interconnection to IP-based Signaling Network Via SG/PSTN Gateway Node Providing Call Control Protocol Interworking

Figure 7 shows example of a traditional SS7 network interconnecting to an IP-based signaling network via a SG/PSTN Gateway providing call control protocol (e.g., ISUP and SIP) interworking. This generic reference model is used to identify the applicable signaling protocols and organize the security requirements in this clause.

From a security perspective, the objective is to protect the availability and integrity of the signaling networks and the supported services and to prevent unauthorized use of the network. This involves continuous security planning, development and implementation of security mitigation services, and planning and implementation of security practices/processes to protect the interconnected network elements and the interconnected interfaces.

9.3.2.1 General Requirements

9.3.2.1.1 Network Design

The requirements and guidelines described in 5.1 are applicable to SS7 network interconnection to IP-based signaling networks.

9.3.2.1.2 Security Plan, Policy, & Practices

The security plan described in 5.2 should include specific rules, policy, and practices for interconnection to IP-based signaling network.

9.3.2.1.3 Network Reliability Interoperability Council (NRIC) Best Practices

NRIC recommended best practices for network reliability and security should be periodically reviewed. Network administrators and vendors should implement NRIC best practices applicable to SS7 network interconnection to IP-based signaling networks.

9.3.2.1.4 Documentation and Specification Safeguard

Guidelines for documentation and specification safeguard described in 5.4 are applicable to SS7 to IP-based signaling network security.

9.3.2.2 Infrastructure Layer

9.3.2.2.1 Access and Authentication Control

9.3.2.2.1.1 Network Element Access

The guidelines and requirement described in 6.1.1 are applicable to network elements in both network domains -- i.e., to network elements in the SS7 network (e.g., SSPs, STPs and databases -- and to network elements in the IP-based signaling network (e.g., SG/PSTN Gateway).

> **<REQ-SEC-SS7-003100>**
>
> The SG/PSTN Gateway shall support security features and mitigation mechanisms for access control as specified in **REQ-SEC 00600**.
>
> **<end of REQ-SEC-SS7-003100>**

9.3.2.2.1.2 Physical Security

Physical security procedures and processes should be implemented to prevent unauthorized access to the physical components and facilities associated with the network interconnection.

It is recommended that procedures and processes be implemented to prevent unauthorized access to the physical components and facilities associated with the SS7 network and the interconnected IP-based signaling network. Specifically, this includes, but is not limited to, the following:

- ♦ Access to locations (e.g., central office buildings) containing network elements (e.g., STPs and SG/PSTN Gateways).
- ♦ Access to any physical component of SS7 link facilities and IP-based network facilities.
- ♦ Access to any physical components, systems, and interface devices of network elements (STPs and SG/PSTN Gateways).
- ♦ Access to any operations, administration, and maintenance interfaces or devices (maintenance channel, input/output and MOC terminals, etc.) of network elements (e.g., STPs and SG/PSTN Gateways).

9.3.2.2.2 Availability

9.3.2.2.2.1 Security Arrangements and Diversity/Redundancy

The requirements, objectives and guidelines described in 6.2 are applicable to SS7 network interconnection to IP-based signaling networks.

<REQ-SEC-SS7-003200>

SS7 network interconnection to IP-based signaling networks shall adhere to the requirements described in 6.2.1.

<end of REQ-SEC-SS7-003200>

<REQ-SEC-SS7-003300>

SS7 network interconnection to IP-based signaling networks shall be designed so that replicated network elements are deployed in diverse geographical locations. Specifically:

- ♦ Mated pairs of STPs shall be deployed in diverse geographical locations so that a common event (e.g., fire, explosion, etc.) would not affect the availability of the interconnection.
- ♦ SG/PSTN Gateways shall be deployed in diverse geographical locations so that a common event (e.g., fire, explosion, etc.) would not affect the availability of the interconnection.

<end of REQ-SEC-SS7-003300>

It is recommended that the signaling link sets used for interconnection to IP-based signaling network support the diversity objective recommended in **OBJ-SEC 00100**.

The SS7 link diversity management process described in 6.2.1 should be extended to consider the availability of the end-to-end signaling relations. Specifically, it is recommended that equivalent signaling network diversity designs be supported in the IP-based network to allow end-to-end signaling availability. The signaling diversity management process described in 6.2.1 should be include diversity management process and practices for interconnection to IP-based signaling networks. This diversity management process should include (but is not limited to):

- Documentation of diversity guidelines for the network interconnection (SS7 side and IP network side).
- Assignment of responsibility and accountability for the network interconnection.
- Periodic review of the network interconnection for proper application of the guidelines.
- Identifying, tracking, and resolving diversity problems.

9.3.2.3 Network Services Layer

9.3.2.3.1 Access and Authentication

9.3.2.3.1.1 SS7 Message Screening

The SS7 message screening requirements and guidelines described in 9.2.4.1.1 are applicable to SS7 network interconnections to IP-based signaling networks.

9.3.2.3.1.2 MTP Layer Screening

<REQ-SEC-SS7-003400>

The SG/PSTN Gateway shall support MTP layer screening as described in 9.2.4.1.2.

<end of REQ-SEC-SS7-003400>

9.3.2.3.1.3 SCCP Layer Screening

<REQ-SEC-SS7-003500>

The SG/PSTN Gateway shall support SCCP layer screening as described in 9.2.4.1.3.

<end of REQ-SEC-SS7-003500>

9.3.2.3.1.4 ISUP Layer Screening

<REQ-SEC-SS7-003600>

The SG/PSTN Gateway shall support ISUP layer screening as described in 9.2.4.1.4.

<end of REQ-SEC-SS7-003600>

9.3.2.3.1.5 TCAP Layer Screening

<OBJ-SEC-SS7-00600>

It is desirable that the SG/PSTN Gateway support TCAP layer screening as described in 9.2.4.1.5.

<end of OBJ-SEC-SS7-00600>

9.3.2.3.1.6 Packet Network Screening

9.3.2.3.1.6.1 IP Layer Screening

<REQ-SEC-SS7-003700>

The SG/PSTN gateway shall support screening procedures to verify the validity of signaling packets. This includes:

- ♦ Validating the IP address of the originating node (by comparing against a predefined list of authorized IP addressed) indicated in the IP packet.
- ♦ Validating the IP address of the destination node (by comparing against a predefined list of IP addresses for the SG).

<end of REQ-SEC-SS7-003700>

9.3.2.3.1.6.2 Transport Layer Screening (SCTP, TCP and UDP)

<REQ-SEC-SS7-003800>

The SG/PSTN Gateway shall support screening procedures to verify the validity of transport layer protocol (SCTP, TCP, or UDP) address headers. This includes:

- ♦ Inspecting and validating the SCTP, TCP, or UDP header, sequence number, and associate it with a valid SCTP, TCP, or UDP association or relation.
- ♦ Inspecting and validating the source port number in the SCTP, TCP, or UDP header against predefined rules.
- ♦ Inspecting and validating the destination port number in the SCTP, TCP, or UDP header against predefined rules.

<end of REQ-SEC-SS7-003800>

9.3.2.3.1.6.3 SIP Screening

<REQ-SEC-SS7-003900>

The SG/PSTN Gateway shall support screening procedures to verify the validity of SIP messages and parameters. This includes:

- ♦ Comparing the interim field (*Via* field) hops (nodes) that the message has traversed to a list of predefined, authorized sources. _*Calls shall only be routed through the SG/PSTN Gateway if they are received from a trusted network entity (e.g., MGC or AS).*
- ♦ Inspecting the *Record-Route* header field based on security/routing policy.

- Inspecting the *Date* field of a SIP message against a list of predefined, authorized date and time schedule.
- Inspecting the *Call-Id* field (in combination with the Message-Tag field where appropriate) to verify if the SIP message is part of a legitimate session control.
- Inspecting the *P-Asserted-Identity* field.

<end of REQ-SEC-SS7-003900>

The SG/PSTN Gateway relies on other network elements in the VoIP network (e.g., SIP servers) through trust relations to assure validity of SIP messages and parameters beyond those described in **REQ-SEC-SS7-003900**.

9.3.2.3.2 Message Monitoring Capabilities

For SS7 interconnection to IP-based signaling networks, each network provider and administrator should use network specific and implementation specific message monitoring systems or tools with functions to detect intrusions that cannot be detected by screening capabilities -- e.g., message deletion, message insertion, and message replay (even if the messages contains valid parameters), and messages in which parameters have been altered.

<REQ-SEC-SS7-004000>

The SG/PSTN Gateway shall support implementation specific monitoring systems or tools capable of detecting attacks or problems through analysis of message patterns (e.g., frequency, contents, message types, etc.) to identify certain threats (e.g., flooding attacks and misuse of management messages).

<end of REQ-SEC-SS7-004000>

Specific functions, capabilities, and algorithms for packet monitoring systems or tools are not specified in this document. Implementation specific mechanism should be designed to detect attacks and problems (e.g., flooding attacks, misuse of management messages) through observation and analysis of packet patterns. For example, baseline traffic characteristics (norms) can be established and algorithms defined to monitor network traffic. The message pattern can be compared with the established norms to identify abnormal events. The pattern algorithms could be keyed to the generic information in the packet message (e.g., IP/port addresses, SCTP, or TCP header, SIP header and protocol parameters), and SS7 protocol information (e.g., TCAP and ISUP parameters).

Implementation specific solutions may involve, but are not limited to the following considerations:

- Monitoring at the network level, individual network element level, component or system level, individual protocol level and at the application/service level.
- Monitoring of packet level information (IP/port addresses, SCTP, or TCP addresses).
- Monitoring SIP protocol address and parameters.
- SS7 protocol address and parameters (e.g., ISUP or TCAP).
- Monitoring of packet traffic volume against established norms.

These solutions may be applied globally or may be applied selectively, based on the source of the traffic.

9.3.2.3.3 Data Confidentiality

The SG/PSTN Gateway shall support at least one IP protocol mechanism (e.g., IPsec) providing confidentiality of SIP messages.

9.3.2.3.4 Privacy

Privacy mechanisms provide protection of certain sensitive information, mostly at the application layer. Assuring privacy may require ensuring data is not observed in transit or when stored. For the SS7 network, the privacy security dimension may be addressed by satisfying the confidentiality security dimension, and ensuring security of the stored data.

Annex A
(informative)

A INFORMATIVE REFERENCES

Telcordia Technologies GR-815-CORE, *Generic Requirements for Network Element/Network System (NE/NS) Security.*[3]

Telcordia Technologies GR-82-CORE, *Signaling Transfer Points (STPs) Generic Requirements.*[4]

Telcordia Technologies GR-905-CORE, *Common Channel Signaling Network Interface Specification (CCSNIS) Supporting Network Interconnection, Message Transfer Part (MTP), and Integrated Services Digital Network User Part (ISDNUP).*[4]

ATIS-0300074, *Guidelines and Requirements for Security Management Systems.*[4]

ATIS-0300276.2008, *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane.*[5]

[3] Telcordia documents are available from Industry Direct Sales, Telcordia, 8 Corporate Place, PYA 3A-184, Piscataway, NJ, 08854-4156, or: < http://telecom-info.telcordia.com >.

[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/default.aspx >