ATIS-0100014

INFORMATION & COMMUNICATIONS SECURITY FOR NGN CONVERGED SERVICES IP NETWORKS AND INFRASTRUCTURE

TECHNICAL REPORT

ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' 17 Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Networked Car, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit < http://www.atis.org >.

ATIS-0100014, *Information & Communications Security for NGN Converged Services IP Networks and Infrastructure*

Is an ATIS Standard developed by the **ATIS Network Performance, Reliability, and Quality of Service Committee (PRQC)**.

Published by

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

ATIS-0100014

Technical Report on

INFORMATION & COMMUNICATIONS SECURITY FOR NGN CONVERGED SERVICES IP NETWORKS AND INFRASTRUCTURE

Alliance for Telecommunications Industry Solutions

Approved October, 2007

Abstract:

This Technical Report provides insight to the applicability of existing security related standards, best practices, regulations, and identifies gaps within said industry specifications. A methodology, by which computing & communications security in IP networks can be systematically addressed will also be provided. The audience for this Technical Report includes industry participants (service providers, product developers, content developers) who are interested in using standards, best practices, etc from inception through operation. This Technical Report is intended to be consistent with current telecom and enterprise standards (such as ANSI, IETF, ITU-T and ISO/IEC standards) and industry best practices (e.g., NIST, NRIC).

.

FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Network Performance, Reliability, and Quality of Service Committee (PRQC) develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. PRQC also develops and recommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

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

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

The PRQC Committee, which was responsible for the development of this document, had the following leadership:

M. Neibert, PRQC Chair

N. Seitz, PRQC Vice-Chair

A. Webster PRQC User Plane Security Task Force Chair

J. Colombo PRQC User Plane Security Task Force Vice-Chair

N. Seitz, PRQC Network QoS Task Force Chair

S. Makris, PRQC Network Reliability Task Force Chair

S. Jacobs, Technical Editor

J. Colombo, Technical Editor

C. Underkoffler, ATIS Chief Editor

Table of Contents

Index of Figures

Index of Tables

ATIS Standard on –

Information & Communications Security for NGN Converged Services IP Networks and Infrastructure

1 Introduction

This Technical Report discusses how to achieve the following security objectives:

- Articulating the security needs of service providers, product developers, and large enterprises as it relates to their functional lifecycle
- Recognizing potential threats & performing vulnerability analysis
- Methodology for developing and using security architectures and using security frameworks
- Understanding how to apply standards, best practices, and governmental regulations
- Recognizing when to use what protocols
- Applying accreditation procedures.

In addition, this Technical Report discusses the role of security policy, guidelines and procedures in achieving these objectives and specific technology related issues.

The development process necessary to produce a secure information system spanning:

- Conceptual definition,
- Functional requirements,
- Functional specifications,
- Software design, implementation and testing,

is beyond the scope of this Technical Report. Likewise, decommissioning is currently beyond the scope of this Technical Report.

This Technical Report provides a user guide for service provider, product developers, and application content developers on how to incorporate security from initiation to decommissioning of services.

This Technical Report is in alignment with the ITU-T X.8xx series Recommendations and ISO/IEC Standard 7498-2 [ISO7498-2]

1.1 Purpose/Goals

This Technical Report (TR) has been developed to help readers understand the standards, best practices, and regulations when considering high level security requirements and deployment of security mechanisms within automated services. The protection of information and system assets is a key consideration in the total view of objectives, threats, performance, interoperability, extensibility, usability, and cost of implementation. This document does not

provide a specification for any particular information system or component. Rather, it specifies security principles and target security capabilities that can be used to guide system security architects in creating specific security architectures that are consistent with this document. As security technology improves, and products incorporate these concepts, specific information systems will achieve more consistency with their individual security-related goals.

The information in this document was developed in the context of NGN services provided by large, highly interconnected Telecommunications Service Providers (TSPs). This includes IP-based transport of voice and data, along with the associated control signaling and management functions. However, the majority of the standards, best practices, and other descriptions of security functionality referenced by this TR apply to a much wider context. In particular, the TR applies to all enterprises (organizations):

- Large and small
- Public and private
- Commercial, non-profit, and governmental.

In particular this document will provide useful guidance to those responsible for information security, which spans both computer and communications security. In particular, the personnel responsible for information security related activities include (a) service provider personnel (b) developers, manufacturers (c) large enterprises such as government agencies. For simplicity, the text usually refers only to Telecommunications Service Providers (TSPs).

This TR can be used to assist in the understanding and determination of:

- Security needs at each point in a functional lifecycle where the functional lifecycle is based on either a service provider, manufacturer/developer, or large enterprise include governmental organizations.
- Security needs driving the complete functional lifecycle for a network: request for information, procurement, deployment-fielding, and OAM&P.
- Security needs driving the complete functional lifecycle for a systems developer: product planning, design development, production, service, and retirement or discontinuation
- Applicability of legislation or regulation specifics for manufacturers, governmental organizations and service providers.
- Which global industry known best practices, regulations, and standards, as of this date of publication, will provide useful guidance in the development of a security program.
- End-to-end and hop-by-hop security needs based on the nature of information flows.

In addition, many of the security aspects of this TR assume pair-wise communication between network nodes. The TR makes no assumption whether the communicating nodes are:

- Owned and operated by one organization
- Owned by one organization but operated by multiple organizations
- Owned by multiple organizations but operated by one organization
- Owned and operated by multiple organizations.

In some cases, reference is made to industry-recognized documents with a narrower scope, e.g., specifications of security requirements at the application layer for a Voice over IP network. These references should be recognized as examples of the application of the principles in this

TR and not as an endorsement of the particular elements of those documents as applying in a broader context.

Readers of this TR will be able to:

- Recognize the what, why, and when to use a security standard or guideline
- Reference and use the illustrative functional lifecycle examples to reinforce the importance and the “how to use” of standards
- List and use threat models to support their specific needs
- Use an example use case to help guide their specific needs
- Use the included comprehensive list of reference sources.

This TR was developed to draw together various information system architectural activities, applications needs, information transport systems, programs, and relevant standards resulting in consistent, efficient, and interoperable solutions from security design to decommissioning of converged services and the next generation infrastructures. Throughout this TR the term Information Security is used to represent a superset containing both communications and computer security.

The justification for using the term Information Security in this manner is that the historically separate architectural communities of communications and computing space are converging. This paradigm shift represents a merger of areas that have focused for decades on differing types of services, customer expectations, technology foundations, operational perspectives.

1.2 References

1.2.1 Identical Recommendations / International Standards

International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) Recommendations[1]	International Organization for Standardization (ISO) Standards[2]
X.200, 1994-07, "Information technology - Open Systems Interconnection - Basic Reference Model: The basic model"	ISO 7498-1, 1994, "Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model"
X.700, 1992-09, "Management framework for Open Systems Interconnection (OSI) for CCITT applications"	ISO 7498-4, 1989, "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management framework"
X.800, 1991-03, "Security architecture for Open Systems Interconnection for CCITT applications"	ISO 7498-2, 1989, "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture"
X.810, 1995-11, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview"	ISO 10181-1, 1996-08-01, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview"
X.811, 1995-04, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework"	ISO 10181-2, 1996-05-15, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework"
X.812, 1995-11, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework"	ISO 10181-3, 1996-09-15, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework"

[1] These documents are available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[2] These documents are available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) Recommendations[1]	International Organization for Standardization (ISO) Standards[2]
X.813, 1996-10, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework"	ISO 10181-4, 1997-04-01, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework"
X.814, 1995-11, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework"	ISO 10181-5, 1996-09-15, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework"
X.815, 1995-11, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework"	ISO 10181-6, 1996-09-15, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework"
X.816, 1995-11, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework"	ISO 10181-7, 1996-08-01, "Information technology - Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework"
ITU-T X.803, 1994-07, "Information Technology - Open Systems Interconnection - Upper Layers Security Model"	ISO 10745, 1995, " Information technology - Open Systems Interconnection - Upper layers security model"

1.2.2 International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) Recommendations[3]

G.983	Broadband optical access systems based on Passive Optical Networks (PON)
G.984	General characteristics for Gigabit-capable Passive Optical Networks (GPON), March 2003
H.248.1	Gateway control protocol: Version 3
H.323	Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service
I.430	Integrated Services Digital Network (ISDN) ISDN User-Network Interfaces, Basic User-Network Interface - Layer 1 Specification
I.431	Integrated Services Digital Network (ISDN) ISDN User-Network Interfaces, Primary Rate User-Network Interface - Layer 1 Specification
M.3016.x	Security for the management plane series of Recommendations
Q.811	Lower layer protocol profiles for the Q and X interfaces
Q.812	Upper layer protocol profiles for the Q and X interfaces
Q.930	Digital Subscriber Signalling System No. 1 (DSS 1) ISDN User-Network Interface Layer 3 General Aspects
Q.931	Digital Subscriber Signalling System No. 1 (DSS 1) ISDN User-Network Interface Layer 3 Specification For Basic Call Control
X.500	Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services
X.509v3	Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks
X.803	Information Technology – Open Systems Interconnection – Upper Layers Security Model
X.805	Security architecture for systems providing end to end communications
Y.2011	General principles and general reference model for Next Generation Network

[3] These documents are available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

Y.2012	Functional requirements and architecture of the NGN of Release 1
Y.2201	NGN release 1 requirements
Y.2701	Security requirements for NGN release 1

1.2.3 International Organization for Standardization (ISO) Standards[4]

ISO/IEC 9001	" Quality management systems - Requirements"
ISO/IEC 9004	" Quality management systems -- Guidelines for performance improvements"
ISO/IEC 9595	"Information Processing Systems - Open Systems Interconnection - Common Management Information Service Definition"
ISO/IEC 9798-1	Information technology - Security techniques - Entity authentication - Part 1: General
ISO/IEC 9798-5	Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero knowledge techniques
ISO/IEC 10007	Quality management systems -- Guidelines for configuration management
ISO/IEC 10116	Information technology - Modes of operation for an n-bit block cipher algorithm
ISO/IEC 15408-1	Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
ISO/IEC 17799:2005 BS 7799-1	Information technology - Security techniques - Code of practice for information security management
ISO/IEC 27000	a vocabulary or glossary of terms used in the ISO 27000-series standards
ISO/IEC 27001	"Information Security Management - Specification With Guidance for Use"
ISO/IEC 27002	the proposed re-naming of existing standard ISO 17799
ISO/IEC 27003	a new ISMP implementation guide
ISO/IEC 27004	a new standard for information security measurement and metrics
ISO/IEC 27005	a proposed standard for risk management, potentially related to the current British Standard BS 7799 part 3
ISO/IEC 27006	a guide to the certification/registration process

1.2.4 ATIS References[5]

ATIS 1000007.2006	Generic Signaling and Control Plane Security Requirements for Evolving Networks
ATIS 1000012.2006	Traditional SS7/BICC Network and NNI Interconnection Security
ATIS 1000019.2007	Network to Network Interface (NNI) Standard for Signaling and Control Security for Evolving VoP/Multimedia Networks
ATIS-0300276.2008	Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane.
ATIS-0300074.2006	Guidelines and Requirements for Security Management Systems
TR-069	"CPE WAN Management Protocol", DSL Forum TECHNICAL REPORT, May 2004

1.2.5 Internet Engineering Task Force (IETF) References[6]

RFC 768	User Datagram Protocol, 28 August 1980
RFC 791	INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981

[4] This document is available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

[5] These documents are 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 >

[6] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

RFC 793	TRANSMISSION CONTROL PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981
RFC 826	An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware, November 1982
RFC 1013	X WINDOW SYSTEM PROTOCOL, VERSION 11, June 1987
RFC 1157	A Simple Network Management Protocol (SNMP), May 1990
RFC 1305	Network Time Protocol (Version 3), Specification, Implementation and Analysis, March 1992
RFC 1321	The MD5 Message-Digest Algorithm, April 1992
RFC 1350	THE TFTP PROTOCOL (REVISION 2), July 1992
RFC 1446	Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2), April 1993
RFC 1831	RPC: Remote Procedure Call Protocol Specification Version 2, August 1995
RFC 1945	Hypertext Transfer Protocol -- HTTP/1.0, May 1996
RFC-2119	Key words for use in RFCs to Indicate Requirement Levels, March 1997
RFC 2131	Dynamic Host Configuration Protocol, March 1997
RFC 2228	FTP Security Extensions, October 1997.
RFC 2246	The TLS Protocol Version 1.0, January 1999
RFC 2401	Security Architecture for the Internet Protocol, November 1998
RFC 2402	IP Authentication Header, November 1998
RFC 2403	The Use of HMAC-MD5-96 within ESP and AH, November 1998
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH, November 1998
RFC 2405	The ESP DES-CBC Cipher Algorithm With Explicit IV, November 1998
RFC 2406	IP Encapsulating Security Payload (ESP), November 1998
RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP, November 1998
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP), November 1998
RFC 2409	The Internet Key Exchange (IKE), November 1998
RFC 2410	The NULL Encryption Algorithm and Its Use With IPsec, November 1998
RFC 2451	The ESP CBC-Mode Cipher Algorithms, November 1998
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 1999
RFC 2960	Stream Control Transmission Protocol, October 2000
RFC 3118	Authentication for DHCP Messages, June 2001
RFC 3149	MGCP Business Phone Packages, September 2001
RFC 3209	RSVP-TE: Extensions to RSVP for LSP Tunnels
RFC 3261	SIP: Session Initiation Protocol, June 2002
RFC 3268	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer, Security (TLS), June 2002
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3); December 2002
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002
RFC 3436	Transport Layer Security over Stream Control Transmission Protocol, December 2002
RFC 3456	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode, January 2003
RFC 3472	Generalized Multi-Protocol Label Switching (GMPLS) Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions
RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003
RFC 3534	Media Gateway Control Protocol (MGCP) Version 1.0, January 2003.
RFC 3546	Transport Layer Security (TLS) Extensions, June 2003
RFC 3550	RTP: A Transport Protocol for Real-Time Applications, July 2003
RFC 3554	On the Use of Stream Control Transmission Protocol (SCTP) with IPsec, July 2003
RFC 3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec, September 2003
RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec, September 2003
RFC 3664	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE), January 2004
RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP), January 2004
RFC 3711	The Secure Real-time Transport Protocol (SRTP), March 2004
RFC 3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model, June 2004

RFC 3830	MIKEY: Multimedia Internet KEYing, August 2004
RFC 3947	Negotiation of NAT-Traversal in the IKE, January 2005
RFC 3948	UDP Encapsulation of IPsec ESP Packets, January 2005
RFC 4030	The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option, March 2005
RFC 4033	DNS Security Introduction and Requirements, March 2005
RFC 4034	Resource Records for the DNS Security Extensions, March 2005
RFC 4035	Protocol Modifications for the DNS Security Extensions, March 2005.
RFC 4086	Randomness Requirements for Security, June 2005
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), June 2005
RFC 4109	Algorithms for Internet Key Exchange version 1 (IKEv1), May 2005
RFC 4217	Securing FTP with TLS, October 2005
RFC 4251	The Secure Shell (SSH) Protocol Architecture, January 2006
RFC 4252	The Secure Shell (SSH) Authentication Protocol, January 2006
RFC 4253	The Secure Shell (SSH) Transport Layer Protocol, January 2006
RFC 4256	Generic Message Exchange Authentication for the Secure Shell Protocol (SSH), January 2006
RFC 4279	Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), December 2005
RFC 4282	The Network Access Identifier, December 2005
RFC 4301	Security Architecture for the Internet Protocol, December 2005
RFC 4302	IP Authentication Header, December 2005
RFC 4303	P Encapsulating Security Payload (ESP), December 2005
RFC 4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP), December 2005
RFC 4306	Internet Key Exchange (IKEv2) Protocol, December 2005
RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2), December 2005
RFC 4308	Cryptographic Suites for IPsec, December 2005
RFC 4309	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP), December 2005
RFC 4344	The Secure Shell (SSH) Transport Layer Encryption Modes
RFC 4345	Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol, January 2006
RFC 4346	The Transport Layer Security (TLS) Protocol Version 1.1, April 2006
RFC 4347	Datagram Transport Layer Security, April 2006
RFC 4359	The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH), January 2006
RFC 4419	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol, March 2006
RFC 4432	RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol, March 2006
RFC 4434	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE), February 2006
RFC 4470	Minimally Covering NSEC Records and DNSSEC On-line Signing, April 2006
RFC 4494	The AES-CMAC-96 Algorithm and Its Use with IPsec, June 2006
RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006
RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol, June 2006
RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models, June 2006
RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms, June 2006
RFC 4543	The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH, May 2006
RFC 4567	Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP), July 2006
RFC 4568	Session Description Protocol (SDP) Security Descriptions for Media Streams, July 2006
RFC 4615	The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE), August 2006
RFC 4650	HMAC-Authenticated Diffie-Hellman for Multimedia Internet KEYing (MIKEY); September 2006
RFC 4718	IKEv2 Clarifications and Implementation Guidelines, October 2006
RFC 4738	MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY), November 2006

RFC 4785	Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS), January 2007
RFC 4819	Secure Shell Public Key Subsystem, March 2007
RFC 4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)., April 2007.
RFC 4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, May 2007
RFC 4869	Suite B Cryptographic Suites for IPsec, May 2007
RFC 4895	Authenticated Chunks for the Stream Control Transmission Protocol (SCTP), August 2007

1.2.6 Institute of Electrical and Electronics Engineers (IEEE) References[7]

IEEE 802.1q	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, December 1998
IEEE 802.1x	IEEE Standards for Local and Metropolitan Area Networks: Port-Based network Access Control, December 2004
IEEE 802.3	IEEE Standard for Information technology— Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, December 2005
IEEE 802.11a	Supplement to IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band, June 2003
IEEE 802.11b	Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, June 2003
IEEE 802.11i	IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, July 2004

1.2.7 Government References[8]

DoD Standard 5200.28	Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), Dec 1985
ITSEC	Information Technology Security Evaluation Criteria Ver 1.2, Department of Trade and Industry, London, June 1991
FIPS 180-2	Secure Hash Standard
FIPS 197	Federal Information Processing Standards Publication (FIPS) 197, " ADVANCED ENCRYPTION STANDARD (AES)", NIST, November 2001
NIST 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems
NISTIR 7359	Information Security Guide for Government Executives

1.2.8 Other References

CMMI for Development, Version 1.2 Model, August 2006[9]
GAISP V3.0, "Generally Accepted Information Security Principles", May 2006[10]
PKCS 12 v1.0: Personal Information Exchange Syntax, RSA Laboratories, June 24, 1999[11]

[7] These documents are available from the Institute of Electrical and Electronics Engineers (IEEE). < http://shop.ieee.org/store/ >

[8] These documents are available from the Government Printing Office at < http://bookstore.gpo.gov/ >.

[9] This document is available from <www.sei.cmu.edu>

[10] This document is available from <www.gaisp.org>.

1.2.9 ETSI References[12]

TS 102 165-1	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis
TS 102 165-2	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures
TR 102 420	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security
TS 102 556	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protection Profile
TS 187 001	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements
TR 187 002	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat and Risk Analysis
TS 187 003	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture
ES 202 382	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles
ES 202 383	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets
EG 202 387	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables
EG 202 549	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities

2 Definitions

This TR uses the definitions of security related terms from ATIS-0100523.2007[13]. The sections below list terms above and beyond those found in the Glossary.

2.1 Basic Reference Model definitions

This Technical Report makes use of the following general security-related terms defined in ITU-T Rec. X.200 (ISO/IEC 7498-1):

(N)-connection;	(N)-data-transmission;	(N)-entity;
(N)-facility;	(N)-layer;	Open system;
Peer entities;	(N)-protocol;	(N)-protocol-data-unit;
(N)-relay;	Routing;	Sequencing;
(N)-service;	(N)-service-data-unit ((N)-SDU);	(N)-user-data;
(N)-unitdata	(N)-userdata	Sub-network;

[11] This document is available from < http://www.rsa.com/rsalabs >

[12] These documents are available from the European Telecommunications Standards Institute (ETSI). < http://www.etsi.org/getastandard/home.htm >

[13] This document can be found at < http://www.atis.org/glossary/ >.

Segmenting;	OSI resource	Transfer syntax;
End system;	application process;	entity;
facility;	function;	real open system;
real system.	service.	

2.2 Security architecture definitions

This Technical Report makes use of the following terms defined in ITU-T Rec. X.800 (ISO 7498-2):

access control list;	access control;	Accountability;
Active threat;	audit (also security audit);	audit trail;
authentication exchange;	authentication information;	authentication;
authorization;	availability;	capability;
channel;	ciphertext;	cleartext;
confidentiality;	connection integrity;	credentials;
cryptanalysis;	cryptographic check value:	cryptography;
data integrity (also integrity);	data origin authentication;	decipherment;
decryption;	denial of service;	digital signature (also signature);
encipherment;	encryption;	end-to-end encipherment
identity-based security policy;	insider threat;	integrity;
key management;	key;	link-by-link encipherment;
manipulation detection;	masquerade;	notarization;
outsider threat;	passive threat;	password;
peer-entity authentication;	physical security;	plaintext;
policy;	privacy;	repudiation;
routing control;	rule-based security policy;	security audit trail (also audit trail, log);
Security Audit;	security label;	security policy;
security service;	selective field protection.	sensitivity;
signature;	threat.	Traffic analysis
Traffic flow confidentiality	Traffic padding	Trusted functionality

2.3 Security framework definitions

This Technical Report makes use of the following general security-related terms defined in ITU-T Rec. X.810 (ISO/IEC 10181-1):

asymmetric cryptographic algorithm;	certification authority;	conditionally trusted entity;
cryptographic chaining;	digital fingerprint;	distinguishing identifier;
hash function;	one-way function;	one-way hash function;
private key;	public key;	revocation certificate;
revocation list certificate;	seal;	sealed;
secret key;	secure interaction policy;	secure interaction rules;
security administrator;	security authority;	security certificate chain;

security certificate;	security domain authority;	security domain;
security information;	security policy rules;	security recovery;
security token;	symmetric cryptographic algorithm;	trust;
trusted entity;	trusted third party;	unconditionally trusted entity;

This Technical Report makes use of the following general security-related terms defined in ITU-T Rec. X.811 (ISO/IEC 10181-2):

Asymmetric authentication method;	Authenticated identity;	Authentication certificate;
authentication initiator;	challenge;	claim authentication information (Claim AI);
claimant;	exchange authentication information (exchange AI);	entity authentication;
off-line authentication certificate;	on-line authentication certificate;	principal;
Symmetric authentication method;	time variant parameter;	unique number;
verification authentication information (verification AI);	verifier;	

This Technical Report makes use of the following general security-related terms defined in ITU-T Rec. X.812 (ISO/IEC 10181-3):

access control certificate;	Access Control Decision Information (ADI);
Access Control Decision Function (ADF);	Access Control Enforcement Function (AEF);
Access Control Information (ACI);	access control policy;
access control policy rules;	access control token;
access request;	access request access control decision information; access request ADI;
access request access control information; access request ACI;	access request-bound access control information; access request-bound ACI;
clearance;	contextual information;
initiator;	initiator access control decision information; initiator ADI;
initiator access control information; initiator ACI;	initiator-bound access control information; initiator-bound ACI;
operand access control decision information; operand ADI;	operand access control information; operand ACI;
operand-bound access control information; operand-bound ACI;	retained ADI;
target;	target access control decision information; target ADI;
target access control information; target ACI;	target-bound access control information; target-bound ACI;

This Technical Report makes use of the following general security-related terms defined in ITU-T Rec. X.813 (ISO/IEC 10181-4):

compromised evidence;
counter-signature;
evidence;
evidence generator;
evidence subject;
evidence user;
evidence verifier;
message authentication code;
Non-repudiation service requester;
notary;
originator;
recipient;

This Technical Report makes use of the following general security-related terms defined in ITU-T Rec. X.814 (ISO/IEC 10181-5):

Confidentiality-protected-environment;
Confidentiality-protected-data;
Confidentiality-protected-information;
hide;
reveal;
hiding confidentiality information;
revealing confidentiality information;
direct attack;
indirect attack;

This Technical Report makes use of the following general security-related terms defined in ITU-T Rec. X.815 (ISO/IEC 10181-6):

Integrity-protected channel;
Integrity-protected data;
Shield;
Unshield;
Validate;

This Technical Report makes use of the following general security-related terms defined in ITU-T Rec. X.816 (ISO/IEC 10181-7):

alarm processor;
audit authority;
audit analyzer;
audit archive;
audit dispatcher;
audit trail examiner;
audit recorder;
audit provider;
audit trail collector;
event discriminator;
security alarm;
security alarm administrator;
security-related event;
security audit message;
security audit record;
security auditor;
security report;

2.4 Additional definitions

This Technical Report makes use of the following general security-related terms defined in ISO/IEC 9798-1:

asymmetric Encypherment system;
asymmetric key pair;
asymmetric signature system;
cryptographic check function;
interleaving attack;
mutual authentication;
private decipherment key;
private signature key;
public Encypherment key;
public key certificate (certificate);
public key information;
public verification key;
random number;
reflection attack;
replay attack;
sequence number;
symmetric cryptographic technique;
symmetric Encypherment algorithm;
time stamp;
token;
unilateral authentication;

This Technical Report makes use of the following general security-related terms defined in ISO/IEC 9798-5:

accreditation authority;
accreditation multiplicity parameter;
exchange multiplicity parameter;
identification data;
private accreditation exponent;
private accreditation information;
private decipherment transformation;
public accreditation verification exponent;
public Encypherment transformation;
redundant identity;
response;
witness;

This Technical Report makes use of the following general security-related terms defined in ISO/IEC 11586-1:

Presentation-context-bound security association;
Single-item-bound security association;
Externally-established security association;
initial encoding rules;
protecting presentation context;
protecting transfer syntax;
protection mapping;

This Technical Report makes use of the following general security-related terms defined in ITU-T X.803 (ISO/IEC 10745):

Association security state;
security association;
security communication function (SCF);
security exchange item;
security exchange function;
Security state;
security exchange;
System security function;
security transformation;
system security object (SSO).

This Technical Report makes use of the following general security-related terms defined in ITU-T X.700 (ISO/IEC 7498-4):

Managed Object;
Management information base (MIB);

This Technical Report makes use of the following general security-related terms defined in ISO/IEC 7498/AD1:

Connectionless-mode transmission

This Technical Report makes use of the following general security-related terms defined in ISO/IEC 10116:

block chaining;

This Technical Report makes use of the following general security-related terms defined in ISO/IEC 17799:

asset
control
guideline
information processing facilities
information security
information security event
information security incident
risk
risk analysis
risk assessment
risk evaluation
risk management
risk treatment
third party
vulnerability

This Technical Report makes use of the following general security-related terms defined in ISO/IEC 15408-1:

evaluation authority	evaluation scheme	extension
external IT entity	family	formal
guidance documentation	human user	identity
informal	element	evaluation
evaluation assurance level (EAL)	iteration	object
organizational security policies	package	product
protection profile (PP)	reference monitor	reference validation mechanism
refinement	role	internal communication channel
internal TOE transfer	inter-TSF transfers	security function policy (SFP)
security objective	security target (ST)	selection
semiformal	strength of function (SOF)	SOF-basic
SOF-medium	SOF-high	subject
secret	security attribute	security function (SF)
TOE security functions (TSF)	TOE security functions interface (TSFI)	TOE security policy (TSP)
TOE security policy mode	transfers outside TSF control	trusted channel
trusted path	TSF data	TSF scope of control (TSC)
user	user data	system
target of evaluation (TOE)	TOE resource	

2.5 New Definitions

The definition of ***certification*** used in this document is: The process/technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

The definition of ***Auditing*** used in this document is: The examination of networks and computer systems by an independent consultant, within a defined scope which may include; determination of an organization's compliance to specified standards and best practices, determination of an organization’s vulnerability to criminal invasion (crackers, virus impact on management, end-use and, control traffic on end-to-end solution, etc.) and determination of an organization’s vulnerability to natural disasters (fire, tornados, earthquakes, etc.).

3 Abbreviations and Acronyms

3DES	Triple DES
ACI	Access Control Information
ACK	Acknowledgment

ADI	Access Control Decision Information
ADF	Access Control Decision Function
ADM	Add-Drop Multiplexer, Layer 2 Optical Intermediate Element
AEF	Access Control Enforcement Function
AER	Service Provider Application Edge Router
AES	Advanced Encryption Standard
AH	Authentication Header
AI	authentication information
AL	Application Layer
ARP	Address Resolution Protocol
ASE	application-service-element
ASO	application-service-object
ATM	Asynchronous Transport Mode Network
BCP	Best Current Practice
BGP	Border Gateway Protocol
BIOS	Basic Input/Output System
BLP	Bell La-Padula
BML	Business Management Layer
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CDI	Constrained Data Item
CEM	Common Evaluation Criteria
CEN	Customer end node
CER	Customer Edge Router
CGI	Common Gateway Interface
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
COTS	commercial off-the-the-shelf
CRL	Certificate Revocation List
CS	Customer/Subscriber
DBMS	Database Management System
DCE	Distributed Computing Environment
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DLL	Data Link Protocol Layer
DMO	Direct Mode Operation
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial-of-Service
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Module
DSLM	DSL Modem
DTLS	Datagram Transport Layer Security
EAL	Evaluation Assurance Level
ECC	Error Correcting Code

EG	ETSI Guide
EML	Element Management Layer
EMS	Element Management System
E-NNI	External Network-Network Interface
ES	ETSI Standard
ESP	Encapsulation Security Payload
FCAPS	Fault, Configuration, Accounting, Performance and Security Management
FCC	Federal Communications Commission
FR	Frame Relay
FTP	File Transfer Protocol
FW	Firewall
GAAP	Generally Accepted Accounting Principles
GAISP	Generally Accepted Information Security Practices
GASSP	Generally Accepted System Security Principles
GLBA	Gramm-Leach-Bliley Act
GP	General Purpose
GULS	Generic Upper Layers Security
HCI	Hiding Confidentiality Information
HMAC	Hashed Messaged Authentication Code
HRU	Harrison-Ruzzo-Ullman
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICMP	Internet Control Message Protocol
ICT	Information, Communications, Technologies
IDS	Intrusion Detection System
I/F	Interface
IFS	Internal Field Separator
IKE	Internet Key Exchange
IL	Inter-networking Protocol Layer
IMS	IP Multimedia Subsystem
I-NNI	Internal Network-Network Interface
IP	Internet Protocol
IPG	Information Program Guide
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPTV	Internet Protocol Television
ISDN	Integrated Services Digital Network
ISMP	Information Security Management Program
ISMS	Information Security Management Systems
ISSA	Information Systems Security Association
IT	Information Technology
ITSEC	Information Technology Security
IVP	Integrity verification procedure
KPA	Key Process Area
L2E	Layer 2 Intermediate Element
LAN	Local Area Network
LDAP	Light-Weight Directory Protocol
LEA	Law Enforcement Agency

MD	Message Digest
MAC	Media Access Control
MAC	Message Authentication Code
MBRA	Model-Based Risk Assessment
MDII	Modification Detection Integrity Information
MGC	Media Gateway Controller
MIB	Management information base
MLS	Multi-level Security
MPLS	Multi-protocol Label Switching
NASS	Network Attachment Subsystem
NAT	Network Address Translation
NDS	Network Domain Security
NEL	Network Element Layer
NGN	Next Generation Network
NIS	Network Information Service
NML	Network Management Layer
NNI	Network-Network Interface
NRIC	Network Reliability and Interoperability Council
NT	Network Termination
NTP	Network Time Protocol
OAM&P	Operations, Administration, Maintenance and Provisioning
OCSP	Online Certificate Status Protocol
OLT	Optical Line Terminator
ONT	Optical Network Terminator
OPSF	Open Shortest Path First
OS	Operating System
OSI	Open Systems Interconnection
OSS	Operations Support System
PCI	Payment Card Industry
PCR	Service Provider Core Router
PDU	Protocol Data Unit
PDV	Presentation Data Value
PER	Service Provider Edge Router
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
POTS	Plain-old Telephone System
PP	Protection Profile
PPR	Service Provider Peering Router
PRI	Primary Rate Interface
PSTN	Public switched Telephone Network
RA	Registration Authority
RAID	Redundant Array of Independent Disks
RBAC	Role-based Access Control
RCI	Revealing Confidentiality Information
RFC	Request for Comments
RIP	Routing Internet Protocol
ROM	Read-only Memory
RSA	Rivest, Shamir, Adleman

RSVP	Resource Reservation Protocol
RTOS	Real-time Operating System
RTP	Real-time Transfer Protocol
RVM	Reference Validation Mechanism
SA	Security Association
SAML	Security Assertion Markup Language
SCF	Security Communication Function
SCP	Signaling & Control Plane Traffic
SCTP	Stream Control Transmission Protocol
SBC	Session Border Controller
SDU	Service Data Unit
SDA	Security Domain Authority
SEC	Security Exchange Commission
SECM	Systems Engineering Capability Model
SEI	Security Exchange Item
SESE	Security Exchange Service Element
SF	Security Function
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SI	Security Information
SII	Shield Integrity Information
SIP	Session Initiation Protocol
SMAP	Security Management Application Process
SMIB	Security management information base
SML	Services Management Layer
SMS	Short Message Service
SMS	Security Management System
SNMP	Simple Network Management Protocol
SoD	Separation of Duty
SOF	Strength of Function
SOX	Sarbanes-Oxley Act
SP	Service Provider
SPAP	Service Provider Application Server Platform
SPDF	Security Policy Decision Function
SPEF	Security Policy Enforcement Function
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
SSO	System Security Object
ST	Security Target
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege
SUID	set user ID command
ST	Security Target
SYN	Synchronization
TCP	Transport Control Protocol
TCSEC	Trusted Computing System Evaluation Criteria
TETRA	TErrestrial Trunked RAdio

TFTP	Trivial File Transfer Protocol
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TL	Transport Protocol Layer
TLS	Transport Layer Security
TMN	Telecommunications Management Network
TOE	Target of Evaluation
TP	Transaction procedure
TR	Technical Report
TS	Technical Specification
TSC	TSF Scope of Control
TSP	Telecommunications Service Provider
TSFI	TOE security functions interface
TSP	Telecommunications Service provider
TTP	Trusted Third Party
TV	Television
TVA	Threat & Vulnerability Analysis
TVRA	Threat, Vulnerability and Risk Analysis
UA	User Agent
UDI	Unconstrained Data Item
UDP	User Datagram Protocol
UID	user ID
Ull	Unshield Integrity Information
UML	Unified Modeling Language
UNI	User-network interface
UP	User Plane
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUCP	UNIX-to-UNIX copy
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
VTA	Vulnerability Threat Analysis
WDM	Layer 2 Lambda Intermediate Element
WiFi	Wireless Fidelity
XML	Extensible Markup Language

4 Security Engineering

Security engineering in the context of this TR begins with an understanding of the operational environment within which they operate and the specific security related objectives. Based on these, the development and execution of a methodology to define a corporate approach to achieving the identified security objectives is achievable. This corporate approach is frequently referred to as "Governance" or a “corporate Information Security Program.” This section describes a security life cycle, provides the approach for this program, and identifies existing standards and generally accepted industry practices that support such an approach. For purposes of simplicity, this document uses TSP primarily in the description and text, but the information is relevant to all enterprises.

4.1 Security Life Cycle

The security life-cycle spans many phases of a product/ service life cycle as shown in the examples and details in this document focus on these items, except for Test and Decommissioning, and are based on the standards, and best practices referenced by this Technical Report. It is important to know the security principles and target security capabilities to guide security architects in creating specific security architectures.

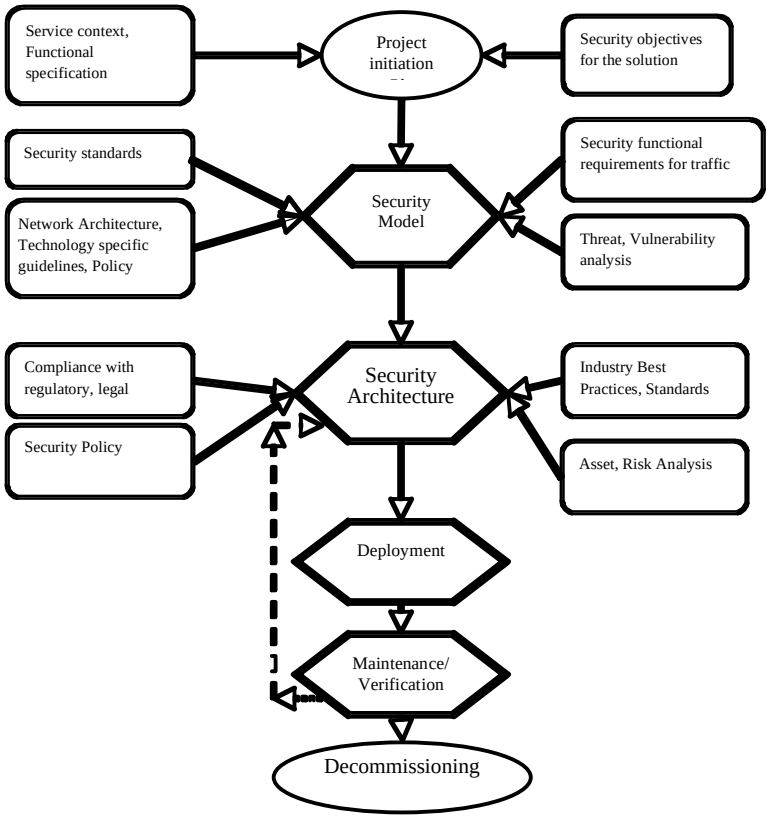

Figure 1 Security Life Cycle

Section 4.2 focuses on those forces/drivers that TSPs must contend with as part of normal business. Sections 4.3 and 4.4 reviews the need to develop and implement a security engineering methodology and those existing methodologies that provide assistance to a TSP establishing a Governance program. Section 4.5 discusses the importance of establishing corporate security policies and how international standards can provide guidance in this effort. Section 4.6 introduces the critical concept of trust/security domains that reflect a TSP's areas of responsibility and control. Section 4.7 provides an in-depth examination of typical TSP infrastructure vulnerabilities, threat analysis and quantification of risks. In conclusion, Section 4.8 examines a number of major formal/informal models for security and what, if any, role these models should play in a TSP security program.

4.2 New Telecommunications Service Provider Operating Environment

An analysis of the operating environment within which TSPs conduct business has to recognize and evaluate the many outside forces impinging on the TSP, specifically:

- Regulations/Legislation,
- Technology Evolution,
- Customers demands and expectations,
- Legal Liability,
- Competition, and
- Terrorism, Cyber crime.

Each of these forces has a significant impact on the TSP's business practices and some actually dictate aspects of the TSP's information security program.

Regulations/Legislation specify legal constraints on a TSP's business, Table 1 presents the most significant regulatory & legislative drivers from an information security perspective.

Table 1 - TSP Regulations/Legislation Drivers

Regulations & Legislation	Common Acronym	Description
Sarbanes-Oxley Act	SOX	(Also known as the Public Company Accounting Reform and Investor Protection Act of 2002) is a U.S. federal law that establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. The Act contains 11 sections, ranging from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law. Key security-related sections deal with: - Requirements for auditor attestation of control disclosures, and - Internal controls of * Information technology * IT controls, IT audit, and SOX * IT Impacts
Gramm-Leach-Bliley Act,	GLBA	(Also known as the Gramm-Leach-Bliley Financial Services Modernization Act) is an Act of the U.S. Congress which repealed the Glass-Steagall Act, opening up competition among banks, securities companies and insurance companies. The Gramm-Leach-Bliley Act (GLBA) allowed commercial and investment banks to consolidate into what is now known as the financial services industry. Key security-related sections deal with the need to safeguard consumer privacy.
An act to amend the Civil Code relating to personal information	SB-1386	This California law requires any businesses that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. More importantly, over 13 other states have enacted the same, or similar, laws to Calif. SB-1386 and a similar bill is under consideration by the U.S. Congress

Regulations & Legislation	Common Acronym	Description
Payment Card Industry Data Security Standard	PCI	The Payment Card Industry (PCI) Council is an open global forum, including representatives of major credit card companies that has created a (non-ANSI) Data Security Standard to safeguard customer information. Visa, MasterCard, American Express, and other credit card associations mandate that merchants and service providers meet certain minimum standards of security when they store, process and transmit cardholder data. The standard requires: ● annual assessment for Level 1 (large) merchants, annual penetration testing and application testing Level 1 and 2 service providers. ● logging of all access to credit card data. ● quarterly scans and annual penetration tests. External scans conducted by an approved vendor: ● requires alerts. ● host and/or network intrusion detection or prevention. ● an appropriately configured and managed firewall. ● two-factor authentication ● 128-bit SSL encryption and effective management of cryptographic key transmission and storage.
Lawful Intercept & Communications Assistance for Law Enforcement Act	LI-CALEA	TSPs are required to support Law Enforcement Agencies (LEAs)as specified in, but not limited to: • Communications Assistance for Law Enforcement Act of 1994 • Title III of the Omnibus Crime Control and Safe Streets Act of 1968, • The Pen Register/Trap & Trace Provisions of Title 18, • The Interception and Pen/Trap provisions of the Foreign Intelligence Surveillance Act. These laws have been interpreted by the U.S. Federal Communications Commission, in its " Third Order and Report" as applying to both telecommunications and information services provided by TSPs. Therefore every TSP shall implement intercept, mediation and distribution mechanisms that allow for intercepting subscriber communications for delivery to LEAs subject to court orders. However the FCC has also ruled that only the specific information specified by said court orders may be shared with LEAs. These requirements necessitate a TSP being able to strictly control who may know about or receive intercept related information or even know about and control intercept activities.

The Regulations/Legislation environment is constantly evolving which will necessitate further study.

Technology now used in modern converged TSP infrastructures is based on generally available commercial off-the-shelf (COTS) technologies and designed upon open standards that are available to the general public. Not only has the technology transitioned from historically proprietary technologies to COTS technologies, these COTS technologies are being deployed in a complex layered manner that is vastly different than traditional POTS infrastructures. Furthermore modern TSP infrastructures have to support subscriber elements that are not simple dumb telephones but are very intelligent computing platforms in their own right.

Customers of modern TSP infrastructures are now demanding an increasingly rich suite of integrated (converged) services from the TSP. Residential voice services, historically considered as strictly 'business services' are now being coupled with data services such as:

- voice-video conferencing,
- networked meetings,

- combined voice & text instant messaging,
- text-voice-video integrated web browsing.

This disappearing boundary between telecommunications and information services results in convergence of the associated service delivery platforms. When coupled with sophisticated subscriber devices, converged service delivery platforms now become subjected many of the 'classic' forms of Internet attacks seen over the last 15 years.

Legal Liability is an ever present issue for corporations and TSPs must be aware of legislation such as CA SB-1386 and its numerous variants that have been enacted in many states..

As TSPs start to deploy video content delivery (as in broadcast, on-demand and IP based TV) services, TSPs will also have to be concerned with Digital Rights Management (DRM) and the liability associated with failure to protect video intellectual property entrusted to the TSP for delivery to video service subscribers.

Competition in the tele/data-communications industries has mushroomed over the last decade with the convergence of these historically separate business spaces. Cable companies are now delivering data and voice services in addition to their initial video services and Telephone companies are now delivering data and video services in addition to their initial voice services resulting an all-inclusive communication industry populated by general TSPs who compete for market share. Most of the historical regulatory constraints against monopolistic behaviors are being dropped with society expecting an open competitive market to prevent TSP misbehavior. However, given the fierce level of competition, inducement to engage in industrial espionage or other unacceptable activities grows due to great advantage that could be derived from such behavior.

Terrorism and Cybercrime are common parts of our 21st century reality. Most governmental entities (Federal, State and Local) rely on TSP communications infrastructures for official communications needs (including air traffic control, emergency services, etc.). Businesses continue to use TSP communications infrastructures for both business back-office and on-line activities. Many business services also represent part of the national critical infrastructure (such as energy generation and distribution, water resources, transportation). Consequently, TSPs must recognize that:

- Cyber attacks are increasing in volume, sophistication, and coordination
- Cyber Attackers are attracted to high value targets, especially those attackers seeking monetary gain through 'cyber-blackmail' and theft of identities, information, services or even money.

Malicious insiders are a growing threat to our critical national infrastructures and the very companies employing these insiders. Industry changes regarding personnel policies, terms of employment and benefits have fostered employee reconsideration of levels of loyalty due their employer. TSPs now have to also recognize that some ideologically motivated organizations are capable of having members infiltrate TSP labor pools where these 'sleeper' subjects behave as normal employees until directed to act maliciously.

4.2.1 TSP Security Responsibilities - Objectives

From a security objectives perspective, a TSP is:

A. Responsible for protecting customers in regard to:

- Ensuring confidentiality and integrity of all customer information entrusted to the TSP and any information the TSP obtains as a result of customer usage of TSP services,
- Maintaining customer contracted service availability in compliance with those service level agreements between the customer and the TSP,

- Enforcing customer access to only authorized features so that the actions of one customer cannot interfere with service availability to, or information about, other customers,
- Ensuring error-free and non-malicious interaction between customers and the TSP infrastructure,

B. Responsible for protecting peering service providers in regard to:

- Ensuring confidentiality and integrity of all peering service provider information entrusted to the TSP, such as routing, subscriber, billing information and video content,
- Maintaining peering service provider contractually obligated availability in compliance with those service level agreements between the peering service provider and the TSP,
- Enforcing peering service provider access to only authorized features so that their actions cannot interfere with service availability to or information about TSP customers,
- Ensuring error-free and non-malicious interaction between peering service providers and the TSP infrastructure,

C. Responsible for protecting the infrastructure itself by.

- Maintaining the confidentiality and integrity of system information be it signaling & control or OAM&P related,
- Enforcing operations personnel access to system attributes based on an authorized 'need-to know' basis,
- Providing error-free and non-malicious interaction between operations personnel and infrastructure components consistent with A and B above.

4.3 Systems Engineering Methodology for Security

Organizations often group their activities within one or more service areas that focus on some subset of the organizations objectives. An information system is a collection of information processing and communications components, and the environment in which they operate, used to support the operations of one or more service areas. A security policy pertains to organizations and their service areas and is based upon the threats to a service offering. A security policy (or, in a more general sense, a collection of security polices) documents the security requirements to be placed upon resources used by an organization. These security requirements express, for the organization's personnel, the organization's desired protection for its information and other system resources.

A security architecture designed to meet a specific service areas security requirements defines appropriate security services and mechanisms and allocates them to components of the service information system architecture. Since a generic security engineering methodology is intended to address the needs of all service providers, it is a more general statement about the common collection of services and mechanisms any information system might offer and allocates the security services and mechanisms to the generic components of an information system architecture.

Security policy and security requirements are derived as a result of examining the threats to a service area and are therefore a subset of the service area's requirements. Therefore, there is a the strong relationship among service infrastructure, users, information, and policy. The service

provider organizations that will employ the generic security engineering methodology have different service areas. The security policy addressed by the generic security engineering methodology is a general expression of the security requirements commonly found among the service area requirements of service provider organizations.

Security requirements are established in the same ways, whether for an entire organization or for a specific service area. The information to be managed is identified; the operational requirements for the use of the information are stated; the value of the information is determined; and the potential threats to the information are identified. Then, the security policy for either the entire organization or a specific service area can be stated in terms of the requirements for:

- Protection of the information based on the potential threats
- Security services that afford the appropriate protection of the information based upon the value of the information and the threats to it.

4.4 Security Engineering Methodology

A methodological approach to security engineering must span all the key components of a security program. Figure 2 depicts the variety of components within a security and their relationships.. Consideration of security models can facilitate the development of access rights assigned to subjects (people and computers/applications) for interacting with objects (information, services, etc.) within the organization. The basic premise of establishing policy is to clearly understand who (i.e. subjects) accesses what (i.e. objects) from where (e.g. over internet, PSTN, wireless LANs etc.). A Threat & Vulnerability Analysis (TVA) based on defined policies will facilitate identifying organizational risks and directly drive the formulation of operational Practices/procedures and the establishment of a specific security architecture the organization's infrastructure must adhere to. Deployment experience will provide a 'feed-back loop' that should be used to evaluate potentially necessary changes to policy, TVA, practices and architecture. It should be noted that security policy can also be refined throughout all stages of the lifecycle as new security risks and requirements are identified.

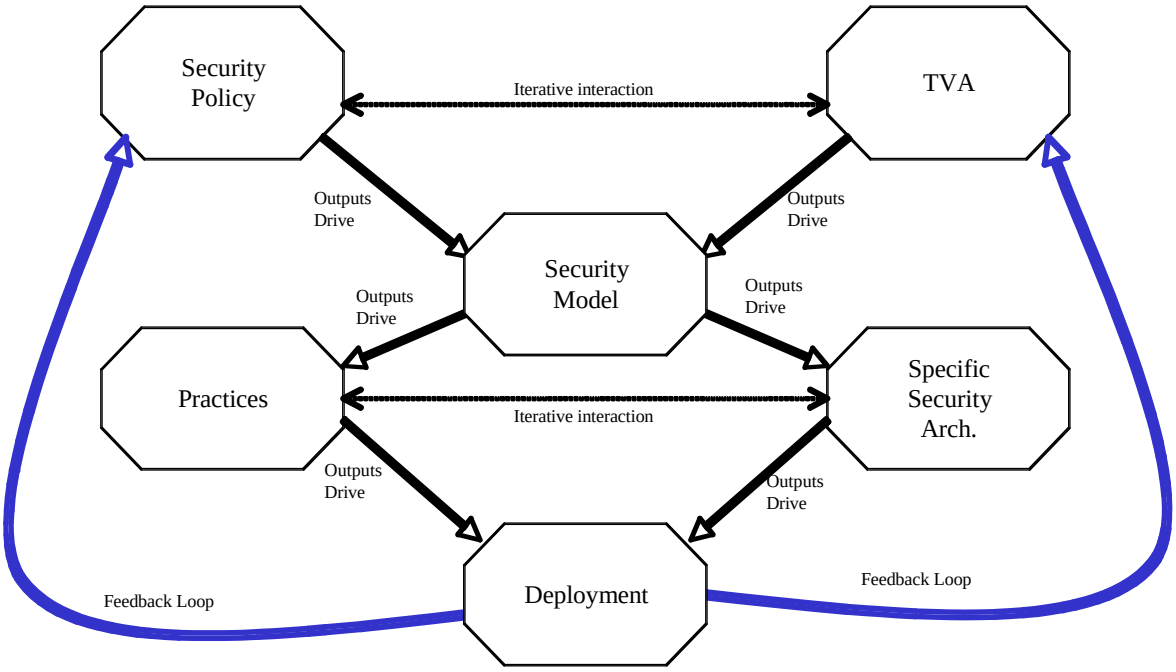

Figure 2- Security Engineering Major Activity Areas

As can be seen from Figure 2, a Systems Engineering approach to security of systems that process information and are used to deliver services is essentially process oriented. One can even say that Information system security engineering focuses on the quality of services. When viewed as a quality oriented process, TSP security engineering can benefit from the following:

- ISO 9000 Processes and Procedures, and
- Capability Maturity Model.

Many TSPs are undertaking significantly complex integration projects to address the convergence of data, voice and video services rather than attempting to purchase turn-key solutions from individual suppliers. This approach forces TSPs to develop system integration capabilities capable of integrating multiple components from a diverse set of suppliers while delivering high quality advanced services to subscribers/service consumers in rapidly shrinking timeframes and budget constraints. Communications product manufacturers are under similar pressure to provide TSPs with components that will interoperate with other suppliers products based on open standards. Both TSPs and equipment manufacturers need systematic approaches within their integration or manufacturing programs to ensure quality objectives (including attention to security issues). By adhering to ISO 9000 Processes and Procedures, combined with appropriate aspects of the CMMI, will allow the communications industry to deliver the type and quality of services 21st century service consumers are now demanding and are willing to buy.

4.4.1 ISO 9000 Processes and Procedures

ISO 9000 is a family of standards, maintained by ISO, for quality management systems. Some of the requirements in ISO 9001 (which is one of the standards in the ISO 9000 family) include:

- a set of procedures that cover all key processes in the business;
- monitoring manufacturing processes to ensure they are producing quality product;
- keeping proper records;

- checking outgoing product for defects, with appropriate corrective action where necessary; and
- regularly reviewing individual processes and the quality system itself for effectiveness.

A company or organization that has been independently audited and certified to be in conformance with ISO 9001 can publicly state that it is "ISO 9001 certified" or "ISO 9001 registered." Certification to an ISO 9000 standard does not guarantee the compliance (and therefore the quality) of end products and services; rather, it certifies that consistent business processes are being applied.

Although the standards originated in manufacturing, they are now employed across a wide range of other types of organizations. A "product", in ISO vocabulary, can mean a physical object, a service, or software. ISO 9000 is composed of the following sections:

- ISO 9000, Quality management systems - Fundamentals and vocabulary. covers the basics of what quality management systems are and also contains the core language of the ISO 9000 series of standards. The latest version is ISO 9000:2005.
- ISO 9001 Quality management systems - Requirements intended for use in organizations which design, develop, manufacture, install and/or services any product or provides any form of service. It provides a number of requirements which an organization needs to fulfill if it is to achieve customer satisfaction through consistent products and services which meet customer expectations. This is the only implementation for which third-party auditors can grant certification.
- ISO 9004 Quality management systems - Guidelines for performance improvements, covers continual improvement, and provides advice on how to enhance a mature system. This standard very specifically states that it is not intended as a guide for implementation.

There are many different standards which are referenced in the ISO 9000 family. A lot of them do not even carry "ISO 900x" numbers. For example, parts of the 10,000 range are also considered part of the 9000 family: ISO 10007 discusses Configuration management, which for most organizations is just one element of a complete management system. To the casual reader, it is usually sufficient to understand that when an organization claims to be "ISO 9000 compliant", it means they conform to ISO 9001. However, even ISO itself is critical of the widespread emphasis on certification to ISO 9001: "The emphasis on certification tends to overshadow the fact that there is an entire family of ISO 9000 standards ... organizations stand to obtain the greatest value when the standards in the new core series are used in an integrated manner, both with each other and with the other standards making up the ISO 9000 family as a whole".

The previous members of the ISO 9000 family, 9001, 9002, and 9003, have all been integrated into 9001 which seeks to set criteria which achieve a goal and is not prescriptive as to methods. The requirements come in Sections 4 to 8 and span: General Requirements, Management Responsibility, Resource Management, Product Realization, and Measurement, analysis and improvement. In each of these areas, ISO 9001 seeks to set out key requirements, which if met will ensure consistency. The standard specifies six compulsory documents:

- Control of Documents
- Control of Records
- Internal Audits
- Control of Nonconforming Product / Service
- Corrective Action

- Preventive Action.

In addition to these, ISO 9001 requires a Quality Policy and Quality Manual (which may or may not include the above documents).

The ISO 9001 standard is generalized and abstract. Its parts must be carefully interpreted, to make sense within a particular organization. Over time, various industry sectors have wanted to standardize their interpretations of the guidelines within their own marketplace. This is partly to ensure that their versions of ISO 9000 reflect their specific requirements, but also to try and ensure that more appropriately trained and experienced auditors are sent to assess them. TL 9000 is the Telecom Quality Management and Measurement System (non-ANSI) standard, an interpretation developed by the telecom consortium, QuEST Forum. The current version is 4.0 and includes standardized product measurements that can be benchmarked.

4.4.2 Capability Maturity Model (CMM)

The Capability Maturity Model (CMM) broadly refers to a process improvement approach that is based on a process model. CMM also refers specifically to the first such model, developed by the Software Engineering Institute (SEI) in the mid-1980s, as well as the family of process models that followed. The CMM can be used to assess an organization against a scale of five process maturity levels. Each level represents a ranking of the organization according to its standardization of processes in the subject area being assessed. The subject areas can be as diverse as software engineering, systems engineering, project management, risk management, system acquisition, information services and personnel management.

The CMM is a way to develop and refine an organization's processes. The first CMM was for the purpose of developing and refining software development processes. A maturity model is a structured collection of elements that describe characteristics of effective processes. A maturity model provides:

- a place to start,
- the benefit of a community’s prior experiences,
- a common language and a shared vision,
- a framework for prioritizing actions,
- a way to define what improvement means for your organization,

and can be used as a benchmark for assessing different organizations for comparison. It describes the maturity of the company based upon the project the company is dealing with and the clients.

The Maturity Levels of CMM provide a layered framework providing a progression to the discipline needed to engage in continuous improvement. Key Process Areas (KPA) identify clusters of related activities that, when performed collectively, achieve a set of goals considered important. The goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area. Common features include practices that implement and institutionalize a key process area. These five types of common features include: Commitment to Perform, Ability to Perform, Activities Performed, Measurement and Analysis, and Verifying Implementation. The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the key process areas.

There are five levels of the CMM:

Level 1 - Initial

At maturity level 1, processes are usually ad hoc and the organization usually does not provide a stable environment. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes. In spite of this ad hoc, chaotic environment, maturity level 1 organizations often produce products and services that work; however, they frequently exceed the budget and schedule of their projects.

Level 2 - Repeatable

At maturity level 2, processes may not repeat for all the projects in the organization. The organization may use some basic project management to track cost and schedule. Process discipline helps ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans. Basic project management processes are established to track cost, schedule, and functionality. The minimum process discipline is in place to repeat earlier successes on projects with similar applications and scope. There is still a significant risk of exceeding cost and time estimates.

Level 3 - Defined

The organization's set of uniform processes, which is the basis for level 3, is established and improved over time. These uniform processes are used to establish consistency across the organization. Projects establish their defined processes by the organization's set of uniform processes according to tailoring guidelines. The organization's management establishes process objectives based on the organization's set of uniform processes and ensures that these objectives are appropriately addressed. A critical distinction between level 2 and level 3 is the scope of uniform processes, process descriptions, and procedures. At level 2, the uniform processes, process descriptions, and procedures can be quite different in each specific instance of the process (for example, on a particular project). At level 3, the uniform processes, process descriptions, and procedures for a project are tailored from the organization's set of uniform processes to suit a particular project or organizational unit.

Level 4 - Managed

Using precise measurements, management can effectively control a project. In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Subprocesses are selected that significantly contribute to overall process performance. These selected subprocesses are controlled using statistical and other quantitative techniques. A critical distinction between maturity level 3 and maturity level 4 is the predictability of process performance. At maturity level 4, the performance of processes is controlled using statistical and other quantitative techniques, and is quantitatively predictable. At maturity level 3, processes are only qualitatively predictable.

Level 5 - Optimizing

Maturity level 5 focuses on continually improving process performance through both incremental and innovative technological improvements. Quantitative process-improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement. The effects of

deployed process improvements are measured and evaluated against the quantitative process-improvement objectives. Both the defined processes and the organization's set of uniform processes are targets of measurable improvement activities. Process improvements to address common causes of process variation and measurably improve the organization's processes are identified, evaluated, and deployed.

The Capability Maturity Model was initially funded by military research. The United States Air Force funded a study at the Carnegie-Mellon Software Engineering Institute to create a model (abstract) for the military to use to objectively evaluate software subcontractors. The result was the Capability Maturity Model, published as Managing the Software Process in 1989. The CMM is no longer supported by the SEI and has been superseded by the more comprehensive Capability Maturity Model Integration (CMMI), of which version 1.2 has now been released.

Although these models have proved useful to many organizations, the use of multiple models has been problematic. Further, applying multiple models that are not integrated within and across an organization is costly in terms of training, appraisals, and improvement activities. The CMM Integration project was formed to sort out the problem of using multiple CMMs. The CMMI Product Team's mission was to combine three source models:

1) The Capability Maturity Model for Software (SW-CMM) v2.0 draft C
2) The Systems Engineering Capability Model (SECM)
3) The Integrated Product Development Capability Maturity Model (IPD-CMM) v0.98
4) Supplier sourcing.

CMMI is the designated successor of the three source models. The SEI has released a policy to sunset the SW-CMM and previous versions of the CMMI. The same can be said for the SECM and the IPD-CMM; these models were superseded by CMMI.

With the release of the CMMI Version 1.2 Product Suite, the existing CMMI has been renamed the CMMI for Development (CMMI-DEV). A version of the CMMI for Services is being developed by a Northrop Grumman-led team under the auspices of the SEI, with participation from Boeing, Lockheed Martin, Raytheon, SAIC, SRA, and Systems and Software Consortium (SSCI). In some cases, CMM can be combined with other methodologies. It is commonly used in conjunction with the ISO 9001 standard.

4.5 Role of Security Governance and Policies

As a process, security governance can be carried out for any size organization from a home business to the largest organizations. A primary purpose of security governance is to assure that the organization achieves its security goals and objectives while avoiding unnecessary risks to itself and those it serves. Security governance should:

- Identify what assets an organization considers of value and establishes the asset sensitivity (e.g. public, proprietary, restricted, copyrighted, Attorney-Client-Privileged)
- Identify organizational subgroups and "need-to-know" by group
- Specify form of authorization required to access an asset
- Drive Security Model development.

A TSP governance program can be assisted by several well known security practices and guidelines as discussed in this section, such as:

- Generally Accepted Information Security Practices (GAISP)
- ISO 17799
- ISO 27001.

4.5.1 Generally Accepted Information Security Practices (GAISP)

The Generally Accepted Information Security Principles (GAISP) are intended to be a set of guidelines similar to the Generally Accepted Accounting Principles (GAAP) that U.S. corporations follow when they submit their financial reports. GAISP will include a set of procedures by which any company can derive its own security architecture. The industry group promoting the principles is the Information Systems Security Association (ISSA). The work began in 1990 under the name GASSP (Generally Accepted System Security Principles), and draws on other work including ISO 17799 which was originally developed by the British Standards Institute. Although GAAP is a U.S.-only ISSA standard--different accounting practices are used in different countries--ISSA hopes to make GAISP a global standard. The potential for recognition as an ANSI standard is not known. The group has mapped the ISO 17799 standard, and others, to GAISP, so that compliance to those principles would automatically imply compliance with the looser IS 17799, which could be useful in countries that might mandate it.

The approach GAISP takes is to note that information security is a combination of preventive, detective, and recovery measures. A preventive measure is a risk control that avoids or deters the occurrence of an undesirable event. A detective measure is a risk control that identifies the occurrence of an undesirable event. Detective measures also provide a means for reporting the occurrence of events. A recovery measure is a risk control that restores the integrity, availability, and confidentiality of information assets to their expected state. GAISP also notes that information security includes education, awareness, and training measures that inform computer users of the “acceptable use” principles and practices that support the protection of information assets. These principles should be constructed to ensure that the information system reduces the risk of a threat event and potential scale of its adverse impact. The intent of GAISP is to:

- Identify and develop Pervasive, Broad Functional, and Detailed GAISP in a comprehensive framework of emergent principles, standards, conventions, and mechanisms that will preserve the availability, confidentiality, and integrity of information,
- Be an authoritative source for opinions, practices, and principles for information owners, information security practitioners, information technology products, and information systems,
- Define, implement, and subsequently operate under the governing GAISP infrastructure,
- Define and establish linkage to the Common Criteria Project.

Candidate principles are organized in a three-level hierarchy comprised of:

- Pervasive Principles - few in number, fundamental in nature, and rarely changing. Target: Governance,
- Broad Functional Principles - subordinate to one or more of the Pervasive Principles, are more numerous and specific, guide the development of more Detailed Principles, and change only when reflecting major developments in technology or other affecting issues. Target: Operational Management,
- Detailed Principles - subordinate to one or more of the Broad Functional Principles, numerous, specific, emergent and change frequently as technology and other affecting issues evolve.

The Pervasive Principles address the following properties of information: Confidentiality, Integrity and Availability and provide general governance-level guidance to establish and maintain the security of information. These principles form the basis of Broad Functional Principles and Detailed Principles. Security of information is achieved through the preservation

of appropriate confidentiality, integrity, and availability. The currently defined pervasive principles are:

- Awareness Principle,
- Ethics Principle,
- Multidisciplinary Principle,
- Proportionality Principle,
- Integration Principle,
- Timeliness Principle,
- Assessment Principle and
- Equity Principle,

The Broad Functional Principles are derived from the Pervasive Principles that represent the broad conceptual goals of information security. By providing the guidance for operational accomplishment of the Pervasive Principles, the Broad Functional Principles are the building blocks (what to do, at a high level) that comprise the Pervasive Principles and allow definition of the basic units of those principles. Because the Broad Functional Principles are smaller in scope, they are easier to address in terms of implementation planning, and execution. The Broad Functional Principles include:

- Information Security Policy,
- Education and Awareness,
- Accountability,
- Information Asset Management,
- Environmental Management,
- Personnel Qualifications,
- Incident Management,
- Information Systems Life Cycle,
- Access Control,
- Operational Continuity and Contingency Planning,
- Information Risk Management,
- Network and Internet Security,
- Legal, Regulatory, and Contractual Requirements of Information Security,
- Ethical Practices.

The Detailed Security Principles, still under development, will specifically address methods of achieving compliance with the Broad Functional Principles with respect to existing environments and available technology. There will be many detailed information security principles supporting one or more Broad Functional Principles. The Detailed Principles will address differing technologies, environments, standards, practices, and concepts that are relevant to the Broad Functional Principles. The Detailed Principles are expected to continuously evolve to meet the challenges of emerging technology and new threats.

4.5.2 ISO 17799

ISO 17799 provides guidelines and voluntary directions for information security program management, but as guidelines this standard is subject to wide interpretation. ISO 17799 now contains the following major topics (clauses):

- Security Policy,
- Organizing Information Security,
- Asset Management,
- Human Resources Security,
- Physical and Environmental Security,
- Communications and Operations Management,

- Access Control,
- Information Systems Acquisition, Development and Maintenance,
- Information Security Incident Management,
- Business Continuity Management, and Compliance.

This standard is meant to provide a high level, general description of the areas currently considered important when initiating, implementing or maintaining information security in an organization and establishes guidelines and general principles.

The standard does not currently cover all areas of importance but is a starting point. It primarily addresses topics in terms of policies and general good practices and identifies the need to manage the following but does not provide specific technical guidance on the specific actions that need to be performed:

Establishing organizational security policy	Organizational security infrastructure
Asset classification and control	Personnel security
Physical and environmental security	Communications and operations management
Access control	Systems development and maintenance
Business continuity management	Compliance

4.5.3 ISO 27001

ISO 27001 is an information security management program (ISMP) standard published in October 2005. This is a certification standard specifying requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMP. The requirements are defined in a structured, formal format suitable for compliance certification. It is intended to be used in conjunction with ISO 17799 which lists security control objectives and recommends a range of specific security controls. Organizations that implement an ISMP in accordance with the best practice advice in ISO 17799 are likely to simultaneously meet the requirements of ISO 27001, but certification is entirely optional.

This standard is the first in a family of information security related ISO standards which are being assigned numbers within the 27000 series. Others are anticipated to include:

- ISO/IEC 27000 - a vocabulary or glossary of terms used in the ISO 27000-series standards
- ISO/IEC 27002 - the proposed re-naming of existing standard ISO 17799
- ISO/IEC 27003 - a new ISMP implementation guide
- ISO/IEC 27004 - a new standard for information security measurement and metrics
- ISO/IEC 27005 - a proposed standard for risk management, potentially related to the current British Standard BS 7799 part 3
- ISO/IEC 27006 - a guide to the certification/registration process.

ISO 27001 was based upon and replaced BS 7799 part 2 which was withdrawn. The ISO 27000-series information security management standards align with other ISO management systems standard, such as those for ISO 9001 (quality management systems), both in terms of their general structure and in the nature of combining best practice with certification standards.

ISO developed this standard to cover all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations) and specifies requirements for establishing,

implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. This standard specifies requirements for the implementation of security controls customized to the needs of individual organizations, or parts thereof, and is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. It is intended to be suitable for several different types of use, such as:

- Formulate security requirements and objectives,
- Ensure that security risks are cost effectively managed,
- Ensure compliance with laws and regulations,
- Process framework for implementation and management of controls that ensure specific security objectives of an organization are met, including:
  - definition of new information security management processes;
  - identification and clarification of existing information security management processes;
  - use by management to determine the status of information security management activities;
  - use by internal and external auditors to determine degree of compliance with policies, directives and standards;
  - use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners, customers & other organizations;
  - implementation of business-enabling information security.

4.5.4 Summary

GAISP has the potential, when further developed, to add value to a TSP governance program conformant with ISO 17799 as well as possibly assisting a TSP in defining comprehensive security policies. However future development of the GAISP Detailed Security Principles will impact the value of this work on the communications industry as a whole and TSPs in particular. ISO 17799 provides general guidance and best practices for ISMS, and yet when used in conjunction with ISO 27001, and ideally with ISO 9001, these three ISO standards provide a TSP with a sound foundation for the establishment of an information security management program (ISMP). Such an ISMP, once instantiated, will provide a high level of assurance that a TSP recognizes security as a significant part of its quality of services.

4.6 Trust Domains

ITU-T X.800 clause 8.1.2 states:

> There can be many security policies imposed by the administration(s) of distributed systems. Entities that are subject to a single security policy, administered by a single authority, are sometimes collected into what has been called a "security domain".

A more common term for Security Domain is Trust Domain. Trust is the characteristic that one entity is willing to rely upon a second entity to execute a set of actions and/or to make set of assertions about a set of subjects and/or scopes.

A Trust Domain is a security space in which the target of a request can determine whether particular sets of credentials from a source satisfy the relevant security policies of the target.

The target may defer trust to a third party thus including the trusted third party in the Trust Domain.

A Trust Domain is a set of nodes that are trusted to exchange information in the sense described below. A node can be a member of a Trust Domain, T, only if the node is expected to be compliant to a certain set of security policies, which characterize the handling of information within the Trust Domain. Trust Domains are constructed by human beings who know the properties of the equipment they are using/deploying. In the simplest case, a Trust Domain is a set of devices with a single owner/operator who can accurately know the behavior of those devices. Such simple Trust Domains may be joined into larger Trust Domains by bi-lateral agreements between the owners/operators of the devices.

We say that a node, A, in the domain is 'trusted by' a node, B, (or 'B trusts A') if and only if:

1) there is a secure connection between the nodes, AND
2) B has configuration information indicating that A is a member of the Trust Domain.

Note that B may or may not be a member of the Trust Domain. For example, B may be a UA which trusts a given network intermediary, A (e.g., its home proxy).

A 'secure connection' in this context means that messages cannot be read by third parties, cannot be modified by third parties without detection and that B can be sure that the message really did come from A. The level of security required is a feature of the Trust Domain i.e., it is defined in the security policies for the Trust Domain.

Within this context, information received by one node FROM a node that it trusts is known to have been generated and passed through the network according to the security policies for the Trust Domain, and therefore can be known to be valid, or at least as valid as specified in the security policies for the Trust Domain. Equally, a node can be confident that signaling information passed to a node that it trusts will be handled according to the security policies for the Trust Domain.

For these capabilities to be useful, the security policies for the Trust Domain shall contain requirements as to how the information is generated, how its privacy is protected and how its integrity is maintained as it is passed around the network. A reader of the security policies for the Trust Domain can then make an informed judgment about the authenticity and reliability of information received from the Trust Domain.

The term 'trusted' (with respect to a given Trust Domain) can be applied to a given node in an absolute sense - it is just equivalent to saying the node is a member of the Trust Domain. However, the node itself may not know whether another arbitrary node is 'trusted', even within the Trust Domain. It does know about certain nodes with which it has secure connections as described above.

Statements such as 'When a node receives information from a trusted node...' are not meaningful in a trust domain sense because one node does not have complete knowledge about all the other nodes in the trust domain. Whereas, statements such as 'When a node receives information from another node that it trusts...' ARE valid, and should be interpreted according to the criteria (1) and (2) above.

The above relationships are illustrated in the following figure:

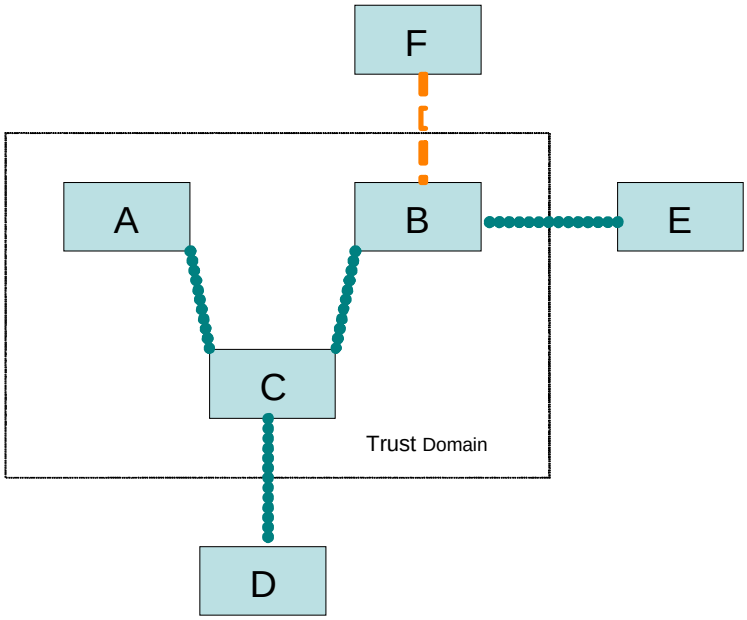

Figure 3 - Trust Domain Relationships

Legend:

Dashed line = Insecure connection

Dotted line = Secure connection

All boxes within the dotted line box are part of the same Trust Domain:

- A, B and C are part of the same trust domain
- A trusts C, but A does not trust B
- since E knows that B is inside of the trust domain, E trusts B, but B does not trust E
- B does not trust F, F does not trust B

An aspect of the definition of a trust domain is that all the elements in that domain are compliant to a set of the security policies for the Trust Domain.

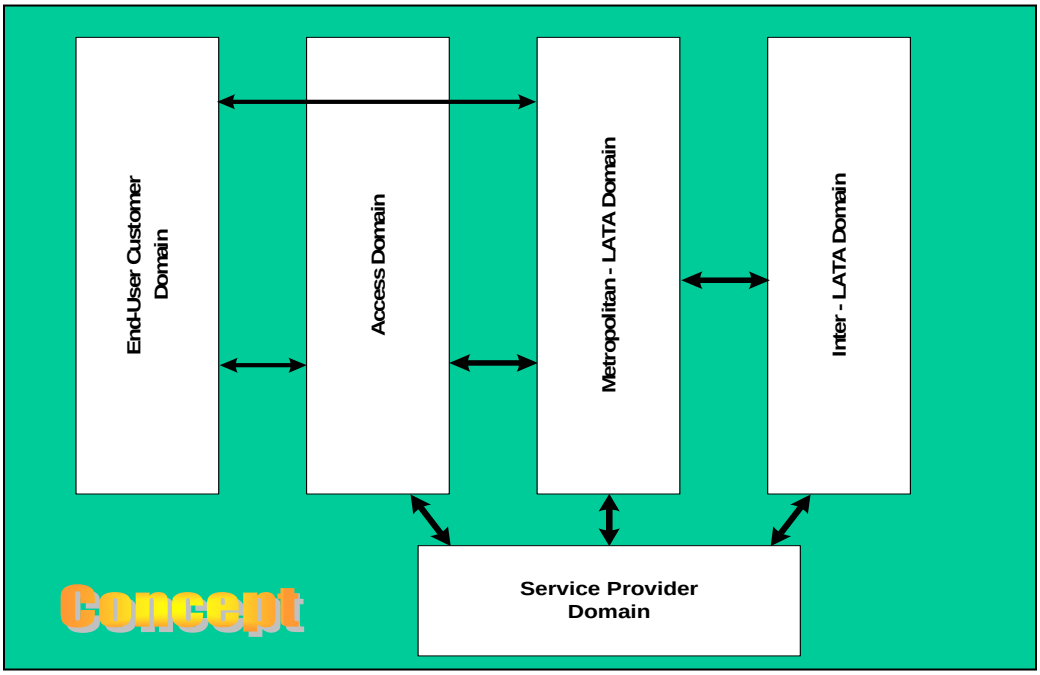

Figure 4 -- Typical Trust/Security Domains to Consider

4.7 Role of Vulnerabilities, Threats & Risk Analysis

The purpose of analyzing vulnerabilities within TSP infrastructures and the threat that can /will target these vulnerabilities is to provide a TSP with an understanding of the degree of risk the TSP faces when providing services to its customers and interacting with other TSPs, and to indicate where mitigation measures are needed. This section methodically reviews many of the vulnerabilities possibly present within TSP infrastructures and sorts the vulnerabilities into the four categories of:

- Operating System vulnerabilities
- Protocol-specific vulnerabilities
- Configuration vulnerabilities
- Application-specific vulnerabilities

within the infrastructure areas of:

- System Controls, Identification, Authentication (section 4.7.1.1)
- Information Resource Protection (section 4.7.1.2)
- Security Audit Logs (section 4.7.1.3)
- System Integrity and Privileged Authority (section 4.7.1.4)
- Availability Protection (section 4.7.1.5)
- Security Administration and Configuration Management (section 4.7.1.6)
- Configuration vulnerabilities (section 4.7.1.7)
- Intermediate and End Node Security (section 4.7.1.8).

The analysis of threats begins with identifying the likely types of Threat Agents and the capabilities each type of agent is most likely to possess. The analysis then proceeds to examine the types of attacks the aforementioned threat agents most probably would use against

the vulnerabilities identified in the above infrastructure areas. Other approaches to analyzing vulnerabilities are then discussed as to their applicability and completeness. The section then concludes with a discussion of how to quantify TSP security risks from the results of a vulnerability and threat analysis.

The analyses of vulnerabilities and threats are very much intertwined. The attacks that are anticipated against assets should reflect the type and nature of vulnerabilities either inherent in the asset or as result of how an asset is deployed, managed or accessed.

4.7.1 Vulnerabilities

There are over 600 known vulnerabilities[14] in TCP/IP, UNIX and Windows environments. New vulnerabilities in software, systems and networks are discovered every week and these exposures are published on the Internet for anyone to review. In fact, within a short time after the publication of a vulnerability, someone will post an automated attack for anyone (regardless of their technical knowledge) to exploit.

Table 2 - Vulnerability Categories

Operating System vulnerabilities	Introduced from within an operating system design or implementation, these are difficult to address in a timely fashion; though vendors do place a relatively high priority on addressing high-profile bugs.
Protocol-specific vulnerabilities	These vulnerabilities are characteristic of a protocol and are often most intractable since modification of the protocol may cause equipment to lose interoperability.
Configuration vulnerabilities	These vulnerabilities come from a variety of sources. Hackers may access a system and introduce configuration changes that weaken security (like a login with a null password); administrators may unwittingly change the configuration to a less-secure state (like leaving tftp enabled); and users may introduce changes to facilitate tedious tasks (like configure a .netrc file with hostname, login, and password for access to another host). Least under control of administrators, users have wide leeway in determining overall system security since many system services offer considerable user capability to configure shortcuts and automated scripts that could compromise security.
Application-specific vulnerabilities	Like operating system vulnerabilities, these are difficult to address since the vendor is in the position to fix security weaknesses. Unlike operating system vulnerabilities, these weaknesses are seen as being limited in scope and application vendors are not likely to give priority to issuing patches for identified vulnerabilities over correcting found bugs in a future release. Margins are thin and the market isn't nearly as wide as for operating systems.

4.7.1.1 System Controls, Identification, Authentication

4.7.1.1.1 LoginID/Password Disclosure

Password data may be disclosed through user guile or foolishness. More than one user may share authentication data for access to a single resource. A user may also select identical

[14] Internet Security Systems (http://www.iss.net).

authentication data for access to several resources. Once this information is disclosed, it might also be used successfully elsewhere. Type: Operating System Vulnerability.

Many networking protocols demand loginID/password information, yet do not protect this data from eavesdropping while in transit. Type: Protocol Vulnerability.

The .netrc file may be set by a user to contain hostname, loginID, and password data in cleartext for access to other hosts. This is often easily disclosed. Type: Configuration Vulnerability.

The UUCP Systems file also contains host address, login, and password data for the uucp login; this is frequently poorly protected. Type: Configuration Vulnerability.

In addition, encrypted password data may be obtained from a host because the system configuration is inadequate to protect that data. Related to this is non-robust password selection. Passwords may be guessed and confirmed by attempted access to the network or by comparison to a purloined encrypted password file. LoginIDs, user names or other data, the blank password, and dictionaries form the basis for guessing attacks. Type: Configuration Vulnerability.

4.7.1.1.2 LoginID/Password Loss

Password data may be lost by the user or by the host. In either case, denial of service results since authentication is blocked. Type: Configuration Vulnerability.

4.7.1.1.3 Inappropriate Authentication Reliance

Many network protocols and servers (router filters, network access servers, firewalls) rely upon an IP address as a source of authenticated identity, however source IP addresses are easily spoofed. Sometimes this authentication is simply assumed on the basis of source IP address. Sometimes an authentication is performed and transitive authentication of all future traffic is assumed authenticated if purported to come from the same IP address. Type: Protocol Vulnerability.

4.7.1.1.4 Inappropriate User authorization

User loginIDs may be assigned privileges greater than those actually appropriate. They may possess a UID of 0 or system/administrator rights; they may be assigned to a group conferring inappropriate authorization. Type: Configuration Vulnerability.

LoginIDs for users no longer authorized to access some resource may remain valid. This may enable an unauthorized user (perhaps the former owner of the LoginID to commandeer the LoginID and gain access the resource, possibly without detection. Type: Configuration Vulnerability.

4.7.1.1.5 Inadequate User Identification

Multiple loginIDs may map to a single UID, complicating auditing and accounting efforts. Type: Configuration Vulnerability.

4.7.1.1.6 Insufficient Privileged User Authentication

Some platforms may be configured to permit privileged login only from an (ostensibly) physically secure console. All other privileged access must be individually authenticated and a separate authentication undertaken to obtain privilege. Type: Configuration Vulnerability.

4.7.1.1.7 NIS Failure

Hosts that receive their password map from an NIS client are commonly configured with "+::0:0:::" as the last line in their /etc/profile. If the ypbind process dies, there exists a "+" loginID with no password and root privileges. Type: Operating System Vulnerability.

4.7.1.2 Information Resource Protection

4.7.1.2.1 Unidentified & Unauthenticated Host Access

Platforms are sometimes configured with accounts with a blank password and a login shell consisting of a command providing system information such as uptime, finger, who, etc. Information worth obtaining is worth being protected by authentication. Type: Configuration Vulnerability.

4.7.1.2.2 Improper Network File Sharing

Network File Systems may be restricted based upon writability and upon hosts permitted to remotely mount the file system. Prudence dictates restricting this access as tightly as possible. Ease of use and speed in the face of changing network topology and computing resource allocation demands the opposite. Wide read-write export of a file system is commonly equivalent to open access to the host. Type: Configuration Vulnerability.

4.7.1.2.3 Improper File or Directory Permissions

World-writeable system files or directories are always a security hazard; they are also commonplace. The same applies to non-privileged files and directories, though the potential downside is not so sweeping. File data may be changed to hide activity, to facilitate future access, or to vandalize. Any user may type "rm -rf *" in the root directory and *somebody* will be very unhappy (since the disk files are deleted); it shouldn't happen, but it does. Type: Configuration Vulnerability.

Often, system files may be owned by an entity other than root (uucp, ftp, http) that is associated with some network system access that may or may not be authenticated. Here it is prudent not to give the owner write access either; only root or some other privileged admin account should be permitted to modify these configuration files, lest unauthorized network access be used to modify configuration files, granting wider system access for the future. Type: Configuration Vulnerability.

Improper umask setting exacerbates this situation and should be set appropriately for all users. Type: Configuration Vulnerability.

4.7.1.2.4 Open Permissions on Temporary Files

If a privileged application opens temporary files with a predictable name and with world-writeable permissions, the filename may be symbolically linked to a system file that will be opened with privilege and may then be modified. Type: Application Vulnerability.

4.7.1.2.5 Unprotected Application Initialization Files

Initialization files like .kshrc, .exrc, .emacs, .profile, .forward, may be modified to perform unauthorized activities with privilege of the owner. Type: Configuration Vulnerability .

4.7.1.2.6 Unprotected Application Initialization Environment Variables

The same initialization may also be done via environment variables and may likewise induce unauthorized actions. Type: Configuration Vulnerability.

4.7.1.2.7 Unprotected sendmail Alias File

Aliases may be set up to perform actions with privilege if mail arrives for a particular address. Type: Configuration Vulnerability.

4.7.1.2.8 Unrealistic Reliance on Insecure Cryptography

Few users (or gurus) recognize that the UNIX *crypt* command utilizes easily-broken cryptography rendered useless due to its small key size. Newer, more robust algorithms are only reliable if key sizes are sufficiently large to prevent or discourage brute force attacks. Unfortunately, algorithms supporting sufficiently large keys cannot be released overseas, by U.S. law. Type: Configuration Vulnerability.

4.7.1.3 Security Audit Logs

4.7.1.3.1 Insufficient Auditing and Accounting

Most platforms permit the configurable enabling of auditing and accounting processes that may be used to reconstruct questionable chains of events or to flag improper resource use (or depletion). Since these are resource sinks themselves, they are often disabled by administrators. Even if they are left operational by Administrators, intruders often disable them since they are valuable event reconstruction tools. Type: Configuration Vulnerability.

4.7.1.4 System Integrity and Privileged Authority

4.7.1.4.1 Applications Run with Unnecessarily High Privileges

Applications that have the SUID flag set that do not change their effective and real user IDs to a non-privileged UID when privileges are no longer needed will perform all their operations with the privileges of the SUID file owner. Any operations performed by the application might be subverted (or intended) to perform privileged operations the real user would not be permitted to perform. Type: Application Vulnerability.

4.7.1.4.2 Shell Script Race Conditions

When running a shell script, there are two operations that cause concern: spawning a shell, and reading the script for execution. There is a point in time when the shell script may be rewritten and an unexpected script executed. This new script may be run with privilege if launched by a privileged user or if SUID to a privileged UID. Type: Operating System Vulnerability.

4.7.1.4.3 Internal Field Separator (IFS) Machinations

The IFS is a character used by the shell to parse character strings on the command line or in scripts into words for interpretation. If the IFS is modified to be different from the default whitespace, unexpected operations may transpire, possibly with privilege if SUID scripts are the target. Type: Operating System Vulnerability.

As an example, it is common to disable an account by setting the login shell to /bin/false, which is simply a short shell script: “exit 255”. If the IFS is set to ‘i’ and a user attempts to su to the login with the proper password, one will not get a shell, but one will be running the ex editor on

file “t” which can be escaped from to a shell. Likewise, the IFS could be set to ‘/’ and malicious scripts entitled “bin” or “etc” could be written to perform unauthorized tasks.

Some shells reset the IFS to a correct value when invoked; some will not.

4.7.1.4.4 Unauthorized SUID Files

Hidden SUID shell files are the simplest way to retain privileged access on an as-needed basis. SUID shell scripts are always a vulnerability and are likely a trap. Even necessary SUID system files may be an avenue for exploitation if currently unknown bugs are discovered. Type: Configuration Vulnerability.

4.7.1.4.5 Unnecessarily Wide Trust Relationships

User .rhosts files may be set to allow any user with that user’s loginID open rlogin, rcp, or rsh to access the host with that user’s privilege. Any trust relationship, proper or improper, may be used to expand the sphere of access an intruder has obtained. Type: Configuration Vulnerability.

The /etc/hosts.equiv file can extend this capability to any username. Type: Configuration Vulnerability.

4.7.1.5 Availability Protection

4.7.1.5.1 DNS Spoofing

By responding to DNS queries directed to a valid server and jamming that server’s response, one may provide incorrect IP address-hostname mapping data that can be used to take advantage of a trust relationship. Type: Protocol Vulnerability.

4.7.1.5.2 Insufficient ICMP Robustness Under Fire

Sending an ICMP Echo Request (“ping”) packet with a payload of 65,536 bytes will cause most hosts’ networking subsystems to freeze up and may cause the entire host to crash. Type: Operating System Vulnerability.

4.7.1.5.3 Insufficient TCP Robustness Under Fire

The TCP protocol initiates a virtual connection by means of a three-way handshake consisting of the initiating network entity sending a SYN packet to another entity. The other then sends a SYN-ACK packet back to the initiator. All succeeding packets (carrying higher-level data) are ACK packets until the connection is torn down by the receipt of a RST packet by either party which responds in kind.

Sending a series of SYN packet forged to appear to come from a nonexistent IP source address will rapidly consume system resources as it waits in vain for responses to the SYN-ACK packets it has sent in response. Hosts are unable to respond to any further legitimate traffic. Subjecting routers and gateways to this attack can disable an entire network behind them. Type: Protocol Vulnerability.

4.7.1.6 Security Administration and Configuration Management

4.7.1.6.1 Lack of Standard Operating Procedures

For the most part, there usually is little security documentation on the proper setup and maintenance of deployed systems. If there is a problem, there needs to be a clear procedure to notify and repair the situation.

4.7.1.7 Configuration vulnerabilities

These vulnerabilities come from a variety of sources. Hackers may access a system and introduce configuration changes that weaken security (like a login with a null password); administrators may unwittingly change the configuration to a less-secure state (like leave tftp enabled); and users may introduce changes to facilitate tedious tasks (like configure a .netrc file with hostname, login, and password for access to another host). Least under control of administrators, user have wide leeway in determining overall system security since they are the most common accessors of a system and many system services offer considerable user capability to configure shortcuts and automated scripts that may compromise security.

4.7.1.7.1 Improper Network Daemon Configuration

Every network daemon is a potential entry point into a host. Any unneeded daemon or active port (IP, serial, X.25) is an unnecessary risk. Type: Configuration Vulnerability.

There are several services that are widely known to be risky:

> finger sometimes has a debug backdoor and can provide reconnaissance information to a potential intruder. Type: Operating System Vulnerability.
>
> tftp provides unidentified and unauthenticated file transfer capabilities. Type: Protocol Vulnerability.
>
> rexd provides unauthenticated command execution capabilities. Type: Protocol Vulnerability.

4.7.1.7.2 Unauthorized Device Files

Hidden, writable device files that grant access to kmem, for example, may be used to modify the running kernel code and obtain privilege. Type: Configuration Vulnerability.

Some versions of UNIX will permit the creation of such files on an exported NFS file system by root on a host that has mounted that file system remotely. Type: Operating System Vulnerability.

4.7.1.7.3 Buffer Overruns

A common coding error is to allocate a fixed-length buffer on the stack to contain user input or some environment variable and write information into that buffer assuming it is of sufficient size to contain the data. Carefully crafted data may be supplied to overrun the end of the buffer with data and place object code onto the stack. This exploit is highly platform dependent, but is commonly available. Type: Application Vulnerability.

This can commonly give non-privileged users privilege on a host if the vulnerable executable is SUID, or may grant privileged access on a server to anyone accessing a vulnerable port, such as a web server or mail server. Type: Operating System Vulnerability.

4.7.1.7.4 Unnecessarily Wide FTP Access

There are a number of loginIDs which should be listed in /etc/ftpusers to prohibit FTP access either because the associated privileges are too sweeping or because the userIDs are not commonly anticipated to be used for interactive host access, or both (for example: root, bin, uucp, daemon, adm, sys, unknown, nobody). Type: Configuration Vulnerability.

4.7.1.7.5 Improper Path for Privileged Accounts

An account with privilege that does not have a short, well-understood PATH, or has a PATH that *includes any* reference to the current working directory (.), is vulnerable to allowing incorrect executables to be used. Type: Configuration Vulnerability.

4.7.1.7.6 Backdoor Code in Applications

There are several well-known examples of this, including the sendmail DEBUG option or backdoors placed in the *login* command. Type: Operating System Vulnerability.

4.7.1.7.7 Unwise use of File Interpreters

Tools such as MIME-enabled mail clients, postscript viewers, shell, awk, or perl interpreters can be used to interpret ostensibly useful files that may contain Trojan horse commands that will perform unauthorized actions. Type: Application Vulnerability.

4.7.1.7.8 Unusual Filenames

Filenames can contain unusual characters that have meaning to the shell and may be invoked to perform unauthorized actions if passed to the shell via the *xargs* or *find* commands. Type: Configuration Vulnerability.

4.7.1.7.9 File Transfer Protocol Misconfigurations

Any protocol that facilitates file transfer (FTP, HTTP) may be misconfigured to permit unauthenticated users to overwrite files. Another pitfall is that anonymous write and read access may be used to set up a non-traceable data transfer point for illicit data distribution. Type: Configuration Vulnerability.

4.7.1.7.10 Poor CGI Script Data Checking

CGI scripts are commonly written quickly, are assumed to have a well-behaved and friendly user sets, and are rarely rigorously tested. Parsing errors, buffer overruns, SUID program concerns, poor file permissions, etc., all apply with the exception that HTTP servers rarely demand any authentication whatsoever. Type: Application Vulnerability.

4.7.1.8 Intermediate and End Node Security

4.7.1.8.1 Operating system vulnerabilities

Introduced from within an operating system design or implementation, these are difficult to address in a timely fashion, although vendors do place a relatively high priority on addressing high-profile bugs.

4.7.1.8.2 Protocol-specific vulnerabilities

These vulnerabilities are characteristic of a protocol and are often most intractable since modification of the protocol may cause equipment to lose interoperability.

4.7.1.8.3 Application-specific vulnerabilities

Like operating system vulnerabilities, these are difficult to address since the vendor is not in the position to fix security weaknesses. Unlike operating system vulnerabilities, these weaknesses are seen as being limited in scope, and application vendors are more likely to spend their time correcting bugs in future releases than to spend their time issuing patches for identified vulnerabilities in deployed systems.

4.7.1.8.4 Weak Physical Security

If an interloper has physical access to a host, no security remedies will be effective. A host can be rebooted from removable media and disks remounted. Disks can be removed altogether for analysis elsewhere. The host can be destroyed. Backup tapes can be stolen.

With physical access to a network, an interloper can eavesdrop on traffic, gathering data for future intrusions to other hosts on the network.

4.7.1.8.5 TCP Hijacking

By guessing the ongoing TCP sequence numbers and forging the IP source address, an intruder can inject forged packets into a TCP session. By setting the source route option on the packets, the intruder can also redirect the victim's traffic from the correct host to the intruder's. Freeware is readily available today that automates attacks against this vulnerability. Type: Protocol Vulnerability.

4.7.1.8.6 X-Windows Vulnerabilities

The X-Windows protocol is notorious for incorporating only the most rudimentary authorization and can permit intruders to monitor or even take over X sessions. Type: Protocol Vulnerability.

4.7.1.8.7 SNMP Vulnerabilities

SNMP v1 agents authenticate based upon two passwords, one for reading and one for writing, stored in cleartext in a configuration file that is readable only with privilege, when properly configured. The default values are commonly "public" and "private" and are rarely changed. Intruders may obtain and perhaps modify system configuration data. These passwords are called community names, and the community name was passed along with the data packet in clear text. This allowed anyone to eves-drop and learn the SNMP community name or password. Type: Configuration Vulnerability.

SNMP v2 was designed to have better security, everything in the packet except for the destination address is encrypted. Inside the encrypted data is the community name and source IP address. SNMPv2 uses the Data Encryption Standard (DES) symmetric secret key encryption algorithm for encrypting the data packets

SNMPv3 provides the latest architecture for SNMP security. It incorporates an SNMP context engine ID to encode and decode SNMP contexts. SNMPv3 provides three levels of security. The highest level is with authentication and privacy. The middle level is with authentication and no privacy and the bottom level is without authentication or privacy. The Data Encryption Standard (DES) symmetric secret key encryption algorithm is still used for encrypting the data packets. A symmetric secret key is used along with a message digest algorithm (MD5) to provide data-origin authentication.

Both SNMPv2 & SNMPv3 rely on the use of symmetric secret keys but do not define any form of key management. Type: Protocol Vulnerability.

Consequently manually performed management is required. Type: Configuration Vulnerability.

4.7.1.8.8 Routing Protocol Vulnerabilities

Only the simplest, most static, or most critical routing tables are maintained by hand; all others rely upon routing protocols for update to respond to network architecture changes or equipment failures. Denial of service attacks are simplest; if one can introduce routing table entries that

produce routing loops or misroute packets to nonexistent routers, packets will be lost. Distance-vector protocols such as RIP, IGRP, BGP-4, and EGP are most vulnerable to this attack. Likewise, routes may be advertised that introduce traffic delays, steal others' bandwidth, or deliver traffic to the attacker's network to eavesdrop or facilitate man-in-the-middle attacks. Routing protocols based on TCP (BGP-3, BGP-4) can be defeated by sending a forged RST packet to a router which tears down the session, and renders the router "dead" from other routers' perspectives. Type: Protocol Vulnerability.

Even static routing tables may be subverted if the router accepts ICMP redirects or is managed via a non-secure management protocol such as SNMPv1/2/3 or CMIP.

Although versions of some routing protocols (RIP v2, OSPF, IS-IS) have been defined that make use of authentication, the default authentication mechanism defined (and the only one implemented thus far) has been plaintext password, which is easily defeated once the password has been purloined through eavesdropping. Even these implementations are uncommon.

4.7.1.8.9 ARP Protocol Vulnerabilities

ARP is a simple protocol used to discover the MAC address of a host given the corresponding IP address. A request with an IP address is broadcast on the network segment and the addressed entity replies with a response containing its MAC address, which the querying entity then caches for several minutes. No authentication is used. Interlopers with access to the network segment or entities on that segment may use ARP spoofing techniques to assume the identity of another network entity for purposes of exploiting trust relationships regarding network file systems, remote command execution or remote procedure calls. Type: Protocol Vulnerability.

4.7.1.9 Vulnerability Summary

Many of the know vulnerabilities are summarized in the table below from: http://www.iss.net (Xforce) and http://www.axent.com (Swat team)

Table 3 - Security Vulnerabilities

System Controls, Identification, Authentication	Information Resource Protection & Networking	Security Auditing	System Integrity & Privileged Authority	Availability Protection	Security Admin & Config. Mgmt	Intermediate & End Node Security
NIS checks	NFS checks	Audit checks	Root & Administrator trust	Unauthorized access attempts	Windows NT and Netbios file system	Information gathering
Password checks	DNS checks	Security patches	Shell config. Checks	Pre-attack probes	HTTPD checks	Vulnerable programs
User checks	Home directory checks		SUID/SGID file checks	Suspicious activity	Remote service checks	Hacker signatures
Group checks	User, system & global trust checks		Malicious code checks	Protocol decodes & exploits	Unauthorized server checks	Physical security
Account setup checks	Insecure file permissions checks				PPP interfaces	Email checks
	Platform specific permissions				System config. checks	Firewall checks

System Controls, Identification, Authentication	Information Resource Protection & Networking	Security Auditing	System Integrity & Privileged Authority	Availability Protection	Security Admin & Config. Mgmt	Intermediate & End Node Security
	RPC checks				Batch checks	Web server checks
	NNTP config.				Startup file checks	Xwindows checks
	SNMP checks				Mount permissions	Web browser checks
	FTP checks				Registry checks	Software version checks
	PPP Interfaces				Printer checks	Application checks
	Network device				Printer config.	
	Mail checks					
	Routing protocol checks					

4.7.2 Threats

4.7.2.1 Threat Agents

An understanding of threats to a Next Generation Network (NGN) is an essential step in formulating an approach that addresses its vulnerabilities. The threats to an NGN are characterized according to a model that takes into account the adversaries, their motivations, their willingness to incur risk, and their likely targets within the NGN architecture. This model is based in part on the US Intelligence community's threat model for information security, although it has been enhanced significantly and refocused to take into account NGN architectures, the specific scenarios under which an NGN will be deployed, and the conditions under which it will operate.

The adversary aspect of the threat model is based on the fact that an adversary is constrained by the resources at his disposal (i.e., backing and equipment), his access, his expertise, and his ability to tolerate risk. An adversary will follow four steps to achieve a successful attack:

1. Identify the objectives of an attack.
2. Identify the target to be attacked, and identify the type of attack that will bring about the desired objectives.
3. Gain access to the target at a level appropriate for the attack.
4. Carry out the attack. This may involve altering the target in ways that cover the evidence of the attack.

Interruption or failure to complete any one of these steps will cause the attack to fail. Therefore the goal of the intended victim is to prevent the adversary from completing at least one of them. A secondary goal is to do this in the most efficient and cost-effective manner.

In the threat model presented here, the adversaries are classed as *insiders* or *outsiders*.

- An **insider** works from within the target organization to attack his targets. An insider is considered extremely dangerous because, by definition, he has a high level of access to potential targets. Furthermore, an insider operates inside the perimeters of protection and has authorization for his actions, has the resources of the target organization at his disposal, and may be highly trusted. In the context of an NGN, the insider threat can be subdivided into three categories: spies, malicious users (e.g., traitors), and users who, through carelessness or ignorance, bring harm to the system or some part of it.
- An **outsider** is an attacker who operates from outside the organization under attack. Such adversaries may make up for this inconvenience through insidious infiltration, brute force attack, guile, or a combination of these. Within the NGN context, outsider adversaries fall into the following categories: terrorists, foreign intelligence, criminals and hackers.

The factors listed above - expertise, access to the target, backing (e.g., money), and tolerance to risk - are considered the adversary's most important constraints. This model characterizes each of these factors on a three-tiered scale of low, medium, and high.

In the area of **expertise**,

- A **High** rating indicates that the adversary has all the knowledge required for a successful, sophisticated, and subtle attack.
- A **Medium** rating indicates that the adversary has a thorough knowledge, but may not be able to pull off a highly sophisticated attack or adapt to changing situations that may require him to modify his attack after he has launched it.
- A **Low** rating indicates that the adversary has rudimentary knowledge sufficient to cause harm, but not sufficient for a complex attack.

In the area of **access**,

- A **High** rating indicates that the adversary has complete access to all resources he needs to mount a successful attack.
- A **Medium** rating indicates that the adversary has total or partial access to some resources necessary to mount an attack.
- A **Low** rating indicates that the adversary has limited access to resources required to mount an attack.

In the area of **backing**, which measures the amount of money, access to expertise, and other factors,

- A **High** rating indicates that the adversary has the backing normally associated with a nation-state or a similar benefactor that deals in annual budgets of billions of dollars.
- A **Medium** rating indicates that the adversary has backing from an organization whose annual budget is measured in millions of dollars.
- A **Low** rating indicates that the adversary has backing from an organization whose annual budget is typically less than a million dollars.

In the area of **risk tolerance**, which indicates how willing the adversary is to accept the severity of the consequences of being caught,

- A **High** rating indicates that the adversary is willing to accept any consequence, including death. Adversaries willing to accept a high risk tolerance often consider themselves to be in a state of war.
- A **Medium** rating indicates that the adversary is willing to sacrifice his job or his freedom, but not his life.
- A **Low** rating indicates that the adversary is unwilling to risk personal loss or harm.

The following table characterizes the adversary model.

Table 4 - Adversary Overview

Adversary		***Expertise***	***Access***	***Financial Backing (Resources)***	***Tolerance to Risk of being caught***
Insider	*Spy*	*Medium to High*	*High*	*Medium/High*	*Low to Medium*
	Disgruntled Employee	*Variable*	*High*	*Low*	*Low*
	Careless or Ignorant User	*Variable*	*High*	*N/R*[2]	*N/R*[2]
	Traitor	*Medium to High*	*High*	*Low*	*Low*
Outsider	*Terrorist*	*High*	*Medium*	*High*	*High*
	Foreign Intelligence	*High*	*High*	*High*	*Medium*
	Criminal	*Low/Medium*	*Medium*	*Low/Medium*	*High*
	Hacker	*Medium*	*Low*	*Low*	*Low*

[1] *Variable* indicates that there is little way to predict the skill set of such adversaries.
[2] *N/R* indicates that the entry is not relevant for that combination of adversary and factor.

Attacks by threat agents typically require use of some form of attack tool, software. The more sophisticated threat agent will frequently develop specialized software for attacking an asset. Some threat agents will rely on existing software that was developed for other purposes, examples of this class of software are vulnerability scanning applications originally developed for valid administrative use. One class of threat agent, know as the "script kiddy", uses software available from web sites that was developed by more sophisticated individuals to facilitate attacks without the user having to know very much about how the attack software works. Currently there are many web sources from which threat agents may obtain attack software and information for launching attacks.

The adversary model helps clarify the source of threats to the NGN architecture, which in turn helps to develop the set of potential threats themselves. The information from the adversary model sets the stage for the explication of the adversary's objectives and the targets he should select to make the attack against those objectives successful, as outlined in steps 1 and 2 of the four steps in a successful attack, above.

Regardless of an adversary's assets and risk tolerance, a target only presents so many general vulnerabilities to be exploited. In the case of an NGN, these vulnerabilities can be found in the following areas: system control, identification and authentication (I&A) mechanisms, information

resources, system integrity, system availability, security administrations, configuration management, communications facilities (the links and equipment itself, as opposed to message contents, which falls under the umbrella of information resources), and the nodes. Therefore these areas represent the general target set for NGN. The following table encapsulates what is known about the adversary model and the objectives of each adversary.

Table 5 - Adversary Targets and Objectives

Adversary	*Targets*	*Example Objectives*
Spy	*Information resources*	*Information, military or economic advantage*
Malicious User	*All, depending on level of expertise and degree of risk tolerance*	*Revenge, retribution, financial gain, institutional change*
Careless or Ignorant User	*All, depending on level of expertise*	*(no malicious objectives)*
Rogue Intelligent Agent	*All, depending on objectives of programming*	*Information, military advantage, chaos, damage to target*
Terrorist	*All*	*Ideological advantage, chaos, damage to target*
Foreign Intelligence	*Information resources, nodes*	*Information; political, military, and economic advantage*
Criminal	*System integrity, availability, communications facilities, nodes*	*Financial gain e, chaos, damage to target*
Hacker	*Information resources, systems controls, I/A, security administration, configuration management, nodes*	*Thrill, challenge, prestige, notoriety*

Although the targets listed in this table apply equally, the ease of acquiring the targets in each case will vary depending on the target's exposure, and the number of people having physical and logical access to it, and of course, the precautions taken to fortify it against attack. However, this threat assessment cannot take these factors into account because they depend on information unavailable at this time. Therefore, an estimate of the likelihood of each type of attack by each adversary cannot be made. Nonetheless, an assessment of specific threats to each of the targets listed above can be made. The following sections provide a brief description of each.

4.7.2.2 Threat - Attack Types

The following table presents an at-a-glance assessment of the targets that each adversary will most likely select when attacking an NGN. This table is derived by inverting Table 2, and is included for the reader's convenience because it indicates the most likely adversaries of each general target.

Table 6 - NGN Adversaries

Target	*Spy*	*Malicious User*	*Careless User*	*Terrorist*	*Foreign Intel.*	*Criminal*	*Hacker*
System Controls, I/A, Audit		*X*	*X*	*X*			*X*
Information Resources	*X*	*X*	*X*	*X*	*X*		*X*
System Integrity		*X*	*X*	*X*		*X*	
Availability		*X*	*X*	*X*		*X*	
Security Administration, Configuration Management		*X*	*X*	*X*			*X*
Communications Facilities		*X*	*X*	*X*		*X*	
Nodes		*X*	*X*	*X*	*X*	*X*	*X*

The threat table shown below indicates the threats associated with each target within an NGN. Together, this table and the one above indicate the nature of the threats and adversaries for each target within the system.

Table 7 - NGN Threats

Target	***Threat***				
	Disclosure	***Denial of Service***	***Illicit Use***	***Modification***	***Damage***
System Controls, I/A, Audit	*X*	*X*	*X*	*X*	*X*
Information Resources	*X*	*X*	*X*	*X*	*X*
System Integrity				*X*	*X*
Availability		*X*		*X*	*X*
Security Administration, Configuration Management		*X*	*X*	*X*	*X*
Communications Facilities		*X*	*X*	*X*	*X*
Nodes		*X*	*X*	*X*	*X*

The following sections address each of the targets listed in the tables above, and assess specific threats against them.

This discussion on targets focuses on assets, irrespective of ownership. The preceding table does not distinguish between assets owned by anyone, e.g., a service provider, residential/business end-user, and any other networked organization.

4.7.2.2.1 System Controls, Identification, Authentication, and Logging

The specific threats resulting from inadequate, poorly managed, or otherwise subverted system entry controls, user identification and authentication, and security audit (logging) are listed in the following three categories: system entry controls, identification & authentication, and security audit.

4.7.2.2.1.1 System Entry Controls

An adversary might take advantage of consoles or other access points on the system if:

- passwords are too simple, thus easy for an adversary to guess

- timeouts for automatic logouts are too long, allowing the adversary to find and commandeer an unattended device
- concurrent sessions are allowed, especially if the sessions can occur simultaneously from access points in different locations (e.g., rooms, buildings), which might permit an adversary to masquerade as a bona fide user even though that user may be logged in to the system elsewhere
- "disabled" or obsolete LoginIDs are not administered correctly, thus allowing an adversary to discover and use them.

It is important that controls meant to limit system entry be administered and maintained correctly in order to reduce the chances of an adversary taking advantage of them. This means that the controls should be set to the most secure configuration that does not prevent users from performing their jobs, that changes to the system entry controls should be subject to security audit (logging), and that the administrators of the controls should be trusted and should be audited (or both, to prevent accidents).

4.7.2.2.1.2 Identification and Authentication

An adversary may steal a LoginID/password combination, the consequences of which could include damage to the systems, theft of data, and denial of service for other users. The adversary may gain access to the LoginID/password combination by forcing or tricking a user into revealing it, by eavesdropping on a network over which it is being transmitted, by identifying trust relationships which enable logins without passwords, by finding a cleartext version stored in another host to which the target machine is linked, or by performing a dictionary attack against a hashed password file.

An adversary might take advantage of a policy that allows many users to use a single LoginID, since such a policy could provide cover for illicit activities by its inability to provide accountability. The threats to the system include damage, theft of data, and denial of service.

4.7.2.2.1.3 Security Audit

A poor or disabled security audit (logging) function raises the threat of malice by adversaries having low to medium risk tolerance. This follows from the deterrent properties of logging, which, by its presence, will discourage adversaries who do not want to risk exposure and who do not have the expertise to subvert the logging facilities.

The logging facility can be subverted if:

1. it is inadequate to provide accountability to the detail necessary to discourage abuse and to trace illicit activity to its source.
2. it cannot protect its audit records (the log itself) from unauthorized access, alteration, or destruction.
3. its configuration and controls can be altered by an adversary to prevent it from operating properly.

A serious adversary can take advantage of any or all of these factors as a prelude to other attacks on the system.

4.7.2.2.2 Information Resource Protection

The specific threats to information resources are theft of sensitive data, destruction of data, and modification of data either overtly or subtly. Information resources may be threatened if an adversary can:

- circumvent weak or incorrectly administered access control mechanisms , for example those meant to protect WIN databases or files within the C^3I system
- take advantage of lax or incorrectly configured file permissions. Files or directories that give read or write permission to the world, or that are configured to permit remote mounting are open to the threats of theft, subversion, and destruction.
- alter the access control permissions on files or directories through poorly secured administrative controls
- exploit weak or nonexistent file permission on temporary files. Temporary files that are not well protected (precisely because they are thought of as temporary, for instance) can be exploited by an adversary in several ways, including: theft of data, subversion of a database by altering a temporary file whose contents will be used to update that database, and subversion of an application that depends on correct data in the temporary file for one reason or another.
- exploit weak or poorly encrypted files (because of inadequate encryption mechanisms) to learn the contents of sensitive data in a file or database
- discover the on-line encryption keys, for example keys that protect WIN information resources
- erase critical data, destroy vulnerable databases, file, or directories
- gain access to data in transit across a network
- force or fool a person into revealing the contents or location of sensitive information
- force or fool a person into revealing the encryption keys used to protect sensitive information
- force or fool a person into executing commands or software.

4.7.2.2.2.1 System Integrity and Privileged Authority

System integrity is subject to the threats of loss or degradation by an adversary who compromises the configuration, the operating system, or one or more applications if that adversary is able to:

- gain control of an application that is running with a higher privilege (e.g., file owner) than its users would normally have
- take advantage of a race condition that might allow the adversary to replace or alter a shell script at a critical time just as it is being loaded and readied for execution
- take advantage of weaknesses, inconsistencies, or “features” in the operating system or shell interpreter to force a shell to grant privileges that a user would not normally have
- take advantage of unnecessarily permissive trust relationships among hosts or nodes to gain access or control of one or more hosts or nodes

- take advantage of weaknesses in software (either published or unpublished) to gain unauthorized access
- insert viruses, Trojan horses, or other subversive or destructive logic into one or more hosts
- compromise intelligent agents, operating systems, or other software or configuration files and controls, either by electronic means or through "social" efforts such as force or trickery
- launch an intelligent agent having the capability to sabotage the mobile agent system to halt all other agents.

4.7.2.2.3 Availability Protection

The threats to availability are brought about by actions that restrict, alter, or halt the normal operations of the system. Availability may be affected at the level of a single user, a group of users, the entire user community (in which case the system is effectively taken out of commission), or the network. An adversary may limit or deny availability if he is able to:

- gain physical access to the system and physically incapacitate or destroy all or part of it
- obtain physical access to control consoles, remote terminals, or other access points, and take over control of the system, hosts, or nodes by using administrative or operations features
- gain logical access and incapacitate the system through modification of onboard software (e.g., applications, operating system), alteration of configuration parameters, removal of critical files (e.g., a password file) or directories
- gain logical access and insert destructive software (e.g., worms, Trojan horses, malicious Intelligent Agents) that causes outages; intermittent problems; erasure of files or data; denial of access to files, data, or applications; alteration of system configuration; or other unwanted effects
- cause the system to engage in unproductive activity to the exclusion of all else. Malicious software that subverts the operating systems scheduler is one cause of this type of problem.
- cause the system's communications to become unavailable. Well-known IP, TCP, and ICMP attacks are among the methods known to create this effect. Some such attacks can result in other types of unavailability as well, as the system allocates more resources to the processing that these attacks trigger.
- subvert backup media or backup systems and render them useless prior to an attack upon the system itself
- disable mechanisms that support automatic restart of the systems after an outage, automatic restoration of communications after a loss, automatic error detection and correction, automatic intrusion detection (should it exist), self-diagnostics, or fault tolerance
- cause a loss of power or a reduction of power sufficient to incapacitate the system (this requires physical or logical access to the electrical distribution facilities or power grid that feeds the system)
- cause a surge of power to destroy the electrical components of the system (this requires physical or logical access to the electrical distribution facilities or power grid that feeds the system)

- effect a disruption of the environmental systems that control temperature, humidity, water levels, and other factors. Environmental systems that can be controlled remotely are susceptible to attack through Internet connections or other network connections.
- create man-made disasters
- incapacitate or eliminate all personnel who are able to operate and maintain the system
- incapacitate the systems and networks due to a natural disaster
- steal equipment or computing time, which could result in a loss of response.

4.7.2.2.4 Security Administration and Configuration Management

The security administration and configuration management become tools of an adversary if he is able to:

- introduce configuration changes that weaken the system's security. Lowering default security access control, turning off security audit mechanisms, and simplifying the password complexity rules are among the ways an adversary might weaken system security.
- take advantage of weak or inconsistent security configurations that may be the result of an administrative error or an attempt to introduce changes or shortcuts that facilitate tedious tasks
- obtain privileges by taking advantage of configuration vulnerabilities, operating system vulnerabilities, or protocol vulnerabilities. Vulnerable programs such as finger, tftp, rexd, and others offer back doors and other entry points for attackers. Errors in assigning paths can also result in vulnerabilities that an adversary can exploit to skirt security.
- find backdoors in applications (published and unpublished), which he can use to circumvent security and configuration barriers
- force or fool a security administrator into revealing passwords, changing security parameters, or altering the configuration of the system to a less secure configuration
- gain administrative control of the system by overriding the administrative console remotely or taking over the administrative console locally (e.g., by force)
- capture Intelligent Agents and decipher sensitive data that can be used to exploit the exposed systems
- capture critical Intelligent Agent infrastructure components (e.g. dispatchers, gatekeepers).

4.7.2.2.5 Intermediate and End Node Security

The end nodes and intermediate nodes are subject to physical assault and logical attack from adversaries who have either direct or remote access, or both. The threats include destruction of the nodes, tampering, subversion, and alteration of the nodes' functions. An adversary can harm the node if he is able to:

- obtain physical access to the node, the infrastructure that houses it, or the communications channels that link it to other nodes
- obtain remote or local access to the node over a communications channel or network.

Once the adversary has obtained access, he may be in a position to threaten other nodes if he can establish communications to them from the subverted node. Such actions could lead to a cascade effect that might eventually corrupt most or all of the nodes in the network.

4.7.2.3 Existing Threat Analyses and Methodologies

Two existing international standards provide some guidance for performing threat analysis: ITU-T X.800/ISO 7498-2 and ITU-T X.805.

4.7.2.3.1 ITU-T X.800/ISO 7498.2 Approach to Threat Analysis

ITU-T X.800/ISO 7498-2 includes an informative annex (ANNEX A) which deals with threat analysis as follows:

> "A.2.4 Threats
>
> The threats to a data communication system include the following:
>
> a) destruction of information and/or other resources;
>
> b) corruption or modification of information;
>
> c) theft, removal or loss of information and/or other resources;
>
> d) disclosure of information; and
>
> e) interruption of services.
>
> Threats can be classified as accidental or intentional and may be active or passive.
>
> A.2.4.1 Accidental threats
>
> Accidental threats are those that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs.
>
> A.2.4.2 Intentional threats
>
> Intentional threats may range from casual examination using easily available monitoring tools to sophisticated attacks using special system knowledge. An intentional threat, if realized, may be considered to be an "attack".
>
> A.2.4.3 Passive threats
>
> Passive threats are those which, if realized, would not result in any modification to any information contained in the system(s) and where neither the operation nor the state of the system is changed. The use of passive wire tapping to observe information being transmitted over a communications line is a realization of a passive threat.
>
> A.2.4.4 Active threats
>
> Active threats to a system involve the alteration of information contained in the system, or changes to the state or operation of the system. A malicious change to the routing tables of a system by an unauthorized user is an example of an active threat.
>
> A.2.5 Some specific types of attack
>
> The following briefly reviews some of the attacks of particular concern in a data processing/data communications environment. In the following sections, the terms authorized and unauthorized appear. "Authorization" means "the granting of rights". Two things implied by this definition are: that the rights are rights to perform some activity (such as to access data); and that they have been granted to some entity, human agent, or process. Authorized behavior, then, is the performance of those activities for which rights have been granted (and not revoked).
>
> A.2.5.1 Masquerade
>
> A masquerade is where an entity pretends to be a different entity. A masquerade is usually used with some other forms of active attack, especially replay and modification of messages. For instance, authentication sequences can be captured and replayed after a valid authentication

sequence has taken place. An authorized entity with few privileges may use a masquerade to obtain extra privileges by impersonating an entity that has those privileges.

A2.5.2 Replay

A replay occurs when a message, or part of a message, is repeated to produce an unauthorized effect. For example, a valid message containing authentication information may be replayed by another entity in order to authenticate itself (as something that it is not).

A.2.5.3 Modification of messages

Modification of a message occurs when the content of a data transmission is altered without detection and results in an unauthorized effect, as when, for example, a message "Allow 'John Smith' to read confidential file 'Accounts" is changed to "Allow Fred Brown' to read confidential file 'Accounts".

A.2.5.4 Denial of service

Denial of service occurs when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions. The attack may be general, as when an entity suppresses all messages, or there may be a specific target, as when an entity suppresses all messages directed to a particular destination, such as the security audit service. The attack may involve suppressing traffic as described in this example or it may generate extra traffic. It is also possible to generate messages intended to disrupt the operation of the network, especially if the network has relay entities that make routing decisions based upon status reports received from other relay entities.

A.2.5.5 Insider attacks

Insider attacks occur when legitimate users of a system behave in unintended or unauthorized ways. Most known computer crime has involved insider attacks that compromised the security of the system. Protection methods that can be used against insider attacks include:

a) careful vetting of stuff;

b) securitization of hardware, software, security policy and system configurations so that there is a degree of assurance that they will operate correctly (called trusted functionality); and

c) audit trails to increase the likelihood of detecting such attacks.

A.2.5.6 Outsider attacks

Outsider attacks may use techniques such as:

a) wire tapping (active and passive);

b) intercepting emissions;

c) masquerading as authorized users of the system or as components of the system; and

d) bypassing authentication or access control mechanisms.

A.2.5.7 Trapdoor

When an entity of a system is altered to allow an attacker to produce an unauthorized effect on command or at a predetermined event or sequence of events, the result is called a trapdoor. For example,. a password validation could be modified so that, in addition to its normal effect, it also validates an attackers password.

A.2.5.8 Trojan horse

When introduced to the system, a Trojan horse has an unauthorized function in addition to its authorized function. A relay that also copies messages to an unauthorized channel is a Trojan Horse."

As can be seen, the X.800 threat analysis does not comprehensively address threat agents nor attack types. The threat analysis in section 4.6.3.1 and 4.6.3.2 go into significant detail beyond that covered in X.800.

4.7.2.3.2 ITU-T X.805 Approach to Threat Analysis

X.805 provides a discussion for performing threat analysis by examining the five ITU-T X.800 threats in the context of the three types of activities (management, control and end user) that occur on network infrastructures, services and applications.. By itself, X.805 is not sufficient in guiding a reader through the performance of a vulnerability and threat analysis. However, X.805 does map security threats against its security dimensions. When coupled with expert assistance, X.805 offers the reader with a focused set of issues to consider.

4.7.2.3.3 STRIDE

In 2003 two Microsoft employees, as part of a Microsoft "Trustworthy Computing" initiative[15], formulated a model for threat analysis named after the following six identified categories of threats:

- **S**poofing identity
- **T**ampering with data
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service, and
- **E**levation of privilege.

These categories actually reflect generic forms of attacks and represent an amalgam of the threats identified in Table 7("- NGN Threats") and can be mapped as follows in Table 8:

Table 8 - Mapping STRIDE Threat Categories to NGN Threats

STRIDE Threat Category	NGN Threats from Table 7
Spoofing identity	Disclosure; Illicit Use; Modification; Damage
Tampering with data	Modification; Damage
Repudiation	Illicit Use; Modification
Information disclosure	Disclosure
Denial of service	Denial of Service
Elevation of privilege.	Disclosure; Illicit Use; Modification; Damage

The primary value to the STRIDE view of threats is as a model to categorize attacks that should be considered when developing software. However the STRIDE approach does not lend itself well to performing a threat analysis of distributed information systems.

4.7.2.3.4 Common Criteria (CC)

The CC's roots go back to 1983 with the US Trusted Computer Security Evaluation Criteria published as DoD 5200.28-std 1985 (a.k.a. TCSEC, "The Orange Book"). Over the following decades, work continued in the U.S., Canada and Europe (ITSEC). Version 1.0 of the CC was published for comment in January 1996 NIST and version 2.0 was adopted as ISO 15408 in 1999. There are three parts to the CC:

- Introduction and General Model (Part 1),
- Security Functional Requirements (Part 2),
- Security Assurance Requirements (Part 3).

[15] Michael Howard, David LeBlanc, "Writing Secure Code", Microsoft Press, 2003

The Common Evaluation Methodology (CEM) expands on Part 3 supplying details on the conduct of assurance activities. The CC and CEM continue to evolve with use and propagated through the use of Interpretations, which are formal changes periodically made to the CC/CEM that have been mutually agreed by the participating producing nations.

The CC is not currently intended for security evaluations of complete communications infrastructures, i.e. complete systems of interconnected processing and communications elements. A Common Criteria security assessment is very individual element (product) focused. An element (product) is referred to as a Target Of Evaluation (TOE) and the analysis is restricted to validating the specifications and implementation rather than the security requirements needed to mitigate threats or vulnerabilities. There are no interoperability considerations for the operational environment.

A description of the applicability of each part of the CC to the three major types of interested parties (Consumers, Developers and Evaluators) is shown in Table 9.

Table 9 - CC Parts related to Parties

	Consumers	**Developers**	**Evaluators**
Part 1: Introduction and General Model	For background information and reference purposes	For background information and reference for the development of requirements and formulating security specifications for TOEs	For background information and reference purposes. Guidance structure for Protection Profiles (PPs) and Security Targets (STs)
Part 2: Security Functional Requirements	For guidance and reference when formulating statements of requirements for security functions	For reference when interpreting statements of requirements and formulating functional specifications of TOEs	Mandatory statement of evaluation criteria when determining whether TOE effectively meets claimed security functions
Part 3: Security Assurance Requirements	For guidance when determining required levels of assurance.	For reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs	Mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs

The CC discusses security using a hierarchical framework of security concepts and terminology as follows:

Table 10 - CC Security Concepts and Terminology

Security environment	Laws, organizational security policies etc, which define the context in which the TOE is to be used. Threats present in the environment are also included.
Security objectives	A statement of intent to counter the identified threats and/or satisfy intended organizational security policies and assumptions.
TOE security requirements	The refinement of the IT security objectives into a set of technical requirements for security functions and assurance, covering the TOE and its IT environment.
TOE security specifications	Define an actual or proposed implementation for the TOE.
TOE implementation	The realization of a TOE in accordance with its specification.

When applying the CC in a development context:

- The application of the CC will require defining a set of IT requirements of known validity which can be used in establishing security requirements for prospective products and systems. The CC also defines the Protection Profile (PP) construct which allows

prospective consumers or developers to create standardized sets of security requirements which will meet their needs.

- The Target of Evaluation (TOE) is that part of the product or system which is subject to evaluation. The TOE security threats, objectives, requirements, and summary specification of security functions and assurance measures together form the primary inputs to the Security Target (ST), which is used by the evaluators as the basis for evaluation.

When applying the CC in an operational context for product evaluation or operation:

- The principal inputs to evaluation are the Security Target, the set of evidence about the TOE and the TOE itself. The expected result of the evaluation process is a confirmation that the ST is satisfied for the TOE, with one or more reports documenting the evaluation findings.
- Once a TOE is in operation, vulnerabilities may surface, or environmental assumptions may require revision. Reports may then be made to the developer requiring changes to the TOE. Following such changes reevaluation may be required.

Protection Profiles (PP) define an implementation-independent set of security requirements and objectives for a category of products or systems which meet similar consumer needs for IT security. A PP is intended to be reusable and to define requirements which are known to be useful and effective in meeting the identified objectives. The PP concept has been developed to support the definition of functional standards, and as an aid to formulating procurement specifications. PPs have been developed for firewalls, relational databases, etc, and to enable backwards compatibility with TCSEC B1 and C2 ratings. A Security Target (ST) contains the IT security objectives and requirements of a specific identified TOE and defines the functional and assurance measures offered by that TOE to meet stated requirements. The ST may claim conformance to one or more PPs, and forms the basis for an evaluation. The evaluation assurance levels used in the CC are shown below along with their relationship to the U.S. TCSEC and European ITESC.

Table 11 - Evaluation assurance level equivalency

Common Criteria	US TCSEC	European ITSEC
-	D: Minimal Protection	EO
EAL1 - functionally tested	-	-
EAL2 - structurally tested	C1: Discretionary Security Protection	E1
EAL3 - methodically tested and checked	C2: Controlled Access Protection	E2
EAL4 - methodically designed, tested and reviewed	B1: Labeled Security Protection	E3
EAL5 - semi formally designed and tested	B2: Structured Protection	E4
EAL6 - semi formally verified design and tested	B3: Security Domains	E5
EAL7 - formally verified design and tested	A1: Verified Design	E6

The primary value of the CC to TSPs is the systematic approach to identifying the vulnerabilities within, and the threats to, each element deployed in the TSPs infrastructure. In theory one

should be able to then develop an aggregate value that represents the level of assurance a TSP should have that its security requirements are being met and the degree to which the TSP is able to obtain its security objectives. Use of the CC by TSPs and suppliers is complementary to any ISMP based on ISO 27001 and CMMI.

4.7.3 Risk Analysis

A quantifiable Risk Analysis (a.k.a. Vulnerability Threat Analysis - VTA) requires the following be performed:

1 Identify each asset and its value (physical and logical, such as equipment, data, services, reputation, …)
2 Identify any vulnerabilities within or related to each asset = type of asset exposure (degree of exposure), duration of asset exposure
3 Identify all threats to each asset = type of threat agent, method of attack by threat agent, probability of attack occurring, probability of attack success, degree of damage to targeted asset as a percentage of asset value

In theory this approach allows one to calculate the probability of damage to an asset over a specified timeframe and can be restated as:

- Asset A_X has a value of $\$_X$, exposure degree of ED_X, exposure timeframe as ET_X
- Threat T_Z is composed of Thread Agent TA_Z, an Attack A_Z, which has a probability of occurrence AO_Z which has a probability of success AS_Z resulting in percent of damage AD_Z

$= T_Z (A_X)$ = Magnitude of damage in $ over timeframe

Unfortunately TSPs, who have to assume a defensive posture, are not in a position to:
- identify all threat agents in advance
- identify all forms of attacks in advance,

and, therefore, do not typically have sufficient statistics on attack frequencies and attack success likelihood.

Furthermore the value of many organizational assets are difficult to quantify so TSPs generally take a Due Diligence approach, rather that strict VTA methodology. The architecturally oriented VTA approach:

- Ensures appropriate security mechanisms are selected and instantiated in appropriate places, and
- Ensures security mechanisms do no degrade services as perceived by authorized users.

The lack, or non-availability, of attack actuarial data and corresponding information on the magnitude of damage inflicted by successful attacks typically results when either:
- the corporation is unwilling to admit it has been the target of a successful attack because it may possibly suffer from a decrease in consumer confidence and possibly an adverse stock market reaction to the disclosure, or
- the corporation does not have security surveillance capabilities or procedures in place to recognize that attacks are occurring whether the attacks are successful or not.

4.7.4 ETSI Security Related Efforts

ETSI TISPAN has conducted a security threat, vulnerability and risk analysis (TVRA, see ETSI TR 187002) in the course during developing their NGN Release 1 security. While TR 187002 does not claim to be complete, at least two important scenarios for release 1 have been security

analyzed: PSTN/ISDN Emulation and NASS-IMS bundled authentication. TR 187002 applies structured and systematic methods to conduct a TVRA as defined by ETSI TS 102 165-1 that requires calculating the risk level by assessing the impact and the occurrence likelihood for each identified security threat and by taking into account the attack potential represented. by rating the attacker's capabilities.

ETSI has also developed:

- ETSI Guide 202 387 is a guide to the development of standards that allow compliant product to be considered for product evaluation under the Common Criteria scheme,
- ETSI ES 202 382 "Security Design Guide; Method and proforma for defining Protection Profiles" provides guidance on the preparation of Protection Profiles (PP) based upon ETSI communication standards,
- ETSI ES 202 383 "Security Design Guide; Method and proforma for defining Security Targets" provides guidance on the preparation of Security Targets (ST) based upon ETSI communication standards. The detailed contents of an ST are specified in ISO/IEC 15408 1, and
- TS 102 556 defines 3 partial Protection Profiles (PPs) for security capabilities in the NGN and conforms to the guidance and PP Proforma available in ES 202 382 with respect to the guidelines found in EG 202 387.

Further study is required to merge ETSI work in these areas with the material and methodology within this TR.

4.8 Security Modeling

Historically a key component of security systems engineering includes selection or development of a security model to:

1) describe the entities (subjects governed by an organization's security policy and
2) define the access rules necessary to instantiate said policy.

These security models typically focus on either confidentiality via access controls or information integrity; where some are formally defined and others informally defined.

The major examples of Security Models are:

- Bell-LaPadula,
- Harrison-Ruzzo-Ullman,
- Chinese Wall Model,
- Biba, and
- Clark-Wilson

Each of these models is discussed in more detail below and conclusions presented as to the value and applicability of each in a converged services infrastructure.

4.8.1 Integrity; Confidentiality Policies versus Integrity Policies

Before discussion security models consideration must be given to the differences between confidentiality and integrity policies. Confidentiality policies consider: 1) Leakage of rights and 2) Information flow; whereas Integrity policies consider: 1) Data integrity (Who may modify data and under what circumstances it may be modified) and 2) Authorization (origin/identity integrity and authentication).

Confidentiality oriented security models mostly focus on hierarchical security levels to control access to objects (information) whereas Integrity oriented security models mostly focus on separation of duties, separation of functions and auditing.

Regarding the “commercial” requirements for confidentiality:

- In the “military” environment, access to a security level brings the ability to access data classified to that level
- In a commercial setting, roles are too informal for the assignment of clearances
  - It would make more sense to have fewer levels and many more categories
  - Organizational structures make the management of levels and categories difficult
  - Commercial enterprises have to deal with the problem of information aggregation
  - Collections of innocuous information can be mined to discover sensitive information

A formal definition of integrity can be stated as:

- If E is a set of entities and I is some information
- then I has the property of integrity with respect to X if all x Є X trust information I.

Although theoretically valid, this is not a very useful definition, something a little more constructive is needed. Lipner (1982) articulated the following set of integrity requirements:

1) Users will not write their own programs, will use existing production programs and databases
2) Programmers:
   - will develop / test programs on non-production system
   - if access needed to actual data, production data supplied via a special process, but used on development system
3) A special process must be followed to install a program from the development system onto the production system
4) The special process in requirement 3 shall be controlled and audited
5) The managers and auditors must have access to both the system state and the system logs that are generated

These requirements reflect the following principles of operation:

- Separation of duties: If two or more steps are required to perform a critical function then at least two different people should perform the steps
- Separation of functions: Developers do not develop new programs on production systems nor process production data on development systems
- Auditing: Logging must be in place to enable one to determine what actions took place when and by whom

4.8.2 Available Security Models

4.8.2.1 Bell-LaPadula

The Bell-LaPadula (BLP) model is one of the earliest ones developed and expresses the security policy that is currently in place. BLP is a state machine model that:

- captures the confidentiality aspects of access control
- Access permissions defined through
  - an access control matrix
  - and security levels

The security policy represented prevents flow of information from a high security level to a low security level via access restrictions used to reflect control of information confidentiality. This type of policy is frequently referred to as Multi-level Security (MLS) even though BLP only considers the information flow that occurs when a subject observes or alters an object. The Bell-LaPedula only addresses data confidentiality and does not address integrity of data. Furthermore BLP, by itself does not include the ability to add subjects, objects and access rights to the access control matrix unless extended as done by the Harrison-Ruzzo-Ullman model below.

4.8.2.2 Harrison-Ruzzo-Ullman

As noted above, BLP has no mechanisms for changing access rights or for the creation and deletion of subjects and objects. The Harrison-Ruzzo-Ullman (HRU) model defines authorization systems that address these issues. The following six primitive operations for manipulating subjects, objects, and the access matrix are specified by HRU:

- **enter** *r* into M_{so} **delete** *r* from M_{so} **create** subject *s* **delete** subject *s* **create** object *o* **delete** object *o*

where r represents a new access right, M_{so} represents the matrix cell for a subject s and an object o. A key purpose of HRU was to:

- Model policies for allocating access rights
- Verify compliance with a given policy, we have to check that no undesirable access rights can be granted.

Most operating systems that provide what is called 'multi-level security' for systems labeled as "compartmented mode workstations" are actually based on the HRU extensions to BLP.

4.8.2.3 Chinese Wall Model

The Chinese Wall Model, also referred to as a multilateral security model, is based on the concept that:

- Access is only granted, to an object by a subject, if the object requested:
  - is in the same dataset as all other objects already accessed by that subject, or
  - the object does not belong to any of the "conflict of interest classes" of all other objects already accessed by that subject, i.e., belongs to an entirely different conflict of interest class.

So this multilateral approach requires keeping track of:

- which objects a subject already had accessed, and
- what conflict of interest class is associated with each object.

Indirect information flow is still possible as in the following example:

- Two competitors, Company A and Company B, have their accounts with the same Bank.
- Analyst A, dealing with Company A and the Bank, updates the Bank portfolio with sensitive information about Company A
- Analyst B, dealing with Company B and the Bank, now has access to information about a competitor’s business

To negate this indirect information flow the write-access must be regulated based on a "conflict of interest class", namely:

- Write access to an object is only granted if no other object can be read which is in a different company dataset and contains un-sanitized information

This security model is extremely difficult to implement, and compliance with it is nearly impossible to verify, making it of marginal value in nearly all modern complex systems.

4.8.2.4 Biba

The Biba model was developed after the BLP model and attempts to ensure the information integrity of data through application of the following two rules:

- A subject with a lower classification cannot write data to a higher classification.
- A subject with a higher classification cannot read data from a lower classification,

so information always flows downwards in this model and never upward.

The Biba integrity model, as a system, consists of a set of subjects S, objects O, integrity levels I, and a domination relation ≤ on I x I where Function i() returns the integrity level of an entity. This model has read/write rules similar to Bell-LaPadula model where:

- s Є S can read o Є O iff i(s) ≤ i(o)
- s Є S can write o Є O iff i(o) ≤ i(s)
- s1 Є S can execute s2 Є S iff i(s2) ≤ i(s1).

[Note:
- the symbol Є (the Greek letter Epsilon) is used in mathematics to represent membership within a set of distinct objects considered as a whole
- the notation i(s) represents the integrity level of subject s
- iff represents 'if and only if']

A basic assumption with Biba is that a subject with a higher classification is more trustworthy than a subject with a lower classification. This assumption may not be valid as a subject with a higher classification may have ulterior motives; hence this model should not be used.

4.8.2.5 Clark-Wilson

The Clark-Wilson model addresses security requirements of commercial applications by addressing three aspects of integrity:

- Modifications to data are not made by unauthorized users or processes,
- Unauthorized modifications to data are not made by authorized users or processes,
- Data is internally and externally consistent; a given input produces an expected output.

Emphasizing *information integrity* as illustrated in the following example:

- A purchasing clerk creates an *order* for a supply, sending copies to the supplier and the receiving department
- Upon receiving the goods, the receiving clerk checks the delivery and, if all is well, signs a *delivery form*. Delivery form and the original order go to the accounting department
- Supplier sends an *invoice* to the accounting department. Accounting clerk compares the invoice with the original order and the delivery form and issues a *check* to the supplier

so that performing these steps in order, performing exactly the steps needed, and authenticating the individuals who perform the steps constitutes a well-formed transaction.

Mechanisms for maintaining *information integrity* are:

- Well-formed transactions and separation of duties
- Well-formed transactions
  - Data items can only be manipulated by a specific set of programs
  - Users have access to programs rather than to data items

- Separation of duties
  - Users have to collaborate to manipulate the data and to collude to penetrate the security system

Well-formed transactions move the system from one consistent state to another so rules are required to ensure someone examines/ certifies that transactions are done correctly. This is achieved using the following entities:

- CDIs: Constrained data items — data subject to integrity controls
- UDIs: Unconstrained data items — data not subject to integrity controls
- IVPs: Integrity verification procedures — procedures to test that CDIs conform to the integrity constraints
- TPs: Transaction procedures — procedures that take the system from one valid state to another

under the constraints of the following certification rules:

- When any IVP is run, it must ensure all CDIs are in a valid state
- Each CDI is are associated with a particular TP where the association defines a certified relation between CDI and TP
- A TP, certified for a set of CDIs, will only transform those CDIs, in a valid state, into a (possibly different) valid state, e.g., The TP “deposit funds” is certified (by whom?) for the CDIs “checking accounts”

and enforcement rules:

- The system shall maintain the certified relations and must ensure that only TPs certified to run on a CDI manipulate that CDI
- The system shall:
  - Associate a user with each TP and set of CDIs
  - Authorize the TP to access those CDIs on behalf of the associated user
  - Assure that no TP can access a CDI on behalf of a user not associated with that TP and CDI
- More simply, the system must.
  - Maintain and enforce the certified relation Restrict access based on user ID.

The above rules result in a set of relations each defined over the entities of a triple: (user, TP, {CDI set}) where the allowed relations shall meet the requirements imposed by the principle of separation of duty. The system shall authenticate each user attempting to execute a TP. However the type of authentication is undefined and depends on the instantiation (implementation). Note that authentication is not required before using “the system,” but is required before manipulation of CDIs (i.e., before using TPs).

Logging is also critical in that an auditor needs to be able to determine what happened during a review of transactions. Thus all TPs must append to an append-only CDI enough information to reconstruct the operation (the append-only CDI is the log).

Handling untrusted input requires that any TP that takes a UDI as input may perform only valid transformations, or no transformations. Consequently the TP must do this for all possible values of the UDI. The transformation either rejects the UDI or transforms it into a CDI and the TP shall validate values and transform them into a CDI before using them. If the validation fails the TP rejects the UDI.

Separation of duties with respect to certified and allowed relations is enforced by:

- Only the certifier of a TP may change the list of entities associated with that TP

- No certifier of a TP, or of an entity associated with that TP, may ever have execute permission with respect to that entity.

From the above discussion, it is apparent that Clark-Wilson satisfies all of Lipner's requirements except for #2 regarding program development and use of production data. Clark-Wilson does not address #2 since this is a procedural requirement so the model doesn't directly cover it. No technical controls can prevent a programmer from developing a program on a production system. The usual operational control relied upon is to simply delete software development tools from the production system. However the "special process" in #2 certainly corresponds to using a TP to sanitize (or simply provide) production data. Administrative controls and policies may also used.

4.8.3 Security Model Summary

To summarize the discussion:

- Bell-LaPadula (BLP) is not really useful as it covers only static relationships which is not realistic
- HRU (Harrison-Ruzzo-Ullman) is the basis of most MLS, or compartmented mode, operating system information access concepts
- Chinese Wall Model (multilateral) is not really useful in the real world
- Biba is the basis of OS integrity ring structuring of modern operating systems, especially since the invalid assumption of human subjects not having ulterior motives does not really apply to OS components
- Clark-Wilson is generally applicable, but not limited to commerce (Accounting AP, AR) activities, Internet business (Merchant vs. Payment Service) and General Transaction Processing and DBMS applications.

4.9 Security Requirements

While security threats are manifold and perception of security risks may vary depending on various criteria, the Telecommunications industry has recognized that it is very beneficial to agree upfront upon a certain set of security requirements when designing security for the next generation networks. Typically, security requirement specifications identify the prioritized security requirements deemed of utmost significance; usually addressing the most severe security threats too. Such security requirements are then satisfied by corresponding security architecture work and security mechanisms and security countermeasures specifications.

Two NGN security requirements analyses: one accomplished by ETSI TISPAN and the other by ITU-T for their Next Generations Networks, are:

- - ETSI TS 187001 defines the security requirements pertaining to TISPAN NGN Release 1. The security requirements specification holds requirements for the various NGN subsystems (such as the Network Attachment Subsystem, Resource Admission Control Subsystem, IP Multimedia Subsystem, PSTN/ISDN Emulation Subsystem) defined at a stage 1 level.
- - ITU-T Recommendation Y.2701 provides security requirements for Next Generation Networks (NGNs) and its interfaces (e.g., UNIs, NNIs and ANIs) by applying ITU-T Recommendation X.805, Security architecture for systems providing end-to-end communications to ITU-T Recommendation Y.2201, NGN release 1 requirements and ITU-T Recommendation Y.2012, Functional requirements and architecture of the NGN.

Further study is required to merge the ETSI and ITU-T work in this area with the material and methodology within this TR.

5 Security Architectures, Services and Mechanisms

5.1 Architectural Types

Information system architectures range in definition and occur in a spectrum from abstract views to specific views of what is to be developed. Experience shows that four types are frequently used: abstract, generic, logical, and specific. Most discussions of architecture occur at the abstract-generic level. The following subsections provide:

- a brief overview of architecture types,
- description of communications and computing security services,
- security mechanisms available to instantiate services,
- a discussion of the management of security mechanisms.

5.1.1 Abstract Architectures

An abstract architecture begins with knowledge of the requirements and defines corresponding functions to be performed. It defines principles and fundamental concepts that guide the selection and organization of functions. Abstract security architectures cite principles, fundamental concepts, and functions that satisfy the typical security requirements. These concepts and functions are allocated to elements of an abstract definition of the information system architecture.

5.1.2 Generic Architecture

The development of a generic architecture is based upon abstract architectural elements. It defines the general types of components and allowable standards to be used, and identifies any necessary guidelines for their application. A generic security architecture proceeds from an initial allocation of security services and functions and defines the types of components and security mechanisms that are available to implement the security services with the desired strengths. Any limitations in combining components and mechanisms because of incompatibility or security degradation should be cited in the guidelines for application.

5.1.2.1 The ITU-T X.800 Generic Architecture

The first communications security architecture to be internationally standardized was ISO 7498-2 (1989) and this was adopted almost verbatim by ITU-T as Rec. X.800 (1991) as the "Security Architecture for Open Systems Interconnection for CCITT Applications". This standard defines the general security-related architectural elements that can be applied to communications systems. 7498-2/X.800 provides a general description of security services and the related mechanisms that can be used to provide the services.

7498-2/X.800 is concerned only with those visible aspects of a communications path that permit networked elements to achieve secure transfer of information between them. It does not attempt to provide any kind of implementation specification and it does not provide the means to assess conformance of any implementation to this or any other security standard. Additionally it

does not indicate, in any detail, the additional security mechanisms needed within networked elements to ensure reliable secure computer operation.

Although 7498-2/X.800 was developed specifically as a communications security architecture, the underlying concepts have broader applicability representing the first international consensus on the definitions of basic security services (*Authentication, Access Control, Data Confidentiality, Data Integrity* and *Non-repudiation*) along with more general (pervasive) services such as *Trusted Functionality, Event Detection* and *Security Audit and Recovery*.

During the development of X.800, the need for additional related communications security standards was identified. As a result, work on a number of supporting standards and complementary architectural Recommendations was initiated following the development of X.800. Some of these Recommendations are discussed below.

5.1.2.1.1 The Security Frameworks (X.810-X.816)

The Security Frameworks were developed to provide comprehensive and consistent descriptions of the security services defined in X.800. They are intended to address all aspects of how the security services can be applied in the context of a specific security architecture, including possible future security architectures. The frameworks focus on providing protection for systems, objects within systems, and interaction between systems. They do not address the methodology for constructing systems or security mechanisms.

The frameworks address both data elements and sequences of operations (excluding protocol elements) that are used to obtain specific security services. These services may apply to the communicating entities of systems as well as to data exchanged between, and managed by systems.

5.1.2.1.2 The Security Framework Overview (X.810)

The Security Framework Overview introduces the other frameworks and describes common concepts including security domains, security authorities and security policies that are used in all the frameworks. It also describes a generic data format that can be used to convey both authentication and access control information securely.

5.1.2.1.3 The Authentication Framework (X.811)

The Authentication Framework occupies a position at the top of a hierarchy of authentication standards that provide concepts, nomenclature and a classification for authentication methods. This framework: defines the basic concepts of authentication; identifies possible classes of authentication mechanism; defines the services for these classes of mechanism; identifies functional requirements for protocols to support these classes of mechanism; and identifies the general management requirements for authentication.

5.1.2.1.4 The Access Control Framework (X.812)

The Access Control Framework describes a model that includes all aspects of access control in Open Systems, the relationship to other security functions (such as Authentication and Audit), and the management requirements for Access Control.

5.1.2.1.5 The Non-repudiation Framework (X.813)

The Non-repudiation Framework extends the concepts of non-repudiation security services as described in X.800 and provides a framework for the development of these services. It also

identifies possible mechanisms to support these services and general management requirements for non-repudiation.

5.1.2.1.6 The Confidentiality Framework (X.814)

The purpose of the confidentiality service is to protect information from unauthorized disclosure. The Confidentiality Framework addresses the confidentiality of information in retrieval, transfer and management by defining the basic concepts of confidentiality, defining the possible classes of confidentiality and the facilities required for each class of confidentiality mechanism, identifying the management and supporting services required, and addressing the interaction with other security services and mechanisms.

5.1.2.1.7 The Integrity Framework (X.815)

The Integrity Framework addresses the integrity of data in information retrieval, transfer and management. It defines the basic concepts of integrity, identifies possible classes of integrity mechanism and the facilities for the class of mechanism, identifies management required to support the class of mechanism, and addresses the interaction of the integrity mechanism and the supporting services with other security services and mechanisms.

5.1.2.1.8 The Audit and Alarms Framework (X.816)

The Audit and Alarms Framework defines the basic concepts and provides a general model of security audit and alarms, identifies the criteria for a security audit and for raising alarms, identifies possible classes of audit and alarms mechanisms, defines the services for these classes of mechanism, identifies functional requirements to support these mechanisms, and identifies general management requirements for security audit and alarms.

5.1.2.2 The ITU-T X.805 Approach to Security

ITU-T Recommendation X.805 provides a framework which can be used to address end-to-end network security. To this end, X.805 defines the concept of security dimensions that span eight aspects of security. The X.800 Access Control, Authentication, Data Confidentiality, Data Integrity and Non-repudiation services align with the X.805 security dimensions of the same name. X.805 provides three additional security dimensions namely:

- Communications Security (imported from the military security environment which focuses on confidentiality and integrity),
- Availability (which recognizes the relationship between security and network availability, best exemplified by the popularity of denial of service attacks) and
- Privacy (which is concerned with protecting against observation of network address allocation such as protocol sniffing or probing) can be mitigated for example by NAT devices.

The granularity of security challenges offered by the eight dimensions of X.805 are relevant to the implementation of regulatory requirements that deal with privacy and non-repudiation, such as HIPAA in the US. As a framework, X.805 facilitates establishing policy, recognizing implementation issues and verification of necessary controls to demonstrate compliance to regulatory mandates.

X.805 partitions a telecommunications network into a three-layered hierarchy of equipment and facilities groupings:

- the infrastructure security layer,
- the services security layer, and
- the applications security layer.

In addition, X.805 defines the three types of activities that can occur at every layer as security planes. The three security planes present at every layer are:

- management security plane,
- control/signaling security plane, and
- end-user security plane.

The Infrastructure layer consists of the network transmission facilities as well as individual network elements. Examples of components that belong to the Infrastructure layer are individual routers, switches and servers as well as the communication links between them. The Services layer addresses security of network services that are offered to customers. The Application layer addresses requirements of the network-based applications used by the customers. Detailed descriptions and examples of the three security layers are provided in X.805 section 7.

X.805 also defines three Security Planes to represent the types of protected activities that take place on a network, namely: (1) the Management plane, (2) the Control plane, and (3) the End-User plane. These Security Planes address specific security needs associated with network management activities, network control or signaling activities, and end-user activities correspondingly. The Management plane is concerned with Operations, Administration, Maintenance and Provisioning (OAM&P) activities such as provisioning a user or a network. The Control plane is associated with the signaling aspects for setting up (modifying and tearing down) end-to-end communication through the network irrespective of the medium and technology used in the network. The End-User plane addresses security of access and use of the network by customers as well as protecting end-user data flows.

This three layer three plane matrix provides a systematic recognition that very different approaches apply to securing network infrastructures, services and applications as well as network management, control and user activities. For example, DoS attacks at the infrastructure layer (e.g., traffic flooding) can be very different than DoS attacks at the services layer, for example a flooding attack against an end-user terminal vs. a malformed SIP signaling packet, and need to be protected against in different ways.

X.805 recognizes that redundant security mechanisms may be avoided by identifying security capabilities in one layer that protect another layer, thus allowing for a reduction of the overall cost of a specific security solution. For example, if the underlying services layer is protected by IPSec, it may not be necessary to protect the applications layer with TLS.

X.805 is a generic security framework and as such does not provide a specification for any particular information system or component. Rather, it specifies security principles and allows identification of target security capabilities required to facilitate end-to-end network security. Other standards such as ISO 27001 provide a broad perspective on security programs; within which X.805 provides technical depth. X.805 presents a higher level and integrated approach to the subjects covered in X.810-815 recommendation series

5.1.2.3 The ISO 27001 Information Security Management Program

ISO 27001 focuses on maintaining, or reviewing a security program over time as well as for the management of security policies, procedures, incident response, recovery plans, and technology architectures.

Certification of an organization's Information Security Management Program (ISMP) against ISO 27001 is one means of providing assurance that the certified organization has implemented a system for the management of information security in line with the standard. Credibility is the key advantage of being certified by a respected, independent and competent third party. Also see section 4.5.3.

5.1.2.4 ETSI Security Counter Measures

ETSI has developed two documents:

- ETSI TS 102 165-2 defines by means of an information model and functional entity behavioral model, the security countermeasures for the ICT in general and where examples are shown they are shown with respect to the NGN. Countermeasures are grouped by their key feature, i.e. Authentication, Integrity.
- ETSI Guide 202 549 gives guidance on the application of security countermeasures to service capabilities. It covers the construction of services from service capabilities and how a security evaluation of a service capability should be performed.

Further study is required to merge ETSI and ITU-T work in this area with the material and methodology within this TR."

5.1.3 Logical Architecture

A logical architecture is a design that meets a hypothetical set of requirements. It serves as a detailed example that illustrates the results of applying a generic architecture to specific circumstances. The only differences between a logical and a specific architecture are that the specific requirements are real, not hypothetical, and since the logical architecture is not intended to be implemented there is no need to perform a cost analysis. In logical security architectures, the logical design is accompanied by an illustration of the security analysis to be performed in specific architectures.

5.1.4 Specific Architecture

The objective of any system architect is to accomplish a level of design specification such that components can be acquired to implement the system. The specific architecture addresses components, interfaces, standards, performance, and cost. Specific security architectures show how all the selected information security components and mechanisms, including doctrine and supporting security management components, combine to meet the security requirements of the specific system under consideration.

Security requirements for components and interfaces for telecommunications networks may be found in ATIS.1000007.2006, ATIS.1000012.2006, and ATIS.1000019.2007. Note that the ATIS PTSC is also developing a standard for User-Network Interface (UNI) Access Signaling and UNI Interconnection.

5.1.4.1 ETSI NGN Security Architecture

ETSI TISPAN has developed a specific security architecture (ETSI TS 187 003) for the first releases of their Next Generation Network (NGN). This security architecture is defined at a stage 2 level to fulfill the corresponding NGN Release 1 security requirements (ETSI TS 187 001). Further study is required to merge ETSI and ITU-T work in this area with the material and methodology within this TR.

5.2 Security Services

Security services that are included in the OSI security architecture and mechanisms which implement those services are discussed here. These security services are basic security services. In practice they will be invoked at appropriate layers and in appropriate combinations, usually with non-OSI services and mechanisms, to satisfy security policy and/or user requirements. Particular security mechanisms can be used to implement combinations of the basic security services. Practical realizations of systems can implement particular combinations of the basic security services for direct invocation.

The authentication services require authentication information comprising locally stored information and data that is transferred (credentials) to facilitate the authentication.

Table 12 - Applicability of Security Services

	Service	Applies to Communications	Applies to Computers
1	Authentication		
1.1	Peer entity authentication	Yes	
1.2	Data origin authentication	Yes	
1.3	User Authentication	Yes	Yes
1.4	Process Authentication		Yes
2	Authorization - Access control		
2.1	Communications Access Controls	Yes	
2.2	Computing System Access Controls		Yes
3	Data confidentiality		
3.1	Connection confidentiality	Yes	
3.2	Connectionless confidentiality	Yes	
3.3	Selective field confidentiality	Yes	Yes
3.4	Traffic flow confidentiality	Yes	
4	Integrity		
4.1	Information integrity		Yes
4.1.1	Separation of duty		Yes
4.1.2	Well formed transactions		Yes
4.1.3	Logging	Yes	Yes
4.2	Data integrity		
4.2.1	Connection integrity with recovery	Yes	
4.2.2	Connection integrity without recovery	Yes	
4.2.3	Selective field connection integrity	Yes	
4.2.4	Connectionless integrity	Yes	
4.2.5	Selective field connectionless integrity	Yes	Yes
5	Non-repudiation		
5.1	Non-repudiation with proof of origin	Yes	Yes
5.2	Non-repudiation with proof of delivery	Yes	Yes
5.3	Non-repudiation of actions	Yes	Yes

ATIS-0300276.2008 and ITU-T M.3016 distribute management security services into a different set of categories and topics than those shown in Table 12. Table 12 considers the generic security services applicable to communications and computing resources and is intended to include all of the specific security functions described in the two standards above.

5.2.1 Authentication

Authentication services provide for the authentication of an identity presented or asserted by an entity (a.k.a. a subject) or the identity of a source of data as described below.

5.2.1.1 Peer entity authentication

Peer entity authentication should be provided for use at the establishment of, or at various times during, the data transfer phase of a connection to confirm the identities of one or more of the connected entities. This service provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorized replay of a previous connection. One-way and mutual peer entity authentication schemes, with or without a liveliness check, are possible and can provide varying degrees of protection, as discussed in ITU-T X.800.

5.2.1.2 Data origin authentication

The data origin authentication service provides corroboration of the source of a data unit. The service does not provide protection against duplication or modification of data units, as discussed in ITU-T X.800.

5.2.1.3 User Authentication

This service provides confirmation of the identity of a human subject when logging into a computer system (network element). This service provides confidence, at the time of log-in, that a human entity is not attempting a masquerade of a different human subject.

5.2.1.4 Process Authentication

This service provides confirmation of the identity of a process (executing software component) when it attempts to access some information or resource (within the same network element). This service provides confidence, at the time of requested access, that the process is not attempting a masquerade of a different process, thus allowing the element access mediation function (see Table 25).

5.2.2 Authorization - Access Control

The following services provide protection against unauthorized use of a resource. This can be a communications resource or a computing resource. This service can be applied to various types of access to a resource (e.g. the use of a communications resource; the reading, the writing, or the deletion of an information resource; the execution of a processing resource) or to all accesses to a resource.

5.2.2.1 Communications Access Control

This service provides protection against unauthorized use of communications resources. The control of access will be in accordance with various security policies, as discussed in ITU-T X.800.

5.2.2.2 Computing System Access Control

This service provides protection against unauthorized use of computing resources. The control of access will be in accordance with various security policies.

5.2.3 Data confidentiality

The following services provide for the protection of data from unauthorized disclosure as described below.

5.2.3.1 Connection confidentiality

This service provides for the confidentiality of all (N)-user-data on an (N)-connection as discussed in ITU-T X.800.

5.2.3.2 Connectionless confidentiality

This service provides for the confidentiality of all (N)-user-data in a single connectionless (N)-SDU as discussed in ITU-T X.800.

5.2.3.3 Selective field confidentiality

This service provides for the confidentiality of selected fields within the (N)-user-data on an (N)-connection or in a single connectionless (N)-SDU as discussed in ITU-T X.800.

Beyond what is in X.800, this service can also provide confidentiality of information within computing system storage devices (i.e., file systems) and dynamic memory.

5.2.3.4 Traffic flow confidentiality

This service provides for the protection of the information which might be derived from observation of traffic flows as discussed in ITU-T X.800.

5.2.4 Integrity

Integrity focuses on the correctness or accuracy of information and takes two forms: information integrity and data integrity.

5.2.4.1 Information integrity

Information integrity service focuses on the quality, or validity, of information rather than whether data has been altered, as with data integrity. The primary approach to achieving information integrity in commercial contexts has been by use of the Clark-Wilson security model which is built upon three foundation principles: 1) separation of duties, 2) well-formed transactions, and 3) logging and auditing

5.2.4.1.1 Separation of duty

Separation of duties (SoD) is the concept of having more than one person required to complete a task. SoD is one of the key concepts of internal control and in basic terms means that no single individual should have control over two or more phases of a transaction or operation, so that a deliberate fraud requires collusion of two or more individuals or parties. With the concept of SoD, critical duties/activities can be categorized into four types of functions, authorization, custody, record keeping and reconciliation. In a perfect system, no one person should handle more than one type of function.

The term Separation of duties is well-known in financial accounting systems. Companies of all sizes understand not to combine roles such as receiving checks (payment on account) and approving write-offs, depositing cash and reconciling bank statements, approving time cards and have custody of pay checks, etc. SoD is commonly used so that no single person is in a position to introduce fraudulent or malicious code or data without detection. Strict control of software and data changes require that different people or organizations perform each of the following roles:

- Identification of a requirement (or change request); e.g. a business person
- Authorization and approval; e.g. an IT governance board or manager
- Design and development; e.g. a developer
- Review, inspection and approval; e.g. another developer or architect.
- Implementation in production; typically a software change or system administrator.

In information systems, SoD reduces the potential damage from the actions of one person. Activities should be organized in a way to achieve adequate separation of duties. When duties cannot be separated, compensating controls should be in place. Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness. If a single person can carry out and conceal errors and/or irregularities in the course of performing his/her day-to-day activities, he/she has been assigned an SoD incompatible set of duties.

5.2.4.1.2 Well-formed transactions

A well-formed transaction is a series of operations that transition a system from one consistent state to another consistent state. The concept of well-formed transactions addresses the integrity of the transaction software that implements the functions comprising a transaction should only be used on production systems after the software has gone through a certification process. The principle of SoD recommends that the certifier of a transaction and the implementer be different entities.

5.2.4.1.3 Logging

Control mechanisms that can help to enforce the separation of duties and well formed transactions include, but are not limited to:

1. Audit trails that enable managers or Auditors to recreate the actual transaction flow from the point of origination to its existence on an updated file. Good audit trails provide information on who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated.
2. Reconciliation of applications, an independent verification process, increases the level of confidence that the application ran successfully.
3. Exception reports that are handled at a supervisory level and backed up by evidence noting that exceptions are handled properly and in timely fashion.
4. Manual or automated system or application transaction logs which record all processed system commands or application transactions.
5. Supervisory review through direct or remote observation and inquiry.

5.2.4.2 Data integrity

These services counter active threats and may take one of the forms described below.

5.2.4.2.1 Connection integrity with recovery

This service provides for the integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion or replay of data within an entire SDU sequence (with recovery attempted) as discussed in ITU-T X.800.

5.2.4.2.2 Connection integrity without recovery

As for 5.2.4.2.1 but with no recovery attempted as discussed in ITU-T X.800.

5.2.4.2.3 Selective field connection integrity

This service provides for the integrity of selected fields within the (N)-user data of an (N)-SDU as discussed in ITU-T X.800.

5.2.4.2.4 Connectionless integrity

This service, when provided by the (N)-layer, provides integrity assurance to the requesting (N+1)-entity as discussed in ITU-T X.800.

5.2.4.2.5 Selective field connectionless integrity

5.2.4.5 Selective field connectionless integrity

This service provides for the integrity of selected fields within a single connectionless SDU and takes the form of determination of whether the selected fields have been modified as discussed in ITU-T X.800.

5.2.5 Non-repudiation

Non-repudiation service ensures that a contract cannot later be denied by either of the parties involved and is the opposite of plausible deniability. In regard to security, non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively, or that a subject actually performed an action.

5.2.5.1 Non-repudiation with proof of origin

With this form of non-repudiation, the recipient of data is provided with evidence of the origin of data. This will protect against an attempt by the sender to falsely deny sending the data or its contents, as discussed in ITU-T X.800.

5.2.5.2 Non-repudiation with proof of delivery

With this form of non-repudiation, the sender of data is provided with evidence of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents, as discussed in ITU-T X.800.

5.2.5.3 Non-repudiation of actions

Non-repudiation of actions service provides evidence of the identity of a subject, either human or software, that performed an action such as changing, reading or deleting information or initiated a process or application. The primary mechanism supporting this security service is Logging and Auditing, as discussed in section 5.2.4.1.3.

5.3 Necessary Communications Security Services

Section 5.3.1 discusses a coherent architectural context for the purpose of security engineering. Section 5.3.2 will then map security services against this architectural context.

5.3.1 Architectural Context for Security Services

The material within this section is based on existing reference architectures from ISO/IEC and ITU-T augmented by IETF concepts.

5.3.1.1 Existing Generic Network Architectural Models

The first international generic architectural model published for packet based networks was ISO/IEC 7498-1 in 1984. A 2nd version was jointly developed by the ISO and the ITU and published as ITU-T X.200 in 1994.

5.3.1.1.1 Protocol Layers and Functional Planes

X.200 states that there is a functional layering of protocols into what is commonly referred to as the ISO/OSI seven layer protocol model comprising:

1 - Physical Layer,
2 - Data Link Layer,
3 - Internetworking Layer,
4 - Transport Layer,
5 - Session Layer,
6 - Presentation Layer, and
7 - Application Layer.

The Internet model is a five layer protocol model comprising:

1 - Physical Layer,
2 - Data Link Layer,
3 - Internetworking Layer,
4 - Transport Layer,
5 - Application Layer,

and for the purpose of this generic network architecture context discussion the 5 layer model is used. Since the publication of X.200, the concept that each protocol layer actually provides communications functionality to three forms of activities, namely:

- User Plane (a.k.a. Data Plane),
- Control Plane[16], and
- Management Plane

have been defined by ITU-T Y.2011, *General principles and general reference model for Next Generation Networks*.

5.3.1.1.2 Management Communications

Management activities pertain to controlling the capabilities and behavior of functions within each protocol layer. In practice from a communications perspective (see Y.2011), a management plane can be null for a particular protocol layer. Management activities are a form of application activities that focus specifically on (as defined in ISO/IEC 7498-4 and ISO/IEC 9595):

- **F**ault Management,
- **C**onfiguration Management,
- **A**ccounting Management,
- **P**erformance Management,
- **S**ecurity Management,

also referred to as FCAPS. Management plane communications are supported by protocols stacks (which address all layers of communications) defined in ITU-T Q.811, *Lower layer protocol profiles for the Q and X interfaces*, and Q.812, *Upper layer protocol profiles for the Q and X interfaces*. According to M.3016.0, *Security for the management plane: Overview*, security services may need to be provided at every protocol layer involved in the communication of management plane information.

[16] Sometimes referred to as the Signaling & Control Plane

5.3.1.1.3 The Physical Layer

Clause 7.7 of X.200 states the Physical Layer

> *"provides the mechanical, electrical, functional and procedural means to activate, maintain, and de activate physical-connections for bit transmission between data-link-entities. A physical-connection may involve intermediate open systems, each relaying bit transmission within the Physical Layer. Physical Layer entities are interconnected by means of a physical medium."*

and as such does not meaningfully decompose into the aforementioned planes of functionality, thus it is reasonable to reference physical layer technologies relative to specific Data Link Layer technologies where relevant.

Another complication is the concept of User-Network Interfaces (UNIs), Internal Network-Network Interfaces (I-NNIs) and Network-Network Interfaces (NNIs) sometime referred to as External Network-Network Interfaces (ENNIs). This document will use the more common ITU-T terminology of NNI rather than ENNI.

The scenarios presented in section 5.3.1.2.2 are a set of use cases that define a generic architectural model of modern packet based network infrastructures.

5.3.1.2 Generic Abstract Architectural Context for Modern Networks

This section discusses a generic networking architectural context appropriate for modern converged services packet based networks that weaves together the concepts of network interface types, protocol layering and functional planes within protocol layers as discussed in the preceding section. The context is discussed via a set of scenarios that present different combinations of end nodes and intermediate notes interacting across multiple security domains (a.k.a. 'trust domains'). These security domains map to organizational infrastructure boundaries and reflect which organization controls the elements with a specific infrastructure.

The use case diagrams do not depict topological connectivity, only logical connectivity. In many of the diagrams the same intermediate node may be shown more than once since each scenario focuses on the logical interfaces, protocols and functional planes involved.

The one primary assumption made in all scenarios is that the Internet Protocol (IP) is used as the basis of the Inter-networking Layer (layer 3). Otherwise, no assumptions are made regarding specific protocols used within the Data Link, Transport and Application Layers.

5.3.1.2.1 Definition of Scenario Components

The following components are used within the various scenario diagrams. Each use case depicts organizational entities, functional entities and interfaces. For brevity multiple functional entities are conceptually bundled into a set of Infrastructure Elements described below. Not all functions typically implemented within these common Infrastructure Elements are discussed herein.

5.3.1.2.1.1 Organizational Entities

The types of organizational entities used in the generic abstract model scenarios are:

CS Customer (a.k.a. Subscriber)
A CS represents any group (multi-family residential, institution, small/medium/large business entity, governmental entity) or individual (private

residential) entity that contracts for services from an Access Service provider. These contracted for services can:

- be limited to basic communications (POTS, leased lines, VLAN, private networking, simple internet-working) capabilities, or
- also include services traditionally viewed as advanced communications/information capabilities, such as web hosting, messaging (as in voice mail, Email, SMS), secure- virtual private networking (VPN), Voice over IP (VoIP), Video (broadcast, on-demand, over IP), and even outsourced applications.

SP Service Provider

There are generally three (3) types of modern SPs:

- Access SPs
- Interconnect (a.k.a., "Backbone") SPs
- Application SPs.

An **Access Service Provider** offers communications/information service capabilities to CSs. As noted above these services can be limited to basic communications or also include services traditionally viewed as advanced communications/information capabilities. Access SPs typically have both Access network infrastructures and Metropolitan Core network infrastructures, where the:

- Access network infrastructure(s) are used to provide connectivity to CSs, and
- Metropolitan Core network infrastructure(s) are used to inter-connect Access network infrastructure(s), as well as inter-connect with the network infrastructures of other Access SPs, Application SPs and Interconnect Service Providers.

Access SPs can directly interconnect with other Access SPs in cases where Access SPs are not prevented from doing so by governmental regulations or laws. Access SPs may be required to use an Interconnect SP when communicating with other Access SPs (as with the regulated telephone companies)

An **Application SP** primarily offers information processing oriented services to CSs, and possibly other SPs. CS oriented services can include, but not limited to:

- web hosting,
- messaging (Email, SMS),
- Voice over IP (VoIP),
- outsourced applications,
- virtual Data Centers;

whereas SP oriented services can include, but not limited to:

- 3rd party billing,
- directory and searching,
- outsourced applications,

- virtual Data Centers.

Application SPs frequently operate very complex premises network infrastructures typically built upon very high speed Data Link Layer technologies such as optical fiber and SONET, Fiber-channel and 1000baseT. An Application SP network infrastructure may be distributed across multiple SP premises.

An **Interconnect Service Provider** primarily offers communications/information service capabilities to Access and Application SPs. These services may be limited to basic communications and could include advanced communications/information capabilities. Interconnect SPs typically have both Inter-Metropolitan network infrastructures and Metropolitan Core network infrastructures, and may also operate international network infrastructures, where the:

- Metropolitan Core network infrastructure(s) are used to support inter-connection with multiple Access SP and Application SP network infrastructure(s), as well as inter-connection with the Interconnect SP's Inter-Metropolitan and International network infrastructure (if present).
- inter-Metropolitan network infrastructure(s) are used to provide connectivity to Interconnect SP Metropolitan Core network infrastructures located in different metropolitan areas, and
- International network infrastructure(s) are used to inter-connect Interconnect SP Inter-Metropolitan network infrastructure located in different countries.

5.3.1.2.1.2 Interface Types

UNI User Network Interface

The UNI interface represents a logical point of interconnection between a CS network infrastructure element and an Access SP network infrastructure element. At the:

- Data Link Layer, two elements (serving as intermediate elements with one in the CS security domain and the other within the SP security domain) will be directly physically interconnected and will exchange signaling & control information for the purpose of information (as frames, cells, datagrams, packets) transfer of bearer (a.k.a., media or user) traffic from/to CS and SP network infrastructures,
- Inter-networking Layer, two elements (serving as intermediate elements with one in the CS security domain and the other within the SP security domain) will rarely be directly physically interconnected but will exchange signaling & control information for the purpose of information (as packets) forwarding of bearer (a.k.a., media or user) traffic from/to CS and SP network infrastructures
- Transport Layer, two elements (serving as end elements with one in the CS security domain and the other within the SP security domain) will not be directly physically interconnected but will exchange bearer (a.k.a., media or user) traffic and signaling & control information (as datagrams or byte

streams) between specific processes executing within each end element on an end-to-end basis within the CS and SP network infrastructures.

- Application Layer, two elements (serving as end elements either with one in the CS security domain and the other within the SP security domain or both in different CS security domains) will not be directly physically interconnected but will exchange bearer (a.k.a., media or user) messages, signaling & control messages, and possibly management messages between specified application functions executing within each end element on an end-to-end basis as defined within each application.

INNI Internal Network-Network Interface

The INNI interface represents a logical point of interconnection between network infrastructure elements within the same security domain. At the:

- Data Link Layer, two elements (both within the same security domain) will be directly physically interconnected and will exchange signaling & control information for the purpose of information (as frames, cells, datagrams, packets) transfer of bearer (a.k.a., media or user) traffic within the network infrastructure,
- Inter-networking Layer, two elements (both within the same security domain) will rarely be directly physically interconnected but will exchange signaling & control information for the purpose of information (as packets) forwarding of bearer (a.k.a., media or user) traffic within the network infrastructure,
- Transport Layer, two elements (serving as end elements both within the same security domain) will not be directly physically interconnected but will exchange bearer (a.k.a., media or user) traffic and signaling & control information(as datagrams or byte streams) between specific processes executing within each end element on an end-to-end basis within the network infrastructure,
- Application Layer, two elements (serving as end elements both within the same security domain) will not be directly physically interconnected but will exchange bearer (a.k.a., media or user) messages, signaling & control messages, and possibly management messages between specified application functions executing within each end element on an end-to-end basis as defined within each application.

NNI Network-Network Interface

The NNI (a.k.a. External-Network-Network Interface) represents a logical point of interconnection between two network infrastructure elements within two different SP security domains. At the:

- Data Link Layer, two elements (serving as intermediate elements with one in a SP security domain and the other within a different SP security domain) will be directly physically interconnected and will exchange signaling & control information for the purpose of information (as frames, cells, datagrams, packets) transfer of bearer (a.k.a., media or user) traffic from/to the two different SP network infrastructures,

- Inter-networking Layer, two elements (serving as intermediate elements with one in a SP security domain and the other within a different SP security domain) will rarely be directly physically interconnected but will exchange signaling & control information for the purpose of information (as packets) forwarding of bearer (a.k.a., media or user) traffic from/to the two different SP network infrastructures,
- Transport Layer, two elements (serving as end elements with one in a SP security domain and the other within a different SP security domain) will not be directly physically interconnected but will exchange bearer (a.k.a., media or user) traffic and signaling & control information (as datagrams or byte streams) between specific processes executing within each end element on an end-to-end basis within the two different SP network infrastructures,
- Application Layer, two elements (serving as end elements either with one in a SP security domain and the other within a different SP security domain) will not be directly physically interconnected but will exchange bearer (a.k.a., media or user) messages, signaling & control messages, and possibly management messages between specified application functions executing within each end element on an end-to-end basis as defined within each application.

5.3.1.2.1.3 Protocol Layers and Functional Planes

Data Link Protocol Layer (DLL)

The DLL can, and does, take many forms in modern networking infrastructures depending whether one is looking at Customer/subscriber Premise Infrastructures, Service Provider Access Infrastructures, Service Provider Metropolitan Core Infrastructures, Service Provider Inter- Metropolitan Infrastructures, Service Provider Intercontinental Infrastructures.

Customer/subscriber Premise Infrastructures typically rely on the following technologies:

- multi-drop ethernet (802.3 5baseT and 2baseT)
- point-to-point ethernet (802.3 10/100/1000baseT)
- wireless (802.11a, 802.11b, 802.11i, 802.16)

Service Provider Access Infrastructures typically rely on the following technologies:

- Digital Subscriber Line (xDSL)
- Passive Optical (BPON, GPON)
- Active Optical (Sonet, ATM/SONET, 1000baseT)
- wireless (802.11a, 802.11b, 802.11i)
- Coaxial Cable (802.3 CATV, DS3)
- Twisted Copper Pair Wiring (Analog dial-up, N-ISDN 2B+D, N-ISDN PRI, T1, FrameRelay/T1)

Service Provider Metropolitan Core Infrastructures typically rely on the following technologies:

- Active Optical (Wave Division Multiplexing, Sonet, ATM/SONET, 1000baseT)
- Coaxial Cable (DS3)
- Twisted Copper Pair Wiring (N-ISDN PRI, T1, FrameRelay/T1)

Service Provider Inter- Metropolitan Infrastructures typically rely on the following technologies:

- Active Optical (Wave Division Multiplexing, Sonet, ATM/SONET, 1000baseT)

- Coaxial Cable (DS3)
- Twisted Copper Pair Wiring (N-ISDN PRI, T1, FrameRelay/T1)

Service Provider Intercontinental Infrastructures typically rely on the following technologies:

- Active Optical (Wave Division Multiplexing, Sonet)
- Coaxial Cable (DS3)
- Satellite

DLL communications traffic can be separated into: 1) Signaling & Control Plane Traffic and 2) User Plane Traffic

DLL-SCP Data Link Layer Signaling & Control Plane Traffic
The type of DLL-SCP traffic will vary based on the specific DLL technology deployed, such as:

- 802.3 5baseT and 2baseT
- 802.3 10/100/1000baseT
- 802.3 CATV
- 802.11a, 802.11b, 802.11i
- 802.16
- Digital Subscriber Line (xDSL) signaling & control occurring within the Application Layer as XML defined messages over TCP & IP as defined by the DSL Forum TR-69 standard
- BPON signaling & control occurring within the DLL as defined by the ITU-T G983 series of standards (a.k.a. the OMCI channel)
- GPON signaling & control occurring within the DLL as defined by the ITU-T G984 series of standards (a.k.a. the OMCI channel)
- Sonet signaling & control occurring within the DLL as defined by ITU-T standards for Section, Line and Path (a.k.a. the Supervisory channel)
- ATM signaling & control occurring within the DLL as defined by ATM Forum standards for switched virtual circuits
- Frame Relay
- Wave Division Multiplexing
- Satellite signaling & control occurring within the DLL as defined by manufacturer specifications
- Analog dial-up signaling & control occurring within the DLL as dual-tone multi-frequency in-band analog signals defined by Telcordia and ATIS standards
- N-ISDN 2B+D, N-ISDN PRI signaling & control occurring within the DLL as defined by ITU-T Q.930 and Q.931 standards
- T1 signaling & control occurring within the DLL as defined by Telcordia and ATIS standards
- DS3 signaling & control occurring within the DLL as defined by Telcordia and ATIS standards

DLL-UP Data Link Layer User Plane Traffic

- 802.3 5baseT and 2baseT, 802.3 10/100/1000baseT, 802.3 CATV, 802.11a, 802.11b, 802.11i, 802.16 user traffic taking the form of ethernet frames defined by IEEE standards

- Digital Subscriber Line (xDSL) user traffic taking the form of ATM cells carrying ethernet frames
- BPON and GPON user traffic taking the form of ATM cells carrying ethernet frames or ethernet frames directly on the fiber as defined by the ITU-T G983 G984 series of standards
- Sonet user traffic taking the form of STS-1 payloads as defined by ITU-T standards
- ATM user traffic taking the form of 53 byte cells as defined by ATM Forum standards
- Frame Relay user traffic taking the form of ethernet frames mapped into T1 193 bit frames or T3 45Mbps links as defined by Frame Relay Forum standards
- Wave Division Multiplexing user traffic taking the form of separate laser light frequencies (lambdas)
- Analog dial-up user traffic taking the form of analog signals within the range of 50Hz and 3KHz defined by Telcordia and ATIS standards
- N-ISDN 2B+D, N-ISDN PRI user traffic taking the form of 64kbps digitized bit streams (B channels) as defined by ITU-T I.430 and I.431 standards
- T1 user traffic taking the form of 56kbps digitized bit streams as defined by Telcordia and ATIS standards (the time slots on T1 are 64 bits wide, the high order bit is not available thereby providing only 56kbps and not the full 64kbps).
- DS3 user traffic taking the form of 56kbps digitized bit streams as defined by Telcordia and ATIS standards (the time slots on DS3 are 64 bits wide, the high order bit is not available thereby providing only 56kbps and not the full 64kbps).

Inter-networking Protocol Layer (IL)

The IL typically takes one form in modern networking infrastructures, either IP version 4 of sometimes IP version 6. IL communications traffic can be separated into: 1) Signaling & Control Plane Traffic and 2) User Plane Traffic

IL-SCP Internetworking Layer Signaling & Control Plane Traffic
IL-SCP traffic uses a number of protocols operating within the IL (such as ARP, ICMP, DHCP) or within the Application Layer (such as BGP, OSPF, RIP, LDP, CR-LDP, RSVP-TE) all of which are defined by IETF RFCs. One can argue that the IPsec suite (IKE, ISAKMP, AH and ESP) are a form of IP signaling & control

IL-UP Internetworking Layer User Plane Traffic
IL-UP traffic is transported in packets in protocols defined by IETF RFCs.

Transport Protocol Layer (TL)

The TL utilizes three primary transport layer protocols in modern networking infrastructures, namely Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Stream Control Transmission Protocol (SCTP). TL communications traffic can be separated into: 1) Signaling & Control Plane Traffic and 2) User Plane Traffic

TL-SCP Transport Layer Signaling & Control Plane Traffic
TCP includes some signaling & control for basic protocol operation such as

retransmission, congestion control and conversion of application protocol messages into fundamental TCP byte streams. One can argue that the Transport Layer Security (TLS) protocol is a form of TCP signaling & control
UDP does not include any intrinsic signaling & control for transport of UDP datagrams. One can argue that the Datagram Transport Layer Security (DTLS) protocol is a form of UDP signaling & control
SCTP includes some signaling & control for basic protocol operation such as acknowledged error-free non-duplicated transfer of user data, data fragmentation, sequenced delivery, optional bundling of multiple user messages, network-level fault tolerance through multi-homing at either or both ends of an association, congestion avoidance behavior, and resistance to flooding and masquerade attacks.

TL-UP Transport Layer User Plane Traffic
TCP user plane traffic is transported as streams of bytes (byte streams).
UDP user plane traffic is transported as datagrams.
SCTP user plane traffic is transported as packets.

Application Protocol Layer (AL)

The AL uses many diverse protocols in modern networking infrastructures. Some of these AL protocols provide both signaling and control and user traffic communications within a common protocol (such as ftp, tftp, telnet, nfs, etc.) while other application protocols provide only support Signaling & Control Plane Traffic (such as H.323 and SIP) or User Plane Traffic (such as RTP).

AL-SCP Application Layer Signaling & Control Plane Traffic
H.323 and SIP are the two primary examples of signaling & control specific application layer protocols. One can argue that there are other protocols (such as NTP, DNS, LDAP, RADIUS, Diameter, DCE/Kerberos, Corba, Java) that are also forms of AL signaling & control.

AL-UP Application Layer User Plane Traffic
RTP is the primary example of a user plane specific application layer protocol

AL-MP Application Layer Management Plane Traffic
There are many application layer protocols used in support of management activities. A partial list would include: all versions of SNMP, X, TMF-814, TL1, RMON.

As noted above, many existing AL protocols combine signaling & control traffic along with user plane traffic within one common protocol.

5.3.1.2.1.4 Infrastructure Elements

Modern networking infrastructures are comprised of many types of networked elements; most of which incorporate multiple types of functional entities. Below are typical Networked Elements found in modern service provider infrastructures. Those elements used in the Generic Network Architecture Context scenarios in Section 5.3.1.2.2 are marked with an asterisk (*). These elements do not represent an exhaustive list, simply those used in the scenarios.

CEN* Customer Host (End Node)
A CEN represents an end node (a.k.a. host) that either is the sender or receiver (Client or Server) of application related communications traffic. The CEN:

- provides at least one data link layer & physical interconnection to the customer/subscriber premises network infrastructure
- provides inter-networking layer functionality for packet transmission and receipt
- provides additional inter-networking layer functionality such as:
  - packet filtering or various types (stateless, stateful, deep packet inspection)
- provides transport layer functionality for transmission and receipt of arbitrary information between processes residing within itself and other end nodes
- provides application layer functionality for generating and processing of application unique messages/information exchanged by application processes residing within itself and other end nodes.

CER* Customer Edge Router (Intermediate Node)
A CER is the egress/ingress point of a customer/subscriber premises network infrastructure. The CER:

- provides at least one data link layer & physical interconnection to the customer/subscriber premises network infrastructure
- provides at least one data link layer & physical interconnection to the Access Service Provider network infrastructure
- provides inter-networking layer functionality for packet forwarding (mandatory)
- may provide additional functionality such as:
  - packet filtering or various types (stateless, stateful, deep packet inspection, application gateway)
  - network address translation
  - dynamic host configuration

DSLM* DSL Modem (Intermediate Node)
A DSLM is an egress/ingress point of an Access Service Provider network infrastructure. This device is typically used when providing access service to subscribers in the residential, small/medium sized commercial, educational and institutional markets. The DSLM:

- provides at least one data link layer & physical interconnection to the customer/subscriber premises network infrastructure
- provides one data link layer & physical interconnection to the Access Service Provider DSLAM.

ONT* Optical Network Terminator (Intermediate Node)
An ONT is an egress/ingress point of an Access Service Provider network infrastructure. This device is typically used when providing access service to subscribers in the residential, small/medium sized commercial, educational and institutional markets. The ONT:

- provides at least one data link layer & physical interconnection to the customer/subscriber premises network infrastructure
- provides one data link layer & physical interconnection to the Access Service Provider OLT.

DSLAM* Digital Subscriber Line Access Module (Intermediate Node)
A DSLAM is an intermediate node associated with DSLMs and terminates the Physical and Data Link protocol mechanisms used by digital subscriber line access technologies. The DSLAM:

- provides at least one data link layer & physical interconnection to the Access Service Provider DSLM(s), and
- provides at least one data link layer & physical interconnection to Access Service Provider network infrastructure intermediate nodes.

OLT* Optical Line Terminator (Intermediate Node)
An OLT is an intermediate node associated with DSLMs and terminates the Physical and Data Link protocol mechanisms used by digital subscriber line access technologies. The OLT:

- provides at least 32 data link layer & physical interconnections to Access Service Provider ONTs
- provides at least one data link layer & physical interconnection to Access Service Provider network infrastructure intermediate nodes
- may provide additional data link layer functionality such as:
  - port access control collaboratively with ONTs (such as 802.1x)
- may provide inter-networking layer functionality for packet forwarding (in which case the OLT also functions as a PER), and
- may provide additional inter-networking layer functionality such as:
  - packet filtering or various types (stateless, stateful, deep packet inspection, application gateway)
  - network address translation
  - dynamic host configuration.

PER* Service Provider Edge Router (Intermediate Node)
A PER is the egress/ingress point between an Access Service Provider network infrastructure and a Service Provider Metropolitan Core network infrastructure. The PER:

- provides at least one data link layer & physical interconnection to the Access Service Provider network infrastructure
- provides at least one data link layer & physical interconnection to the Service Provider Metropolitan Core network infrastructure
- provides inter-networking layer functionality for packet forwarding (mandatory), and
- may provide additional functionality such as:
  - packet filtering or various types (stateless, stateful, deep packet inspection, application gateway)
  - network address translation
  - dynamic host configuration.

PCR* Service Provider Core Router (Intermediate Node)
A PCR resides within a Service Provider Metropolitan Core network infrastructure. The PVR:

- provides at least two data link layer & physical interconnections to the Service Provider Metropolitan Core network infrastructure
- provides inter-networking layer functionality for packet forwarding (mandatory).

AER* Service Provider Application Edge Router (Intermediate Node)
An AER resides within a Service Provider Metropolitan Core network infrastructure. The AER:

- provides at least one data link layer & physical interconnection to the Service Provider Metropolitan Core network infrastructure
- provides at least one data link layer & physical interconnection to a Service Provider Application Server complex for such services as Voice over IP
- provides inter-networking layer functionality for packet forwarding (mandatory).

PPR* Service Provider Peering Router (Intermediate Node)
A PPR is the egress/ingress point between the Service Provider Metropolitan Core network infrastructure and a:

- PPR belonging to a different Service Provider Metropolitan Core network infrastructure,
- Service Provider Inter- Metropolitan network infrastructure, or
- Service Provider Intercontinental network infrastructure.

The PPR:

- provides at least one data link layer & physical interconnection to the Service Provider Metropolitan Core network infrastructure
- provides at least one data link layer & physical interconnection to a PPR belonging to a different Service Provider Metropolitan Core network, Service Provider Inter- Metropolitan network, or Service Provider Intercontinental network
- provides inter-networking layer functionality for packet forwarding (mandatory)
- and may provide additional functionality such as:
  - packet filtering or various types (stateless, stateful, deep packet inspection, application gateway).

L2E* Layer 2 Intermediate Element, such as an 802.3 Switch, 802.11 Access Point, 802.3 Bridge, etc. (Intermediate Node)
An L2E is an Intermediate Node of a network infrastructure. This device provides Data Link Layer frame forwarding within the infrastructure and may support either:

- shared link layer media (bridging), as with 802.3 10base5 ('thick wire' ethernet), 10base2 ('thin wire' ethernet) and 802.11 versions a, b, I (WiFi), or
- point-to-point link layer media (switching) as in 802.3 10baseT (over CAT-5/6 cables), 100baseT (over CAT-5/6 cables), 1000baseT (over fiber or coax).

The L2E:

- typically is used to attach multiple end nodes into the network infrastructure with one connection used for direct attachment into the 'back-bone' infrastructure physical media and Data Link Layer technology and multiple connections for end nodes
- typically provides connections supporting either 4, 6, 8, 12, 16, 24 or 48 end nodes,
- data link layer & physical interconnections do not have to be identical. For example:
    - one connection could be 100baseT and from one to 48 additional connections could be 10baseT as found in many multi-port ethernet bridges and switches, or
    - when using 802.11 versions a, b, I on one (or two connections), as found in most wireless access points, there is usually only one other connection usually 10baseT or 100baseT, or
    - when using 10base5 or 10base2, there are usually only two connections supported given that these media types have stringent limitation on the number of 'daisy-chained' end nodes allowed on each physical media segment and segments cannot exceed specified distances.
- may include additional functionality beyond basic datagram forwarding, such as spanning tree filtering, virtual LANs (802.1q), spanning ports for monitoring, port authentication/authorization (802.1x) and other capabilities.

ADM Layer 2 Optical Intermediate Element, such as (Reconfigurable) Optical Add-Drop SONET Multiplexer (Intermediate Node)
An ADM can serve as either:

- an egress/ingress point of an Access Service Provider Access network infrastructure,
- an egress/ingress point of an Access Service Provider Metropolitan Core network infrastructure, or
- an egress/ingress point of an 'Back-bone' Service Provider network infrastructure.

This device is typically used when providing access service to subscribers in the large to very large commercial, educational and institutional markets. The ADM:

- provides at least one data link layer & physical interconnection to the customer/subscriber premises network infrastructure
- provides one data link layer & physical interconnection to the Access Service Provider ADM.

WDM Layer 2 Lambda Intermediate Element, such as a course or dense Wave Division Multiplexer (Intermediate Node)
A WDM is an egress/ingress point of an Access Service Provider network infrastructure. This device is typically used when providing access service to other TSPs. The WDM:

- provides at least one data link layer & physical interconnection to the customer/subscriber premises network infrastructure
- provides one data link layer & physical interconnection to the Access Service Provider WDM.

ATM-FR Layer 2 Logical Intermediate Element, such as an Asynchronous Transport Mode or Frame Relay Switch (Intermediate Node)
An ATM-FR switch is an egress/ingress point of an Access Service Provider network infrastructure. This device is typically used when providing access service to subscribers in the medium sized commercial, educational and institutional markets. The ATM-FR switch:

- provides at least one data link layer & physical interconnection to the customer/subscriber premises network infrastructure
- provides one data link layer & physical interconnection to the Access Service Provider ATM-FR switch.

SPAP* Service Provider Application Server Platform (End Node)
This element represents any type of end element that provides an application service(s) to other elements. These services include, but are not limited to: network time, remote backup, network file and database storage, SIP Proxy/Registrars, Authentication, Print Servers, Web Servers, DNS/directory servers, etc. These elements may act as either 'clients' or servers within a peer-to-peer or client-server relationship with other elements. All information exchanged with these elements to/from other elements occurs as Application Layer traffic.

EMS* Service Provider Element Management System (End Node)
This element represents any type of end element that provides management services (FCAPS) used to manage other intermediate and end elements. These FCAPS services focus on those FCAPS capabilities within the TMN Element and Network Management Layers (EML, NML). These elements may act as either 'clients' or servers within a peer-to-peer or client-server relationship with their assigned managed elements. All information exchanged with these elements occur as Application Layer traffic.

OSS* Service Provider Operations Support System (End Node)
This element represents any type of end element that provides management services (FCAPS) used to manage other intermediate and end elements. These FCAPS services focus on those FCAPS capabilities within the TMN Element and Network Management Layers (EML, NML). These elements may act as either 'clients' or servers within a peer-to-peer or client-server relationship with their assigned managed elements. All information exchanged with these elements occur as Application Layer traffic.

IPS Intrusion Prevention System (Intermediate Node)
This element represents any type of intermediate element that provides inspection and either deletion or change of packets, based on the contents of application layer protocol data based on a set of rules, policies or behaviors.

FW Standalone Packet Filtering System, such as a Stateful Firewall (Intermediate Node)
This element represents any type of intermediate element that either forwards or drops packets between differed networks, or network segments, based on the contents of fields within the internetworking and transport protocol headers as specified by a set of rules, policies or behaviors.

5.3.1.2.1.5 Layering of Interface Types, Protocols and Functional planes

The following depicts the hierarchy from interface types through protocol layer to protocol functional plane.

- User-Network Interface (UNI)
  - Data Link Layer (DLL)
    - Data Link Layer Signaling & Control Plane Traffic (DLL-SCP)
    - Data Link Layer User Plane Traffic (DLL-UP)
  - Inter-networking Protocol Layer (IL)
    - Internetworking Layer Signaling & Control Plane Traffic (IL-SCP)
    - Internetworking Layer User Plane Traffic (IL-UP)
  - Transport Protocol Layer (TL)
    - Transport Layer Signaling & Control Plane Traffic (TL-SCP)
    - Transport Layer User Plane Traffic (TL-UP)
  - Application Protocol Layer (AL)
    - Application Layer Signaling & Control Plane Traffic (AL-SCP)
    - Application Layer User Plane Traffic (AL-UP)
    - Application Layer Management Plane Traffic (AL-MP)
- Internal Network-Network Interface (I-NNI)
  - Data Link Layer (DLL)
    - Data Link Layer Signaling & Control Plane Traffic (DLL-SCP)
    - Data Link Layer User Plane Traffic (DLL-UP)
  - Inter-networking Protocol Layer (IL)
    - Internetworking Layer Signaling & Control Plane Traffic (IL-SCP)
    - Internetworking Layer User Plane Traffic (IL-UP)
  - Transport Protocol Layer (TL)
    - Transport Layer Signaling & Control Plane Traffic (TL-SCP)
    - Transport Layer User Plane Traffic (TL-UP)
  - Application Protocol Layer (AL)
    - Application Layer Signaling & Control Plane Traffic (AL-SCP)
    - Application Layer User Plane Traffic (AL-UP)
    - Application Layer Management Plane Traffic (AL-MP)
- Network-Network Interface (NNI)
  - Data Link Layer (DLL)
    - Data Link Layer Signaling & Control Plane Traffic (DLL-SCP)
    - Data Link Layer User Plane Traffic (DLL-UP)
  - Inter-networking Protocol Layer (IL)
    - Internetworking Layer Signaling & Control Plane Traffic (IL-SCP)
    - Internetworking Layer User Plane Traffic (IL-UP)
  - Transport Protocol Layer (TL)
    - Transport Layer Signaling & Control Plane Traffic (TL-SCP)

Transport Layer User Plane Traffic (TL-UP)
Application Protocol Layer (AL)
Application Layer Signaling & Control Plane Traffic (AL-SCP)
Application Layer User Plane Traffic (AL-UP)
Application Layer Management Plane Traffic (AL-MP)

5.3.1.2.2 Generic Network Architecture Context Scenarios

The following six (6) typical examples of interconnection scenarios depict in greater detail the interplay between interface types, protocol layer and protocol functional plane. As there are options available as to what may be used across these interfaces, these scenarios identify the assumptions made in regards to each interface.

5.3.1.2.2.1 Scenario 1 Two End Nodes communicating via a Common ISP

In this scenario an End Node within the “Alice” customer security domain is communicating with an End Node within the "Bob" customer security domain. These two End Nodes are attached to the same Service Provider’s network

Interface Discussion

IF-A1 This interface is a customer security domain I-NNI and represents the networking infrastructure on the "Alice" customer premises.

Layer 2: At the Data Link Protocol Layer, it is assumed 802.3 (10baseT, 100baseT) is used, there may be zero (0) or more layer 2 devices such as bridges or switches between the CEN and the CER.

Layer 3: At the Inter-networking Protocol layer it is assumed that the infrastructure uses IPv4 with non-routable "private" IP addresses, there may be zero (0) or more routers between the CEN and the CER.

Layer 4: At the Transport Protocol layer it is assumed that a transport protocol (TCP, UDP, SCTP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes simply ignore the data component of IP packets.

Layer 5: At the Application protocol layer it is assumed that an appropriate application protocol is used that operates on an application process to application process basis such that intermediate nodes simply ignore the data component of transport protocol messages.

The customer end node could be either a 'client' machine interacting with a server within the "Bob" customer premises or the reverse. The CER may either be owned & managed by the customer, owned by the customer and managed by the service provider, owned by the customer and managed by a 3rd party or owned and managed by the service provider.

IF-A2 This interface is a service provider security domain UNI and represents the interface between the "Alice" customer premise and the service provider.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (10baseT, 100baseT) is used at layer 2 between the service provider facing CER interface and the service provider DSL modem or ONT.

Layer 3: At the Inter-networking Protocol layer it is assumed that IPv4 is used with a service provider assigned IP address for the service provider facing CER interface. Layer 3 Signaling & Control protocols used over this interface will most likely be ARP, DHCP and ICMP.

Layer 4: At the Transport Protocol layer it is assumed a transport protocol (TCP, UDP, SCTP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets.

Layer 5: At the Application Protocol layer it is assumed application protocols (such as http, ftp, telnet, SMTP, etc.) are used over a transport protocol (TCP, UDP, SCTP) that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets.

IF-A3 This interface is a service provider security domain I-NNI and represents the interface between the service provider customer premises network termination device (DSL Modem or ONT) and the service provider access network termination device (DSLAM or OLT).

Layer 2: At the Data Link Protocol Layer it is assumed xDSL or PON (G.983, G.984) at layer 2 are used between the service provider facing DSL Modem or ONT interface and the service provider DSLAM or OLT.

Layer 3: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-A4 This interface is a service provider security domain I-NNI and represents the interface between the service provider access network termination device (DSLAM or OLT) and the service provider access network edge router.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE) is used at layer 2 between the service provider DSLAM or OLT and the service provider access network edge router. Layer 2 Signaling & Control protocols used over this interface will most likely be IEEE 802.1q, 802.1x.

Layer 3: At the Inter-networking Protocol layer it is assumed that IPv4 is used with a service provider assigned IP address for the service provider facing CER interface. Layer 3 Signaling & Control protocols used over this interface will most likely be ARP, DHCP and ICMP.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-A5 This interface is a service provider security domain I-NNI and represents the interface between the service provider access network edge router and the service provider metropolitan network core router.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE), G-MPLS/GFP is used at layer 2 between the service provider access network edge router and the service provider metropolitan network core router. Layer 2 Signaling & Control protocols used over this interface will most likely be IEEE 802.1q.

Layer 3: At the Inter-networking Protocol layer it is assumed that IPv4 is used with a service provider assigned IP address for the service provider PER interfaces. Layer 3 Signaling & Control protocols used over this interface will most likely be CR-LDP, RSVP-TE, LDP, RSVP, DHCP and ICMP.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-A6 This interface is a service provider security domain I-NNI and represents the interface between the service provider metropolitan network core router and the service provider access network edge router.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE), G-MPLS/GFP is used at layer 2 between the service provider access network edge router and the service provider metropolitan network core router. Layer 2 Signaling & Control protocols used over this interface will most likely be IEEE 802.1q.

Layer 3: At the Inter-networking Protocol layer it is assumed that IPv4 is used with a service provider assigned IP address for the service provider PER interfaces. Layer 3 Signaling & Control protocols used over this interface will most likely be CR-LDP, RSVP-TE, LDP, RSVP, DHCP and ICMP.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-A7 This interface is a service provider security domain UNI and represents a combination of interfaces IF-A2, IF-A3 and IF-A4 between the service provider access network edge router and the customer edge router.

IF-A8 This interface is a customer security domain I-NNI and represents the networking infrastructure on the "Bob" customer premises.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (10baseT, 100baseT) is used where there may be zero (0) or more layer 2 devices such as bridges or switches between the CEN and the CER.

Layer 3: At the Inter-networking Protocol layer it is assumed that the infrastructure uses IPv4 with non-routable "private" IP addresses where there may be zero (0) or more routers between the CEN and the CER.

Layer 4: At the Transport Protocol layer it is assumed a transport protocol (TCP, UDP, SCTP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes simply ignore the data component of IP packets.

Layer 5: At the Application protocol layer an appropriate application protocol is used that operates on an application process to application process basis such that intermediate nodes simply ignore the data component of transport protocol messages.

The customer end node could be either a 'client' machine interacting with a server within the "Alice" customer premises or the reverse. The CER may either be owned & managed by the customer, owned by the customer and managed by the service provider, owned by the customer and managed by a 3rd party or owned and managed by the service provider.

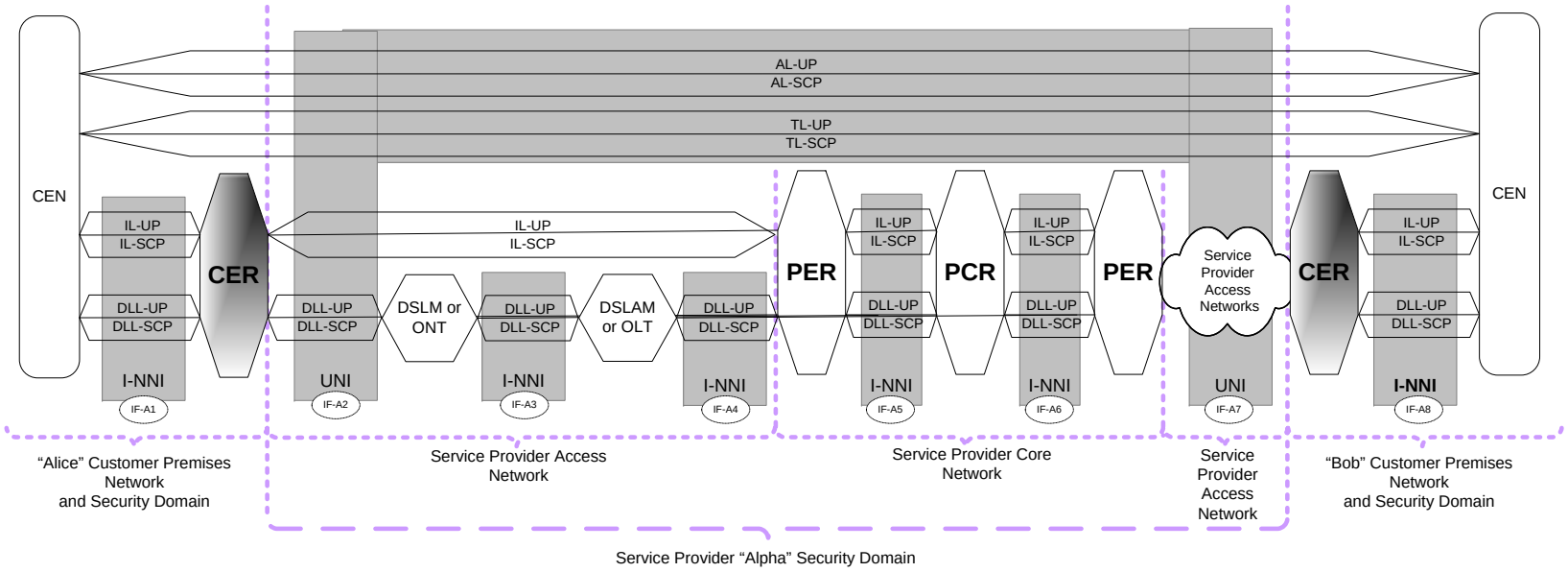

Figure 5- Scenario 1

5.3.1.2.2.2 Scenario 2 Two End Nodes communicating via Two Different ISPs

In this scenario an End Node within the “Alice” customer security domain is communicating with an End Node within the "Bob" customer security domain. These two End Nodes are attached to different Service Providers have a direct Peering Relationship.

Interface Discussion

IF-B1 This interface is a customer security domain I-NNI and represents the networking infrastructure on the "Alice" customer premises and is the same as interface IF-A1.

The customer end node could be either a 'client' machine interacting with a server within the "Bob" customer premises. The CER may either be owned & managed by the customer, owned by the customer and managed by the service provider, owned by the customer and managed by a 3rd party or owned and managed by the service provider.

IF-B2 This interface is a service provider security domain UNI and is the same as interface IF-A2.

IF-B3 This interface is a service provider security domain I-NNI and is the same as interfaces IF-A3 and IF-A4.

IF-B4 This interface is a service provider security domain I-NNI and represents the interface between the service provider access network edge router and the service provider peering-point router with the communication between these service provider routers possibly traversing one or more the service provider metropolitan network core routers. This interface is the same as interfaces IF-A5 and IF-A6.

IF-B5 This interface is a service provider security domain NNI and represents the interface between the two service providers' peering-point routers.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE), G-MPLS/GFP is used at layer 2 between the two different service provider peering-point routers. Layer 2 Signaling & Control protocols used over this interface will most likely be IEEE 802.1q.

Layer 3: At the Inter-networking Protocol layer it is assumed that IPv4 is used with a service provider assigned IP address for each service provider's PPR interfaces. Layer 3 Signaling & Control protocols used over this interface will most likely be CR-LDP, RSVP-TE, LDP, RSVP, DHCP, ICMP and IPsec.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-B6 Same as interface IF-B4 but different service provider.

IF-B7 Same as interface IF-A7 but different service provider.

IF-B8 Same as interface IF-A8 but different service provider

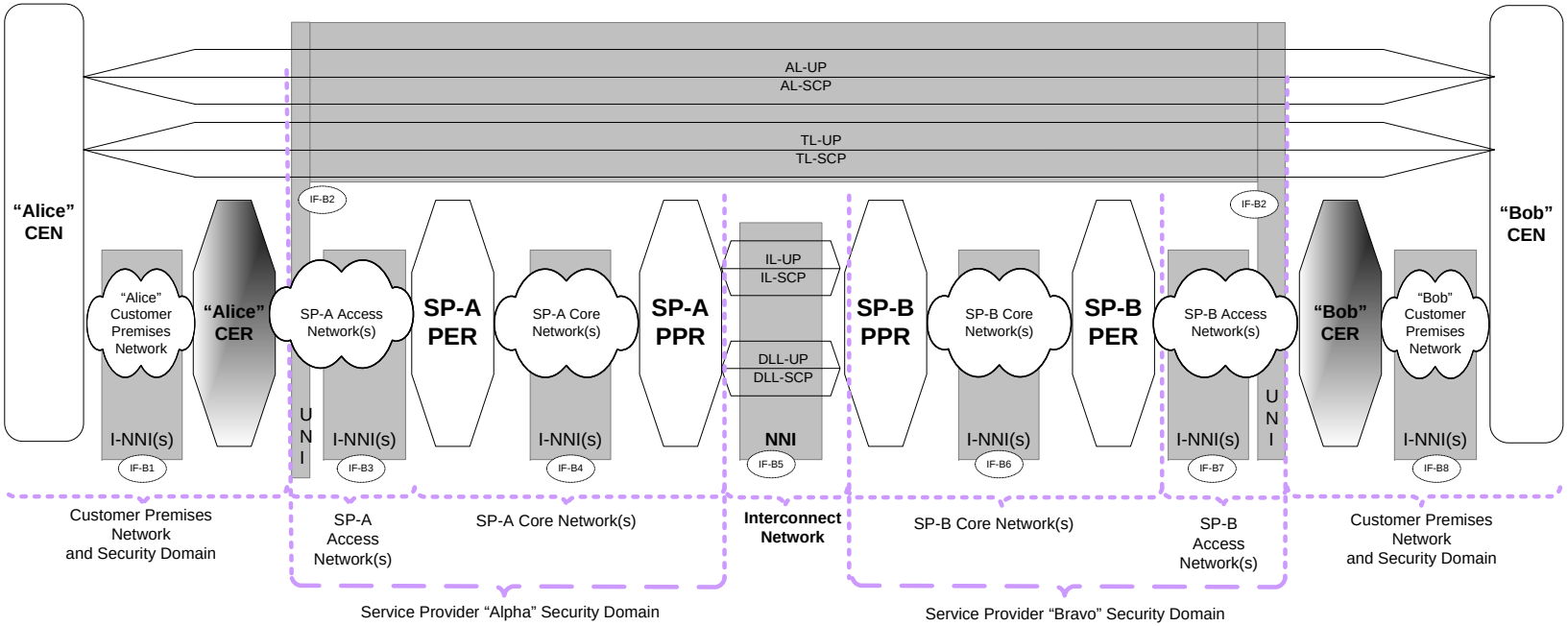

Figure 6 - Scenario 2

5.3.1.2.2.3 Scenario 3 Two End Nodes communicating via Two Different ISPs & A Backbone SP

In this scenario an End Node within the “Alice” customer security domain is communicating with an End Node within the "Bob" customer security domain. These two End Nodes are attached to different Service Providers who do not have a direct Peering Relationship rather they Interconnect via a 3rd (“BackBone”) Service Provider.

Interface Discussion

IF-D1 This interface is a customer security domain I-NNI and represents the networking infrastructure on the "Alice" customer premises and is the same as interface IF-A1.

IF-D2 This interface is a service provider security domain UNI and is the same as interface IF-A2.

IF-D3 This interface is a service provider security domain I-NNI and is the same as interfaces IF-B3.

IF-D4 This interface is a service provider security domain I-NNI and is the same as interface IF-B4.

IF-D5 This interface is a service provider security domain NNI and represents the interface between the two service providers' peering-point routers and is the same as interface IF-B5.

IF-D6 This interface is a service provider security domain I-NNI and is the same as interface IF-B4.

IF-D7 This interface is a service provider security domain NNI and represents the interface between the two service providers' peering-point routers and is the same as interface IF-D5.

IF-D8 Same as interface IF-D4 but different service provider.

IF-D9 Same as interface IF-A2 but different service provider.

IF-D10 Same as interface IF-A8 but different service provider

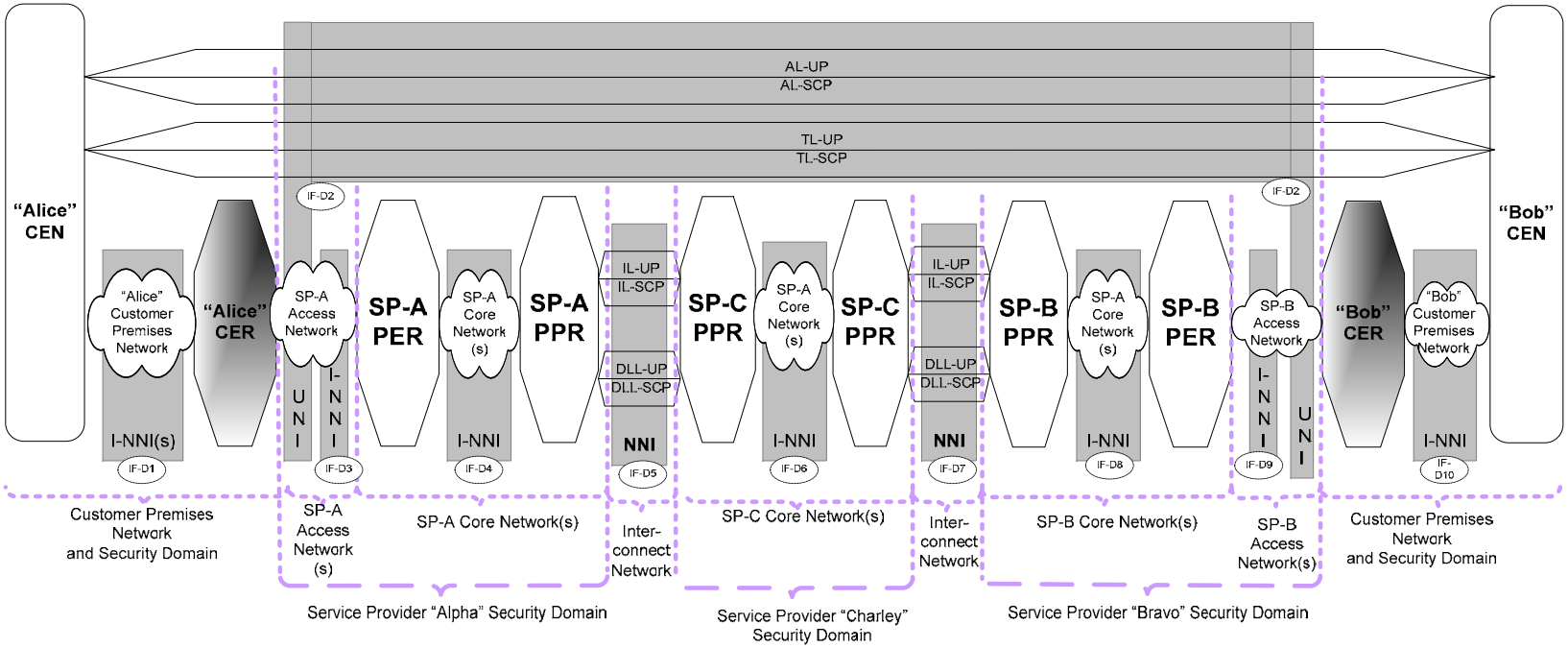

Figure 7 - Scenario 3

5.3.1.2.2.4 Scenario 4 A CP Router managed by an ISP EMS

In this scenario a Customer owned edge router within the “Alice” customer security domain is remotely managed by a service provided (element) management system. It should be noted that this scenario is not consistent with the management scenarios discussed in ITU-T M.3060.

Interface Discussion

IF-C1 This interface is a customer security domain I-NNI and represents the networking infrastructure on the "Alice" customer premises and is the same as interface IF-A1.

IF-C2 This interface is a service provider security domain UNI and represents the interface between the "Alice" customer premise and the service provider.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (10baseT, 100baseT) is used at layer 2 between the service provider facing CER interface and the service provider DSL modem or ONT.

Layer 3: At the Inter-networking Protocol layer it is assumed that IPv4 is used with a service provider assigned IP address for the service provider facing CER interface. Layer 3 Signaling & Control protocols used over this interface will most likely be ARP, DHCP and ICMP.

Layer 4: At the Transport Protocol layer it is assumed a transport protocol (TCP, UDP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets.

Layer 5: At the Application Protocol layer it is assumed application management protocols over transport protocol (TCP, UDP) are used that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets.

IF-C3 This interface is a service provider security domain I-NNI and represents the interface between the service provider customer premises network termination device (DSL Modem or ONT) and the service provider access network termination device (DSLAM or OLT) and is the same as IF-A3.

IF-C4 This interface is a service provider security domain I-NNI and represents the interface between the service provider access network termination device (DSLAM or OLT) and the service provider access network edge router and is the same as IF-A4.

IF-C5 This interface is a service provider security domain I-NNI and represents the interface between the service provider access network edge router and a different service provider edge router with the communication between these service provider routers possibly traversing one or more the service provider metropolitan network core routers. This interface is the same as interfaces IF-A5 and IF-A6.

IF-C6 This interface is a service provider security domain I-NNI and is the same as interface IF-A4.

IF-C7 This interface is a service provider security domain I-NNI and is the same as interface IF-A4.

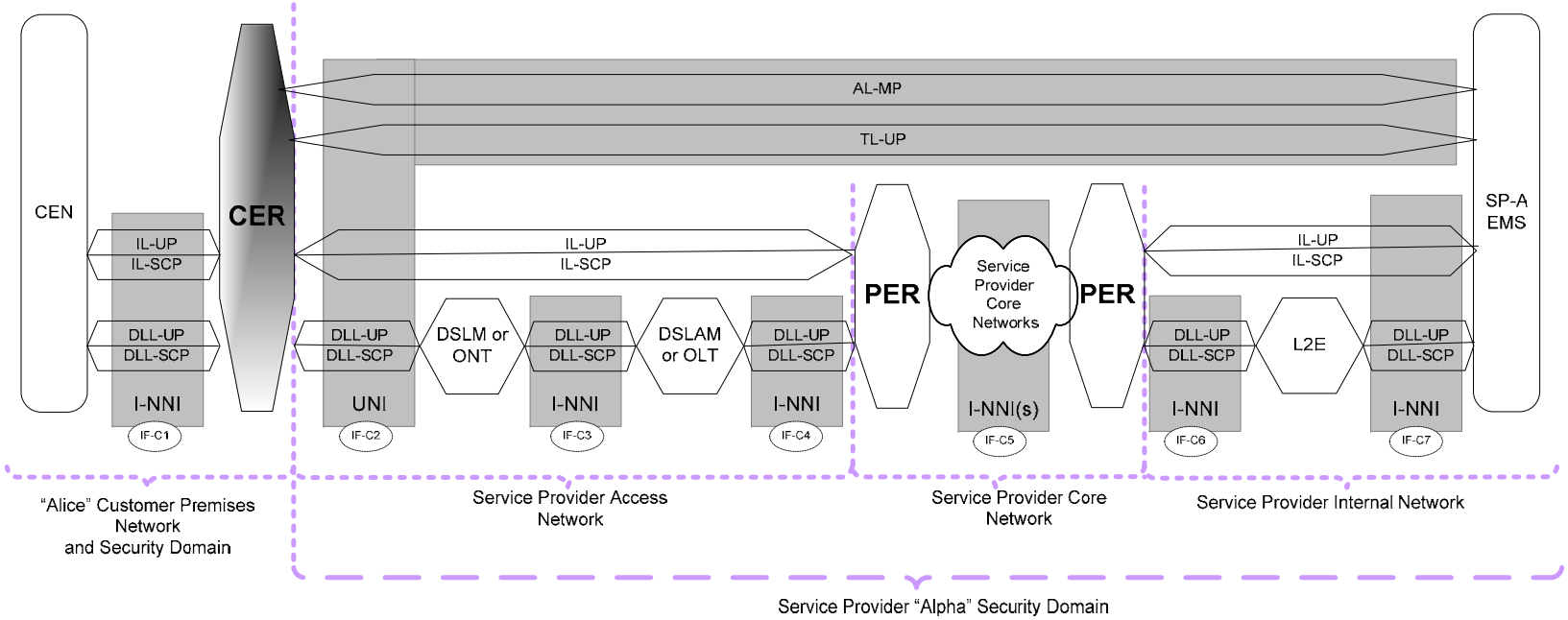

Figure 8 - Scenario 4

5.3.1.2.2.5 Scenario 5 Two ISP OSSs Collaboratively Communicating (Peering)

In this scenario an Operations Support System End Node within Service Provider "Alpha" security domain is communicating with an Operations Support System End Node within Service Provider "Bravo"security domain. These two End Nodes are attached to different Service Providers who have a direct Peering Relationship.

It should be noted that ITU-T Q.812 discusses protocol profiles between Service Providers when ISO-OSI protocols are in use and this does not conflict with ITU-T M.3016/ANSI T1.276, or the discussion within this section, when IP/TCP based protocol stacks are in use.

Interface Discussion

IF-E1 This interface is a service provider security domain I-NNI and is the same as interface IF-A4.

IF-E2 This interface is a service provider security domain I-NNI and is the same as interface IF-A4.

IF-E3 This interface is a service provider security domain I-NNI and represents the interface between the service provider access network edge router and a different service provider edge router with the communication between these service provider routers possibly traversing one or more the service provider metropolitan network core routers. This interface is the same as interfaces IF-A5 and IF-A6.

IF-E4 This interface is a service provider security domain NNI and represents the interface between the two service providers' peering-point routers.

- Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE), G-MPLS/GFP is used at layer 2 between the two different service provider peering-point routers. Layer 2 Signaling & Control protocols used over this interface will most likely be IEEE 802.1q.
- Layer 3: At the Inter-networking Protocol layer assumes that IPv4 is used with service provider assigned IP address is used for each service provider's PPR interfaces. Layer 3 Signaling & Control protocols used over this interface will most likely be CR-LDP, RSVP-TE, LDP, RSVP, DHCP, ICMP and IPsec.
- Layer 4: At the Transport Protocol layer it is assumed a transport protocol (TCP, UDP, SCTP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets.
- Layer 5: At the Application Protocol layer it is assumed application management protocols over transport protocol (TCP, UDP, SCTP) are used that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets.

IF-E5 This interface is the same as interface IF-E3.

IF-E6 This interface is a service provider security domain I-NNI and is the same as interface IF-A4.

IF-E7 This interface is a service provider security domain I-NNI and is the same as interface IF-A4.

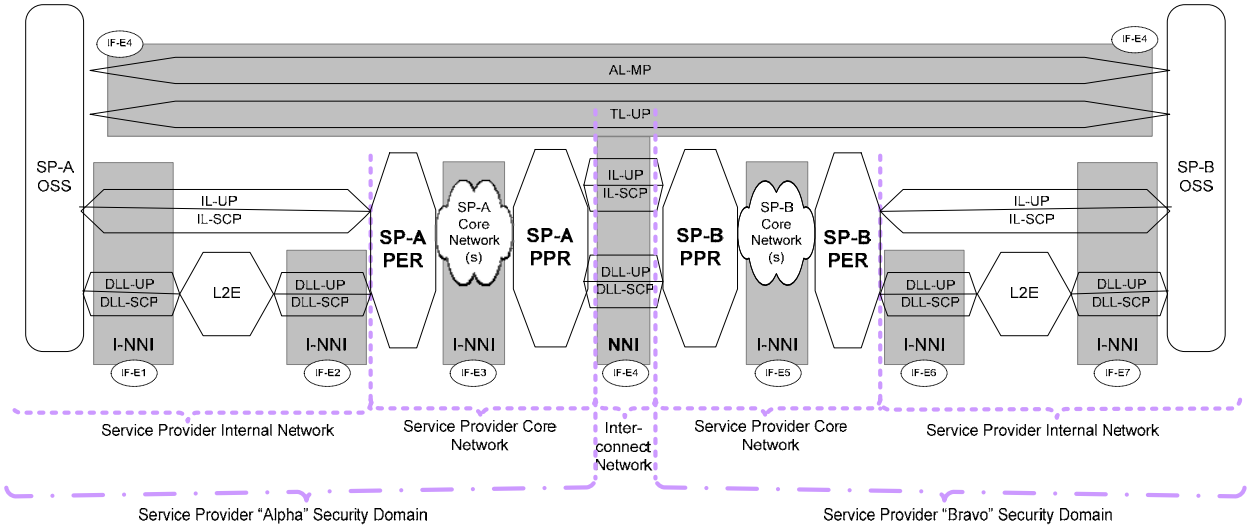

Figure 9 - Scenario 5

5.3.1.2.2.6 Scenario 6 Two End Nodes communicating using VoIP via Two Different ISPs

In this scenario:

- an End Node within the “Alice” customer security domain is communicating with a Service Provider Application Platform End Node within the Service Provider "Alpha" security domain
- an End Node within the “Bob” customer security domain is communicating with a Service Provider Application Platform End Node within the Service Provider "Bravo" security domain
- the Service Provider Application Platform End Nodes within the Service Provider "Alpha" and "Bravo" security domains are communicating, and
- these two End Nodes are attached to different Service Providers who do not have a direct Peering Relationship rather they Interconnect via a 3rd (“Backbone”) Service Provider.

Interface Discussion

IF-F1 This interface is a customer security domain I-NNI and represents the networking infrastructure on the "Alice" customer premises and is the same as interface IF-A1.

IF-F2 This interface is a service provider security domain UNI and is the same as interface IF-A2.

IF-F3 This interface is a service provider security domain I-NNI and is the same as interfaces IF-A3.

IF-F4 This interface is a service provider security domain I-NNI and is the same as interface IF-A4.

IF-F5 This interface is a service provider security domain NNI and represents the interface between the two service providers' peering-point routers and is the same as interface IF-B5.

IF-F9 Same as interface IF-A7, but different service provider.

IF-F10 This interface is a customer security domain I-NNI and represents the networking infrastructure on the "Alice" customer premises and is the same as interface IF-A8.

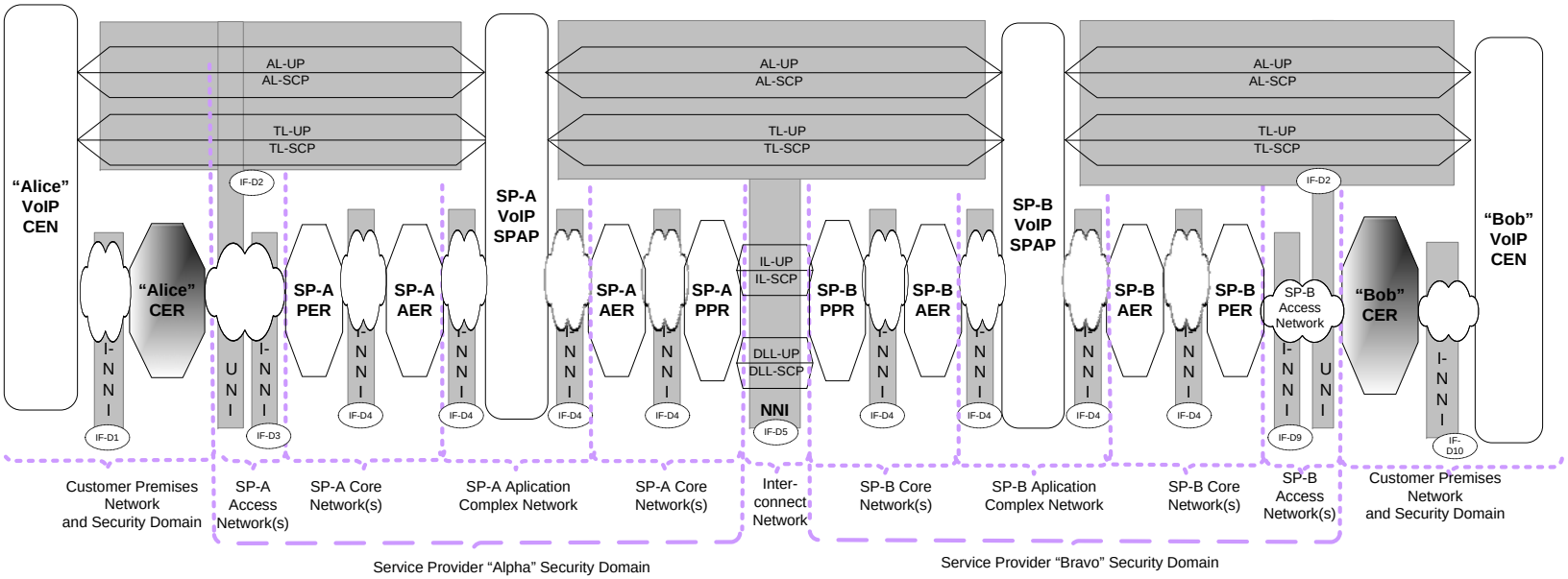

Figure 10 - Scenario 6

5.3.2 Mapping Security Services to the Architectural Model

The following tables depict which security services, discussed in section 5.2, apply within the hierarchy of network interfaces, protocol layers and protocol functional planes discussed in section 3.1.

Table 13- Data Link Layer User Plane

I/F Type	Security Service	Currently Needed?
UNI	Peer-Entity Authentication	Not necessary
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	Not necessary
	Connectionless Confidentiality	Not necessary
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	Not necessary
I-NNI	Peer-Entity Authentication	Not necessary
	Data-Origin Authentication	Not necessary
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	Not necessary
	Connectionless Confidentiality	Not necessary
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
		Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	Not necessary
NNI	Peer-Entity Authentication	Not necessary
	Data-Origin Authentication	Not necessary
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	Not necessary
	Connectionless Confidentiality	Not necessary
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	Not necessary

Table 14 - Data Link Layer Signaling & Control

I/F Type	Security Service	Currently Needed?
UNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	Not necessary
	Connectionless Confidentiality	Not necessary
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	Not necessary
I-NNI	Peer-Entity Authentication	Not necessary
	Data-Origin Authentication	Not necessary
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	Not necessary
	Connectionless Confidentiality	Not necessary
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**

I/F Type	Security Service	Currently Needed?
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	Not necessary
NNI	Peer-Entity Authentication	Not necessary
	Data-Origin Authentication	Not necessary
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	Not necessary
	Connectionless Confidentiality	Not necessary
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	Not necessary

I/F Type	Security Service	Currently Needed?
UNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
I-NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**

Table 15 - Internetworking Layer User

I/F Type	Security Service	Currently Needed?
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**

Table 16 - Internetworking Layer Signaling & Control)

I/F Type	Security Service	Currently Needed?
UNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
I-NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**

Table 17 - - Transport Layer User Plane

I/F Type	Security Service	Currently Needed?
UNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	**As Required**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
I-NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not

I/F Type	Security Service	Currently Needed?
		necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**

Table 18 - Transport Layer Signaling & Control

I/F Type	Security Service	Currently Needed
UNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	**As Required**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
I-NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	Not necessary
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	Not necessary
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	Not necessary
	Connection Integrity without Recovery	Not necessary
	Selective Field Connection Integrity	Not necessary
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	Not necessary
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**

Table 19 - Application Protocol Layer User Plane

I/F Type	Security Service	Currently Needed?
UNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	**As Required**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	**As Required**
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	**As Required**
	Connection Integrity without Recovery	**As Required**
	Selective Field Connection Integrity	**As Required**
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	**As Required**
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
I-NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	**As Required**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	**As Required**
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	**As Required**
	Connection Integrity without Recovery	**As Required**
	Selective Field Connection Integrity	**As Required**
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	**As Required**
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	**As Required**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	**As Required**
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	**As Required**
	Connection Integrity without Recovery	**As Required**
	Selective Field Connection Integrity	**As Required**
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	**As Required**
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**

Table 20 - Application Protocol Layer Signaling & Control

I/F Type	Security Service	Currently Needed?
UNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	**As Required**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	**As Required**
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	**As Required**
	Connection Integrity without Recovery	**As Required**
	Selective Field Connection Integrity	**As Required**
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	**As Required**
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
I-NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	**As Required**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	**As Required**
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	**As Required**
	Connection Integrity without Recovery	**As Required**
	Selective Field Connection Integrity	**As Required**
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	**As Required**
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**
NNI	Peer-Entity Authentication	**As Required**
	Data-Origin Authentication	**As Required**
	User Authentication	**As Required**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	**As Required**
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	**As Required**
	Connection Integrity without Recovery	**As Required**
	Selective Field Connection Integrity	**As Required**
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	**As Required**
	Non-repudiation with Proof of Origin	**As Required**
	Non-repudiation with Proof of Delivery	**As Required**

Table 21 - Application Protocol Layer Management Plane

I/F Type	Security Service	Currently Needed?
UNI	Peer-Entity Authentication	**Necessary**
	Data-Origin Authentication	**Necessary**
	User Authentication	**Necessary**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	**As Required**
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	**As Required**
	Connection Integrity without Recovery	**Necessary**
	Selective Field Connection Integrity	**As Required**
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	**As Required**
	Non-repudiation with Proof of Origin	**Necessary**
	Non-repudiation with Proof of Delivery	**Necessary**
I-NNI	Peer-Entity Authentication	**Necessary**
	Data-Origin Authentication	**Necessary**
	User Authentication	**Necessary**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	**As Required**
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	**As Required**
	Connection Integrity without Recovery	**Necessary**
	Selective Field Connection Integrity	**As Required**
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	**As Required**
	Non-repudiation with Proof of Origin	**Necessary**
	Non-repudiation with Proof of Delivery	**Necessary**
NNI	Peer-Entity Authentication	**Necessary**
	Data-Origin Authentication	**Necessary**
	User Authentication	**Necessary**
	Access Controls	**Necessary**
	Connection Confidentiality	**As Required**
	Connectionless Confidentiality	**As Required**
	Selective Field Confidentiality	**As Required**
	Traffic Flow Confidentiality	Not necessary
	Logging	**Necessary**
	Connection Integrity with Recovery	**As Required**
	Connection Integrity without Recovery	**Necessary**
	Selective Field Connection Integrity	**As Required**
	Connectionless Integrity	**Necessary**
	Selective Field Connectionless Integrity	**As Required**

	Non-repudiation with Proof of Origin	**Necessary**
	Non-repudiation with Proof of Delivery	**Necessary**

5.4 Security Mechanisms

This section discusses general security mechanisms including operating systems, application frameworks, security protocols, cryptographic algorithms, cryptographic key sizes, and other security facilities which can be used to instantiate and enforce security policies.

5.4.1 Operating System Security Mechanisms and Hardening

5.4.1.1 TSP Element Security Overview

All TSP infrastructure deployed elements contain some form of operating software. This software can take the form of:

Type 1	a general purpose Operating System (OS), typically some form of unix like multi-tasking OS, along with a full complement of file-system, graphical interface, command interpreters, network protocol stack and application server capabilities (as in DNS, http, ftp, VoIP, packet/message filtering, etc.),
Type 2	a general purpose OS, typically some form of unix like multi-tasking OS with real-time scheduling capabilities, with a minimized set of file-system, graphical interface, command interpreters, network protocol stack and application service capabilities configured to perform a limited set of functions,
Type 3	a real-time OS (RTOS), typically some form of embedded OS, along with file-system, graphical interface, command interpreters, network protocol stack and application server capabilities (as in DNS, http, ftp, VoIP, packet/message filtering, etc.), or
Type 4	a basic input-output set of functions for storage, memory, clock and interrupt management tightly bound with a single application service capability (as in DNS, http, ftp, VoIP, packet/message filtering, etc.)

A security architecture for elements (i.e., end elements, end nodes, hosts) and intermediate elements (i.e., intermediate notes, relay systems) applies to a wide range of applications and environments. Among the many possible implementations, some unifying structure must be created that permits a generic approach to security. This structure accommodates the primary security allocations made in Section 5.2. This section refines several concepts, including security allocations, types of functions that are required to support the security allocations, types of devices that make up end elements and intermediate elements, and technologies that should be considered in specific implementations.

Generally, intermediate elements provide services that require the same kinds of underlying support as end elements, except that they do not provide support for direct user interactions, only administrative interactions. Thus, a single security architecture for end elements and intermediate elements is appropriate. The remainder of this section refers to both end elements and intermediate elements simply as elements.

The element security architecture focuses on conventional computer systems (Types 1 and 2 above), which represent a large portion of all elements. Other element types may need to implement only portions of the element security architecture (Type 3 above). In extreme cases,

such as simple sensor or probe devices, the element functions may be so limited that only specialized implementations of a small portion of the element security architecture are appropriate (Type 4 above).

In Section 5.2, fundamental allocations of security services are made to elements within security domains. Element security makes additional security service allocations to element hardware and software. Not every security service allocation needs to be made identically in every element.

Security service allocations are implemented as physical and administrative security mechanisms within the security domain. The primary security service allocations to the security domain are access control to facilities and some aspects of authentication of personnel.

5.4.1.1.1 The Hardware Protects the Software

There are a variety of security mechanism choices available between the hardware and software portions of each element, but certain general allocations and properties can be stated for the hardware. The hardware is relied upon to function correctly, to enforce isolation of software functions, and to contribute to the protection of the integrity of the system applications and the OS. It provides protected paths between users and trusted parts of the software. The hardware indirectly supports the isolation of information processed and stored in the element by protecting the integrity of the software. In some environments, specific hardware technologies (e.g., hardened or alarmed chassis) may be necessary to protect against tampering with element components. Availability of an element may be enhanced through technologies such as fault-tolerant and fault-detecting hardware features. Hardware cryptographic mechanisms are employed as needed to support various security services. Other hardware mechanisms (e.g., memory management/mapping) support specific aspects of the software architecture and are noted in the element security architecture discussion (section 5.4.1.2).

5.4.1.1.2 The Software Protects Information

The security service allocations made to software are wide ranging. The networking subsystem supported by the element software is responsible for the confidentiality and integrity of information transferred amongst elements, for the authentication of elements to one another, and for user authentication and access control in distributed systems. The details of how the networking subsystem is supported by elements are presented in Sections 5.3 and 5.4.

Security services and the mechanisms that implement them must be managed. The software applications that support security management in elements are discussed in Section 5.5.

The element software is responsible for user authentication and access control, and for the integrity of information being processed and in storage. Correct operation of certain software is required to ensure element availability. Additionally, the software is expected to provide functions that support the security policies and requirements that are not directly expressed as security services, such as support for multiple security policies. The remainder of this section refines the element security architecture, which primarily is concerned with software structure.

5.4.1.2 Element Security Architecture Description

An element security architecture must respond to the security allocations discussed earlier, and it must be sufficiently flexible to encompass changing technology. The element security architecture presented in Figure 11 is an example and not an implementation specification, and might be realized in several ways. The element security architecture concentrates on support

for multiple security domains with distinct security policies, where these security (sub-) domains may be 'fine grained' down to specific functions within an element. No distinction will be made between security domains and sub-domains henceforth. Attention is paid to strict separation of security (sub-) domains, management of element resources, and controlled sharing and transfer of information among security domains. The element security architecture also relies upon an engineering approach that seeks to isolate security-critical functions into relatively small modules that are related in well-defined ways. This approach has advantages in implementation and certification by limiting the scope of particular portions of these activities. Recently, commercial OS vendors have adopted design and implementation strategies that share significant aspects of the element security architecture.

A security context is a combination of all the security domain, hardware, system software, user application software, and information supporting the activities of a user (or system function) operating in a security (sub-) domain. A security context builds on the common OS notion of a user process space (sometimes called a context) as supported by hardware features and OS functions. The primary distinctions between an ordinary user process space and a security context are that aspects of protection provided by the security domain are explicitly included, and that user applications operate in a controlled process space subject to a security domain security policy. Security contexts are described in more detail in Section 5.4.1.2.2.

A kernel manipulates the protection features of the element hardware (e.g., processor state registers, memory mapping registers) to maintain strict separation among security contexts by creating separate address spaces for each of them. A kernel also controls communications among security contexts to allow sharing or transfer of information, and to allow services to be performed by one security context for another. All user security contexts and many system function security contexts are constrained to make requests for basic element services on the kernel through a common kernel interface. The kernel is described further in Section 5.4.1.2.1. The functions that make and enforce security policy decisions are intimately related to the kernel. These are described in Sections 5.4.1.2.1 and 5.4.1.2.3.

In Figure 11, element software is divided into trusted and untrusted parts for practical evaluation. The trusted parts of the software are those that are considered so important to the secure operation of the element that they should undergo strict evaluation procedures and be under strict configuration management control. In Section 5.2, fundamental allocations of security services were made to element within security domains. Element system security makes additional security service allocations to element hardware and software. Not every security service allocation needs to be made identically in every element.

Security service allocations are implemented as physical and administrative security mechanisms. The primary security service allocations to the security domain are access control to facilities and some aspects of authentication of personnel. In addition, some aspects of information confidentiality and integrity, and system integrity and availability are allocated to the security domain.

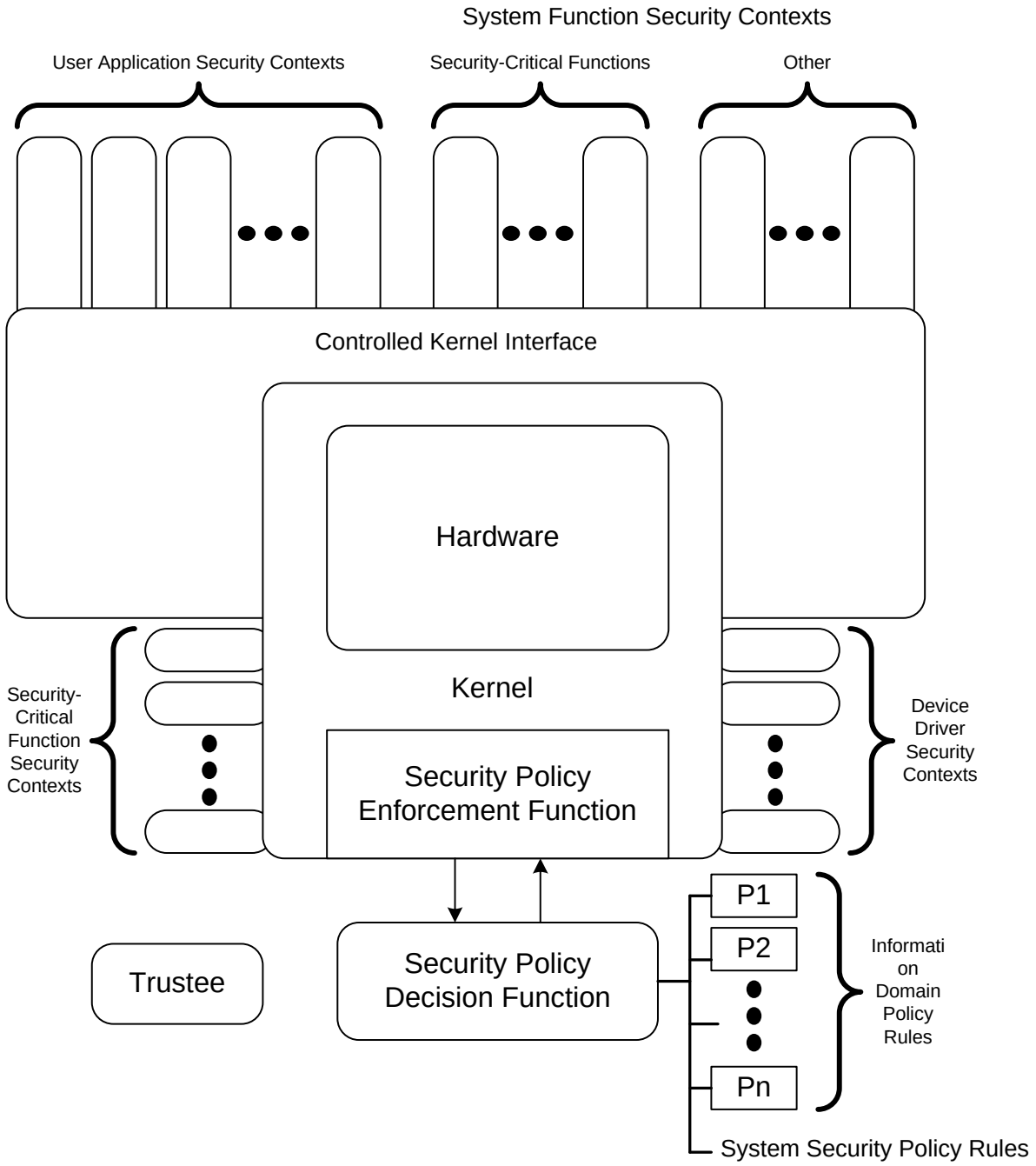

Figure 11- Element Security Architecture Generic View

The hardware (including any microcode or firmware) is considered very highly trusted in the sense that its operation is assumed to be correct. Less than highly trusted software is able to perform operations on basic system resources only through invocations of security-critical

functions that are mediated by the kernel; inter-security context operations (e.g., inter-security domain communications) are performed by security-critical functions within the kernel.

Trusted security-related functions (such as security management applications, portions of networking subsystem components, intrusion detection, configuration monitoring, host packet filtering and anti-virus) are expected to operate correctly to satisfy user operational needs, but need not be subjected to the rigorous scrutiny applied to the security-critical functions. Security-related software is not assumed to be free of security defects, although it is certainly prudent to obtain such software from reliable sources, test it before use, apply integrity safeguards to ensure it remains unchanged, and apply configuration management to it. Service functions (such as:

- Corba, DCE, Java Virtual Machines and .NET Application Framework software and
- ftp, ntp, dns, Email, VoIP type application servers

should be assumed safe and obtained from reliable sources, and integrity safeguards and configuration management should be applied. Application Software (obtained from less than reliable sources) should be considered untrusted and may need to be inspected more carefully, test it before use, inspect it for viruses and malware, apply integrity safeguards to ensure it remains unchanged, and apply configuration management to it. Under these conditions, if faulty application software is introduced into a system it will, at worst, prevent certain operations, but information compromise will not result because of the combination of strict isolation of security domains enforced by the element, testing, and configuration management.

The following subsections provide additional detail on the element security software components, primarily for the kernel, security contexts, security-critical functions, and OS implementations.

5.4.1.2.1 The Kernel

Significant general OS research has concentrated on organizing basic OS functions into a collection called a kernel. The kernel presents abstractions of the fundamental resource management mechanisms to other, less primitive, service providers (information system functions and applications). In OS implementations that attempt to provide a basis for secure information processing, the kernel software is carefully constructed and evaluated. To aid the evaluation process, the kernel functions are implemented as relatively small programs that are independent of one another to the maximum extent possible. A kernel is charged with the critical task of providing separation among process spaces by manipulating the protection features of the element hardware.

Until recently, most secure OS designs have been limited with regard to security policy specification and enforcement. Particular limitations include support for only a single security policy (usually an access control policy) and the inability to change security policy conveniently. The traditional OS kernel functions are divided among the kernel, security policy enforcement and decision functions, and the remainder of the trusted OS functions, called the security-critical functions. The kernel serves as the ultimate security policy enforcement function by mediating all use of the basic information system resources. The kernel notion is the foundation of the element security architecture.

The element security architecture generalizes an approach that is becoming widely accepted concerning access control, namely the independence between the decision of whether or not an access to a resource is allowed and the enforcement of that decision. The separation of access control decision-making and access control enforcement functions allows the support of multiple

access control policies. ITU-T X.812 designates these functions the Access control Decision Function (ADF) and the Access control Enforcement Function (AEF), respectively. In fact, most existing secure OS designs have concerned themselves only with access control policy. This element architecture extends the AEF concept to include the enforcement of all aspects of a security domain security policy. The resulting function is called the Security Policy Enforcement Function (SPEF). Similarly, the ADF concept is extended to a Security Policy Decision Function (SPDF), see Section 5.4.1.2.3. The kernel is the implementation of the SPEF in this element security architecture.

The kernel also is an extension (beyond access control) of the Reference Validation Mechanism (RVM) described in the Trusted Computer System Evaluation Criteria (DoD 5200.28-STD). The RVM shall be invoked for every kernel implementation and for every security-critical operation, the RVM must be small enough to be verified, and its integrity must be maintained. The kernel is reflected in Figure 12 as residing within ring 0. The concept of rings directly reflects the Biba Integrity model where integrity levels are associated with subjects and objects, such that

- A subject can have write access to objects on its own level or below but not above
- A subject can have read access to objects on its own level or above but not below

and information flows downwards in this model. Integrity levels are not security levels as the issue is trustworthiness, not disclosure (access/confidentiality) so the higher the level, the more confidence that data is accurate/reliable or that a program will execute correctly. From an element software perspective this is depicted in the following Table 22.

Table 22- Ring Structure of Integrity Levels

Software Processing Ring	Integrity Level	Object
0	Highly Trusted	Kernel
1	Trusted	Non-kernel OS functions
2	Assumed Safe	Service functions
3	Untrusted	Application functions

The common interface to the kernel is a single strongly controlled mechanism for functions residing within rings 1, 2 and 3 to make requests on kernel functionality.

5.4.1.2.2 Security Contexts

From the perspective of the kernel, a security context is defined by a set of data and programs operating in accordance with a security domain security policy. As noted earlier, a security context also includes the physical and administrative security mechanisms of the security domain, and the hardware-based resources (e.g., registers, memory, disks) that are in use when the element is serving a particular user (or system function). That is, a security context encompasses all element resources and security mechanisms that support the activity of a user operating in a security domain. The kernel is responsible for maintaining all the information needed to isolate one security context from another. When the element ceases performing operations in one security context and begins performing operations in another security context, no information can be allowed to pass from one security context to the other unless a specific request is made and it is allowable under the security policies of the security domains involved.

Examples of information that element security-critical functions (including the kernel) must maintain to support the operation and isolation of security contexts include:

- A unique identification for each security context
- The identification of the security domain being supported
- Hardware register values related to control of element resources, including virtual memory and all devices in or attached to the element
- The authenticated identity of the user being served
- The users security attributes (permissions)
- Data structures needed to operate security-related functions and other untrusted system applications.

Each security context supports a user (or a system function) operating in a particular security domain. Over a period of time, an element may maintain several security contexts to support one or more users operating in one or more security domains. A particular user might use (simultaneously or serially) security contexts operating in the same or different security domains. Different users may employ security contexts operating in the same or different security domains.

Since security contexts are isolated from one another by the kernel, communications among security contexts (requests for service or information transfer) in an element can only take place in accordance with the security policies of the security domains supported by the security contexts. If the security policies of the supported security domains do not explicitly permit inter-security domain transfer, the SPDF will necessarily deny the request and the kernel will enforce that decision. Since a security domain contains the information of a particular user community, it would be unusual for a security domain security policy to prohibit information sharing between two security contexts supporting the same security domain.

Many element activities are not carried out on behalf of a specific user (either an individual or the entire membership of a security domain as a group), but rather for basic element operation and management. Examples of such activities include many of the security-critical system functions and element management activities. These activities are carried out within element security contexts on behalf of one or more of the security domains supported by the element. The security policies of these element security domains are created to exercise appropriate control of element resources for all of the user security domains supported by the element. Some example uses of element security domains include the control and manipulation of login applications, and management security domains.

Before a security context can be created for the activities of a user in a particular security domain, the system must be informed which security domain is to be used. Ordinarily, the user's identity is obtained and authenticated to determine if the user is a member of the requested security domain. One way of performing this startup function is to create a login security context that represents one of the element security domains. The activities allowed in the login security context are limited to authenticating the user identity and starting a security context for the requested security domain (there might be a default security domain for a user recorded in the element security management information base).

One useful resource control concept is role enforcement; only users filling a specified "role" are authorized to initiate a particular function. In turn, the functions that are allowed to invoke other functions can be controlled by careful specification of role types. It is possible to impose a particular implementation of role enforcement by making specific security-critical roles members

of particular element security subdomains. Thus, only member functions of an element security subdomain could invoke specific executable element functions.

A consequence of the strict isolation aspects of the element architecture is that many aspects of covert channels, both timing and storage, either cease to be concerns or are easily controlled. Possible storage channels are reduced to those between security contexts. If security domain/subdomain policies are properly stated and the security policy, strict isolation, and interprocess communications functions are performing properly, there will be no covert storage channels available. To exploit timing channels between security contexts requires that a complete security context list is available so that a user can determine which security contexts (including element security contexts) are in operation. Such information is part of one or more management security domains. It is not likely, and certainly not necessary, that an arbitrary user would be able to access such information. Even for those security contexts in which management information is available to its users, timing information for other security contexts should not be made available to those users.

5.4.1.2.3 Security-Critical Functions

The security-critical functions described in this section implement the various security services allocated to the element and several additional supporting services.

Security Policy Decision Function (SPDF)

The separation of security mechanisms from security policy enforcement and decisions is crucial to the flexibility of the element security architecture. The SPDF is responsible for making all security policy decisions. The primary role of the SPDF is to isolate the rest of the element software from knowledge of security policies. The importance of this approach is threefold.

1. First, the support of multiple security domains with different policies is accomplished easily because the security policies are represented in only one place and are interpreted by only one function. In many current secure system designs, it is difficult to point to the actual software code that implements the single security policy of those systems because it is embedded and scattered throughout code that performs multiple functions.
2. Second, by keeping security policy representations in one place, it is relatively easy to install, modify, or even replace the security policy for a security domain. It is not necessary to rewrite trusted software that implements the security policy. Rather, the rules that the SPDF interprets for a security domain are updated or replaced.
3. Third, changing the implementation of the SPDF would be transparent to the operation of the remainder of the element software. Any correct implementation of the SPDF is acceptable, but it may be useful to standardize the representation of security attributes and security policy rules.

The SPDF approach will allow security-critical functions to be implemented independently of particular security policies. There is the potential in this approach that a computer vendor could support its entire customer base within a single element software design. To illustrate this concept, consider an example of three enterprises with different, or even conflicting, security policies. The first is a DoD organization using a conventional DoD security policy. The second is a corporation with requirements for data integrity and data separation based solely on need-to-know authorization. The third is a university research laboratory that does not have any special security needs except a basic privacy-based access control policy. Without a policy-

independent architecture, these three differing security policies would result in three different OS implementations that could cause serious compatibility problems for a vendor trying to support all three environments. Using the SPDF approach, any or all of the three policies could be supported by the same element software. If necessary, the three enterprises could be served by the same element or (using the network subsystem) they could share information as necessary across different elements.

5.4.1.2.3.1 Authentication Function

The authentication function invokes one or more mechanisms used by an element to identify and authenticate users (and to authenticate an element to users), and for elements to authenticate one another in a distributed environment. A common interface to the authentication function is used that is independent of the any security domain security policy or the authentication mechanisms employed. That is, the authentication function is the service interface to the mechanisms used to identify and authenticate users and elements. The exact mechanisms selected will depend on the security domain policies in effect. An element supporting multiple security domain policies may need to implement more than one authentication mechanism.

An authenticated user identity may be passed between information systems rather than the information used to authenticate that identity. That is, an element supporting a particular security domain would be expected to accept that the authentication function has been performed reliably and correctly by other elements supporting that security domain. In some cases, it may be necessary to pass information about the authentication mechanisms used to validate the user identity. The network subsystem is expected to protect the authenticated user identity as it is passed between security domains.

5.4.1.2.3.2 Audit Function

The audit function accepts audit messages from functions in the element in accord with security domain and management security domain security policies. Audit records may become part of the security management information that is part of an information management domain (for one or more security domains or element domains). Audit records may be directed to multiple repositories. In some cases, the audit information may best be used by an individual user (for example, time and method of most recent element or security domain use). The audit function guarantees that audit messages cannot be lost and that the ordering of messages is preserved. As part of a distributed audit system, audit functions can forward the audit data they collect to a base-level, regional, or central audit center to alleviate local audit data storage requirements and to coordinate audit information from different elements or security domains. Audit data should be protected from unauthorized access or modification. Audit data from different network elements should have uniform timestamps, the same level of detail in content and the same format to be most useful in recreating events after the fact.

5.4.1.2.3.3 Process Scheduling Function

In OSs that share the element processor among multiple processes, the process scheduling function determines which of the processes next uses the processor (or processors in a multiprocessor element) and for how long. The process scheduling function is included among the security-critical functions so that no process can deny the processor to other processes either purposefully or inadvertently.

5.4.1.2.3.4 Device Management Functions and Device Controllers

The remainder of the security-critical functions are each responsible for a particular class of element resources described below. These resources include memory, storage devices, display systems, interprocess communications, cryptographic services, and any other input/output devices controlled by the element.

- The memory management function is responsible for controlling the use of memory by all software, including security-critical functions. It maintains memory-mapping information and controls the hardware functions that perform memory mapping.
- The file management function is responsible for controlling the use of storage media devices. Like the memory management function, it maintains disk-mapping (or other media-specific) information that provides basic virtualizations of the actual storage media. Other software (e.g., database programs) may build upon these virtualizations to provide even more abstract file structures to applications and users.
- The display management function is responsible for controlling the use of display devices (including screens and printers), keyboard devices, and pointing devices (e.g., trackballs, mice). The display management function provides basic display device operations. Because a single display device may be used to present information from multiple domains at the same time (typically through multiple windows or on paper), the display management function maintains information that associates particular information to be displayed with the appropriate security context. Other software (e.g., an X Window System implementation) may provide requests to the display management function to achieve a particular display format.
- The interprocess communications management function is responsible for controlling the interprocess communications mechanisms (e.g., locks, semaphores, messages) used by all software processes in the element. In particular, inter-context (e.g., inter-security domain) transfers are carried out through this function.
- The cryptographic services management function is responsible for controlling all of the cryptographically based security mechanisms in an element. The security services it may support include confidentiality, data integrity, data origin authentication, and non-repudiation. The cryptographic management function may control a number of alternative cryptographic mechanisms to support different services and to provide different levels of protection that satisfy different security policies. The choice of mechanism may be based on many factors including the sensitivity of the data being protected, the security service requested, and the mechanisms available on other elements for data that will be transferred.
- Each of the physical devices in the element, including memory, disks and other storage devices, displays, cryptographic engines, specific user authentication devices, and communications interface controllers, has a corresponding software program that controls and passes information to and from it. These software programs collectively are called device drivers. Every device driver should be considered security critical because this software ultimately determines how a device operates. Although device drivers in older element platforms were often quite large and complex, many contemporary devices contain much of the former device driver function in the device logic or in their own programs. Thus, many device drivers are now reasonably straightforward and follow well-

known paradigms, which make their evaluation easier, although great reliance is placed on the correct implementation of the device.

5.4.1.2.4 Security-Related Functions

Some software functions within the element are required to manage information or to provide an interface to the security-critical functions, but are not critical to system security. Of particular interest here are residual OS functions, security management functions, and networking subsystem functions.

5.4.1.2.4.1 Operating System (OS) Structure

Most of the security-critical functions are part of traditional OS structures. Many other OS components are not included in the security-critical functions, such as the user interface, utility functions, and high-level abstractions of information. These functions are present in varying forms in all traditional OSs. The user interface, the particular utility functions, and the information abstractions provided characterize a particular OS. That is, they distinguish one OS from another even though they provide essentially the same services to a user. Because the security-critical functions provide commonly used, low-level services, many different OSs can be implemented using them. Figure 12 is an abstract illustration of the software supporting a single security context.

Since security contexts are separated from one another, each can rely upon a different OS structure. Thus, a single element can support different OS environments concurrently. Applications that were written to operate with a particular OS should not require change unless they were allowed to directly manipulate basic OS functions now controlled by security-critical functions.

Existing OS implementations will need to be modified to use the common kernel interface and the services provided by the security-critical functions. The degree of difficulty in making these modifications will be reduced if the original OS implementation was

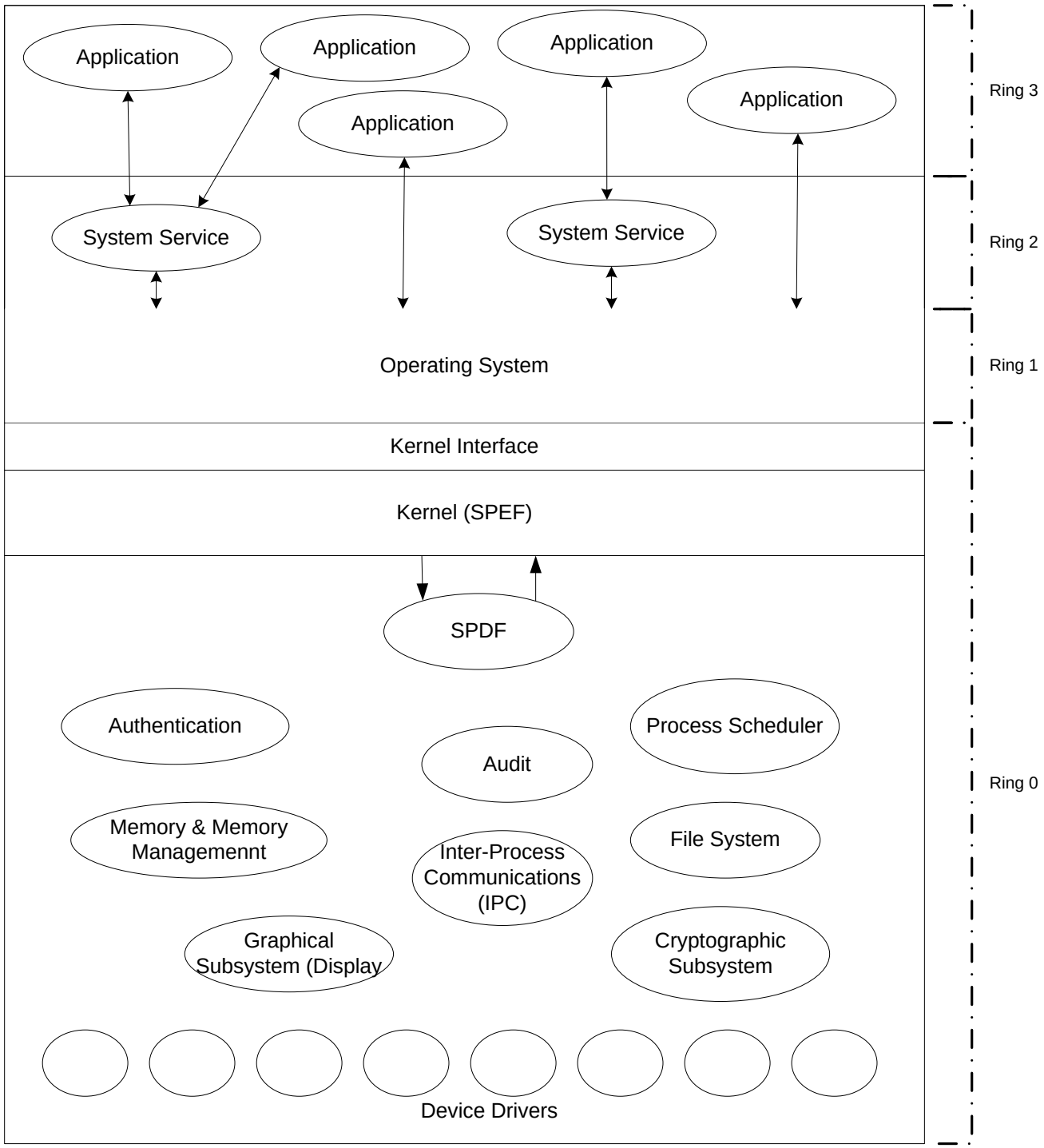

Figure 12- Security Context Software Component Relationships

well structured and modular. Some existing secure OS implementations will adapt relatively easily to the use of the common kernel interface, and many of the security-critical functions will already be present.

OS implementations structured to use the common kernel interface to obtain basic services should be able to be closely controlled from an authorization perspective relatively easily since most hardware dependencies will be visible only in the kernel and the device drivers.

5.4.1.2.4.2 Security Management Function

The primary role of the security management function is to control information needed by security-critical and security-related functions within the element security architecture. Security management is a particular instance of general management functions. Examples of the information manipulated by the security management function include security domain security policy rules used by the SPDF, configuration parameters for security mechanisms (e.g., cryptographic algorithms), configuration parameters for cryptographic mechanisms and element devices, and audit information. Some information is managed for specific security domains and some is managed for elements or security domains. Details on security management are contained in Section 5.5.

5.4.1.2.4.3 Networking Subsystem Function

The networking subsystem is defined in accordance with ITU-T X.200 and X.800. Communications applications and communications protocols used to communicate with other elements are implemented as untrusted applications within the element security architecture. These applications make requests for security services (which process information and generate protocol information) that provide required protection. For information to be transferred between elements and within a security domain, a distributed security context is established through the use of security management and transfer system applications, and security-critical functions.

5.4.1.3 Security Mechanisms for TSP Deployed Operating Systems (OSs)

The allocation of security services within a TSP security domain requires specific mechanisms to support those services. Physical (as in physical access controls, fire suppression, video surveillance, etc.) and administrative security mechanisms (as in security guards, personnel screening, security policies, etc.) are the first lines of defense used to achieve TSP security objectives. Other areas and mechanisms to support the necessary security services are allocated TSP deployed hardware and software, especially the OS used to control hardware operation and application software functionality. TSPs frequently deploy many different types of OSs which fall into four basic categories:

- General Purpose OSs (Type 1)
- Minimized General Purpose Operating Systems (Type 2)
- Embedded ("real-time") Operating Systems (Type 3) and
- Basic Input/Output Systems (BIOSs) (Type 4)

as previously noted in Section 5.4.1.1. The capabilities of the hardware platforms upon which these types of OS reside frequently differ in capabilities, including processor execution rates, quantity and types of storage (as in dynamic memory, static memory, non-volatile memory/storage), and many other built-in capabilities. Thus a discussion of Element OS security shall include coverage of available hardware mechanisms that are either necessary to, or augment, OS security mechanism availability and capabilities.

5.4.1.3.1 General Purpose (GP) OSs (Type 1)

Herein are discussed those security mechanisms potentially present within GP OSs and the hardware upon which these OSs typically reside. The types of TSP elements using General Purpose OSs are frequently used for Application Servers for: file sharing services, Web services, Email services, Instant Messaging services, Gaming services, Infrastructure management, Voice over IP services, Video services as in IPTV and IPG, as well as DNS, DBMS, Authentication services, etc.

5.4.1.3.1.1 Hardware Mechanisms for GP OS Usage

Technologies that are implemented in element hardware have a direct effect on satisfying those security services necessary to achieve TSP security objectives. The allocation of security services to the hardware requires specific mechanisms to support those services. Major hardware areas and mechanisms that impact/support OS security services and mechanisms are listed below in Table 23:

Table 23 - - Desirable GP OS Platform Hardware Security Related Mechanisms

Area and Mechanism	Computer Hardware Based Security Services				
	Availability	Strict Isolation - Access Control	Integrity	Confidentiality	Authentication
Fault Tolerance					
• Common H/W Redundancy	Supports		Supports		
• Circuit Card Redundancy	Supports		Supports		
• Full H/W Redundancy	Supports		Supports		
Fault Detection					
• ECC Memory	Supports		Supports		
• Parity Memory			Supports		
Memory Management					
• Virtual Memory	Supports	Supports		Supports	
• Separate Process Spaces	Supports	Supports	Supports	Supports	
Protected Mode/Multistate Processors					
• 4 Integrity Levels/States	Supports	Supports	Supports	Supports	
• 3 Integrity Levels/States	Supports				
• 1 or 2 Integrity Levels/States					
Encryption Support					
• Cryptographic H/W Engine(s)				Supports	Supports
• Hardware Key Storage Unit		Supports		Supports	Supports
• Smartcard Reader/Port		Supports	Supports	Supports	Supports
• Biometric Reader/Port		Supports	Supports		Supports
Management Interface (I/F)					
• Multiple Network I/Fs	Supports	Supports	Supports		
• Serial I/Fs		Supports	Supports	Supports	
Removable Media					
• H/W Disablement of Booting	Supports	Supports	Supports		Supports
• H/W Authentication at mount	Supports	Supports	Supports		Supports
Basic I/O System (BIOS)					
• H/W Authentication to access	Supports	Supports	Supports	Supports	Supports
Chassis & Front Panel					
• H/W detection of chassis open	Supports	Supports	Supports	Supports	Supports
• H/W detection of Panel access	Supports	Supports	Supports	Supports	Supports

Each of the above identified hardware mechanisms are further described and discussed below in Table 24:

Table 24 - Hardware Mechanism Descriptions

Area and Mechanism	Description
Fault Tolerance	-
• Common H/W Redundancy	This type of redundancy typically covers, but is not limited to, power supplies, fans/fan units, and rotating storage like redundant disks (as in RAID subsystems)
• Circuit Card Redundancy	This type of redundancy addresses forms of redundancy for circuit cards and packs including "hot-plugin/removal" and sparing which includes: "1-for-1" substitution, "1-for-n" substitution.
• Full H/W Redundancy	This type of redundancy typically involves complete "1-for-1" replication of all critical hardware components with some form of hardware based fault detection and automatic failover to "hot-standby" spare components.
Fault Detection	-
• ECC (Error Correcting Code) Memory	This type of fault detection allows the element dynamic/static memory subsystem to recognize when single, or multi-bit errors occur within units of physical memory and actually "correct", or recover, the information that has been stored, or written into, a memory unit that has a failed storage bit.
• Parity Memory	This type of fault detection allows the element dynamic/static memory subsystem to recognize when single, or multi-bit errors occur within units of physical memory. However this mechanism does NOT actually "correct", or recover, the information that has been stored, or written into, a memory unit that has a failed storage bit.
Memory Management	-
• Virtual Memory	This type of memory management provides a mapping of physical memory to multiple logical memory address spaces allowing software to not have to consider physical memory limitations or non-available memory constraints.
• Separate Process Spaces	This type of memory management constrains application and service software components into discrete logical memory address (process) spaces and controls access across logical memory spaces thereby preventing software within one process space from interfering with of modifying other process spaces.
Protected Mode / Multistate Processors	-
• 4 Integrity Levels/States	This type of Protected Mode / Multistate Processor fully allows the software to be structured according to different integrity levels, as discussed in Section 5.4.1.2 and depicted in Figure 12, thereby facilitating availability, strict isolation - access control and integrity.
• 3 Integrity Levels/States	This type of Protected Mode / Multistate Processor only partially allows the software to be structured according to different integrity levels and only assists with facilitating availability. This processor design typically forces non-kernel OS and Service software functions to reside within the same level/ring thereby allowing a successful security breach within a service to likely negatively affect the OS functions residing with the same level/ring.

Area and Mechanism	Description
• 1 or 2 Integrity Levels/States	These types of Protected Mode / Multistate Processor minimally, if at all, allow the software to be structured according to different integrity levels and does not assist with facilitating any software security mechanism deployments. These processor designs typically forces Kernel, non-kernel OS and Service software functions to reside within the same level/ring thereby allowing a successful security breach within a service to likely negatively affect all service, OS and kernel functions residing with the same level/ring.
Encryption Support	-
• Cryptographic H/W Engine(s)	This type of encryption support provides hardware dedicated to processing symmetric and/or asymmetric cryptographic algorithms thereby reducing the time required to perform encryption and decryption activities, as compared to software implemented encryption/decryption functions, under control of the OS Kernel, or less desirably controlled by a non-kernel OS function.
• Hardware Key Storage Unit	This type of encryption support provides hardware dedicated to cryptographic symmetric and asymmetric key and digital certificate storage under control of the OS Kernel, or less desirably controlled by a non-kernel OS function.
• Smartcard Reader/Port	This type of encryption support allows use of Smartcards that include on-board cryptographic processing logic and cryptographic asymmetric key and digital certificate storage under control of the OS Kernel, or less desirably controlled by a non-kernel OS function.
• Biometric Reader/Port	This type of encryption support allows entry of human biometric information under control of the OS Kernel, or less desirably controlled by a non-kernel OS function as part of OS authentication of user attempting to locally access the element.
Management Interface (I/F)	-
• Multiple Network I/Fs	Network interfaces, separate from those used for non-management functions, support isolation and integrity of management activities from non-management activities. The number available for element management impacts availability of remote manageability. With only one interface available, any network disruption may prevent remote management access
• Serial I/Fs	Element management over a serial link is intrinsically isolated from non-management activities. However this approach does not necessarily improve availability and integrity as independent network management interfaces do.
Removable Media	-
• H/W Disablement of Booting	This control over removable media is vital to preventing the element from being booted from said media without authorization. Hardware control is not as easily bypassed as software control.
• H/W Authentication at mount	This control over removable media is very useful in preventing unauthorized installation of software onto the element or un-authorization transfer of information from the element. Hardware control is not as easily bypassed as software control.
Basic I/O System (BIOS)	-
• H/W Authentication to access	This control is critical in preventing un-authorized access to the ROMed BIOS of the element used to define/configure basic hardware components. However great care must be exercised over what is used as the BIOS access password, where and how it is stored/located and who has access to it.
Chassis & Front Panel	-

Area and Mechanism	Description
• H/W detection of chassis open	This mechanism is vital in detecting access into the element chassis, cabinet or enclosure <shelf>. The detection mechanism should trigger an alarm either locally and/or remotely. When correlated with authorized maintenance activities allows the TSP to detect unauthorized access.
• H/W detection of Panel access	This mechanism is vital in detecting access to any switches or controls located on the element's front, or maintenance panel when the panel is located behind an access door. The detection mechanism should trigger an alarm either locally and/or remotely. When correlated with authorized maintenance activities allows the TSP to detect unauthorized access.

5.4.1.3.1.2 Software Functional Entities for General Purpose (GP) OS Contexts

The allocation of security services and other security-critical functions to the software requires specific mechanisms to support those services**.** Within the context of elements that use a GP OS, some areas and mechanisms fo**r** necessary security services are listed in Table 25. The Ring 0 Kernel functions are all Security-critical functions and provide the foundation for authentication, confidentiality, integrity, access control and non-repudiation with the element. These functions are the fundamental element Security policy decision functions and Security policy enforcement functions. The Ring 1 Non-kernel OS functions are all Security-relevant functions and rely on the Ring 0 Security policy decision and Security policy enforcement functions. The Ring 2 Service Functions are essentially Trusted applications that rely on the integrity of Ring 1 and Ring 0 functions.

Table 25 - GP OS Context Security Related Software Functions

Functional Entity	Security Service									
	Entity Authentication	User Authentication	Process Authentication	Access Control	Confidentiality	Information Integrity	Data Integrity	Availability	Strict Isolation	Non-Repudiation
Ring 0 Kernel Functions										
• Interprocess communications				Yes					Yes	
• Authentication	Yes	Yes	Yes							
• Access Mediation				Yes		Yes	Yes		Yes	
• Cryptographic Subsystem	Yes	Yes	Yes		Yes	Yes	Yes			
• Process Scheduling				Yes				Yes	Yes	
• Auditing - Logging				Yes	Yes	Yes	Yes	Yes		Yes
Ring 1 Non-kernel OS Functions										
• File Systems				Yes	Yes	Yes	Yes	Yes	Yes	
• Command Interpreters				Yes	Yes					
• Network Subsystem	Yes	Yes	Yes	Yes	Yes		Yes	Yes		
• Remote Procedures										
• Anti-Virus Detection					Yes	Yes	Yes	Yes		
• Packet Filtering				Yes		Yes	Yes	Yes	Yes	
• Graphical Subsystem and X-Windows Servers		Yes		Yes	Yes					
• Element Management & Administration	Yes	Yes		Yes	Yes	Yes	Yes	Yes		Yes
• OS Login Process		Yes		Yes	Yes				Yes	
Ring 2 Service Functions										
• File Sharing Servers (nfs, samba/smb)	Yes		Yes	Yes			Yes	Yes	Yes	Yes
• DBMS Servers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
• Windows/Desktop Managers	Yes	Yes	Yes	Yes			Yes			Yes
• Application Frameworks (DCE, Corba, Java, .NET)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ring 3 Application Functions										
• File Transfer Servers	Yes	Yes		Yes		Yes	Yes		Yes	Yes
• Web Servers	Yes	Yes		Yes		Yes	Yes		Yes	Yes
• Email Servers	Yes	Yes		Yes	Yes		Yes		Yes	
• Voice over IP (VoIP) Servers (Proxies, Registrars, MGCs, MGs, etc.)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
• Domain Name Servers	Yes						Yes	Yes		Yes
• Other Application Servers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
• Other Application Clients	Yes	Yes		Yes	Yes	Yes	Yes			Yes

Each of the above identified software mechanisms are further described and discussed below in Table 26.

Table 26 - GP OS Context Security Related Software Functions

Functional Entity	Description
Ring 0 Kernel Functions	-
• Interprocess communications	This function provides the ability for one process context to pass or share information with other process contexts. As such, this function should rely on the Kernel Access Mediation function to decide if such inter-process communication is allowed.
• Authentication	This function is responsible for the storage, retrieval and processing of basic information/credentials (such as user passwords, private keys, digital certificates, public keys) used to authenticate asserted identities of other infrastructure elements, element users and processes within the element. This function should rely on the Kernel Cryptographic Subsystem function for the actual cryptographic processing associated with public keys, private keys, secret keys and digital certificates, as well as the encryption/decryption of any stored passwords. The behavior of this function should be governed by a set of security domain authentication policy rules contained in the Element SMIB (see Section 5.5.4.2)
• Access Mediation (a.k.a. Reference Monitor)	This function is responsible for deciding if requested access by a subject (whether user, process or other element) is allowed or should be denied. As such, this function relies on the Kernel Authentication function to validate asserted identities of subjects prior to this function approving or denying the access request. The behavior of this function should be governed by a set of security domain authorization policy rules contained in the Element SMIB (see Section 5.5.4.2) in conjunction with subject or role access rights mapped against object access privileges.
• Cryptographic Subsystem	This function provides the basic capabilities to cryptographically process information (both encryption and decryption) via a suite of cryptographic algorithms that may be implemented in hardware or software. This function should support irreversible (as in keyed hashs) and reversible algorithms (both symmetric and asymmetric). The behavior of this function should be governed by a set of security domain cryptographic policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Process Scheduling	This function provides the ability for sequencing which process context will next be granted control of the element cpu(s) for the execution of process machine instructions. As such, this function should rely on the Kernel Access Mediation function to decide if such process context instruction execution is allowed and for how long relative to process context priorities and policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Auditing - Logging	This function provides the basic logging capabilities for adding log entries to the Element system and security log files, as well as the generation of alarm events which should be passed to the Ring 1 Element Management & Administration function . As such, this function should rely on the Kernel Access Mediation function to control access to said log files. The behavior of this function should be governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
•	
Ring 1 Non-kernel OS Functions	-
• File Systems	These functions provide other Ring 1, 2 and 3 functions the ability to store and retrieve information on/from both element associated fixed and removable media. As such, this function should rely on the Kernel Access Mediation function to decide if such media access is allowed governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).

Functional Entity	Description
• Command Interpreters	These functions provide process contexts the ability to invoke Ring 1 OS functions, Ring 2 services and Ring 3 application programs. As such, this function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if such media access is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Network Subsystem	This function provides Ring 1 OS functions, Ring 2 services and Ring 3 application programs the ability to communicate with other elements using network protocol communications. As such, this function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if network protocol communication is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Remote Procedures	These functions provide Ring 1 OS functions, Ring 2 services and Ring 3 application programs the ability to invoke Ring 1 OS functions, Ring 2 services and Ring 3 application programs resident on other elements using network protocol communications. As such, this function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if remote procedure invocation is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Anti-Virus Detection	This function provides the capability to inspect data within the element for the presence of various forms of "malware" such as viruses, worms, Trojans and spyware based on rules contained in the Element SMIB (see Section 5.5.4.2). This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to data, including malware signatures, within the element is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Packet Filtering	This function provides the capability to inspect data entering into or leaving the element via a network communications interface and determine if said data is to be dropped or passed on based on filtering rules contained in the Element SMIB (see Section 5.5.4.2). This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to the packet filtering rules is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Graphical Subsystem and X-Windows Servers	This function provides Ring 1 OS functions, Ring 2 services and Ring 3 application programs the ability to receive input from and supply output to the data entry and display components of Element. This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to the Element graphical subsystem components is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Element Management & Administration	This function is responsible for the administration and management of all other functions within the Element (see Section 5.5.4 for a description of Element Security Management & Administration). This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to the Element graphical subsystem components is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• OS Login Process	This function is responsible for interacting with those local or remote users who want to interact with the element via the Element Graphical Subsystem or the Element Network Subsystem. This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to the Element is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
Ring 2 Service Functions	**-**

Functional Entity	Description
• File Sharing Servers (nfs, samba/smb)	These functions receive from and deliver to Ring 2 Service and Ring 3 Application Functions data to/from an Element File System. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to File System directories and files is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• DBMS Servers	These functions receive from and deliver to Ring 2 Service and Ring 3 Application Functions data to/from the DBMS. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to DBMS data structures is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Windows/Desktop Managers	These functions provide Element users the ability to control the 'look' and 'feel' of the graphical interface provide to the user over the Element Graphical Subsystem. This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to the Windows/Desktop Manager configuration components is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Application Frameworks (DCE, Corba, Java, .NET)	These functions provide application developers the ability to distribute parts on a Ring 2 Service or Ring 3 Application function over multiple Elements where the Application Framework provides communication amongst, and other general functionality to, the distributed components of the Service or Application. These functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to, or amongst, distributed Service and Application components is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
Ring 3 Application Functions	-
• File Transfer Servers	These functions present web content to, and interact with, Ring 3 web clients (application programs). As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if web based interaction with requesting clients is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Web Servers	These functions present web content to, and interact with, Ring 3 web clients (application programs). As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if web based interaction with requesting clients is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Email Servers	These functions receive from and deliver to Ring 3 mail clients (application programs) electronic messages (Email). As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to Email accounts is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Voice over IP (VoIP) Servers (Proxies, Registrars, MGCs, MGs, Gatekeepers, etc.)	These functions either receive from and deliver to Ring 3 VoIP clients (application programs) VoIP calls or interact amongst themselves to manage and complete VoIP calls. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to each other and to/from VoIP clients is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Domain Name Servers	These functions receive from and deliver to Ring 3 mail clients (application programs) requests for and replies of mappings between IP addresses and FQDNs, as well as other requests for DNS stored information. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to DNS stored information is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).

Functional Entity	Description
• Other Application Servers	These functions receive from and deliver to Ring 3 mail clients (application programs) many types of requests associated with client-server functionality. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to Email accounts is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Free-standing Applications	These functions perform numerous forms of application information processing either upon request from Element users or when invoked by other applications within the Element. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to Email accounts is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).

5.4.1.3.2 Minimized General Purpose Operating Systems (Type 2)

Many TSP elements use a GP OS configured with a minimal set of capabilities, services and functions. This is commonly done so industry can leverage implementations of functions based on standards and open source resources. Herein are discussed those security mechanisms potentially present within Minimized GP OSs and the hardware upon which these OSs typically reside. The types of TSP elements using Minimized GP OSs are frequently used for Application Servers for: file sharing services, Web services, Email services, Instant Messaging services, Gaming services, Infrastructure management, Voice over IP services, Video services as in IPTV and IPG, as well as DNS, DBMS, Authentication services, etc.

5.4.1.3.2.1 Hardware Mechanisms for Minimized GP OS Usage

Technologies that are implemented in element hardware have a direct effect on satisfying those security services necessary to achieve TSP security objectives. The allocation of security services to the hardware requires specific mechanisms to support those services. The major hardware areas and mechanisms that impact/support OS security services and mechanisms are the same as listed and discussed in Section 5.4.1.3.1.1 above.

5.4.1.3.2.2 Software Mechanisms for Minimized GP OS Usage

The allocation of security services and other security-critical functions to the software requires specific mechanisms to support those services**.** Within the context of Elements that use a Minimized GP OS, the areas and mechanisms fo**r** necessary security services are the same as for non-Minimized GP OSs discussed in Section 5.4.1.3.1.2 above. The Ring 0 Kernel functions are all Security-critical functions and provide the foundation for authentication, confidentiality, integrity, access control and non-repudiation with the Element. These functions are the fundamental Element Security policy decision functions and Security policy enforcement functions. The Ring 1 Non-kernel OS functions are all Security-relevant functions and rely on the Ring 0 Security policy decision and Security policy enforcement functions. The Ring 2 Service Functions are essentially Trusted applications that rely on the integrity of Ring 1 and Ring 0 functions.

5.4.1.3.3 Embedded ("real-time") Operating Systems (Type 3)

Many TSP elements use an Embedded, a.k.a. real-time, OS that differs from (Minimized-) GP OSs in a number of crucial ways. Embedded OSs typically do not:

- provide virtual memory capabilities,
- support multiple process spaces, or

- provide time-slicing (scheduling) between application processes.

This approach is commonly used when functions must be performed within very tight timeframes. Herein are discussed those security mechanisms potentially present within Embedded OSs and the hardware upon which these OSs typically reside. The types of TSP elements using Embedded OSs are frequently used for translation between different communications types such as Media Gateways, Media Gateway Controllers, Switches, Multiplexers, routers, etc.

5.4.1.3.3.1 Hardware Mechanisms for Embedded OS Usage

Technologies that are implemented in element hardware have a direct effect on satisfying those security services necessary to achieve TSP security objectives. The allocation of security services to the hardware requires specific mechanisms to support those services. Major hardware areas and mechanisms that impact/support OS security services and mechanisms are listed below in Table 27.

Table 27 - Desirable Embedded OS Platform Hardware Security Related Mechanisms

Area and Mechanism	Computer Hardware Based Security Services				
	Availability	Strict Isolation - Access Control	Integrity	Confidentiality	Authentication
Fault Tolerance					
• Common H/W Redundancy	Supports		Supports		
• Circuit Card Redundancy	Supports		Supports		
• Full H/W Redundancy	Supports		Supports		
Fault Detection					
• ECC Memory	Supports		Supports		
• Parity Memory			Supports		
Encryption Support					
• Cryptographic H/W Engine(s)				Supports	Supports
• Hardware Key Storage Unit		Supports		Supports	Supports
• Smartcard Reader/Port		Supports	Supports	Supports	Supports
• Biometric Reader/Port		Supports	Supports		Supports
Management Interface (I/F)					
• Multiple Network I/Fs	Supports	Supports	Supports		
• Serial I/Fs		Supports	Supports	Supports	
Removable Media					
• H/W Disablement of Booting	Supports	Supports	Supports		Supports
• H/W Authentication at mount	Supports	Supports	Supports		Supports
Basic I/O System (BIOS)					
• H/W Authentication to access	Supports	Supports	Supports	Supports	Supports
Chassis & Front Panel					
• H/W detection of chassis open	Supports	Supports	Supports	Supports	Supports
• H/W detection of Panel access	Supports	Supports	Supports	Supports	Supports

Each of the above identified hardware mechanisms is as described and discussed in Section 5.4.1.3.1.1 above. Even though Embedded OSs typically use the same hardware as General Purpose OSs use, Embedded OSs will not utilize all the capabilities available and used by General Purpose OSs.

5.4.1.3.3.2 Software Mechanisms for Embedded OS Usage

The allocation of security services and other security-critical functions to the software requires specific mechanisms to support those services**.** Within the context of Elements that use an Embedded OS, some areas and mechanisms fo**r** necessary security services are listed in Table 28. Embedded OSs do not follow the ring structure as these OSs are implemented as a single "load image", or file, that includes all Kernel, non-kernel OS, Server and Application functionality. Consequently all Security-critical functions, Security policy decision functions, Security policy enforcement functions, Security-relevant functions and Trusted applications co-exist within a common binary/executable file.

Table 28 - Embedded OS Context Security Related Software Functions

Functional Entity	Security Service									
	Entity Authentication	User Authentication	Process Authentication	Access Control	Confidentiality	Information Integrity	Data Integrity	Availability	Strict Isolation	Non-Repudiation
• Authentication	Yes	Yes	Yes							
• Access Mediation				Yes		Yes	Yes		Yes	
• Cryptographic Subsystem	Yes	Yes	Yes		Yes	Yes	Yes			
• Auditing - Logging				Yes	Yes	Yes	Yes	Yes		Yes
• File Systems				Yes	Yes	Yes	Yes	Yes	Yes	
• Command Interpreters				Yes	Yes					
• Network Subsystem	Yes	Yes	Yes	Yes	Yes		Yes	Yes		
• Remote Procedures										
• Packet Filtering				Yes		Yes	Yes	Yes	Yes	
• Graphical Subsystem and X-Windows Servers		Yes		Yes	Yes					
• Element Management & Administration	Yes	Yes		Yes	Yes	Yes	Yes	Yes		Yes
• File Sharing Servers (nfs, samba/smb)	Yes		Yes	Yes			Yes	Yes	Yes	Yes
• File Transfer Servers	Yes	Yes		Yes		Yes	Yes		Yes	Yes
• Web Servers	Yes	Yes		Yes		Yes	Yes		Yes	Yes
• Voice over IP (VoIP) Servers (MGCs, MGs, etc.)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
• Other Application Servers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Each of the above identified software mechanisms are further described and discussed below in Table 29.

Table 29 - Embedded OS Context Security Related Software Functions

Functional Entity	Description
• Authentication	This function is responsible for the storage, retrieval and processing of basic information/credentials (such as user passwords, private keys, digital certificates, public keys) used to authenticate asserted identities of other infrastructure elements, element users and processes within the element. This function should rely on the Kernel Cryptographic Subsystem function for the actual cryptographic processing associated with public keys, private keys, secret keys and digital certificates, as well as the encryption/decryption of any stored passwords. The behavior of this function should be governed by a set of security domain authentication policy rules contained in the Element SMIB (see Section 5.5.4.2)
• Access Mediation (a.k.a. Reference Monitor)	This function is responsible for deciding if requested access by a subject (whether user, process or other element) is allowed or should be denied. As such, this function relies on the Kernel Authentication function to validate asserted identities of subjects prior to this function approving or denying the access request. The behavior of this function should be governed by a set of security domain authorization policy rules contained in the Element SMIB (see Section 5.5.4.2) in conjunction with subject or role access rights mapped against object access privileges.
• Cryptographic Subsystem	This function provides the basic capabilities to cryptographically process information (both encryption and decryption) via a suite of cryptographic algorithms that may be implemented in hardware or software. This function should support irreversible (as in keyed hashs) and reversible algorithms (both symmetric and asymmetric). The behavior of this function should be governed by a set of security domain cryptographic policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Auditing - Logging	This function provides the basic logging capabilities for adding log entries to the Element system and security log files, as well as the generation of alarm events which should be passed to the Element Management & Administration function . As such, this function should rely on the Kernel Access Mediation function to control access to said log files. The behavior of this function should be governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• File Systems	These functions provide other functions the ability to store and retrieve information on/from both element associated fixed and removable media. As such, this function should rely on the Kernel Access Mediation function to decide if such media access is allowed governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Command Interpreters	These functions provide process contexts the ability to invoke OS, services and application functions. As such, this function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if such media access is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Network Subsystem	This function provides OS, services and application functions the ability to communicate with other elements using network protocol communications. As such, this function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if network protocol communication is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).

Functional Entity	Description
• Remote Procedures	These functions provide OS, services and application functions the ability to invoke OS, services and application functions resident on other elements using network protocol communications. As such, this function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if remote procedure invocation is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Packet Filtering	This function provides the capability to inspect data entering into or leaving the element via a network communications interface and determine if said data is to be dropped or passed on based on filtering rules contained in the Element SMIB (see Section 5.5.4.2). This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to the packet filtering rules is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Graphical Subsystem and X-Windows Servers	This function provides OS, services and application functions the ability to receive input from and supply output to the data entry and display components of Element. This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to the Element graphical subsystem components is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Element Management & Administration	This function is responsible for the administration and management of all other functions within the Element (see Section 5.5.4 for a description of Element Security Management & Administration). This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to the Element graphical subsystem components is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• File Sharing Servers (nfs, samba/smb)	These functions receive from and deliver to Service and Application Functions data to/from an Element File System. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to File System directories and files is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• File Transfer Servers	These functions present web content to, and interact with, clients (application programs). As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if web based interaction with requesting clients is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Web Servers	These functions present web content to, and interact with, web clients (application programs). As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if web based interaction with requesting clients is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Voice over IP (VoIP) Servers (MGCs, MGs, Gatekeepers, etc.)	These functions either receive from and deliver to VoIP clients (application programs) VoIP calls or interact amongst themselves to manage and complete VoIP calls. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to each other and to/from VoIP clients is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Other Application Servers	These functions receive from and deliver to clients (application programs) many types of requests associated with client-server functionality. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).

5.4.1.3.4 Basic Input - Output Systems (BIOS) (Type 4)

Many TSP elements use a BIOS that differs from (Minimized-) GP OSs and Embedded OSs in a number of crucial ways. BIOSs typically do not provide:

- any memory management capabilities,
- fault tolerance,
- fault detection,
- removable media,
- multiple process spaces, or
- time-slicing (scheduling) between application processes.

This approach is commonly used when only basic functions must be performed by the element. Herein are discussed those security mechanisms potentially present within BIOSs and the hardware upon which they typically reside. TSP elements using Embedded OSs include, but are not limited to, monitoring probes, intelligent hubs and access points.

5.4.1.3.4.1 Hardware Mechanisms for BIOS Usage

Technologies that are implemented in element hardware have a direct effect on satisfying those security services necessary to achieve TSP security objectives. The allocation of security services to the hardware requires specific mechanisms to support those services. Major hardware areas and mechanisms that impact/support BIOS security services and mechanisms are listed below in Table 30:

Table 30 - Desirable BIOS Platform Hardware Security Related Mechanisms

Area and Mechanism	Computer Hardware Based Security Services				
	Availability	Strict Isolation - Access Control	Integrity	Confidentiality	Authentication
Encryption Support					
• Cryptographic H/W Engine(s)				Supports	Supports
• Hardware Key Storage Unit		Supports		Supports	Supports
• Smartcard Reader/Port		Supports	Supports	Supports	Supports
• Biometric Reader/Port		Supports	Supports		Supports
Management Interface (I/F)					
• Multiple Network I/Fs	Supports	Supports	Supports		
• Serial I/Fs		Supports	Supports	Supports	

Each of the above identified hardware mechanisms are as described and discussed in Section 5.4.1.3.1.1 above.

5.4.1.3.4.2 Software Mechanisms for BIOS Usage

The allocation of security services and other security-critical functions to the software requires specific mechanisms to support those services**.** Within the context of Elements that use a BIOS, some areas and mechanisms fo**r** necessary security services are listed in Table 31. BIOSs do not follow the ring structure as these OSs are frequently structured as a single "load image", or file, that includes all Kernel, non-kernel OS, Server and Application functionality. Consequently all Security-critical functions, Security policy decision functions, Security policy enforcement functions, Security-relevant functions and Trusted applications co-exist within a common binary/executable file.

Table 31 - Embedded OS Context Security Related Software Functions

Functional Entity	Security Service									
	Entity Authentication	User Authentication	Process Authentication	Access Control	Confidentiality	Information Integrity	Data Integrity	Availability	Strict Isolation	Non-Repudiation
• Authentication	Yes	Yes	Yes							
• Access Mediation				Yes		Yes	Yes		Yes	
• Cryptographic Subsystem	Yes	Yes	Yes		Yes	Yes	Yes			
• Auditing - Logging				Yes	Yes	Yes	Yes	Yes		Yes
• File Systems				Yes	Yes	Yes	Yes	Yes	Yes	
• Command Interpreters				Yes	Yes					
• Network Subsystem	Yes	Yes	Yes	Yes	Yes		Yes	Yes		
• Element Management & Administration	Yes	Yes		Yes	Yes	Yes	Yes	Yes		Yes
• File Transfer Servers	Yes	Yes		Yes		Yes	Yes		Yes	Yes
• Web Servers	Yes	Yes		Yes		Yes	Yes		Yes	Yes
• Other Application Servers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Each of the above identified software mechanisms is further described and discussed below in Table 32.

Table 32 - Embedded OS Context Security Related Software Functions

Functional Entity	Description
• Authentication	This function is responsible for the storage, retrieval and processing of basic information/credentials (such as user passwords, private keys, digital certificates, public keys) used to authenticate asserted identities of other infrastructure elements, element users and processes within the element. This function should rely on the Kernel Cryptographic Subsystem function for the actual cryptographic processing associated with public keys, private keys, secret keys and digital certificates, as well as the encryption/decryption of any stored passwords. The behavior of this function should be governed by a set of security domain authentication policy rules contained in the Element SMIB (see Section 5.5.4.2)
• Access Mediation (a.k.a. Reference Monitor)	This function is responsible for deciding if requested access by a subject (whether user, process or other element) is allowed or should be denied. As such, this function relies on the Kernel Authentication function to validate asserted identities of subjects prior to this function approving or denying the access request. The behavior of this function should be governed by a set of security domain authorization policy rules contained in the Element SMIB (see Section 5.5.4.2) in conjunction with subject or role access rights mapped against object access privileges.
• Cryptographic Subsystem	This function provides the basic capabilities to cryptographically process information (both encryption and decryption) via a suite of cryptographic algorithms that may be implemented in hardware or software. This function should support irreversible (as in keyed hashs) and reversible algorithms (both symmetric and asymmetric). The behavior of this function should be governed by a set of security domain cryptographic policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Auditing - Logging	This function provides the basic logging capabilities for adding log entries to the Element system and security log files, as well as the generation of alarm events which should be passed to the Element Management & Administration function . As such, this function should rely on the Kernel Access Mediation function to control access to said log files. The behavior of this function should be governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• File Systems	These functions provide other functions and application programs the ability to store and retrieve information on/from both element associated fixed and removable media. As such, this function should rely on the Kernel Access Mediation function to decide if such media access is allowed governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Command Interpreters	These functions provide process contexts the ability to invoke OS, services and application programs. As such, this function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if such media access is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Network Subsystem	This function provides OS, services and application programs the ability to communicate with other elements using network protocol communications. As such, this function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if network protocol communication is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).

Functional Entity	Description
• Element Management & Administration	This function is responsible for the administration and management of all other functions within the Element (see Section 5.5.4 for a description of Element Security Management & Administration). This function should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to the Element graphical subsystem components is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• File Transfer Servers	These functions present web content to, and interact with, clients (application programs). As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if web based interaction with requesting clients is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Web Servers	These functions present web content to, and interact with, web clients (application programs). As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if web based interaction with requesting clients is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).
• Other Application Servers	These functions receive from and deliver to clients (application programs) many types of requests associated with client-server functionality. As such, these functions should rely on the Kernel Authentication and Kernel Access Mediation functions to decide if access to Email accounts is allowed as governed by policy rules contained in the Element SMIB (see Section 5.5.4.2).

5.4.2 Applicable Protocol Security Mechanisms

Tables 13 through 21 discussed security services in the context of the need for them at various interfaces. This section discusses specific security mechanisms including security protocols, cryptographic algorithms, cryptographic key sizes, and other security facilities which can be used to instantiate and enforce security policies at the interfaces identified in Tables 13 through 21.

An overview of the generic requirements for security in a telecommunications network may be found in ATIS. 1000007.2006. More specific security requirements for the Network-Network Interface (NNI) for the traditional SS7 network (for both bearer and control signaling) may be found in ATIS-1000012.2006. The corresponding NNI security requirements for packet networks may be found in ATIS-1000019.2007. Additional security requirements for the User Network Interface (UNI) are under development in ATIS PTSC. These standards should be adhered to.

The following sections demonstrate the mapping of communications protocol security mechanisms to necessary or recommended communications security services:

5.4.2.1 Data Link Layer (DLL)

5.4.2.1.1 DLL User Plane UNI Security Mechanisms

As noted in section 5.3 Table 13 the following security services:

- Data-Origin Authentication and Non-repudiation with Proof of Origin should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary

Appropriate security mechanisms to provide security services include:

- IEEE 802.1X provides Access Control for 802.3 physical ports

- IEEE 803.11i provides Data-Origin Authentication, Non-repudiation with Proof of Origin access control for 802.11 wireless connectivity
- DHCP Option 90 provides Peer-Entity Authentication, Data-Origin Authentication, Access Controls, Connectionless Integrity.

Non-repudiation with Proof of Origin necessitates the use of Public Key Infrastructure (PKI) issued credentials. Each Element should provide logging capabilities as basic functionality.

5.4.2.1.2 DLL User Plane I-NNI Security Mechanisms

As noted in section 5.3 Table 13 the following security services:

- Non-repudiation with Proof of Origin should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary

The appropriate security mechanisms to provide security services are:

- IEEE 802.1X provides Access Control for 802.3 physical ports
- IEEE 803.11i provides Data-Origin Authentication, Non-repudiation with Proof of Origin access control for 802.11 wireless connectivity
- DHCP Option 90 provides Peer-Entity Authentication, Data-Origin Authentication, Access Controls, Connectionless Integrity.

Non-repudiation with Proof of Origin necessitates the use of Public Key Infrastructure (PKI) issued credentials. Each Element should provide logging capabilities as basic functionality.

5.4.2.1.3 DLL User Plane NNI Security Mechanisms

As noted in section 5.3 Table 13 the following security services:

- Non-repudiation with Proof of Origin should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary

The appropriate security mechanisms to provide the aforementioned security services are:

- IEEE 802.1X provides Access Control for 802.3 physical ports
- IEEE 803.11i provides Data-Origin Authentication, Non-repudiation with Proof of Origin access control for 802.11 wireless connectivity
- DHCP Option 90 provides Peer-Entity Authentication, Data-Origin Authentication, Access Controls, Connectionless Integrity.

Non-repudiation with Proof of Origin necessitates the use of Public Key Infrastructure (PKI) issued credentials. Each Element should provide logging capabilities as basic functionality.

5.4.2.1.4 DLL Signaling & Control Plane UNI Security Mechanisms

As noted in section 5.3 Table 14 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication and Non-repudiation with Proof of Origin should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary

The appropriate security mechanisms to provide the aforementioned security services are:

- IEEE 802.1X provides Access Control for 802.3 physical ports
- IEEE 803.11i provides Data-Origin Authentication, Non-repudiation with Proof of Origin access control for 802.11 wireless connectivity
- DHCP Option 90 provides Peer-Entity Authentication, Data-Origin Authentication, Access Controls, Connectionless Integrity.

Non-repudiation with Proof of Origin necessitates the use of Public Key Infrastructure (PKI) issued credentials. Each Element should provide logging capabilities as basic functionality.

5.4.2.1.5 DLL Signaling & Control Plane I-NNI Security Mechanisms

As noted in section 5.3 Table 14 the following security services:

- Non-repudiation with Proof of Origin should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary

The appropriate security mechanisms to provide the aforementioned security services are:

- IEEE 802.1X provides Access Control for 802.3 physical ports
- IEEE 803.11i provides Data-Origin Authentication, Non-repudiation with Proof of Origin access control for 802.11 wireless connectivity
- DHCP Option 90 provides Peer-Entity Authentication, Data-Origin Authentication, Access Controls, Connectionless Integrity.

Non-repudiation with Proof of Origin necessitates the use of Public Key Infrastructure (PKI) issued credentials. Each Element should provide logging capabilities as basic functionality.

5.4.2.1.6 DLL Signaling & Control Plane NNI Security Mechanisms

As noted in section 5.3 Table 14 the following security services:

- Non-repudiation with Proof of Origin should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary

The appropriate security mechanisms to provide the aforementioned security services are:

- IEEE 802.1X provides Access Control for 802.3 physical ports
- IEEE 803.11i provides Data-Origin Authentication, Non-repudiation with Proof of Origin access control for 802.11 wireless connectivity
- DHCP Option 90 provides Peer-Entity Authentication, Data-Origin Authentication, Access Controls, Connectionless Integrity.

Non-repudiation with Proof of Origin necessitates the use of Public Key Infrastructure (PKI) issued credentials. Each Element should provide logging capabilities as basic functionality.

5.4.2.2 Internetworking Layer (IP versions 4 and 6)

5.4.2.2.1 Internetworking Layer User Plane UNI Security Mechanisms

As noted in section 5.3 Table 15 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality and Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- IPsec provides Peer-Entity Authentication (IKE), Data-Origin Authentication (ESP-nul), Connection Confidentiality (ESP-AES or ESP-3DES), Connectionless Confidentiality (ESP-AES or ESP-3DES), Connectionless Integrity (ESP)
- Statefull packet filtering provides Access Controls.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of

Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.2.2 Internetworking Layer User Plane I-NNI Security Mechanisms

As noted in section 5.3 Table 15 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality and Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- IPsec provides Peer-Entity Authentication (IKE), Data-Origin Authentication (ESP-nul), Connection Confidentiality (ESP-AES or ESP-3DES), Connectionless Confidentiality (ESP-AES or ESP-3DES), Connectionless Integrity (ESP)
- Statefull packet filtering provides Access Controls.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.2.3 Internetworking Layer User Plane NNI Security Mechanisms

As noted in section 5.3 Table 15 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality and Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- IPsec provides Peer-Entity Authentication (IKE), Data-Origin Authentication (ESP-nul), Connection Confidentiality (ESP-AES or ESP-3DES), Connectionless Confidentiality (ESP-AES or ESP-3DES), Connectionless Integrity (ESP)
- Statefull packet filtering provides Access Controls.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.2.4 Internetworking Layer Signaling & Control Plane UNI Security Mechanisms

As noted in section 5.3 Table 16 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality and Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- IPsec provides Peer-Entity Authentication (IKE), Data-Origin Authentication (ESP-nul), Connection Confidentiality (ESP-AES or ESP-3DES), Connectionless Confidentiality (ESP-AES or ESP-3DES), Connectionless Integrity (ESP)

- Statefull packet filtering provides Access Controls.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.2.5 Internetworking Layer Signaling & Control Plane I-NNI Security Mechanisms

As noted in section 5.3 Table 16 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality and Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- IPsec provides Peer-Entity Authentication (IKE), Data-Origin Authentication (ESP-nul), Connection Confidentiality (ESP-AES or ESP-3DES), Connectionless Confidentiality (ESP-AES or ESP-3DES), Connectionless Integrity (ESP)
- Statefull packet filtering provides Access Controls.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.2.6 Internetworking Layer Signaling & Control Plane NNI Security Mechanisms

As noted in section 5.3 Table 16 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality and Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- IPsec provides Peer-Entity Authentication (IKE), Data-Origin Authentication (ESP-nul), Connection Confidentiality (ESP-AES or ESP-3DES), Connectionless Confidentiality (ESP-AES or ESP-3DES), Connectionless Integrity (ESP)
- Statefull packet filtering provides Access Controls.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.3 Transport Layer

5.4.2.3.1 Transport Layer User Plane UNI Security Mechanisms

As noted in section 5.3 Table 17 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- TLS provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity
- SSH provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity

As an alternative to TLS or SSH, one could rely on IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.3.2 Transport Layer User Plane I-NNI Security Mechanisms

As noted in section 5.3 Table 17 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- TLS provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity
- SSH provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity

As an alternative to TLS or SSH, one could rely on IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.3.3 Transport Layer User Plane NNI Security Mechanisms

As noted in section 5.3 Table 17 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- TLS provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity
- SSH provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity

As an alternative to TLS or SSH, one could rely on IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

As an example, note that ATIS.1000019.2007 provides standard requirements for applying these principles to a telecommunications network.

5.4.2.3.4 Transport Layer Signaling & Control Plane UNI Security Mechanisms

As noted in section 5.3 Table 18 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- TLS provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity
- SSH provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity

As an alternative to TLS or SSH, one could rely on IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.3.5 Transport Layer Signaling & Control Plane I-NNI Security Mechanisms

As noted in section 5.3 Table 18 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- TLS provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity
- SSH provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity

As an alternative to TLS or SSH, one could rely on IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.3.6 Transport Layer Signaling & Control Plane NNI Security Mechanisms

As noted in section 5.3 Table 18 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- TLS provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity
- SSH provides Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Non-repudiation with Proof of Delivery, Access Controls, Connectionless Integrity

As an alternative to TLS or SSH, one could rely on IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on PKI issued credentials.

5.4.2.4 Application Layer

Within the application protocol layer reside many types of protocols that are used by application services. Common application services include, but are not limited to:

- Remote login (i.e., telnet, TL1, X-Windows),
- File transfer (i.e., ftp, tftp)
- Messaging (i.e., SMTP, POP3, IMAP, IM, SMS)
- Voice over IP (i.e., H.323, SIP/SIPT, RTP)
- Layer 3 Signaling and Control (i.e., RSVP, RSVP-TE, LDP, CR-LDP, BGP, OSPF, IS-IS, RIP)
- Infrastructure Services (i.e., DNS, LDAP, NTP, Corba, Java, DCE)
- Web Services (http, SOAP, .NET)

- Information/Message Formatting Mechanisms (html, XML, MIME, SMIME).

Those protocols used to support Management activities are also application protocols and are covered here.

5.4.2.4.1 Application Layer User Plane UNI Security Mechanisms

As noted in section 5.3 Table 19 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Connection Confidentiality, Connectionless Confidentiality, Selective Field Confidentiality, Connection Integrity with Recovery, Connection Integrity without Recovery, Selective Field Connection Integrity, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- XML - SAML provide Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Selective Field Confidentiality, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery when used with XML Digital Signatures and XML-Encryption.

As an alternative to XML - SAML, one could rely on

- IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity,
- TLS at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connection Confidentiality, Access Controls, Connection Integrity without recovery. However TLS does not provide these security services above the transport protocol layer and restricted to TCP traffic.
- SSH at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Access Controls, Connection Integrity. However SSH does not provide these security services above the transport protocol layer, or
- Access control of most application protocols, including information integrity checking should be provided through the use of 'deep packet inspection' functional entities, as in Intrusion Protection Systems (IPSs).

Access control of RTP "pin-holes" should be provided for RTP through the use of Session Border Controller functional entities.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on issued credentials.

5.4.2.4.2 Application Layer User Plane I-NNI Security Mechanisms

As noted in section 5.3 Table 19 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Connection Confidentiality, Connectionless Confidentiality, Selective Field Confidentiality, Connection Integrity with Recovery, Connection Integrity without Recovery, Selective Field Connection Integrity, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- XML - SAML provide Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Selective Field Confidentiality, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery when used with XML Digital Signatures and XML-Encryption.

As an alternative to XML - SAML, one could rely on

- IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.
- TLS at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connection Confidentiality, Access Controls, Connection Integrity without recovery. However TLS does not provide these security services above the transport protocol layer, and is restricted to TCP traffic.
- SSH at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Access Controls, Connection Integrity. However SSH does not provide these security services above the transport protocol layer
- Access control of most application protocols, including information integrity checking should be provided through the use of 'deep packet inspection' functional entities, as in Intrusion Protection Systems (IPSs).
- Access control of RTP "pin-holes" should be provided for RTP through the use of Session Border Controller functional entities.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on issued credentials.

5.4.2.4.3 Application Layer User Plane NNI Security Mechanisms

As noted in section 5.3 Table 19 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Connection Confidentiality, Connectionless Confidentiality, Selective Field Confidentiality, Connection Integrity with Recovery, Connection Integrity without Recovery, Selective Field Connection Integrity, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- XML - SAML provide Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Selective Field Confidentiality, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery when used with XML Digital Signatures and XML-Encryption.

As an alternative to XML - SAML, one could rely on

- IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.
- TLS at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connection Confidentiality, Access Controls, Connection Integrity without recovery. However TLS does not provide these security services above the transport protocol layer, and is restricted to TCP traffic.
- SSH at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Access Controls, Connection Integrity. However SSH does not provide these security services above the transport protocol layer

- Access control of most application protocols, including information integrity checking should be provided through the use of 'deep packet inspection' functional entities, as in Intrusion Protection Systems (IPSs).
- Access control of RTP "pin-holes" should be provided for RTP through the use of Session Border Controller functional entities.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on issued credentials.

5.4.2.4.4 Application Layer Signaling & Control Plane UNI Security Mechanisms

As noted in section 5.3 Table 20 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Connection Confidentiality, Connectionless Confidentiality, Selective Field Confidentiality, Connection Integrity with Recovery, Connection Integrity without Recovery, Selective Field Connection Integrity, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- XML - SAML provide Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Selective Field Confidentiality, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery when used with XML Digital Signatures and XML-Encryption.

As an alternative to XML - SAML, could rely on

- IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.
- TLS at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connection Confidentiality, Access Controls, Connection Integrity without recovery. However TLS does not provide these security services above the transport protocol layer, and is restricted to TCP traffic.
- SSH at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Access Controls, Connection Integrity. However SSH does not provide these security services above the transport protocol layer
- Access control of most application protocols, including information integrity checking should be provided through the use of 'deep packet inspection' functional entities, as in Intrusion Protection Systems (IPSs).
- Access control of RTP "pin-holes" should be provided for RTP through the use of Session Border Controller functional entities.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on issued credentials.

An overview of the generic requirements for security in a telecommunications network may be found in ATIS-1000007.2006. More specific security requirements for the User Network Interface (UNI) are under development in ATIS PTSC. These standards should be adhered to as they become finalized.

5.4.2.4.5 Application Layer Signaling & Control Plane I-NNI Security Mechanisms

As noted in section 5.3 Table 20 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Connection Confidentiality, Connectionless Confidentiality, Selective Field Confidentiality, Connection Integrity with Recovery, Connection Integrity without Recovery, Selective Field Connection Integrity, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and
- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- XML - SAML provide Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Selective Field Confidentiality, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery when used with XML Digital Signatures and XML-Encryption.

As an alternative to XML - SAML, one could rely on

- IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.
- TLS at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connection Confidentiality, Access Controls, Connection Integrity without recovery. However TLS does not provide these security services above the transport protocol layer, and is restricted to TCP traffic.
- SSH at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Access Controls, Connection Integrity. However SSH does not provide these security services above the transport protocol layer
- Access control of most application protocols, including information integrity checking should be provided through the use of 'deep packet inspection' functional entities, as in Intrusion Protection Systems (IPSs).
- Access control of RTP "pin-holes" should be provided for RTP through the use of Session Border Controller functional entities.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on issued credentials.

An overview of the generic requirements for security in a telecommunications network may be found in ATIS-1000007.2006. More specific security requirements for the Network-Network Interface (NNI) for the traditional SS7 network (for both bearer and control signaling) may be found in ATIS-1000012.2006. The corresponding NNI security requirements for packet networks may be found in ATIS-1000019.2007. These standards should be adhered to as they become finalized.

5.4.2.4.6 Application Layer Signaling & Control Plane NNI Security Mechanisms

As noted in section 5.3 Table 20 the following security services:

- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Connection Confidentiality, Connectionless Confidentiality, Selective Field Confidentiality, Connection Integrity with Recovery, Connection Integrity without Recovery, Selective Field Connection Integrity, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery should be provided as required, and

- Access Controls, Logging, Connectionless Integrity are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- XML - SAML provide Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Selective Field Confidentiality, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery when used with XML Digital Signatures and XML-Encryption.

As an alternative to XML - SAML, one could rely on

- IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.
- TLS at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connection Confidentiality, Access Controls, Connection Integrity without recovery. However TLS does not provide these security services above the transport protocol layer, and is restricted to TCP traffic.
- SSH at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Access Controls, Connection Integrity. However SSH does not provide these security services above the transport protocol layer
- Access control of most application protocols, including information integrity checking should be provided through the use of 'deep packet inspection' functional entities, as in Intrusion Protection Systems (IPSs).
- Access control of RTP "pin-holes" should be provided for RTP through the use of Session Border Controller functional entities.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on issued credentials.

An overview of the generic requirements for security in a telecommunications network may be found in ATIS. 1000007.2006. More specific security requirements for the Network-Network Interface (NNI) for the traditional SS7 network (for both bearer and control signaling) may be found in ATIS-1000012.2006. The corresponding NNI security requirements for packet networks may be found in ATIS-1000019.2007. These standards should be adhered to as they become finalized.

5.4.2.4.7 Application Layer Management Plane UNI Security Mechanisms

As noted in section 5.3 Table 21 the following security services:

- Connection Confidentiality, Connectionless Confidentiality, Selective Field Confidentiality, Connection Integrity with Recovery, Selective Field Connection Integrity, Selective Field Connectionless Integrity should be provided as required, and
- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Access Controls, Logging, Connection Integrity without Recovery, Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- XML - SAML provide Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Selective Field Confidentiality, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery when used with XML Digital Signatures and XML-Encryption.

As an alternative to XML - SAML, one could rely on

- IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.
- TLS at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connection Confidentiality, Access Controls, Connection Integrity without recovery. However TLS does not provide these security services above the transport protocol layer, and is restricted to TCP traffic.
- SSH at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Access Controls, Connection Integrity. However SSH does not provide these security services above the transport protocol layer
- Access control of most application protocols, including information integrity checking should be provided through the use of 'deep packet inspection' functional entities, as in Intrusion Protection Systems (IPSs).
- Access control of RTP "pin-holes" should be provided for RTP through the use of Session Border Controller functional entities.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on issued credentials.

ANSI standard ATIS-0300276.2008 (ITU-T recommendation M.3016) specifies a minimally acceptable set of requirements for securing management communication.

5.4.2.4.8 Application Layer Management Plane I-NNI Security Mechanisms

As noted in section 5.3 Table 21 the following security services:

- Connection Confidentiality, Connectionless Confidentiality, Selective Field Confidentiality, Connection Integrity with Recovery, Selective Field Connection Integrity, Selective Field Connectionless Integrity should be provided as required, and
- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Access Controls, Logging, Connection Integrity without Recovery, Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- XML - SAML provide Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Selective Field Confidentiality, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery when used with XML Digital Signatures and XML-Encryption.

As an alternative to XML - SAML, one could rely on

- IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.
- TLS at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connection Confidentiality, Access Controls, Connection Integrity without recovery. However TLS does not provide these security services above the transport protocol layer, and is restricted to TCP traffic.
- SSH at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Access Controls, Connection Integrity. However SSH does not provide these security services above the transport protocol layer
- Access control of most application protocols, including information integrity checking should be provided through the use of 'deep packet inspection' functional entities, as in Intrusion Protection Systems (IPSs).

- Access control of RTP "pin-holes" should be provided for RTP through the use of Session Border Controller functional entities.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on issued credentials.

ANSI standard ATIS-0300276.2008 (ITU-T recommendation M.3016) specifies a minimally acceptable set of requirements for securing management communication.

5.4.2.4.9 Application Layer Management Plane NNI Security Mechanisms

As noted in section 5.3 Table 21 the following security services:

- Connection Confidentiality, Connectionless Confidentiality, Selective Field Confidentiality, Connection Integrity with Recovery, Selective Field Connection Integrity, Selective Field Connectionless Integrity should be provided as required, and
- Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Access Controls, Logging, Connection Integrity without Recovery, Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery are necessary.

The appropriate security mechanisms to provide the aforementioned security services are:

- XML - SAML provide Peer-Entity Authentication, Data-Origin Authentication, User Authentication, Selective Field Confidentiality, Selective Field Connectionless Integrity, Non-repudiation with Proof of Origin, Non-repudiation with Proof of Delivery when used with XML Digital Signatures and XML-Encryption.

As an alternative to XML - SAML, one could rely on

- IPsec at layer 3 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connectionless Confidentiality, Access Controls, Connectionless Integrity.
- TLS at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Connection Confidentiality, Access Controls, Connection Integrity without recovery. However TLS does not provide these security services above the transport protocol layer, and is restricted to TCP traffic.
- SSH at layer 4 for Peer-Entity Authentication, Data-Origin Authentication, Connection Confidentiality, Access Controls, Connection Integrity. However SSH does not provide these security services above the transport protocol layer

Access control of most application protocols, including information integrity checking should be provided through the use of 'deep packet inspection' functional entities, as in Intrusion Protection Systems (IPSs). Access control of RTP "pin-holes" should be provided for RTP through the use of Session Border Controller functional entities.

Peer-Entity Authentication requires use of PKI issued credentials. Each Element should provide logging capabilities as basic functionality. Non-repudiation with Proof of Origin and with Proof of Delivery necessitates the use of digital signatures within the application protocol based on issued credentials.

ANSI standard ATIS-0300276.2008 (ITU-T recommendation M.3016) specifies a minimally acceptable set of requirements for securing management communication.

5.4.3 Major Security Protocols

5.4.3.1 IPsec and IKE Protocols

This section discusses security features when use of IPsec is required for a given interface. IPsec is preferable for providing authentication, confidentiality and data integrity as it is able to do so for all protocols transported via TCP and UDP. In fact SCTP requires IPsec based security for SCTP transported signaling and & control messages when necessary (RFC 3554).

The document references both IPsec Version 1 and its key management system IKEv1/ISMKMP and the newer IPSec Version 2 and IKEv2 since IPSecv2/IKEv2 are still fairly new and are not so widely implemented yet.

5.4.3.1.1 IPsec Security Modes

IPsec supports two modes of operation: transport mode and tunnel mode. See reference [RFC 4301] for IPSec version 2 and [RFC 2401] for IPsec Version 1 for a complete discussion of IPsec modes of operation. Tunnel Mode is primarily used when:

- some degree of Traffic Flow Confidentiality is required, or
- communications must traverse intermediate nodes that perform Network Address Translation (NAT) and modify packet header contents.

Transport mode is more appropriate than tunnel mode when protection is required for the signaling and control communications and NATs are not an issue. Layer 3 packet inspection is also simplified when transport mode is used.

5.4.3.1.2 IPsec Protocols

IPsec provides two protocols; the Encapsulation Security Payload (ESP) [RFC 4303, RFC4835]and version 1 of ESP [RFC 2406] protocol and the Authentication Header (AH) [RFC 4302, RFC 4835] and the version 1 of AH [RFC 2402] protocol. The ESP protocol provides data confidentiality, data integrity, and data origin authentication for the payload of an IP protocol data unit (payload). The AH protocol provides only data integrity and data origin authentication but covers virtually all of an IP packet including most header fields. The ESP protocol is the preferred protocol since it can provide data confidentiality in addition to data integrity/data origin authentication. When data integrity/data origin is required without data confidentiality, the ESP protocol can be used with null encryption. Given that AH covers most IP header fields, AH cannot be used where NAT is deployed except when used in tunnel mode or used in conjunction with UDP encapsulation. Both ESP and AH can, in theory rely on some form of out-of-band' symmetric shared key distribution but this is strongly recommended against do to the non-availability of electronic symmetric shared key management systems. Another problem with using symmetric shared keys is the lack of peer-entity authentication.

RFC 4835 states the security requirements for implementing the crypto algorithms within IPSec ESP or within IPSec AH.

5.4.3.1.3 IPsec Encryption Algorithms

IPsec relies on the following underlying cryptographic algorithms:

Null encryption [RFC 2410], which is ideal for data-origin authentication and data integrity, or

3DES CBC-mode [RFC 2451] (with 3 independent 56 bit keys) for confidentiality and data integrity, or
AES CBC [RFC 3602], AES-counter mode [RFC 3686], AES CCM [RFC 4309] (with 128 bit key), Galois/counter mode [RFC 4106] for confidentiality and some limited data integrity or
Crypto Suites for IPsec [RFC 4308, RFC 4869]

to provide encryption services. However it is recommended that 3DES CBC-mode and AES CBC should only be used with some additional data-origin authentication mechanism, see also RFC 4305.

5.4.3.1.4 IPsec Implementation Authentication Algorithms

IPsec relies on the following underlying cryptographic algorithms:

HMAC-SHA1-96 [RFC 2404] (with 160 bit key), or HMAC-SHA with key lengths of 256, 384 and 512 bits [RFC 4868] or

HMAC-MD5-96 [RFC 2403] (with 128 bit key), or

AES-XCBC [RFC 3566] (with 128 bit key), or

AES CMAC [RFC 4494]

to provide data origin authentication/data integrity services. One of these services should be used when IPsec is being used. Note that AES-XCBC is emerging as an improved message authentication algorithm based on AES. MD5 is currently widely implemented; however, it has been found to have collision weaknesses in some other applications so HMAC-SHA1-96 is preferred over HMAC-MD5-96.

RFC 4359 specifies how to apply the RSA digital signature algorithm for data origin authentication of the IP packet, for example to authenticate the sender when using IP multicast packet. Since computing and verifying digital signatures are processing intensive operations, applying RSA digital signatures to IPSec should be taken with great care to secure performance critical applications.

5.4.3.1.5 IPsec Implementation Selectors

Selectors support a packet filtering capability within the IPsec architecture. This enable IPsec implementations to selectively process or discard packets based on matching selector criteria. The following parameters are used to manage IPsec ESP and AH Security Associations (SAs):

Source IP address

Destination IP address

Transport layer protocol (UDP, TCP or SCTP)

Transport layer protocol (UDP, TCP or SCTP) port numbers. and

Wildcards.

These ESP and AH SA selector parameters should not be confused with identifying information necessary for peer-entity authentication within IKE.

5.4.3.1.6 Support for Internet Key Exchange (IKE)

The Internet Key Exchange (IKE) is used to provide peer-entity authentication and an automatic mechanism for symmetric shared key generation, distribution and re-keying. Two versions of

IKE are available: IKEv1 [RFCs, 2407, 2408, 2409, and 4109] and IKEv2 [RFC 4306, RFC 4307, RFC 4718, RFC 4615]. Currently IKEv1 is widely implemented and IKEv2 has only recently been standardized.

5.4.3.1.7 IKEv1 Implementation Modes

IKEv1 provides two modes of operation: main mode and aggressive mode. Main mode is more secure however takes more time to complete than aggressive mode. Support for aggressive mode may not be required by all products.

Note: Implementation modes will depend on the IKE version selected.

5.4.3.1.8 IKE Implementation Encryption Algorithms

IKE shall use one of the following underlying encryption algorithms

3DES [3DES] (with three independent 56 bit keys)
AES [FIPS-197] (with 128 bit key)
AES [FIPS-197] (with 196 bit key)
AES [FIPS-197] (with 256 bit key)
AES XCBC Pseudo random function [RFC 4434] with 128 bit key

to provide confidentiality services when performing ESP and AH SA negotiation and SA re-keying.

5.4.3.1.9 IKE Implementation Secure Hash Algorithms

IKE relies on the following underlying secure hash algorithms:

MD5 [RFC 1321] (with 128 bit message digest) , or
SHA-1 [FIPS 180-2] (with 160 bit message digest)

to provide data integrity services.

5.4.3.1.10 IKE Implementation Authentication Methods

IKE supports authentication of device identities as part of the key exchange protocol using either:

Pre-shared keys (out-of-band' symmetric shared key), or
Digital signatures (RSA) with a 1024 bit or greater key

As already noted, pre-shared keys should not be used due to the non-availability of electronic symmetric shared key management systems and the lack of peer-entity authentication. Digital Signatures provides peer-entity authentication and simplified key distribution electronically when supported by a Public Key Infrastructure (PKI).

5.4.3.1.11 IKE Public Key Infrastructure Interoperability

When IKE is used with Public Key Infrastructures (PKIs) when using digital certificates, The IKE implementation should support:

X.509v3 digital certificates, including extensions
On-line Certificate Status Protocol (RFC 2560)
LDAP retrieval of digital certificates
LDAP retrieval of certificate revocation lists (CRLs) , or
CA Trust Hierarchy traversal.

5.4.3.1.12 IKE Implementation Oakley groups

Different Oakley groups are used within IKE during the Diffie-Hellman key derivation process depending on security and speed of processing requirements. Oakley Group 14 is recommended to provide sufficient security when IKE is used to establish security associations with 128 bit symmetric encryption. Reference [RFC 2409], [RFC 3526]. All IKE implementations should support the following groups:

Group 1 (768 bit prime MODP group)
Group 2 (1024 bit prime MODP group)
Group 3 (Elliptic curve group over GF[2^155])
Group 4 (Elliptic curve group over GF[2^185])
Group 5 (1536 bit prime MODP group), and
Group 14 (2048 bit prime MODP group)

5.4.3.1.13 IKE Support of Perfect Forward Secrecy

Perfect Forward Secrecy, where new keys are derived independently from old keys, is necessary and is the preferred method to ensure a high security level for IKE.

5.4.3.1.14 Random number generators for IPsec/IKE

Software based random number generation implementations tend to be weak. Many semiconductor manufacturers are adding secure random number generators to their integrated circuits, which should be used if available. If no hardware random number generator is available, then strong pseudo-random number generator software may optionally be used in keeping with the IETF informational RFC – Randomness Requirements for Security [RFC 4086].

5.4.3.2 Transport Layer Security (TLS) Protocol Requirements

This section specifies security features that support use of Transport Layer Security (TLS) for a given interface [RFC 4346, RFC 3546, RFC 2246]. Note that TLS is the IETF standardized successor to the Secure Socket Layer (SSL) protocol. TLS has security enhancements over the SSL protocol in addition to being an IETF standard whereas all versions of SSL are only specified in either an informational RFC (SSLv3) or now expired Internet Draft documents.

5.4.3.2.1 TLS Authentication

TLS supports within the protocol either:

no authentication where neither party authenticates it's identity to the other party,

uni-directional authentication where only the server is authenticated to the client only, or

bi-directional authentication where both client and server authenticate to each other.

Unidirectional authentication is the usual method used in the public Internet. With this method, the server uses a digital signature and X.509v3 server certificate to authenticate its identity and the client uses an ID and password to authenticate its identity. For network signaling and control applications, bidirectional authentication, using digital signatures and X.509v3 certificates, is necessary to allow each party to know it is communicating with the desired endpoint.

5.4.3.2.2 TLS Authentication Algorithms

TLS relies on the HMAC-SHA-1 (with 160 bit key) cryptographic algorithm to provide data origin authentication and data integrity services. These services should always be used when TLS is being used. Note that AES-XCBC is emerging as an improved message authentication algorithm based on AES.

5.4.3.2.3 Key Exchange Algorithms for TLS

TLS specifies various methods for key exchange. Recommended methods for key exchange within the TLS protocol include:

Rivest Shamir Adleman (RSA) asymmetric encryption, and

Diffie Hellman (DH)

5.4.3.2.4 TLS Encryption Algorithms

TLS relies on the following underlying cryptographic algorithms:

3DES CBC-mode (with 3 independent 56 bit keys)

AES CBC (with 128 bit key), or

Null encryption,

to provide encryption services.

5.4.3.2.5 Cipher suites for TLS

TLS specifies various cipher suites for use within the TLS protocol, as discussed in detail in Reference [RFC 3268], [RFC 4279], [RFC 4785]. Recommended cipher suites to be used within the TLS protocol include:

TLS_RSA_WITH_NULL_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA, and

TLS_DH_RSA_WITH_AES_128_CBC_SHA

5.4.3.2.6 Random number generators for TLS

Software based random number generation implementations tend to be weak. Many semiconductor manufacturers are adding secure random number generators to their integrated circuits, which should be used if available. If no hardware random number generator is available, then strong pseudo-random number generator software may optionally be used in keeping with the IETF informational RFC – Randomness Requirements for Security [RFC 4086].

5.4.3.3 Datagram Transport Layer Security (DTLS)

DTLS was recently approved as an IETF standard [RFC 4347] the same forms of authentication, confidentiality and data integrity for UDP transported protocols that TLS provides to TCP UDP transported protocols. However it may be some time before commercially available implementations of DTLS exist.

5.4.3.4 Secure Shell (SSH)

SSH [RFC 4251, RFC 4252, RFC 4253, RFC 4344, RFC 4345, RFC 4419, RFC 4432, RFC 4819] was originally developed by the OpenBSD Project and:

- Encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other attacks directed at many application layer protocols
- Provides secure tunneling capabilities and several authentication methods
- Replaces rlogin and telnet with the ssh program, rcp with scp, and ftp with sftp.

Along with supporting a number of encryption algorithms (3DES, Blowfish, AES, Arcfour), SSH provides authentication using Public Keys and X.509v3 certificates, One-Time Password or Kerberos.

Other than IPsec, SSH is the only mechanism that can currently provide proper authentication and confidentiality when deploying the X11 X Window protocol and associated application functionality.

5.4.3.5 RADIUS

RADIUS is an authentication protocol for providing authentication services to:

- IEEE 802.1x layer 2 port access control
- remote dial-up user access authentication
- central management of computer login accounts
- web site client authentication.

5.4.3.6 Diameter

Diameter has become a primary user authentication and authorization protocol within the IP Multimedia Subsystem (IMS) architecture currently being developed. Although quite appropriate for retrieval of IMS subscriber profile and authentication information over interfaces, such as over the Zb interface, Diameter has not been shown to be a robust protocol for any form of asymmetric or symmetric encryption key distribution.

5.4.3.7 Keyed Digest

The use of Keyed Digest based data-origin authentication relies on the use of symmetric shared secret keys (pre-shared keys). A management problem exists with use of pre-shared secret keys due to the non-availability of electronic symmetric shared key management systems and the lack of peer-entity authentication. Digital Signatures provides peer-entity authentication and simplified key distribution electronically when supported by a Public Key Infrastructure (PKI).

5.4.3.8 Public key infrastructures

Public Key Infrastructures (PKIs) focus on providing a robust approach to Identity Management when asymmetric encryption algorithms, and their associated public and private keys, provide the basis for authenticating subject identities. For every subject, a public and private key pair is generated, where the private key is retained by the subject and never shared with any other party. A subject's public key needs to be shared with all other subjects who communicate with the subject possessing the private key. Parties possessing a valid copy of a subject's public key are able to encrypt information that only the subject possessing the corresponding private key can decrypt. Conversely, anything a subject encrypts with their private key, all parties who have a valid copy of the subject's public key can decrypt. This asymmetry is especially useful for:

- digitally signing messages prior to transmission,
- digitally signing message receipts following receiving a message
- protecting the "Diffy-Helman" Key exchange protocol from "Man-in-the-middle" attacks.

The critical component to the above operations is that each party either already have, or be able to get, a valid copy of the other party's public key. The PKI Certificate (CA) and Registration Authority (RA) Servers, in conjunction with a digital certificate (certificate) repository, certificate revocation list and certificate status servers provide a subject with the ability to:

- request generation of certificates
- retrieve valid certificates for other subjects, and
- check the status of a certificate associated with a subject.

The CA that issues a certificate, which cryptographically binds a subject's identity with that subject's public key, servers as a "trusted introducer" or "trusted 3rd party" of the subject to other entities that need a valid copy of the public key associated with the identity of the subject in question. The RA is the entity that a subject interacts with when requesting creation of a certificate for the subject. A PKI provides the ability to:

- deliver certificates to requesters typically via DNS or LDAP servers
- provide current validity status of a certificate issued by the PKI via retrieval of certificate revocation lists (CRLs) which will include entries for all certificates revoked by the PKI, and
- provide current validity status of a certificate issued by the PKI via direct status query using the Online Certificate Status Protocol (OCSP).

The certificates discussed above are ITU-T X.509 version 3 compliant data structures which bind descriptive information about a subject (such as subject name/identity, associated public key, public key usage, alias identities, etc.) via a digital signature produced by the issuing CA using it's private key. The certificate also states the temporal window within which the certificate is valid, the identity of the CA issuing the certificate and other information specific to this certificate.

The general format of an X.509v3 certificate is:

```
Certificate ::= {
    OutputFile ::= “alice-1.bin"
    SerialNumber ::= 1000340
    SubjectName  ::= <C=US,O=Company-XYZ, CN=Alice>
    IssuerName   ::= <C=US,O=Company-XYZ, CN=Operations-Personnel CA>
    Validity ::= {
        NotBefore ::= “2005 Jul 30th, 19:30:00"
        NotAfter ::= "2007 Jan 1st, 12:00:00"
        }
    PublicKeyInfo ::= {
        Size ::= 1024
        Type ::= rsaEncryption
        PublicKey ::= "alice.pub"
       }
    Signature ::= {
        CASigned
        SignatureAlgorithm ::= md5WithRSAEncryption
       }
    Extensions ::= {
```

```
            SubjectAltNames ::= {
                IP ::= 132.197.164.214
                EMAIL ::= alice@ Company-XYZ.com
               }
            BasicConstraints ::= {
                 CA
                PathLength ::= 0
               }
            KeyUsage ::= {
                DigitalSignature
                KeyCertSign
               }
            CRLDistributionPoints ::= [
                {
                    FullName ::= {
                        DN ::= <C=US,O=Company-XYZ,CN=CRL1>
                     }
                    CRLIssuer ::= {
                        DN ::= <C=US,O=Company-XYZ,CN= Operations-Personnel CA>
                                KeyCompromise
                         }
                         { IssuerRelativeDN ::= <C=Company-XYZ,CN= Operations-Personnel
                              CA,CN=CRL1>
                        CRLIssuer ::= {
                            DN ::= <C=FI,O=Company-XYZ,CN=Test CA> CaCompromise
                                AffiliationChanged Superseded CessationOfOperation
                                CertificateHold
                            }
                }
             ]
        }
    }
```

(also depicted in Figure 13) where the primary fields are:

- **OutputFile**. The certificate file which contains the generated certificate in raw binary format.
- **SerialNumber**. The serial number is a unique identifier for the certificate under the signing Certificate Authority. Serial number and issuer name can be uniquely used to revoke a certificate.
- **SubjectName**. In practice subject name fields describes the X.500 distinguished name. The structure of a distinguished name is a hierarchical one, often following some X.500 directory structure. The name consist of many parts, some of which are: country (e.g. "C=FI"), organization name (e.g. "O=SSH Communication Security"), organization unit (e.g. "OU=Marketing"), common name of the subject (e.g. "CN=Johnny Smith").
- **IssuerName**. As above, thus equals the distinguished name of issuing CA.
- **NotBefore**. The date since when the certificate becomes valid.
- **NotAfter**. The date after which the certificate is invalid.
- **PublicKeyInfo**. The size, type and actual public key associated with this subject.
- **Signature**. The signature algorithm used (e.g., md5WithRSAEncryption or dsaWithSHA-1) to sign the certificate and whether the certificate is self signed by the subject or signed by an issuing CA.

An important addition to version 3 of X.509 is the availability of certificate extensions where the more important extensions are the:

- **SubjectAltNames**. This extension is used for alternative naming methods for subject. This may consist of the subject, the Domain Name Server (DNS) name of the subject (e.g. "ssh.fi") and email address of the subject (e.g. "info@ssh.fi").
- **KeyUsage**. This extension identifies if the private key associated with this subject public key can be used: only for generating digital signatures, only for encryption to provide confidentiality, digitally signing certificates, etc..
- **CRLDistributionPoints.** This extension identifies the X.500 identity of the element responsible for producing a certificate revocation list entry should this certificate be revoked prior to the **NotAfter** date.

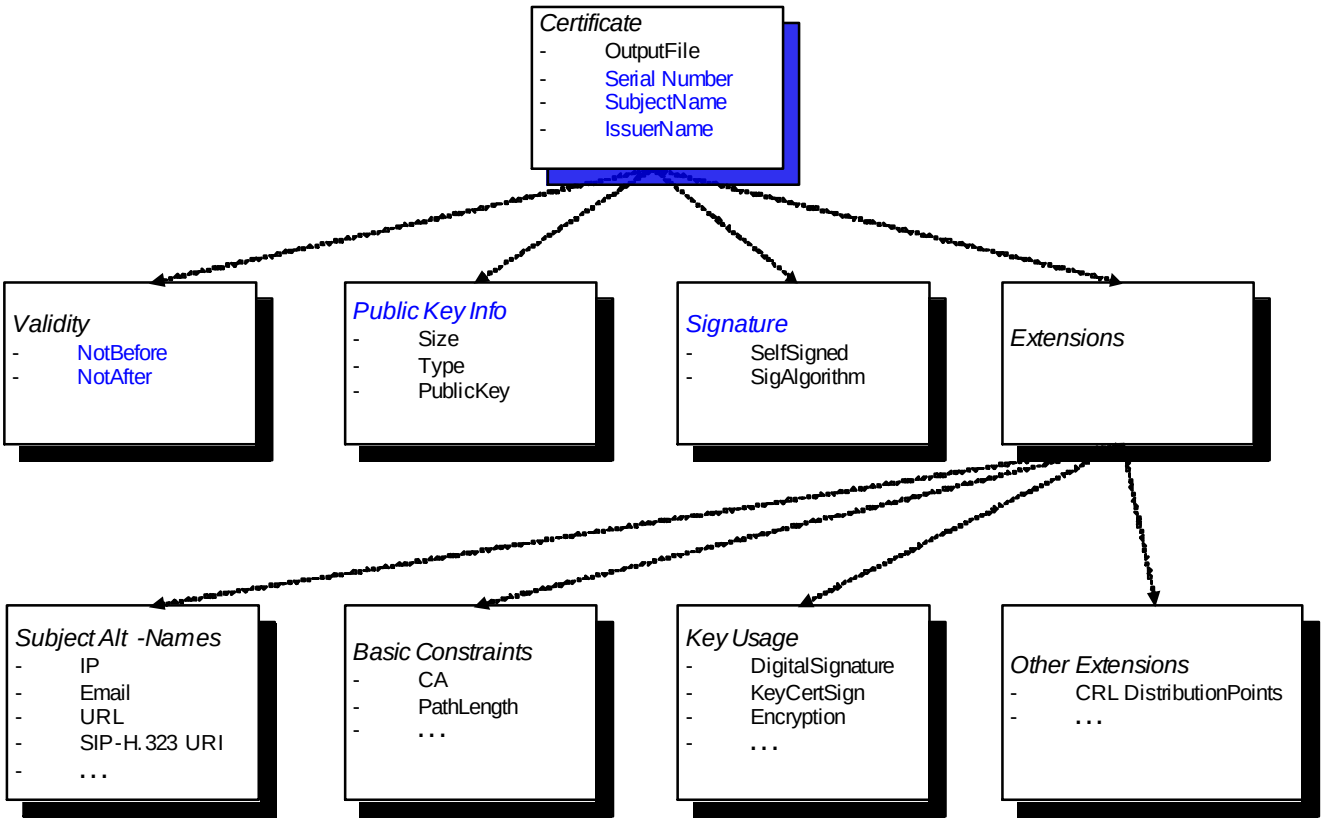

Figure 13- X.509v3 Digital Certificate Structure

Certificates are typically supplied to subjects within self-securing data structures that comply with the PKCS 12v1.0 specification[17]. This data structure will also contain the private key of the subject. The contents of a PKCS 12 structure is encrypted using a symmetric encryption algorithm using "*Password privacy mode"* for key management.

The CAs within a PKI are organized in a tree structure, frequently a non-binary tree. Figure 14 depicts a simplified hierarchy of CAs depending from a common Root CA.

[17] PKCS 12 v1.0: Personal Information Exchange Syntax, RSA Laboratories, June 24, 1999

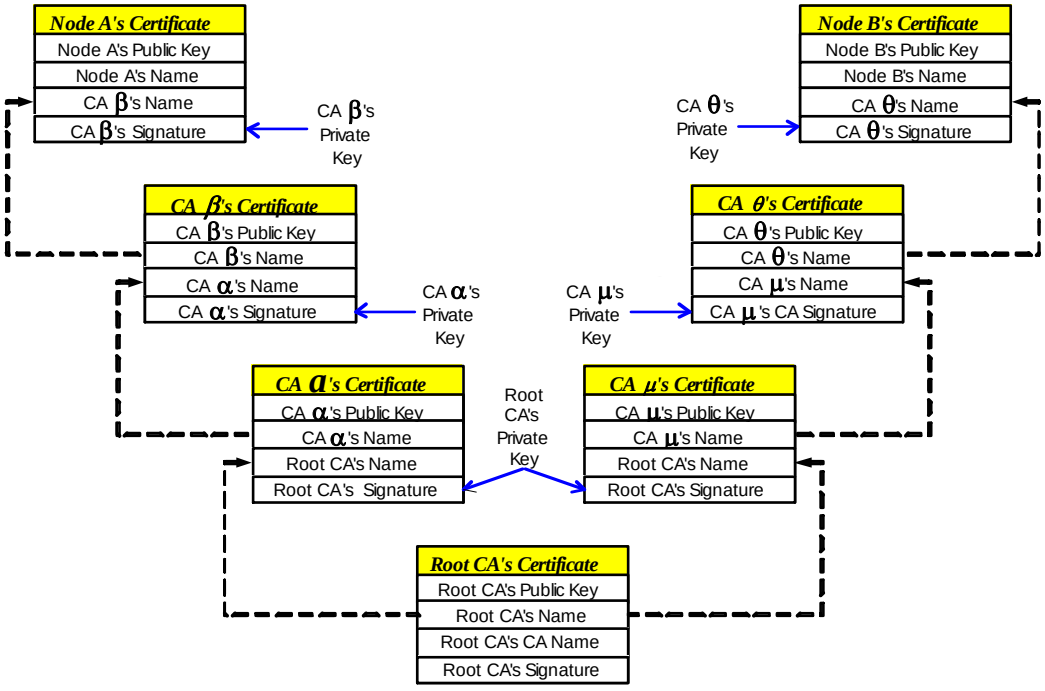

Figure 14 - Simple CA Hierarchy

Whenever a subject receives the certificate of another subject, the receiving subject needs to locate the CA that issued the sending subject's certificate; this operation is called CA hierarch traversal. Since trust is transitive across a hierarchy of CAs, a certificate receiver can traverse the hierarchy of CAs that share the same Root CA. In Figure 14 above:

- since Node A trusts CA β, which trusts CA α, which trusts the Root CA, thus allowing Node A to trust all CAs up to, and including the Root CA.
- since Node B trusts CA θ, which trusts CA μ, which trusts the Root CA, thus allowing Node B to trust all CAs up to, and including the Root CA.

Because Node A is able to locate CA θ as part of the overall CA hierarchy, Node A can use a copy of CA θ's public key to validate Node B's certificate and thereby be assured that the Node B public key is a valid key for Node B.

5.4.3.8.1 Public vs. Private PKIs

The decision by TSPs, and other organizations, to rely on a public vs. a private PKI for management if subject identities and authentication of these identities is one of control. Use of a public PKI, one operated by a third party which is not subject to the security policies of a TSP, means that the TSP may not have full control over, but not limited to:

- the form in which subject identities are specified (i.e., Distinguished names, fully qualified domain names, IP addresses, SIP URIs, http URLs, etc.)

- how subject asymmetric key pairs are generated and protected prior to inclusion within certificates
- timeliness and availability of certificate revocation lists (CRLs), CRL entry updates or usage of the On-line certificate status protocol (OCSP)
- to whom certificates will be issued and under what conditions
- liability for certificate issuance errors
- cost for certificates issued.

For the above reasons a TSP will typically operate its own PKI, especially for issuing certificates to elements within the TSP infrastructure. On the other hand, a TSP should consider supporting public PKI issued certificates that subscribers present for selected application service authentication purposes.

5.4.3.8.2 Certificate and Registration Authorities

When a TSP deploys a private PKI, the TSP should have a hierarchy of CAs as discussed in section 5.4.3.8 above. With such a hierarchy, the Root CA should not be network attached, but should be operated in a stand-alone manner given that this CA will only be issuing certificates for subordinate CAs. Each subordinate CA will need to be networked with a corresponding Registration Authority (RA).

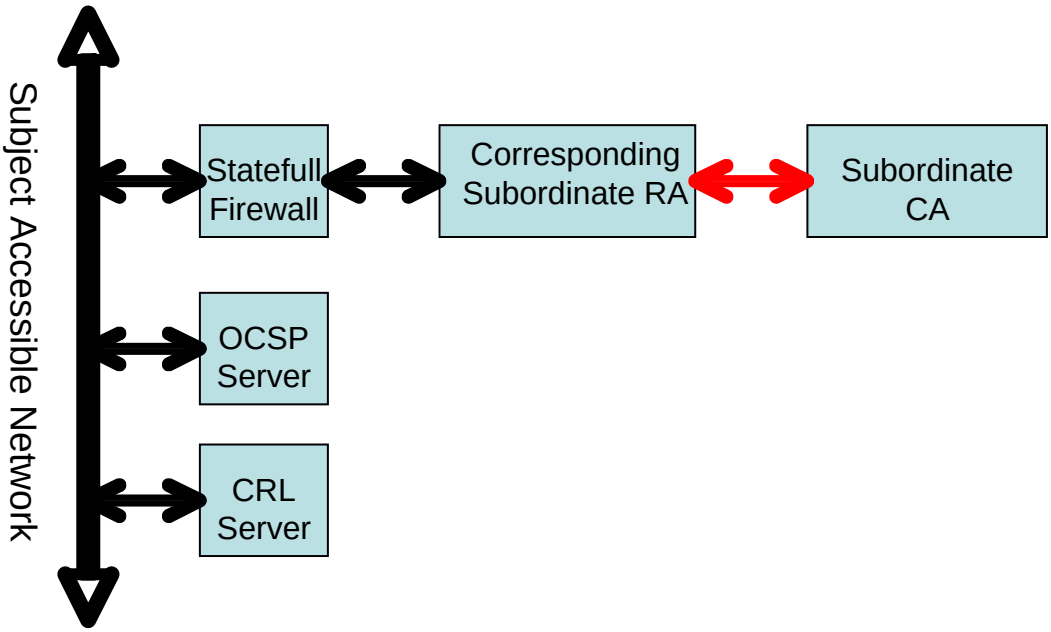

Figure 15 - Connectivity of RAs, CAs, OCSP and CRL Servers

Figure 15 above depicts how subordinate CAs are deployed where subject requests for certificates are sent to the associated RA after being inspected by an intervening firewall element. Once the RA has verified the validity of the certificate request, the RA will forward the request to the CA. Certificates generated by the CA travel back to the RA before being transmitted to the requesting subject. This deployment approach provides two layers of CA protection from network based attacks.

5.4.3.8.3 Certificate Revocation & status checking

The two primary approached for checking if a certificate has been revoked prior to its NotAfter date and time are to query:

- a CRL server and retrieve any certificate revocation lists posted by the certificate issuing CA via LDAP or
- an OCSP server as to the current status of the certificate in question via the OCSP protocol.

These servers should be highly available to all elements that use certificates when doing identity authentication. CRL support should be considered the default and OCSP the preferred approach.

5.4.4 Application Frameworks

Application frameworks, also frequently referred to as 'middleware' are used to provide a consistent set of services to distributed applications independent of the underlying operating systems and networking technologies used. Examples of such application frameworks are Java, Corba, Web Services and Microsoft .NET. Any use of such frameworks should be done in a manner consistent with framework security capabilities that instantiate the security services identified in section 5.4.1.3.1.2 for Ring 2 Service Functions and Ring 3 Application Functions, as well as section 5.4.2.4 for Application Layer protocol security.

5.5 Management of Security Mechanisms

Security management provides supporting services that contribute to the protection of information and resources in open systems in accordance with applicable trust domain and information system security policies.

5.5.1 Integrated Security Management

Security management requires management functionality within the Telecommunications Management Network (TMN) Services Management Layer (SML), which in the TSP environment is typically referred to as Operational Support System (OSS). The purpose of a Security Management OSS (a.k.a. Security Management System) is to manage the security mechanisms deployed throughout a TSP infrastructure. The necessary requirements for such Security Management Systems) are specified in ANSI standard ATIS-0300074.2006.

5.5.2 Securing management Related Communications

Another aspect of infrastructure management within the TMN is securing management traffic that flows between system elements within the:

Business Management Layer (BML)
Services Management Layer (SML)
Network Management Layer (NML)
Element Management Layer (EML)
Network Element Layer (NEL)

as well as across the five layers. ANSI standard ATIS-0300276.2008 specifies a minimally acceptable set of requirements for securing this management communication.

ANSI ATIS-0300276.2008 and ITU-T M.3016, do not exactly match the description of security services within this Technical Report as these two standards did not consider management communications as basically a set of targeted applications activities that must also reflect

different security needs depending on the type of interface said management activities occur over. The difference identified herein does not constitute any deficiency in securing management of security mechanisms.

5.5.3 Storage of Security Information

Security management is concerned with the management of security services and mechanisms. Such management requires distribution of management information to these services and mechanisms as well as the collection of information concerning the operation of these services and mechanisms.

The security management information base (SMIB) is the conceptual repository for all security relevant information. This concept does not suggest any form for the storage of the information or its implementation. However, each end system shall contain the necessary local information to enable it to enforce an appropriate security policy. The SMIB is a distributed information base to the extent that it is necessary to enforce a consistent security policy in a (logical or physical) grouping of end systems. In practice, parts of the SMIB may or may not be integrated with the MIB.

5.5.4 Security Management within Elements

Each deployed element includes some set of security mechanisms and therefore must also include a local mechanism for managing these local security mechanisms. Local security management functionality is typically embodied within the general management/administrative functions within the element, referred to herein as a Security Management Application Process (SMAP).

One or more elements within the same security domain may support a particular security service with more than one security mechanism, but it may not be known in advance of attempted communications which of these security mechanisms may be implemented in a specific element. In such cases, the specific security mechanisms to be employed must be negotiated between the SMAPs in the elements at the time a security association is established between them.

The invocation of security services and security mechanisms within an element involves several functions. Since all security services are security-critical, they should be accessible only within the kernel, and applications should invoke them only through a standard kernel interface. Since most applications will rely upon the operating system for use of this standard kernel interface, the use of the interface should be transparent to those applications. If a request for a security service does not specify a security mechanism, the SMAPs should make a choice among the available security mechanisms based on the security domain policy and invokes it through an appropriate operating system call. Otherwise, the SMAPs invokes the specified security mechanism.

5.5.4.1 Element Security Management Controls

Consistent with ITU-T X.800, element security mechanism management is concerned with the management of particular security mechanisms. The following list of security mechanism management functions is typical but not exhaustive:

- key management (for use with encryption, digital signature, data integrity, authentication and notarization mechanisms);
- encryption management;
- digital signature management;

- access control management;
- data integrity management;
- authentication management;
- traffic padding management;
- routing control management;
- notarization management;
- availability management.

5.5.4.1.1 Key Management

X.800 describes key management as follows:

> Key management may involve:
> - generating suitable keys at intervals commensurate with the level of security required;
> - determining, in accordance with access control requirements, of which entities should receive a copy of each key; and,
> - making available or distributing the keys in a secure manner to entity instances in real open systems.

Exchange of session keys for use during security association establishment and renegotiation within security protocols such as within IPsec IKE, TLS, DTLS and SSH. Key management functions for distribution of key distribution keys (master keys) and keys used in peer-entity authentication may be performed as part of a key management service such as a PKI.

TSP infrastructure element key management functionality should include the ability to securely store multiple sets of master keys (especially multiple asymmetric encryption private keys and associated X.509v3 certificate chains) as well as multiple shared secret keys used with symmetric encryption and 'keyed' hash based data origin authentication mechanisms. The element SMIB will be expected to support the ability to store security policy rules governing keys and their usage within a TSP security domain.

5.5.4.1.2 Encypherment (Encryption) Management

X.800 describes encryption management as follows:

> Encypherment management may involve:
> interaction with key management;
> establishment of cryptographic parameters; and,
> cryptographic synchronization.

Selection of cryptographic algorithms, parameters, synchronization and keys will typically be negotiated within the security association establishment and renegotiation mechanisms of security protocols such as within IPsec-ISAKMP, TLS, DTLS and SSH. These security protocols will require interaction with the element's key management functionality for access to master keys when a security protocol is performing peer entity authentication. The element SMIB will be expected to support the ability to store security policy rules governing encryption usage within a TSP security domain.

5.5.4.1.3 Digital Signature Management

X.800 describes digital signature management as follows:

> Digital signature management may involve:
> interaction with key management;
> establishment of cryptographic parameters and algorithms; and

use of protocol between communicating entities and possibly a third party.
Note: Generally, there exist strong similarities between digital signature management and encryption management.

When digital signatures support a non-repudiation service that relies upon a trusted third party, additional security management responsibilities may be required within the element with respect to long-term archiving of keys and algorithm identifiers so that transactions can be verified well after they occur. This additional capability will typically reside within the application functionality of an element. The element SMIB will be expected to support the ability to store security policy rules governing long-term archiving of keys and algorithm identifiers within a TSP security domain along with the actual storage of keys and algorithm identifiers used in transactions.

5.5.4.1.4 Access Control Management

X.800 describes access control management as follows:

> Access control management may involve distribution of security attributes (including passwords) or updates to access control lists or capabilities lists. It may also involve the use of a protocol between communication entities and other entities providing access control services.

The distribution of security attributes includes their initial installation in a SMIB. Since not all the information in a security domain SMIB is necessarily locally present in every element that is part of a TSP security domain, it may be necessary to distribute access control attributes between elements. TSP infrastructure elements should support of the use of standards based protocols, such as RADIUS, Diameter and SNMP, for the distribution, or retrieval, of access control attributes. Given the complex nature of the application functionality now residing on TSP elements, it is strongly recommended that the element implement Role-Base Access Control mechanisms (RBAC) for both general element and application specific access control. These elements should support secure reliable interaction with a TSP security management system within the TSPs security domain. The element SMIB will be expected to support the ability to store security policy rules governing access controls within the TSP security domain.

5.5.4.1.5 Data Integrity Management

X.800 describes data integrity management as follows:

> Data integrity management may involve:
> interaction with key management;
> establishment of cryptographic parameters and algorithms; and,
> use of protocol between communicating entities.

When using cryptographic techniques to support the data integrity service, similarities exist between data integrity management and encryption management. For information residing within an element, data integrity can be attained by use of strong access control mechanisms on memory and storage subsystems. When a strong communications data integrity service is required, reversible (symmetric) or non-reversible (hashing) cryptographic mechanisms are necessary. Selection of cryptographic data integrity mechanisms , parameters, and keys will typically be negotiated within the security association establishment and renegotiation mechanisms of security protocols such as within IPsec-ISAKMP, TLS, DTLS and SSH. The element SMIB will be expected to support the ability to store security policy rules governing both element internal and communications data integrity within the TSP security domain.

5.5.4.1.6 Authentication Management

X.800 describes authentication management as follows:

> Authentication management may involve distribution of descriptive information, passwords or keys (using key management) to entities required to perform authentication. It may also involve use of a protocol between communicating entities and other entities providing authentication services.

Authentication mechanisms rely upon particular authentication information (credentials) to validate a given identity. The authentication information against which user-supplied authentication information is verified is stored in the SMIB (where element data structures such as password files and registry heaps constitute part of the SMIB) and is subject to similar considerations as access control attributes. The element should provide support for peer-entity, data-origin and user login authentication, Selection of authentication mechanisms will typically be negotiated within the security association establishment and renegotiation mechanisms of security protocols such as within IPsec-IKE, TLS, DTLS and SSH. Element support for some form of security domain 'single-sign on' is highly desirable to reduce element user login account authentication workload. TSP infrastructure elements should support of the use of standards based protocols, such as RADIUS and Diameter for the distribution or retrieval, of authentication related information. These elements should support secure reliable interaction with a TSP security management system within the TSPs security domain. The element SMIB will be expected to support the ability to store security policy rules and information governing both local and remote authentication to elements within the TSP security domain.

5.5.4.1.7 Traffic Padding Management

X.800 describes traffic padding management as follows:

> Traffic padding management may include maintenance of the rules to be used for traffic padding. For example, this may include:
> pre-specified data rates;
> specifying random data rates;
> specifying message characteristics such as length; and
> variation of the specification, possibly in accordance with time of day and/or calendar.

Traffic padding in physical layer communications devices is often managed as a configuration parameter. In a TSP infrastructure, traffic padding in the physical layer will occur infrequently. Traffic padding in application layer protocols could be invoked as the result of a user request or as the result of a security domain security policy requirement applied to all or some class of communications. The critical management aspect of satisfying such a request is to assure that the padding is applied at the correct stage of processing with respect to other security services, such as data integrity or data confidentiality.

5.5.4.1.8 Routing Control Management

X.800 defines routing control management as follows.

> Routing control management may involve the definition of the links or sub-networks which are considered to be either secured or trusted with respect to particular criteria.

In a TSP infrastructure, routing control should be effected through the use of strong peer-entity and data-origin authentication of data link and internetworking signaling & control protocols used

to disseminate switching and routing information. This capability will require interaction between routing control, encryption and authentication management functions within the element.

5.5.4.1.9 Notarization Management

X.800 defines notarization management as follows.

> Notarization management may include:
> the distribution of information about notaries;
> the use of a protocol between a notary and the communicating entities; and
> interaction with notaries.

In a TSP infrastructure, notarization management is highly unlikely to be provided.

5.5.4.1.10 Availability Management

Availability management is not described in X.800. Availability management applies to:

- interactions within a TSP infrastructure or TSP infrastructure management facilities for notifications of outages and, if applicable, alternate service information, and
- for those TSP elements that interconnect with other security domains, the ability to contend with likely Denial-of-Service (DoS and distributed DoS) attack events.

The element SMIB will be expected to support the ability to store security policy rules and information governing the recognition of, logging information about, generation and distribution of alarms relative DoS/DDoS attacks targeting elements within the TSP security domain.

5.5.4.2 Element security information storage

Just as there is a need for an infrastructure wide SMIB, each element must also contain the necessary local information to enable it to enforce an appropriate security policy. The local SMIB is part of the distributed infrastructure. Element SMIBs contain information for management and use of security functions and resources within the element the use of which is required by the security domain security policy, including hardware resources, security-critical functions (particularly security services and mechanisms), and supporting applications (e.g., key management). The following example classes illustrate information objects included in the element SMIB:

End system security policy rules
Security services management information
Security mechanisms management information
Supporting services and mechanisms management information (e.g., alarm reporting, information system auditing, cryptographic key distribution, security contexts, security-critical functions, security-related applications operating for the element).

5.6 Certification, Auditing & Accreditation

This section provides general information on the existing certification and accreditations related to security and it relevance to industry participants (service providers, product developers, content developers).

The definition of *certification* used in this document is; *The process/technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements*.

The definition of *Auditing* used in this document is: *The examination of networks and computer systems by an independent consultant, within a defined scope which may include; determination of an organization's compliance to specified standards and best practices, determination of an organization's vulnerability to criminal invasion (crackers, virus impact on management, end-use and, control traffic on end-to-end solution etc.) and determination of an organization's vulnerability to natural disasters (fire, tornados, earthquakes, etc.)*

From a global industry perspective, the most well known examples of certification for quality, management, and security are the ISO/IEC 9000, ISO/IEC 14000, and ISO/IEC 27001 standards. ISO/IEC are publishers of standards and do not issue certifications of conformity to any standard. Certificates of conformity to specified standards are issued by certification/registration bodies, which are independent of ISO and of the businesses they certify. These registration bodies are accredited third parties which visit an organization to assess their management system which includes access to their processes, documentation and issue certificates to show the organization meets the intent of the standard.

Separately, product certification is specific to the business it is used in. Like other certifications, product certification provides users and regulators information that the certified product complies with the standard(s) specified on the certificate. Product certification may be limited to compliance with one or more standards even though the product may be subject to many standards.

From a United States Government perspective, there are a number of guidelines issued by NIST which discuss the process of certification for the civilian government agencies. These guidelines for the purpose of this document have been added as additional best practice references to consider when doing business with government agencies. Examples of such documents are NIST 800-37, Guide *for the Security Certification and Accreditation of Federal Information Systems* and the recent document NISTIR 7359 *Information Security Guide for Government Executives*.

An example of product type of certification recognized by the US government is known as the Common Criteria. The Common Criteria (CC) is an international standard (ISO/IEC 15408) for computer security. Common Criteria describes a framework in which the security requirements can be specified, implemented and evaluated by the users, vendors and testing laboratories respectively. This product certification allows the user to know that the requirements specified by vendors or users are met in implementations.

The CC is an international initiative where US organizations NIST and NSA are participants. It is considered to be in alignment with, and consistent with, development of the existing European, US, and Canadian criteria (ITSEC, TCSEC, and CTCPEC respectively).

Whereas *certification* is appropriate for certain Government Applications (e.g., common Criteria/ EAL), *auditing* is appropriate for networks and the service they support. Auditing may be initiated by a service provider at the behest of a client, or on their own initiative, to determine the extent to which they meet specified standards and best practices and to determine vulnerability to security threats. The audit would typically be carried out by a third party to ensure a degree of independence from the service provider.

The audit process provides a snapshot of security status at the time of examination and it is specific to the defined scope, technology, and processes under consideration. Industry participants may use the results of an audit as a vehicle to demonstrate to their customers, staff

or investors that their network and services comply with specified standards and best practices, and are secure against identified (tested) threats.

5.6.1 Common Criteria

The issue of certification in the context of the CC has value in that a CC security assessment performed by an independent evaluator may be perceived as more objective than a product developer evaluation. Furthermore, if the independent evaluation organization has been accredited by a respected third party as having sufficient expertise and a rigorous evaluation process (perhaps is ISO 9001 certified) then the evaluation results have increased validity. Also see section 4.7.2.3.4.

5.6.2 Capability Maturity Model

The issue of certification in the context of the CMMI is of most use when bidding on a government contract that requires CMMI certification. Also see section 4.4.2.

5.6.3 ISO 9000

ISO does not itself certify organizations. Many countries have formed accreditation bodies to authorize certification bodies, which audit organizations applying for ISO 9001 compliance certification. It is important to note that it is not possible to be certified to ISO 9000. Although commonly referred to as ISO 9000:2000 certification, the actual standard to which an organization's quality management can be certified is ISO 9001:2000. Both the accreditation bodies and the certification bodies charge fees for their services. The various accreditation bodies have mutual agreements with each other to ensure that certificates issued by one of the Accredited Certification Bodies (CB) are accepted world-wide.

The applying organization is assessed based on an extensive sample of its sites, functions, products, services, and processes and a list of problems ("action requests" or "non-compliances") made known to the management. If there are no major problems on this list, the certification body will issue an ISO 9001 certificate for each geographical site it has visited, or if there are existing problems it will issue it once it receives a satisfactory improvement plan from the management showing how any problems will be resolved.

An ISO certificate is not a once-and-for-all award, but must be renewed at regular intervals recommended by the certification body, usually around three years. In contrast to the Capability Maturity Model there are no grades of competence within ISO 9001.

Two types of auditing are required to become registered to the standard ISO 9001: auditing by an external certification body (external audit) and audits by internal staff trained for this process (internal audits). The aim is a continual process of review and assessment, to verify that the system is working as it's supposed to, find out where it can improve, and to correct or prevent problems identified. It is considered healthier for internal auditors to audit outside their usual management line, so as to bring a degree of independence to their judgment. The ISO 9011 standard for auditing applies to ISO 9000.

TSPs certified as conforming to ISO 9001 by an independent organization provides additional assurance to the TSPs customers, the industry as a whole and other interested parties that the TSP has truly made a 'good faith' effort at conformance and is not making false compliance claims. However TSP certification should remain a voluntary activity given the commercial competitive environment in which TSPs operate.

5.6.4 Generally Accepted Information Security Practices (GAISP)

It is premature to discuss certification or accreditation in the context of the GAISP at this time given the evolving state of the GAISP. Upon GAISP finalization this subject should be revisited

5.6.5 ISO 27001/27002

Organizations may be certified ISO 27001 compliant by a number of accredited certification bodies worldwide. ISO 27001 certification usually involves a two-stage audit process:

Stage 1 is a "table top" review of the existence and completeness of key documentation like the Security Policy, Statement of Applicability, Information Security Management System (ISMS).

Stage 2 is a detailed, in-depth audit involving testing the existence and effectiveness of the controls stated in the ISMS as well as their supporting documentation.

Certification involves periodic reviews to confirm that the ISMP continues to operate as intended.

For TSPs being certified as conforming to ISO 27001 by an independent organization provides additional assurance to the TSPs customers, the industry as a whole and other interested parties that the TSP has truly made a 'good faith' effort at conformance and is not making false compliance claims. However TSP certification should remain a voluntary activity given the commercial competitive environment in which TSPs operate.

Appendix A: Security 'Best Practices'

A.1 NRIC/NSTAC

The following has been extracted from an ATIS Security Focus Group Work Plan[18] and is included verbatim.

> "APPENDIX E: NRIC Best Practices
>
> The following contains text from the NRIC VI Homeland Security Physical Security Final Report, , December 2003, Karl F. Rauscher, Lucent Technologies, Bell Labs.
>
> For over a decade, the FCC Network Reliability and Interoperability Council (NRIC) Best Practices have been recognized as the most authoritative guidance in the world for optimizing the reliability of communications networks. They result from broad industry cooperation that engages vast expertise and considerable voluntary resources. Nowhere else in the world has such a broad range of communications industry expertise come together to so rigorously examine the approaches, effectiveness, risks, and costs, as within NRIC.[19] The most recent Council had turned its focus on Homeland Security.
>
> The primary objective of Best Practices is to provide guidance from assembled industry expertise and experience. This guidance is highly valuable because it is not easy to duplicate on an individual company basis. A detailed description of the NRIC Best Practices' intended use, ease of access, management by keywords, and other information is provided in the body of the report.
>
> The Best Practices, while not industry requirements or standards, are highly recommended for implementation. As the First Council stated, "Not every recommendation will be appropriate for every company in every circumstance, but taken as a whole, the Council expects that these findings and recommendations [when implemented] will sustain and continuously improve network reliability." This statement can now be extended to include security. NRIC Best Practices result from broad industry cooperation that engages vast expertise and considerable voluntary resources. Efforts by government authorities to impose these as regulations may jeopardize the industry's willingness to work together to provide such guidance in the future.
>
> In developing Best Practices, it is recognized that the degree to which Best Practices and recommendations are implemented is significantly dependent upon Business Continuity Plans and the enterprise's risk assessments plans as a result, which include the appropriate business case, and that decisions to implement and implementation levels will vary from organization to organization. While one hundred percent implementation of all security Best Practices by all companies is clearly not attainable, an optimal balance of Best Practice adoption, in conjunction with incentives for industry to implement (e.g., government resources, research, support), can maximize the level of security across all industry segments, particularly with respect to meeting critical Homeland and National security needs.

---

[18] ATIS Security Issues Work-Plan to Achieve Interoperable, Implementable, End-To-End Standards and Solutions April 20, 2004

[19] Network Reliability Best Practices Final Report, Network Reliability and Interoperability Council V; January 2002.

Physical and Cyber Security

The security Best Practices work was divided into cyber and non-cyber categories. Neither the world nor the potential threats against the communications infrastructure are divided neatly into two such categories. In addition, it was understood that there are very complex interactions between the two domains. In order to ensure that issues did not “fall between the cracks,” special Blended Physical and Cyber Attack analysis was conducted and additional Best Practices were defined.

Checklists

Checklists are shortcuts that allow a user to quickly find applicable, suggested action items, and were first introduced for Best Practices under the Fifth Council with the provision of Keywords in an effort to make the Best Practices easier to use. Keywords are provided to allow an individual to identify the Best Practices associated with a particular job function. The checklists can be generated via the NRIC web site <http://www.nric.org >.

Best Practices Principles[20]

Best Practices are statements that describe the industry’s guidance to itself for the best approach to addressing a concern. The following principles are helpful in understanding how Best Practices are distinct from standards or regulations.

The implementation of specific Best Practices is intended to be voluntary. In addition, the applicability of each Best Practice for a given circumstance depends on many factors that need to be evaluated by individuals with appropriate experience and expertise in the area the Best Practice is addressing.

1. “People Implement Best Practices"[21]: The Best Practices are intended for daily use by the many thousands of individuals who support the communications infrastructure. To this end, the Best Practices address the following four values:
   - Applicability of Best Practices to Individual Job Functions
   - Appreciation for the Value of Best Practices
   - Accessibility to Appropriate Best Practices
   - Continuous Improvement of Best Practices[22]

   Even though NRIC Best Practices have been developed to be easily understood, their essence is often not immediately apparent to those who are inexperienced with the associated job functions.[23] Therefore, caution should be taken to ensure that those managing Best Practices within organizations have sufficient experience.
2. Best Practices do not endorse commercial or specific "pay for" documents, products or services, but rather stress the essence of the guidance provided by such (e.g., formal quality management vs. "TL9000") practices. Helpful examples are identified in the "References Columns" available on the web site. This is a place that can be enhanced with the addition of more standards references.
3. Best Practices are more effective and appropriate when they address (help prevent, mitigate, etc.) classes of problems. Detailed fixes to specific problems are not Best Practices.

---

[20] The term “Best Practices” is capitalized when referring to specific NRIC Best Practices.

[21] Richard P. Harrison, various tutorials on NRIC Best Practices, 1993-1999.

[22] Section 7, NRIC V Best Practices Subcommittee Final Report, January 2002.

[23] The Keywords provide associations between job functions and Best Practices.

4. Best Practices are already implemented by some, if not many, companies. Many fascinating and impressive ideas can be generated by the highly regarded list of organizations assembled for this effort. However, such ideas do not qualify as Best Practices if no one is "practicing them." The recommended Best Practices being provided to the industry in this document have been demonstrated to be effective, feasible, and capable of being implemented.
5. Best Practices are developed by industry consensus. In particular, the parties with "skin in the game" (i.e., Service Providers, Network Operators, Equipment Suppliers) are able to bring their expertise from across the industry to weigh in on the "best" approach to addressing a concern.
6. Best Practices are verified by a broader set of industry members – from outside the Focus Group - to ensure that those who have not been a part of the process can provide feedback. An industry survey is planned for 2003.
7. Best Practices are presented to the industry only after sufficient rigor and deliberation has warranted the inclusion of both the conceptual issue and the particular wording of the practice. Discussions among experts and stakeholders include consideration of:
    - Existing implementation level of a proposed Best Practice.
    - Effectiveness of a proposed Best Practice.
    - Feasibility to implement a proposed Best Practice.
    - Risk not to implement a proposed Best Practice.
    - Alternatives to the proposed Best Practice.

Coordination with Other Stakeholders

Like other industries, the communications industry has received numerous requests to provide support to Homeland Security efforts. In order to avoid unnecessary duplication of effort and to better realize synergies, the leaders of NRIC and other key entities have appropriately agreed to coordinate their activities. In addition, the focus groups participated in the Steering Committee's aggressive national outreach program.

Government and industry stakeholders include the following organizations and their constituents:

- Alliance for Industry Solutions (ATIS)
    - Network Reliability Steering Committee (NRSC)
- American National Standards Institute (ANSI)
- American Society for Industrial Security International (ASIS)
- Association of Public Safety Communications Officials (APCO)
- Cellular Telecommunications and Internet Association (CTIA)
- Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP Commission)[24]
- Financial Services Roundtable (BITS)
- Institute of Electrical and Electronics Engineers (IEEE)
    - Communications Society (COMSOC)

[24] The EMP Commission was established by Congress under the provisions of the Floyd D. Spence Defense Authorization Act of 2001, Public Law 106-398, Title XIV. The EMP Commission was chartered to conduct a study of the potential consequences of a high altitude nuclear detonation on the domestic and military infrastructure, and to issue a report containing its findings and recommendations to the Congress, the Secretary of Defense, and the Director of FEMA.

  - Technical Committee on Communications Quality & Reliability (CQR)
- International Engineering Consortium (IEC)
- National Association of (NARUC)
- National Institute of Standards and Technology (NIST)
- National Public Safety Telecommunications Council (NPSTC)
- National Telecommunications and Information Administration (NTIA)
- North American Network Operators' Group (NANOG)
- Organization for the Promotion and Advancement of Small Telecommunications Companies (OPATSCO)
- President's National Security Technical Advisory Council (NSTAC)
- Upper Great Lakes Transmission Coalition (UGPTC)
- United States Congress
- United States Department of Homeland Security
  - National Communications System (NCS)[25]
  - National Coordinating Center for Telecommunications (NCC)
  - Telecom ISAC (Information Sharing and Analysis Center)
- United States Telecommunications Association (USTA)
- White House Office of Homeland Security
- Wireless Emergency Response Team (WERT)
- Wireless Infrastructure Association (PCIA)

. . . and numerous industry conferences, and state and local governments.

Systematic Vulnerability Approach

The Mission of the Physical and Cyber Security Focus Groups directed these groups to "assess vulnerabilities" of the communications infrastructure. An approach that focuses on vulnerabilities was emphasized at the Sixth Council's first meeting.[26] Comparisons have been made between the common approach of many industries to learn mostly from past historic events, with an approach that addresses all vulnerabilities – regardless of whether or not a specific vulnerability has been exercised by a threat before. The prime example that articulates the distinction is the cockpit door in aircraft, which previous to September 11, 2001 had been identified by the aviation industry as a security vulnerability. But since the cockpit door had not been previously exercised by a threat, it was not addressed. An approach that systematically addresses vulnerabilities is vital to effectively protecting the communications infrastructure. The communications infrastructure is one of the pillars of pillars among critical infrastructures.[27]

Prior to the Sixth Council, NRIC's Best Practices were developed from an historic analogy perspective. This meant that Best Practices were developed to address past events (i.e., outages), using the industry's expertise developed from analyzing these events. A vulnerability perspective was introduced in the work of the Fifth Council's Best Practices

[25] Effective March 1, 2003, the NCS officially transitioned into the new Department of Homeland Security under the Information Analysis and Infrastructure Protection (IAIP) Directorate.

[26] Richard A. Clarke, Chair - President's Critical Infrastructure Protection Board, Comments at NRIC VI Council Meeting, March 22, 2002. FCC Commission Meeting Room, Washington, D.C.

[27] John Tritak, Director - Critical Infrastructure Assurance Office (CIAO), Comments at NRIC VI Council Meeting, March 22, 2002. FCC Commission Meeting Room, Washington, D.C.

Subcommittee.[28] The IEEE Communications Society Technical Committee on Communications Quality & Reliability (CQR) outlined characteristics of the Packet Switched Public Telecommunications Network Services (PSPTNS) that have, or can potentially have, a negative impact on the reliability of such services. The Best Practices Subcommittee used this outline as a high level Checklist to evaluate the Best Practices coverage. An NRIC V Area for Attention was "the observation that the NRIC Best Practices address aspects of each of the areas identified in the Checklist."[29]

Vulnerabilities and Threats [30]

The major benefit of systematically addressing the Vulnerabilities is that protection is provided, independent of knowing what the threats may be. While the fundamental Vulnerabilities of the communications infrastructure seldom change, the types of Threats that can exercise those vulnerabilities are constantly changing.

"One fact dominates all homeland security assessments: terrorists are strategic actors. They choose their targets deliberately based on the weaknesses they observe in our defenses and our preparedness. We must defend ourselves against a wide range of means and methods of attack. Our enemies are working to obtain chemical, biological, radiological, and nuclear weapons for the purpose of wreaking unprecedented damage on America.

Terrorism depends on surprise. With it, a terrorist attack has the potential to do massive damage to an unwitting and unprepared target."[31] [emphasis added]

While the industry can be surprised by the method of a particular attack, it should not be surprised about our Vulnerabilities. The industry designed and built these systems and networks. The industry knows their intrinsic properties . . . and their limitations. The systematic vulnerability approach covers the fundamental characteristics for each aspect of the communications infrastructure that are susceptibilities exercisable by attacks. By systematically addressing the vulnerabilities we are able to indirectly prepare for any number of unknown Threats attempting to exercise those vulnerabilities.

A.2 NIST[32]

Below are security-related Special Publications:

Draft SP 800-104 Draft Special Publication 800-104A, A Scheme for PIV Visual Card Topology

Draft SP 800-103 Draft Special Publication 800-103 An Ontology of Identity Credentials, Part I: Background and Formulation

Draft SP 800-101 Draft Special Publication 800-101, Guidelines on Cell Phone Forensics

---

[28] Section 5.4, Network Reliability and Interoperability Council V Subcommittee 2A.2, Network Reliability Best Practices Final Report.

[29] Ibid. The high level list included Hardware, Firmware, Software, Protocols, Interoperability, Human Performance and Procedures, Physical Environment, Network Design and Planning, Network Congestion/Traffic Engineering, Power, Rapid Pace of Growth, Change, Complexity, Malicious Attacks, Security, Disasters. Note that this NRIC VI Focus Group recognized some of these as Threats, as distinct from Vulnerabilities.

[30] The terms Vulnerabilities and Threats are capitalized in this document when they refer to a specific list.

[31] National Strategy for Homeland Security, Office of Homeland Security, July 2002, Executive Summary, pages vii-viii.

[32] These documents are available at the National Institute of Standards and Technology (NIST) at < http://www.itl.nist.gov/fipspubs/ >.

SP 800-100	Information Security Handbook: A Guide for Managers
SP 800-98	Draft Special Publication 800-98, Guidance for Securing Radio Frequency Identification (RFID) Systems
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
SP 800-96	PIV Card / Reader Interoperability Guidelines
Draft SP 800-95	Draft Special Publication 800-95, Guide to Secure Web Services
SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)
SP 800-92	Guide to Computer Security Log Management
SP 800-90	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-88	Guidelines for Media Sanitization
SP 800-87	Codes for the Identification of Federal and Federally-Assisted Organizations
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-85B	PIV Data Model Conformance Test Guidelines
SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)
SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800-83	Guide to Malware Incident Prevention and Handling
Draft SP 800-82	Draft NIST Special Publication 800-82, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
Draft SP 800-80	Draft Special Publication 800-80, Guide for Developing Performance Metrics for Information Security
SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
Draft SP 800-78-1	Draft Special Publication 800-78-1, Cryptographic Standards and Key Sizes for Personal
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-77	Guide to IPsec VPNs
SP 800-76-1	Biometric Data Specification for Personal Identity Verification
SP 800-73	Revision 1 Interfaces for Personal Identity Verification
SP 800-72	Guidelines on PDA Forensics
SP 800-70	Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers

SP 800-69	Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process
SP 800-64	Security Considerations in the Information System Development Life Cycle
SP 800-63	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
SP 800-61	Computer Security Incident Handling Guide
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-59	Guideline for Identifying an Information System as a National Security System
SP 800-58	Security Considerations for Voice Over IP Systems
SP 800-57	Recommendation for Key Management
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-55	Security Metrics Guide for Information Technology Systems
Draft SP 800-54	Draft Special Publication 800-54, Border Gateway Protocol Security
Draft SP 800-53A	Draft Special Publication 800-103 An Ontology of Identity Credentials, Part I: Background and Formulation
SP 800-53	Rev. 1 Recommended Security Controls for Federal Information Systems
SP 800-53	Annex 1: Baseline Security Controls for Low-Impact Information Systems
SP 800-53	Annex 2: Baseline Security Controls for Moderate-Impact Information Systems
SP 800-53	Annex 3: Baseline Security Controls for High-Impact Information Systems
SP 800-53	Recommended Security Controls for Federal Information Systems
SP 800-52	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-50	Building an Information Technology Security Awareness and Training Program

SP 800-49	Federal S/MIME V3 Client Profile
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45	Version 2 Guidelines on Electronic Mail Security
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-43	Systems Administration Guidance for Windows 2000 Professional
SP 800-42	Guideline on Network Security Testing
SP 800-41	Guidelines on Firewalls and Firewall Policy
Draft SP 800-38D	Draft Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
SP 800-38A	Recommendation for Block Cipher Modes of Operation - Methods and Techniques
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-35	Guide to Information Technology Security Services
SP 800-33	Underlying Technical Models for Information Technology Security
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-31	Intrusion Detection Systems (IDS)
SP 800-30	Risk Management Guide for Information Technology Systems
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-27	Rev. A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A
Draft SP 800-26	Rev. 1 NIST DRAFT Special Publication 800-26, Revision 1: Guide for Information Security Program Assessments and System Reporting Form
SP 800-26	Security Self-Assessment Guide for Information Technology Systems
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication

SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-21-1	Second Edition, Guideline for Implementing Cryptography in the Federal Government
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
SP 800-19	Mobile Agent Security
SP 800-18	Rev. 1 Guide for Developing Security Plans for Federal Information Systems
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172)
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-12	An Introduction to Computer Security: The NIST Handbook

A.3 IETF[33]

Below are security-related BCP Requests for Comments:

RFC 2350 (BCP 0021) Expectations for Computer Security Incident Response

RFC 2827 (BCP 0038) Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

RFC 3013 (BCP 0046) Recommended Internet Service Provider Security Services and Procedures

RFC 3704 (BCP 0084) Ingress Filtering for Multihomed Networks

Other BCPs can be found on the http://www.rfc-editor.org/categories/rfc-best.html

[33] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

A.4 ITU

The ITU-T does not publish document that explicitly present security 'best practices'. However the ITU-T handbook "Security in Telecommunications and Information Technology" provides 'an overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications'.

Appendix B - Current Security Capabilities by Protocol

The following sections depict the authentication, confidentiality and key management mechanisms either mandated within each protocol or as optional intrinsic protocols or augmentations. Also provided is information on optional mechanisms available to compensate for deficiencies within the basic protocols. Note that this is not intended to be an exhaustive list.

B.1 Layer 2 (Data Link) Protocol Security Capabilities

The following table depicts the more common protocols used within layer 2.

Table 33 - Layer 2 (Data Link) Protocol Security Capabilities

Protocol	Described in	Usage	Mandatory Authentication / Confidentiality Mechanism(s) & Key Management		Optional Authentication / Confidentiality Mechanism(s) & Key Management	
			Strength	Scaleable	Strength	Scaleable
WDM & Sonet Supervisory	ISO	Signaling & Control (S&C)	None	No	None	No
803.1q	IEEE 802.1q	VLANs	None	No	Low (clear-text password)	No
					High (Keyed MD5)	No
802.1x	IEEE 802.1x	L2 port control	High (Option 90 w/ RADIUS)	Only via RADIUS admin	n/a	n/a
802.11a, b (WEP)	IEEE	Wireless LANs	Low (shared key) broken implementation	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
802.11g (WPA)	Wi-Fi Alliance	Wireless LANs	High (802.1x, AES)	Only via RADIUS admin	Low (p-phrase based pre-shared key)	No
802.11i (WPA2)	IEEE	Wireless LANs	High (802.1x, AES)	Only via RADIUS admin	Low (p-phrase based pre-shared key)	No
CR-LDP	IETF RFCs	Logical private networking at layer 2 or sub-L3	None	No	Keyed MD5	No
					High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
RSVP-TE	IETF RFCs	Logical private networking at layer 2 or sub-L3	None	No	Keyed MD5	No
					High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)

B.2 Layer 3 (Networking) Protocol Security Capabilities

The following table depicts the more common protocols used within layer 3.

Table 34 - Layer 3 (Networking) Protocol Security Capabilities

Protocol	Described in	Usage	Mandatory Authentication / Confidentiality Mechanism(s) & Key Management		Optional Authentication / Confidentiality Mechanism(s) & Key Management	
			Strength	Scaleable		
IPv4	RFC 791	Packet Forwarding	None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
ARP	RFC 826	MAC to IPv4 address resolution	None	No	None	No
DHCP	RFC 2131, RFC 3118, RFC 3456, RFC 4030	IPv4 address assignment	Low / None	No	High (Option 90 w/ RADIUS)	Only via RADIUS admin

On IPv4 based network segments, ARP provides no security and can even serve as a component in Denial-of-Service (DoS) and IP address spoofing attacks.

B.3 Layer 4 (Transport) Protocol Security Capabilities

The following table depicts the more common protocols used within layer 4.

Table 35 - Layer 4 (Transport) Protocol Security Capabilities

Protocol	Described in	Usage	Mandatory Authentication / Confidentiality Mechanism(s) & Key Management		Optional Authentication / Confidentiality Mechanism(s) & Key Management	
			Strength	Scaleable	Strength	Scaleable
TCP	RFC 793	End-to-end reliable transport	None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
					High (TLS)	Yes (PKI)
					High / None (Keyed MD5)	No
UDP	RFC 768	End-to-end best-effort transport	None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
SCTP	RFC 2960, RFC 4895	End-to-end reliable transport	High (IPsec IKE and ESP)	High (IPsec IKE and ESP)	High (HMAC-SHA-1)	n/a

B.4 General Application Protocol Security Capabilities

The following table depicts the more common application protocols.

Table 36 - General Application Protocol Security Capabilities

Protocol	Described in	Usage	Mandatory Authentication / Confidentiality Mechanism(s) & Key Management		Optional Authentication / Confidentiality Mechanism(s) & Key Management	
			Strength	Scaleable	Strength	Scaleable
FTP	RFC 2228, RFC 4217	File Transfer	Low / None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
			Low / None	No	High (SSH)	Yes (PKI)
TFTP	RFC 1350	File Transfer	None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
TELNET	Numerous RFCs	Remote Login	Low / None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
			Low / None	No	High (SSH)	Yes (PKI)
HTTP	RFC 1945	HTML document transfer	Low / None	No	High (MD5)	No
			Low / None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
X	RFC 1013	Remote Login	Low / None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
rpc	RFC 1831	Remote Execution	Low / None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
H.323	ISO H.323	Voice over IP Signaling	Low / None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
SIP	RFC 3261	Voice over IP Signaling	Low / None	No	High (MD5)	No
			Low / None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
RTP, SRTP	RFC 3550, RFC 3711	Voice/Video over IP Media	None High (HMAC-SHA1, SDES/MIKEY)	No High (AES-CM, SDES/MIKEY)	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI) Yes (AES-f8, SDES/MIKEY)
(G-)MPLS	Numerous RFCs	L2 & L3 MPLS	Low / None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
BGP,OSPF, …	Numerous RFCs	L3 Routing Control	Low / None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
others						

SRTP can provide end-to-end confidentiality, however there might be some instances where SRTP might be barred due to varying national or international laws.

B.5 Management Application Protocol Security Capabilities

The following table depicts the more common management protocols.

Table 37 - Management Application Protocol Security Capabilities

Protocol	Described in	Usage	Mandatory Authentication / Confidentiality Mechanism(s) & Key Management		Optional Authentication / Confidentiality Mechanism(s) & Key Management	
			Strength	Scaleable		
SNMPv1	RFC 1157	Element management	None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
SNMPv2	RFC 1446	Element management	Medium & None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
SNMPv3	RFC 3414, RFC 3415, RFC 3826	Element management	High & High	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
CORBA	OMG Specifications	Distributed applications	None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
			None	No	High (SSH, TLS)	Yes (PKI)
TL1	Bellcore/Telcordia specifications	Remote management	Low & None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
NTP	RFC 1305	Network Time	None	No	High (keyed MD5) & None	No
LDAP	RFC 4510, RFC 4512, RFC 4513	Directory access	Low & None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
DNS	RFC 4033, RFC 4034, RFC 4035, RFC 4470	Domain Name Service	None	No	High (IPsec IKE and ESP)	Yes (IPsec IKE and PKI)
XML	WWW Consortium specifications	Multiple Applications	None	No	High (xml signatures, xml encryption)	Yes (xmlkeymgt)
…						

Appendix C - Voice over IP Security Use Case

This high level VoIP use case illustrates how the methodology described in this document can be helpful in designing a secure network. The security life-cycle spans across many phases from project initiation to decommissioning as shown in Figure 16. Key aspects of the security life cycle are listed below:

- Conceptual definition,
- Functional requirements,
- Functional specifications,
- Design,
- Implementation,
- Test,
- Periodic Audits/ Maintenance,
- Decommissioning.

The high level VoIP Use case focuses mainly on the planning, design, and development of security architecture based on the standards described in the document.

C.1 Voice over IP Context Use Case

This use case does not constitute a specification for any particular information system or component. Rather, it describes security principles and target security capabilities that can guide VoIP security architects in creating a security architecture that is based on the standards.

The security aspects of the Use case relate to the shaded boxes shown in Figure 16. The focus is on how the security architecture is developed to meet the policy, standards and guidelines. For simplicity, this Use case does not discuss deployment, maintenance/ verification and decommissioning phases in detail.

Assumptions for the Use case are as follows:

- The use case is not targeted towards any particular technology or vendor or service provider's implementation.
- The use case does not recommend any particular information system or component. Rather, it illustrates the target security capabilities that are consistent with the appropriate standards described in this document.
- Both end-to-end and/ or hop-by-hop security may be acceptable for VoIP based on the access/transport and peering arrangements. When hop-by-hop security is implemented, Network & Service providers ensure the security of VoIP traffic within their network.
- The threats and vulnerabilities listed are for example purpose only and they are not intended to be a comprehensive list of all known or potential VoIP security issues.

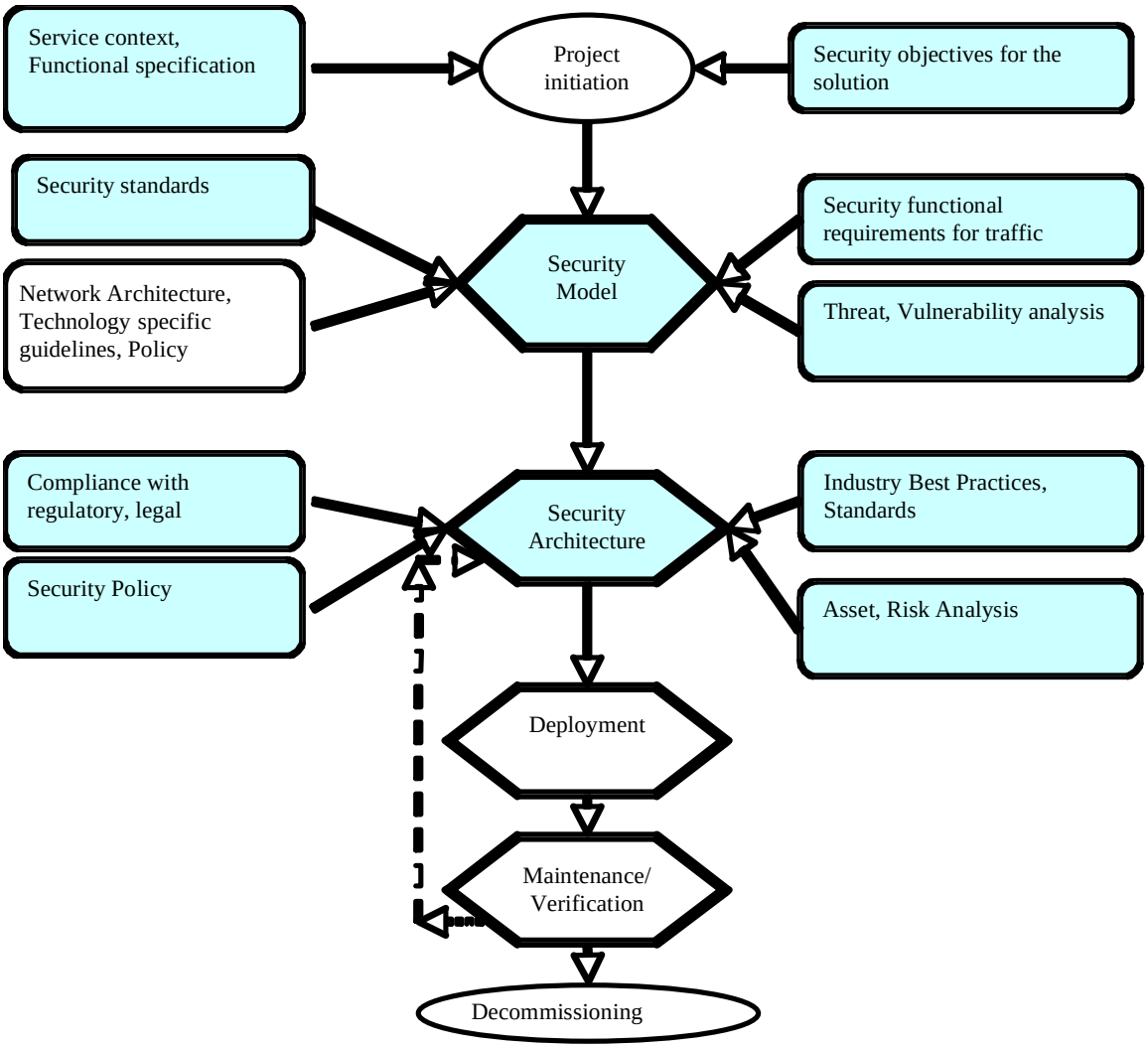

Figure 16- Project Security Phases

C.1.1 Service Context

VoIP service security should include protecting the end-user data and ensuring the availability of the service for its intended use. The set of pre-defined critical OAM&P assets, functions, TSP network elements, and interfaces should be secured to ensure the VoIP service availability. Thus, the goals of the service are to provide:

- high availability
- secure interfaces with other networks (e.g. PSTN and other TSPs)
- prevent fraud, theft of services, and loss of revenue
- secure relevant types of user, management and control information to protect the confidentiality and integrity of relevant information objects
- support legal requirements such as Lawfully Authorized Electronic Surveillance, and Communications Assistance for Law Enforcement Act (LAES/CALEA)

This VoIP use case applies the security systems engineering methodology of this Technical Report to identify the necessary security services, mechanisms and life-cycle processes to be implemented as well as develop an appropriate security architecture. When properly implemented and operated, these mechanisms and processes will help to protect the TSP assets as per the security policy, service and legal compliance requirements.

Figure 17 shows a generic representation of the VoIP service between two users “Alice” and “Bob.”. The end-to-end VoIP service can involve multiple TSPs, however the example scenario in Figure 17 shows one TSP.

There are many different technologies that can be used to implement customer premises and TSP Access networks. For example, the TSP Access network can be implemented by using 2/Wire, xDSL, Cable, Fiber to the curb (FTTC), Fiber to the Premises/Home (FTTH) or wireless technologies and associated customer premises devices. The details of access technology specific issues are not discussed in this document as the case study deals with generic security aspects of VoIP that are common to many of these technologies.

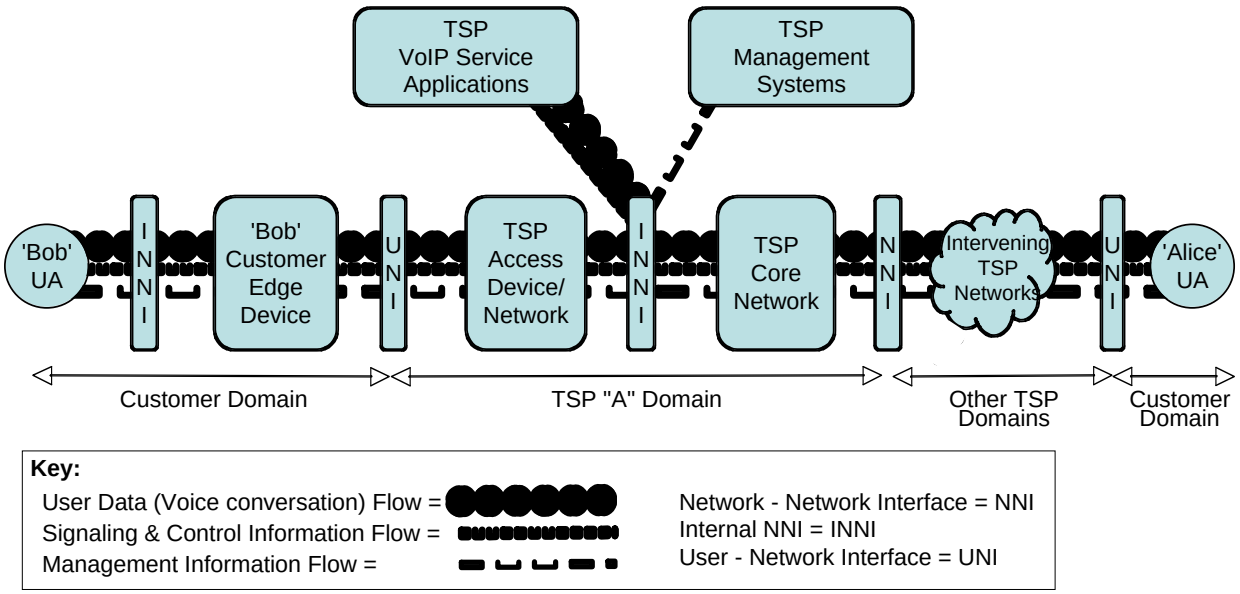

Figure 17 - Generic Architecture for Use Case

C.1.2 Security Policies

Security policy guidelines should cover the different domains ("Bob" Customer Premise, Service Provider "A" and "Alice" Customer Premise) shown in Figure 17 above. This Use Case addresses these issues from a TSP-A point of view. How one should go about developing security policies is dealt with in XXX. The list below shows the areas that this use case security policy protects:

- Enforcing customer access to only authorized features so that the actions of one customer cannot interfere with service availability to, or information about, other customers
- Maintaining the confidentiality and integrity of system information be it signaling & control or OAM&P related,
- Enforcing operations personnel access to those system attributes based on an authorized 'need-to know' basis,

By applying the concepts in 4.5, a policy would result in a set of documents describing the policy requirements relating, but not limited, to:

1) VoIP User data protection
2) Threat impact containment and minimization
3) Separation of management traffic from other network traffic
4) Customer service and help desk security
5) Authentication and access control requirements to interface with other TSP
6) Fraud prevention, reporting and handling
7) Security event management and Incident response
8) Organizational roles and responsibilities
9) Security audits
10) Patch updates
11) Physical security

C.2 Regulatory and Legislative

VoIP networks should comply with Communications Assistance for Law Enforcement Act (CALEA) of 1994. This law applies to both telecommunications and information services provided by TSPs. Therefore every TSP shall implement intercept, mediation and distribution mechanisms that allow for intercepting subscriber communications for delivery to LEAs subject to court orders. The requirements necessitate a TSP being able to strictly control who may know about or receive intercept related information or even know about and control intercept activities. This will require implementation of access control, confidentiality, integrity, privacy and no-repudiation security measures to carry out CALEA operations.

C.3 Network Assets, Vulnerabilities and Threats

The types of assets to be secured, and the vulnerabilities and threats which can impact the security of these assets, are discussed herein. The assets can belong to users (human), network elements (machine) and applications (information). A TSP also has intangible assets as in reputation, name recognition and intellectual property. The subsections provide a partial enumeration of subjects.

C.3.1.1 Human Subjects

A VoIP service infrastructure interacts with Human Subjects that belong to the following domains.

1) Customer Domain service users and administrators.
2) Government Domains including Law Enforcement personnel intercept service users.
3) Peering Service Provider Domain OAM&P Personnel.
4) TSP OAM&P Personnel.

Note that a human may belong to multiple domains but not at any given instant in time.

C.3.1.2 Machine Subjects

The VoIP service infrastructure includes, and interacts with Machine Subjects that belong to either Customer, a TSP Peer or the TSP security domains.

1) Customer Domains:
   a. VoIP User Agents (UAs) (such as an IP Phone, PC)
   b. Home Gateways (such as a broadband Home Router)
2) Government Domains:
   a. VoIP User Agents (UAs) (such as an IP Phone, PC)
   b. Intercept Reception Systems
3) Peering Service Provider Domains:
   a. VoIP Application elements (such as Proxies, SBC, IPS, SoftSwitches, feature servers)
   b. Transport elements (such as Switches, Routers, ROADMS, ADMs, WDM)
   c. Service Control elements (such as dynamic directory, time, configuration and authentication/authorization Servers)
   d. OAM&P elements (such as E/N/SML OSSs and Server Systems along with OAM&P workstations)

4) TSP (Sub-)Domain(s):
   a. VoIP Application elements (such as Proxies, SBC, IPS, SoftSwitches, feature servers)
   b. Transport elements (such as Switches, Routers, ROADMS, ADMs, WDM, MGWs, MGCs, SGWs, PON)
   c. Service Control elements (such as dynamic directory, time, configuration and authentication/authorization Servers)
   d. E/N/SML OAM&P elements (such as OSSs, Billing and Surveillance Systems along with OAM&P workstations).

C.3.1.3 Assets

VoIP assets include data, network elements as well as processes and applications that are critical to service functioning. For instance:

C.3.1.3.1 Information Assets

C.3.1.3.1.1 Customer Information assets
1) Mac, IP, transport address and routing/switching information
2) Encryption keys, passwords, shared secrets
3) User profiles
4) User IDs (and credentials)
5) Customer proprietary information (i.e., employees, customers, plans, technology)
6) Customer intellectual property (i.e., video, audio, textual material)
7) Customer reputation and financial solvency

C.3.1.3.1.2 TSP Information Assets
1) Mac, IP, transport address and routing/switching information
2) Encryption keys, passwords, shared secrets
3) Element operating system and application software
4) Customer identifiable information (accounts, contracts, billing information)
1) Customer service profiles
5) TSP Personnel profiles
8) Authentication information and credentials
9) Surveillance, Monitoring and Configuration Information
6) TSP reputation and financial solvency.

C.3.1.3.2 Physical Asset

C.3.1.3.2 .1 Customer Premises
1) VoIP terminal elements
2) Residential GW
3) Other network attached devices

C.3.1.3.2 .2 TSP Network
1) Transport elements (such as Modems, Switches, Routers, ROADMS, ADMs, WDM, MGWs, MGCs, SGWs, PON)
   e.
2) Service Control elements (such as dynamic directory, time, configuration and authentication/authorization Servers)
3) E/N/SML OAM&P elements (such as OSSs, Billing and Surveillance Systems along with OAM&P workstations).

4) VoIP Application elements (such as Proxies, SBC, IPS, SoftSwitches, feature servers)

C.4 Vulnerabilities & Threats

The VoIP assets described in section 8.3 potentially have vulnerabilities that can be subject to threats originating from within Customer, TSP Peering or TSP networks. These threats can be service disruptive. Vulnerabilities can exist in any TSP element, its services and systems. Following is a generic list of potential vulnerabilities:

- Operating System vulnerabilities
- Protocol-specific vulnerabilities
- Configuration vulnerabilities
- Application-specific vulnerabilities within the infrastructure areas of System Controls, Identification, Authentication
- Information storage and processing
- System Integrity and Privileged level implementation
- Security Administration and Configuration Management

The threats include the following types:

a) destruction of information and/or other resources;
b) corruption or modification of information;
c) theft, removal or loss of information and/or other resources;
d) disclosure of information; and
e) interruption of services.

C.4.1.1 Example Attack Scenarios

C.4.1.1 .1 Spoofing

An attacker may attempt to send a false message to a switch, such as a spoofed disconnect message. For example, in a non-secure VoIP environment, Alice could spoof a message from Bob asking to un-register from the server. Any such attack should be detected by message authentication and integrity checks.

C.4.1.1 .2 Corruption

An attacker may attempt to modify the media payload. For example an attacker may insert a voice message (such as an advertisement) into a media stream. With an integrity check, the receiver will drop the modified packet. Without an integrity check), an attacker can easily introduce noise into the media stream

C.4.1.1 .3 DoS attacks targeted towards elements

An attacker can launch DoS attacks on elements exploiting lack of adequate access controls or OS hardening leading to service disruption.

C.4.1.1 .4 Disclosure

Eavesdropper reads bearer control messages resulting in potential disclosure of the content in RTP packets.

C.4.1.1 .5 Attacker Masquerades as Network Entity

An attacker can masquerade as any networked entity, such as a switch, an endpoint, act in a 'man-in-the-middle' attack and then read, decrypt, process, modify, packets to and from the

masqueraded host, without raising suspicion. Preventing such attacks requires strong mutual authentication of the communicating parties and integrity of the messages exchanged

C.4.1.1 .6 Malicious Administrator Adjusts Call Processing Behavior

Administrators have capabilities to disrupt VoIP service to a particular user/users. For example, the administrator could reroute calls for certain businesses or individuals to its competitors. Attacks like these can be prevented by privilege levels and RBAC mechanisms.

C.4.2 Network interfaces & trust domains

The multiple networking segments defined by their terminating devices (UAs, CERs, PERs, LCRs, AERs, VoIP SP APs) and the network interfaces (UNI, I-NNI, NNI) represent domains that have different security requirements and implementations.

Reviewing scenario 6 from a security Use Case perspective:

- an End Node within the “Alice” customer security domain is communicating with a Service Provider Application Platform End Node within the Service Provider "Alpha" security domain
- an End Node within the “Bob” customer security domain is communicating with a Service Provider Application Platform End Node within the Service Provider "Bravo" security domain
- the Service Provider Application Platform End Nodes within the Service Provider "Alpha" and "Bravo" security domains are communicating, and
- these two End Nodes are attached to different Service Providers do not have a direct Peering Relationship rather they Interconnect via a 3rd (“Backbone”) Service Provider.

The three figures used to depict this use case for the VoIP scenario show logical groupings of functional entities as discrete platforms, namely:

- Router (AER or PPR) that performs packet forwarding based on routing polities
- Firewall (F/W) that performs stateless/state-full packet filtering based on IP Header address fields, Transport protocol Hearer “port” fields and Transport protocol state conditions to either forward or drop/discard based on filtering polities
- Intrusion Protection System (IPS) that performs deep packet inspection of Application protocol syntax and semantics to either forward or drop/discard based on filtering polities, malicious code signatures or flow behaviors
- RTP Control (SBC) that either forwards or drops/discards RTP application protocol containing packets based on presence and state of corresponding SIP session information. The SBC function may either eves-drop on SIP as basis fir RTP allow/drop decisions OR be under the control of a TSP VoIP Application processing complex.

However, there are many products on the market that include one or more of these functional entities within a common chassis/box.

Interface Discussion

The discussion of the interfaces shown in Figure 18 will proceed from left to right.

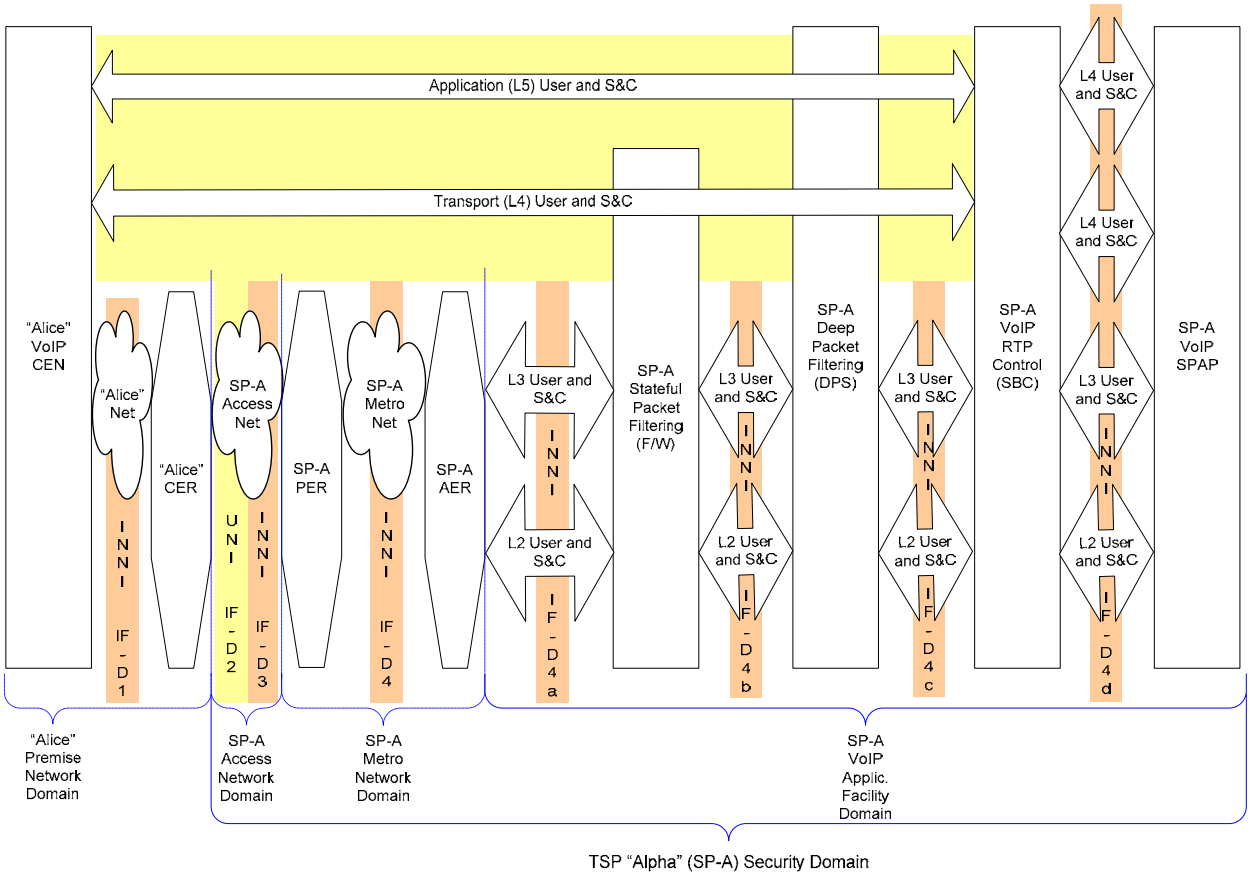

Figure 18 - Entities Interacting with, or supporting the "Alice" SIP UA

IF-D1 This interface is a customer security domain I-NNI and represents the networking infrastructure on the "Alice" customer premises. The customer end node could be either a 'client' desk-top/lap-top machine upon which a SIP UA is executing or a SIP VoIP telephone. The CER may either be owned & managed by the customer, owned by the customer and managed by the service provider, owned by the customer and managed by a 3rd party or owned and managed by the service provider.

Layer 2: The Data Link Protocol Layer it is assumed 802.3 (10baseT, 100baseT) where there may be zero (0) or more layer 2 devices such as bridges or switches between the CEN and the CER. It is the responsibility of the customer to provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for both Signaling & Control Information and User/Media Information as appropriate within this layer.

Layer 3: The Inter-networking Protocol layer assumes that the infrastructure uses IPv4 with non-routable "private" IP addresses where there may be zero (0) or more routers between the CEN and the CER. It is the responsibility of the customer to provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for both Signaling & Control Information and User/Media Information as appropriate within this layer.

Layer 4: The Transport Protocol layer it is assumed a transport protocol (TCP and UDP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes simply ignore the data component of IP packets.

Layer 5: At the Application protocol layer an appropriate application protocol is used that operates on an application process to application process basis such that intermediate nodes simply ignore the data component of transport protocol messages.

IF-D2 This interface is a service provider security domain UNI and represents the interface between the "Alice" customer premise and the service provider.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (10baseT, 100baseT) is used at layer 2 between the service provider facing CER interface and the service provider DSL modem or ONT. To provide Authentication and Authorization for:
Signaling & Control Information

For this use case, The TSP would deploy 802.1x (either within an ONT, DSLAM or OLT) to authenticate and authorize the CER prior to DHCP assigning an IP address to the CER and allowing the CER to source any IP packets. Use of 802.1x authentication will mitigate threat of spoofed CER identities and theft of service.

User/Media Information

The TSP would deploy 802.1x (either within an ONT, DSLAM or OLT) to authenticate and authorize the CER prior to DHCP assigning an IP address to the CER and allowing the CER to source any IP packets.

Use of 802.1x authentication will mitigate threat of spoofed CER identities and theft of service.

Layer 3: At the Inter-networking Protocol layer assumes that IPv4 is used with a service provider assigned IP address for the service provider facing CER interface. Layer 3 Signaling & Control protocols used over this interface would be ARP, DHCP and ICMP. It is unlikely that the TSP will enforce any Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for a UNI interface. Currently the only security technology at layer 3 is via IPsec which is highly unlikely to be used by a TSP across an UNI.

Layer 4: At the Transport Protocol TCP and UDP are used over IP that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets. The TSP will specify the mechanisms to provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for:
Signaling & Control Information

TLSv1.0 should be deployed for those RFC 3261 conformant SIP UAs able to take advantage of TLSv1.0 protection of SIP signaling sent to TSP SBC function. Use of TLSv1.0 authentication authorization and integrity will mitigate threat of spoofed SIP UA identities and theft of service.

User/Media Information

The TSP is unlikely to require any mechanisms for this traffic at this layer and interface.

Layer 5: At the Application Protocol layer it is assumed application protocols (such as http, ftp, SIP, RTP, etc.) is used over transport protocol (TCP and UDP) that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets. To provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for:
Signaling & Control Information

SIP signaling should be protected by use of the http digest mechanism at a minimum with TLSv1.0 support at layer 4 preferable. Use of http digest authentication and integrity will mitigate threat of spoofed SIP UA identities and theft of service.

SIP body parts, for UA to UA interaction) may be protected using SMIME at the discretion of the called and calling subscribers.

SIP User Agent (UA) profile information retrieval should be protected by https (http over TLSv1.0) or ftp over ssh when in transit. Use of TLSv1.0 and ssh authentication, authorization, confidentiality and integrity will mitigate threat of spoofed SIP UA identities, theft of customer identifiable information and theft of service.

User/Media Information

SIP UA sent/received RTP filtering provided by TSP SBC functional entity to mitigate threat of unauthorized RTP flows traversing the TSP infrastructure.

IF-D3 This interface is a service provider security domain I-NNI and represents the interface between the service provider customer premises network termination device (DSL Modem or ONT, through the TSP DSLAM or OLT, to the TSP PER.

Layer 2: The Data Link protocol layer between the TSP DSL Modem or ONT interface to the TSP DSLAM or OLT over xDSL or PON (G.983, G.984). To provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for:
Signaling & Control Information

For this use case, the TSP will rely on the PON or xDSL security mechanisms.

User/Media Information

For this use case, the TSP will rely on the PON or xDSL security mechanisms.

The Data Link protocol layer between TSP DSLAMs or OLTs and PERs assumes that GigE is used. To provide Authentication, Authorization, for:
Signaling & Control Information

For this use case, the TSP may deploy 802.1q based authentication to mitigate threat of spoofed DSLAM or OLT identities and disruption of service. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface

User/Media Information

For this use case, the TSP may deploy 802.1q based authentication to mitigate threat of spoofed DSLAM or OLT identities and disruption of service. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface

Layer 3: The Inter-networking Protocol layer between TSP DSLAMs or OLTs and PERs assumes that IPv4 is used. Layer 3 Signaling & Control protocols used over this interface would be ARP, DHCP and ICMP. To provide Authentication, Authorization, for:
Signaling & Control Information

The TSP may deploy state-full packet filtering within the PER to mitigate the threat of rogue protocols, malformed packets and other layer 3 attacks. The figure does not show separate packet filtering functionality which may be deployed within the PER or as an independent element. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

User/Media Information

The TSP may deploy state-full packet filtering within the PER to mitigate the threat of rogue protocols, malformed packets and other layer 3 attacks. The figure does not show separate packet filtering functionality which may be deployed within the PER or as an independent element. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-D4 This interface is a service provider security domain I-NNI and represents the interface between the service provider access network edge router (PER) across the TSP metropolitan core network (including LCRs) to the destination TSP Application Edge Router (AER).

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE) is used at layer 2 between the PER and AER, although the TSP may deploy MPLS rather than 802.1q. Layer 2 Signaling & Control protocols used over this interface would be IEEE 802.1q. For this use case, the TSP may deploy 802.1q based authentication mitigate threat of spoofed PER, LCR and AER identities and disruption of service.. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 3: At the Inter-networking Protocol layer assumes that IPv4 is used between the PER, LCRs and AER. Layer 3 Signaling & Control protocols used over this interface would be ARP, DHCP and ICMP. To provide Authentication, Authorization, for:
Signaling & Control Information

For this use case, the TSP may deploy IPsec based authentication and integrity for route distribution protocols such as BGP, OSPF, LDP, etc.). Deployment of IPsec for layer 3 signaling and control authentication, authorization and integrity mitigate threat of spoofed PER, LCR and AER identities and disruption of service. The TSP may deploy state-full packet filtering within the AER to mitigate the threat of rogue protocols, malformed packets and other layer 3 attacks, however the figure depicts packet filtering as deployed within a separate element. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

User/Media Information

The TSP may deploy state-full packet filtering within the AER to mitigate the threat of rogue protocols, malformed packets and other layer 3 attacks, however the figure depicts packet filtering as deployed within a

separate element. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-D4a This interface is a service provider security domain I-NNI and represents the interface between the TSP AER and a separate TSP Statefull packet filtering element (F/W).

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE) is used at layer 2 between the AER and F/W, although the TSP may deploy MPLS rather than 802.1q. Layer 2 Signaling & Control protocols used over this interface would be IEEE 802.1q. For this use case, the TSP may deploy 802.1q based authentication mitigate threat of spoofed AER and F/W identities and disruption of service.. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 3: At the Inter-networking Protocol layer assumes that IPv4 is used with service provider assigned IP addresses. Layer 3 Signaling & Control protocols used over this interface would be ARP, DHCP and ICMP. To provide Authentication, Authorization, for:
Signaling & Control Information

It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

User/Media Information

It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-D4b This interface is a service provider security domain I-NNI and represents the interface between the TSP Statefull packet filtering element (F/W) and a TSP Deep Packet Filtering Function (DPS).

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE) is used at layer 2 between the F/W and DPS, although the TSP may deploy MPLS rather than 802.1q. Layer 2 Signaling & Control protocols used over this interface would be IEEE 802.1q. The TSP may deploy 802.1q based authentication mitigate threat of spoofed F/W and DPS identities and

disruption of service.. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 3: At the Inter-networking Protocol layer assumes that IPv4 is used with service provider assigned IP addresses. Layer 3 Signaling & Control protocols used over this interface would be ARP, DHCP and ICMP. To provide Authentication, Authorization, for:
Signaling & Control Information

It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

User/Media Information

It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: For this use case, the TSP deployed DPS will scan the complete contents of all packets to identify the present of malicious content, including all application layer protocol messages. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

IF-D4c This interface is a service provider security domain I-NNI and represents the interface between the TSP DPS and the TSP deployed SBC function.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE) is used at layer 2 between the DPS and the SBC. Layer 2 Signaling & Control protocols used over this interface would be IEEE 802.1q. The TSP may deploy 802.1q based authentication mitigate threat of spoofed F/W and DPS identities and disruption of service.. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 3: At the Inter-networking Protocol layer assumes that IPv4 is used with service provider assigned IP addresses. Layer 3 Signaling & Control protocols used over this interface would be ARP, DHCP and ICMP. To provide Authentication, Authorization, for:
Signaling & Control Information

It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

User/Media Information

It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-D4d This interface is a service provider security domain I-NNI and represents the interface between the TSP SBC and the TSP VoIP application service complex of elements (SPAP).

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE) is used at layer 2 between the SBC and the SPAP. Layer 2 Signaling & Control protocols used over this interface would be IEEE 802.1q. The TSP may deploy 802.1q based authentication mitigate threat of spoofed F/W and DPS identities and disruption of service.. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 3: At the Inter-networking Protocol layer assumes that IPv4 is used with service provider assigned IP addresses. Layer 3 Signaling & Control protocols used over this interface would be ARP, DHCP and ICMP. To provide Authentication, Authorization and integrity, for:
Signaling & Control Information

The TSP may deploy IPsec security mechanisms such as ESP-nul to SIP signaling messages sent between the SBC and SPAP. Use of IPsec authentication, authorization and integrity will mitigate threat of spoofed SIP UA identities and theft of service.. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

User/Media Information

It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 4: At the Transport Protocol layer it is assumed a transport protocol (TCP and UDP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets. The TSP will specify the mechanisms to provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for:
Signaling & Control Information

TLSv1.0 may be deployed, instead of relying on Layer 3 IPsec mechanisms, for those RFC 3261 conformant SIP UAs able to take advantage of TLSv1.0 protection of SIP signaling sent between SBC

and SPAP. Use of TLSv1.0 authentication authorization and integrity will mitigate threat of spoofed SIP UA identities and theft of service.

User/Media Information

For this use case, the TSP is unlikely to require any mechanisms for this traffic at this layer and interface.

Layer 5: At the Application Protocol layer it is assumed application protocols (such as http, ftp, SIP, RTP, etc.) is used over transport protocol (TCP and UDP) that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets. To provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for:
Signaling & Control Information

SIP signaling should be protected by use of preferably IPsec, secondarily TLSv1.0 or thirdly the http digest mechanism. Use of these authentication and integrity mechanisms will mitigate threat of spoofed SIP UA identities and theft of service.

SIP User Agent (UA) profile information retrieval should be protected by https (http over TLSv1.0) or ftp over ssh when in transit. Use of TLSv1.0 and ssh authentication, authorization, confidentiality and integrity will mitigate threat of spoofed SIP UA identities, theft of customer identifiable information and theft of service.

User/Media Information

For this use case, the TSP is unlikely to require any mechanisms for this traffic at this layer and interface.

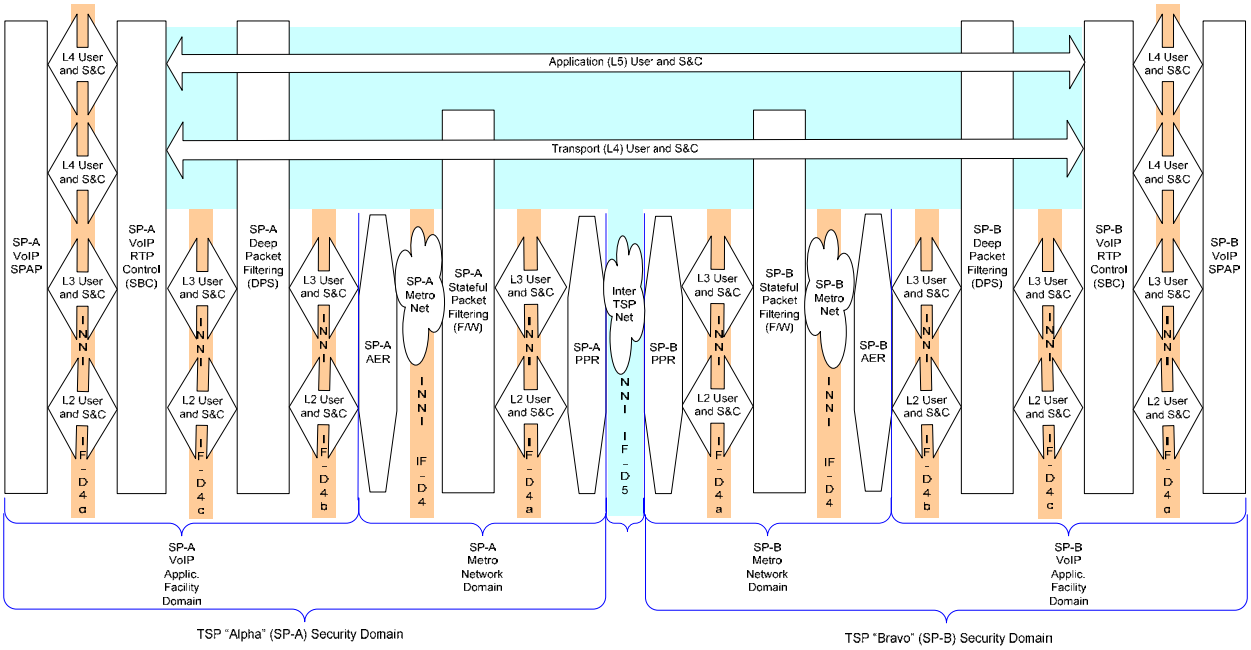

Figure 19 - Inter-TSP Entities in support of SIP VoIP Peering

The discussion of the interfaces shown in Figure 19 will proceed from left to right.

IF-D4d This interface is a service provider security domain I-NNI and represents the interface between the TSP SBC and the TSP VoIP application service complex of elements (SPAP). This is identical to the preceding IF-D4d security discussion.

IF-D4c This interface is a service provider security domain I-NNI and represents the interface between the TSP DPS and the TSP deployed SBC function. This is identical to the preceding IF-D4c security discussion.

IF-D4b This interface is a service provider security domain I-NNI and represents the interface between the TSP Statefull packet filtering element (F/W) and a TSP Deep Packet Filtering Function (DPS). This is identical to the preceding IF-D4b security discussion.

IF-D4 This interface is a service provider security domain I-NNI and represents the interface between the TSP peering router (PPR) across the TSP metropolitan core network (including LCRs) to the destination TSP Application Edge Router (AER). This is identical to the preceding IF-D4 security discussion.

IF-D4a This interface is a service provider security domain I-NNI and represents the interface between the TSP AER and a separate TSP Statefull packet filtering element (F/W) This is identical to the preceding IF-D4a security discussion.

IF-D5 This interface is a service provider security domain NNI and represents the interface between the two service providers' peering-point routers.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (GigE) is used at layer 2 between the AER and F/W, although the TSPs may deploy MPLS rather than 802.1q. Layer 2 Signaling & Control protocols used over this interface would be IEEE 802.1q. The TSPs may deploy 802.1q based authentication mitigate threat of spoofed PPR identities and disruption of service.. It is unlikely that the TSPs will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an NNI interface.

Layer 3: The Inter-networking Protocol layer assumes that IPv4 is used with each service provider assigning IP addresses. Layer 3 Signaling & Control protocols used over this interface would be ARP and ICMP. To provide Authentication, Authorization, for:
Signaling & Control Information

Both TSPs may deploy IPsec security mechanisms such as ESP-nul to SIP signaling messages sent between the PPR of TSP "Alpha" and the PPR of TSP "Bravo". Use of IPsec authentication, authorization and integrity will mitigate threat of spoofed SIP UA identities and theft of service.. It is unlikely that the TSPs will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an NNI interface.

User/Media Information

It is unlikely that the TSPs will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an NNI interface.

Layer 4: At the Transport Protocol layer it is assumed a transport protocol (TCP and UDP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets. The TSPs will specify the mechanisms to provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for:
Signaling & Control Information

TLSv1.0 may be deployed, instead of relying on Layer 3 IPsec mechanisms, for those RFC 3261 conformant SBCs able to take advantage of TLSv1.0 protection of SIP signaling sent between SBC and SBC. Use of TLSv1.0 authentication authorization and integrity will mitigate threat of spoofed SIP UA identities and theft of service.

User/Media Information

The TSPs are unlikely to require any mechanisms for this traffic at this layer and interface.

Layer 5: At the Application Protocol layer it is assumed application protocols (such as SIP, RTP, etc.) is used over transport protocol (TCP and UDP) that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets. To provide Authentication, Authorization, Confidentially, Integrity

and Non-repudiation for:
Signaling & Control Information

SIP signaling should be protected by use of preferably IPsec, secondarily TLSv1.0 or thirdly the http digest mechanism. Use of these authentication and integrity mechanisms will mitigate threat of spoofed SIP UA identities and theft of service.

User/Media Information

The TSP is unlikely to require any mechanisms for this traffic at this layer and interface.

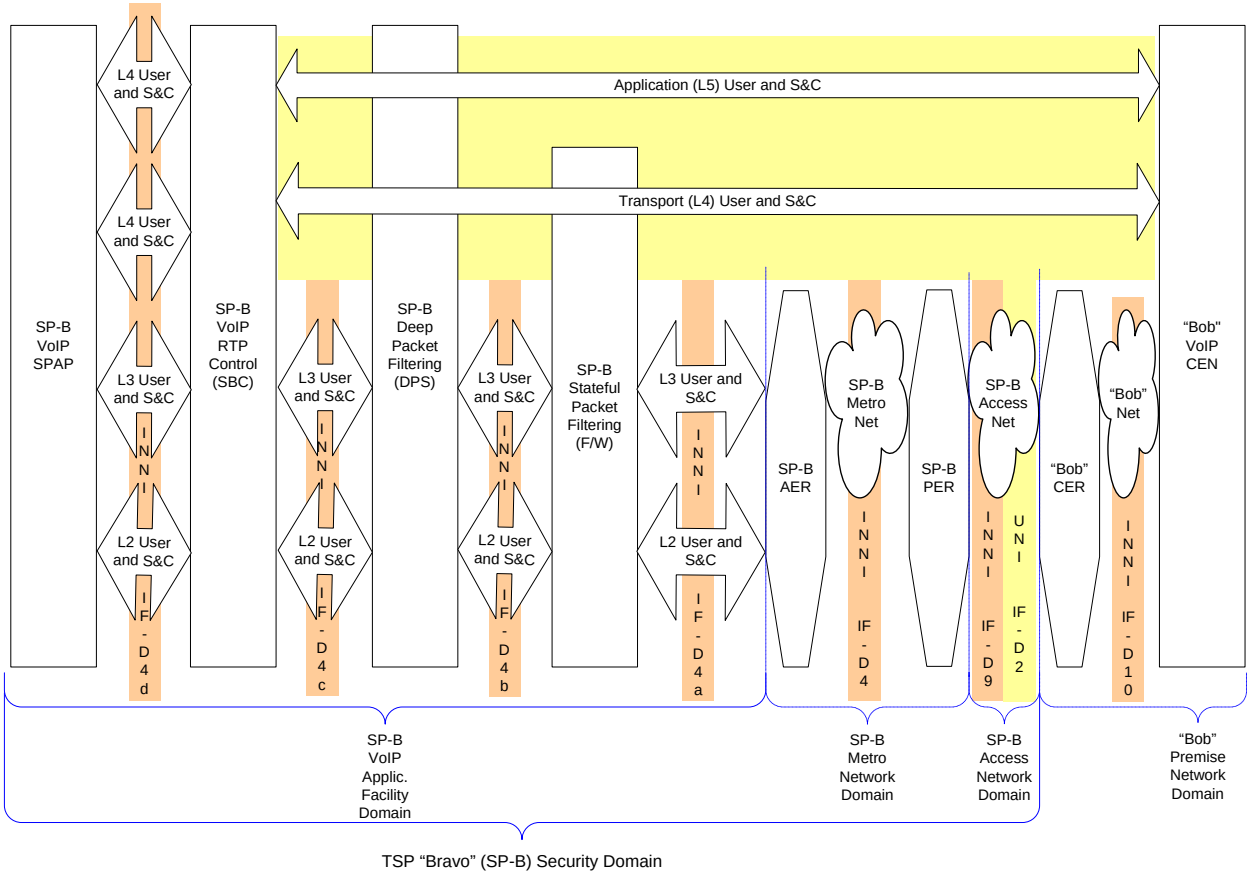

Figure 20 - Entities Interacting with, or supporting the "Bob" SIP UA

The discussion of the interfaces shown in Figure 20 will proceed from right to left.

IF-D10 This interface is a customer security domain I-NNI and represents the networking infrastructure on the "Bob" customer premises. The customer end node could be either a 'client' desk-top/lap-top machine upon which a SIP UA is executing or a SIP

VoIP telephone. The CER may either be owned & managed by the customer, owned by the customer and managed by the service provider, owned by the customer and managed by a 3rd party or owned and managed by the service provider.

Layer 2: The Data Link Protocol Layer it is assumed 802.3 (10baseT, 100baseT) where there may be zero (0) or more layer 2 devices such as bridges or switches between the CEN and the CER. It is the responsibility of the customer to provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for both Signaling & Control Information and User/Media Information as appropriate within this layer.

Layer 3: The Inter-networking Protocol layer assumes that the infrastructure uses IPv4 with non-routable "private" IP addresses where there may be zero (0) or more routers between the CEN and the CER. It is the responsibility of the customer to provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for both Signaling & Control Information and User/Media Information as appropriate within this layer.

Layer 4: The Transport Protocol layer it is assumed a transport protocol (TCP and UDP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes simply ignore the data component of IP packets.

Layer 5: At the Application protocol layer an appropriate application protocol is used that operates on an application process to application process basis such that intermediate nodes simply ignore the data component of transport protocol messages.

IF-D2 This interface is a service provider security domain UNI and represents the interface between the "Bob" customer premise and the service provider.

Layer 2: At the Data Link Protocol Layer it is assumed 802.3 (10baseT, 100baseT) is used at layer 2 between the service provider facing CER interface and the service provider DSL modem or ONT. To provide Authentication and Authorization for:
Signaling & Control Information

For this use case, the TSP would deploy 802.1x (either within an ONT, DSLAM or OLT) to authenticate and authorize the CER prior to DHCP assigning an IP address to the CER and allowing the CER to source any IP packets. Use of 802.1x authentication will mitigate threat of spoofed CER identities and theft of service.

User/Media Information

For this use case, the TSP would deploy 802.1x (either within an ONT, DSLAM or OLT) to authenticate and authorize the CER prior to DHCP assigning an IP address to the CER and allowing the CER to source any IP packets. Use of 802.1x authentication will mitigate threat of spoofed CER identities and theft of service.

Layer 3: At the Inter-networking Protocol layer assumes that IPv4 is used with a service provider assigned IP address for the service provider facing CER

interface. Layer 3 Signaling & Control protocols used over this interface would be ARP, DHCP and ICMP. It is unlikely that the TSP will enforce any Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for a UNI interface.

Layer 4: At the Transport Protocol layer it is assumed a transport protocol (TCP and UDP) is used over IP that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets. The TSP will specify the mechanisms to provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for:
Signaling & Control Information

TLSv1.0 should be deployed for those RFC 3261 conformant SIP UAs able to take advantage of TLSv1.0 protection of SIP signaling sent to TSP SBC function. Use of TLSv1.0 authentication authorization and integrity will mitigate threat of spoofed SIP UA identities and theft of service.

User/Media Information

The TSP is unlikely to require any mechanisms for this traffic at this layer and interface.

Layer 5: At the Application Protocol layer it is assumed application protocols (such as http, ftp, SIP, RTP, etc.) is used over transport protocol (TCP and UDP) that operates on an end-node to end-node basis such that intermediate nodes (service provider devices) simply ignore the data component of IP packets. To provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for:
Signaling & Control Information

SIP signaling should be protected by use of the http digest mechanism at a minimum with TLSv1.0 support at layer 4 preferable. Use of http digest authentication and integrity will mitigate threat of spoofed SIP UA identities and theft of service.

SIP body parts, for UA to UA interaction) may be protected using SMIME at the discretion of the called and calling subscribers.

SIP User Agent (UA) profile information retrieval should be protected by https (http over TLSv1.0) or ftp over ssh when in transit. Use of TLSv1.0 and ssh authentication, authorization, confidentiality and integrity will mitigate threat of spoofed SIP UA identities, theft of customer identifiable information and theft of service.

User/Media Information

SIP UA sent/received RTP filtering provided by TSP SBC functional entity to mitigate threat of unauthorized RTP flows traversing the TSP infrastructure.

IF-D9 This interface is a service provider security domain I-NNI and represents the interface between the service provider customer premises network termination device (DSL Modem or ONT, through the TSP DSLAM or OLT, to the TSP PER.

Layer 2: The Data Link protocol layer between the TSP DSL Modem or ONT interface to the TSP DSLAM or OLT over xDSL or PON (G.983, G.984). To provide Authentication, Authorization, Confidentially, Integrity and Non-repudiation for:
Signaling & Control Information

For this use case, the TSP will rely on the PON or xDSL security mechanisms.

User/Media Information

For this use case, the TSP will rely on the PON or xDSL security mechanisms.

The Data Link protocol layer between TSP DSLAMs or OLTs and PERs assumes that GigE is used. To provide Authentication, Authorization, for:
Signaling & Control Information

For this use case, the TSP may deploy 802.1q based authentication to mitigate threat of spoofed DSLAM or OLT identities and disruption of service. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface

User/Media Information

For this use case, the TSP may deploy 802.1q based authentication to mitigate threat of spoofed DSLAM or OLT identities and disruption of service. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface

Layer 3: The Inter-networking Protocol layer between TSP DSLAMs or OLTs and PERs assumes that IPv4 is used. Layer 3 Signaling & Control protocols used over this interface would be ARP, DHCP and ICMP. To provide Authentication, Authorization, for:
Signaling & Control Information

For this use case, the TSP may deploy state-full packet filtering within the PER to mitigate the threat of rogue protocols, malformed packets and other layer 3 attacks. The figure does not show separate packet filtering functionality which may be deployed within the PER or as an independent element. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

User/Media Information

For this use case, the TSP may deploy state-full packet filtering within the PER to mitigate the threat of rogue protocols, malformed packets

and other layer 3 attacks. The figure does not show separate packet filtering functionality which may be deployed within the PER or as an independent element. It is unlikely that the TSP will enforce any additional Authentication, Authorization, Confidentially, Integrity or Non-repudiation services at this layer for an I-NNI interface.

Layer 4: None, Protocols at this layer are not interacted with by devices communicating over this interface.

Layer 5: None, Protocols at this layer are not interacted with by devices communicating over this interface.

IF-D4 This interface is a service provider security domain I-NNI and represents the interface between the service provider access network edge router (PER) across the TSP metropolitan core network (including LCRs) to the destination TSP Application Edge Router (AER). This is identical to the preceding IF-D4 security discussion.

IF-D4a This interface is a service provider security domain I-NNI and represents the interface between the TSP AER and a separate TSP Statefull packet filtering element (F/W). This is identical to the preceding IF-D4a security discussion.

IF-D4b This interface is a service provider security domain I-NNI and represents the interface between the TSP Statefull packet filtering element (F/W) and a TSP Deep Packet Filtering Function (DPS). This is identical to the preceding IF-D4b security discussion.

IF-D4c This interface is a service provider security domain I-NNI and represents the interface between the TSP DPS and the TSP deployed SBC function. This is identical to the preceding IF-D4c security discussion.

IF-D4d This interface is a service provider security domain I-NNI and represents the interface between the TSP SBC and the TSP VoIP application service complex of elements (SPAP). This is identical to the preceding IF-D4d security discussion.

C.4.3 Residual Risks

Residual risks remaining after all planned security mechanisms of the security architecture, as a result of TVA, should be re-examined based on the:

- Security measurements, SLAs and technology used in the infrastructure for maintenance and verification through out the security lifecycle
- Cyclic views defined in the security policy
- cost benefit analysis.

C.4.4 Summary

This use case shows:

- how security mechanisms should be considered as a part of concept design & architecture to achieve service security policy objectives, and
- how standards, and best practices, can facilitate achieving service security policy objectives.

The methodology applied herein is based on the international and national standards, as discussed in sections 4 and 5, specifically identified in the references section 1.3.