**November 12, 2002**

# T1M1

Internetwork Operations, Administration, Maintenance, and Provisioning

A Technical Subcommittee of Standards Committee T1 Telecommunications
www.t1.org

Accredited by the American National Standards Institute

Michael J. Fargano
Chairman

James T. Stanco
Vice Chairman

*A Sponsored Committee of*

Alliance for Telecommunications Industry Solutions

***Michael J. Fargano***
***Qwest Communications***
***4001 Discovery Dr.***
***Boulder, CO 80303***
***303 541 5141 (T)***
***303 541 5351 (F)***
***email: mfargan@qwest.com***



***Subject: Security Requirements for the Management Plane***

Fellow Industry Leaders:

At the T1M1 Plenary session on November 7, 2002, it was agreed to send the draft proposed American National Standard (dpANS) on ***Security Requirements for the Management Plane*** for a Committee T1 Letter Ballot. We understand that that there may be similar work in progress in your organization, and we invite your comments and specific suggestions for the improvement of this dpANS. Alternatively, your members may wish to send their own comments via the Committee T1 Letter Ballot process. The dpANS (document T1M1/2002-125R2) is attached. The document is also posted on the T1M1 file server at **ftp://ftp.t1.org/T1M1/NEW-T1M1.5/2m151252.zip**.

The Letter Ballot will close on January 7, 2003 and there will be a meeting to resolve comments on January 15, 2003 in Washington, DC. Representatives and/or delegates should plan to take part in the resolution of comments, as appropriate (if comments are provided).

Thank you for your cooperation and coordination on this important subject matter. Please contact me if there are any questions or concerns.

Best regards,

*Mike Fargano*
**T1M1 Chairman**

cc: Jim Stanco, T1M1 Vice Chair
Lakshmi Raman, T1M1.5 Chair
Tom Grim, T1M1.5 Security AHG Chair
Committee T1 TSC Leaders
Committee T1 Officers

# COMMITTEE T1 – TELECOMMUNICATIONS
## Working Group T1M1.5 T1M1.5/2002-125R2
## San Diego; November 4-8, 2002

**DOCUMENT TYPE: DRAFT AMERICAN NATIONAL STANDARD**

**TITLE:** **Baseline Security Requirements for the Management Plane**

**SOURCE*:** **T1M1.5 Security Requirements Ad Hoc Group**

**PROJECT:** Management Services, TMN

---

**ABSTRACT**

This contribution is a revision to T1M1.5/2002-125. It captures changes agreed to during the T1M1.5 meeting November 5-6, 2002 in San Diego, California. Since the ATIS/T1 Chief Editor will remove and replace any table of contents supplied by the Technical Editor and since the Chief Editor has requested that auto-numbering headers not be used in draft standards, no table of contents is supplied at this time with this draft standard. Additional formatting issues noted in the contribution will be resolved during the ballot process.



* CONTACT: Tom Grim; E-mail: tgrim@tri.sbc.com; Tel: 512-372-5835; Fax: 512-372-5891

Draft proposed American National Standard

for Telecommunications

# Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

**Secretariat**

**Alliance for Telecommunications Industry Solutions**

Approved Month__, 20__

**American National Standards Institute, Inc.**

## Abstract

This standard contains a set of baseline security requirements for the Management Plane. The President's National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchange (NSIE) and Government NSIE jointly established a Security Requirements Working Group (SRWG) to examine the security requirements for controlling access to the public switched network, in particular with respect to the emerging next generation network. In the telecommunications industry, this access incorporates operation, administration, maintenance, and provisioning for network elements and various supporting systems and databases. Members of the SRWG, from a cross-section of telecommunications carriers and vendors, developed an initial list of security requirements that would allow vendors, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure. This initial list of security requirements was submitted as a contribution to Committee T1 – Telecommunications, Working Group T1M1.5 for consideration as a standard. The requirements outlined in this document will allow vendors, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure.

## Foreword

The information contained in this foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the standard.

Executive Orders, Presidential directives, and Presidential commissions have identified eight infrastructures as critical national assets necessary for the defense and economic security of the United States. Telecommunications is one of these critical infrastructures. The President's National Security Telecommunications Advisory Committee (NSTAC) Network Security and Information Exchange (NSIE) and Government NSIE established a Security Requirements Working Group (SRWG) to examine the security requirements for controlling access to the public switched network, in particular with respect to the emerging next generation network. In the telecommunications industry, this access incorporates operation, administration, maintenance, and provisioning for network elements and various supporting systems and databases (i.e., operational support system).

Members of the SRWG, from a cross-section of telecommunications carriers and vendors, developed an initial list of security requirements that would allow vendors, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure. This initial list of security requirements was submitted as a contribution to Committee T1 – Telecommunications, Working Group T1M1.5 for consideration as a standard.

Although these requirements employ telecommunications terms and formats, the underlying principles should apply equally to the management of computing elements in the other infrastructures. Other infrastructures may wish to modify and apply these recommendations as appropriate to their respective infrastructure.

This document is entitled Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane. There are three annexes in this standard that are informative and are not considered part of this standard. Footnotes are not officially part of this standard.

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

Suggestions for improvement of this standard are welcome. These should be sent to the Alliance for Telecommunications Industry Solutions, T1 Secretariat, 1200 G Street, NW, Suite 500, Washington, DC 20005.

T1M1.5 Committee members list:

Working Group T1M1.5 – Security Requirements Ad Hoc Group developed this standard. Over the course of its development, the following individuals participated in the group's discussion and made significant contributions to the standard:

Michael McGuire, Chair
Tom Grim, Vice Chair
Michael Lee, Technical Editor
Greg Shannon, Technical Editor
Marcia McGowan, Editor
Andrea Livero-Scott, Editor

Brennan Baybeck
Bob Beeman
Kathy Blasco
David Dumas
Jack Edwards
Mike Fargano
Mike Frank
Martin Hogg
Frank Horsfall
Stuart Jacobs
John Kimmins
Hing-Kam Lam
Chris Lonvick
Hank Mauldin
Kevin McMahon
Moshe Rozenblit
Jim Stanco
Fred Staples
Rod Wallace
Joe Wolfkiel
Bob Wright

**Table of Contents**

**Table of Tables**

**Table of Figures**

Ad Hoc Group Editor's Note:  Will be generated prior to publication.

Draft proposed American National Standard for Telecommunications –

# Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

## 0 Introduction

Executive Orders, Presidential directives, and Presidential commissions have identified telecommunications as a critical infrastructure, necessary for the defense and economic security of the United States. Appropriate security for the network management functions controlling this infrastructure is essential. Many standards for network management security exist. However, compliance is low and implementations are inconsistent across the various telecommunications equipment and software components. This document identifies a minimum set of requirements to allow vendors, government departments and agencies, and service providers to implement a secure network management infrastructure. The business case for security features is complex and implementation is a significant expense. Hence, a consistent baseline will improve critical telecommunications industry infrastructure security and reduce costs for vendors and service providers. Although the present baseline represents the current understanding of the state of the art, technologies will advance and conditions will change. To be successful, this document must evolve as conditions warrant. At the same time, service providers may use this document as a foundation and include unique requirements to meet specific needs over and above those in this baseline.

## 1 Scope, Purpose, and Application

In the past, management and control traffic were most often transmitted out of band, being carried on a separate network from that carrying the service provider's end-user traffic. Security threats to the management and control planes were completely isolated from any malicious activity on the end-user plane. The management and control planes were relatively easy to secure because access to these planes was restricted to known administrators and traffic was restricted to typical known management and control activities.

Now, however, management and control traffic is being sent in-band, where it is combined on a single network with the service provider's end-user traffic. Combining traffic in this manner minimizes costs by requiring only a single integrated network infrastructure; however, many new security challenges are introduced. Threats in the end-user plane now become threats to the network management and control planes. Management and control planes now become accessible to the multitude of end-users and many types of malicious activities become possible. The purpose of this document is to recommend minimum baseline security mechanisms to help mitigate these security risks.

The requirements in this standard are applicable to network elements (NE) and management systems (MS) to be deployed in the future. For NEs, that do not meet all the mandatory security requirements, in the network, the overall security requirements at the network architecture design should be supported. This document addresses security for network element (NE), element management systems (EMS), and management system (MS) equipment, and does not specifically address security for other equipment such as customer premise equipment (e.g., voice over IP telephones) or independent test gear. For such

other equipment, all mandatory requirements in this document should be considered objective recommendations.

### 1.1 Framework and Model

In the context of this document, to secure something means to protect it (i.e., computers, networks, data, or other resources) from unauthorized use or activity. Losses of data, denial of service (DoS), theft of service, and loss of customer confidence are only some of the results of security incidents. System and network administrators need to protect systems and their component elements from users and from attackers. Although security is multifaceted (spanning operations, physical, communications, processing, and personnel), of concern here are security problems resulting from weaknesses inherent in commonly employed configurations and technology. Table 1 lists some of the security threats considered.

**Table 1 – Threats**

| Threat Category*) | Examples of Threats |
|---|---|
| Unauthorized Access | Hacking (i.e., unlawful accessing of system resources for entertainment or glory, or both)<br>Unauthorized system access to carry out other types of attack<br>Theft of service |
| Masquerade | Session replay<br>Session hijacking<br>Man-in-the-middle attacks |
| Threats to Integrity | Unauthorized manipulation of system configuration files<br>Unauthorized manipulation of system data |
| Threats to Confidentiality | Eavesdropping<br>Session recording and disclosure<br>Privacy violations |
| Denial of Service | Transmission Control Protocol (TCP) flood<br>Malformed packet attacks<br>Distributed DoS |
| *) Derived from T1.233 and International Organization of Standardization (ISO) 7498-2. | |

These security threats may be minimized or mitigated within a network system (NS) or NE platform or application by inclusion of security services (as defined in International Organization for Standardization [ISO] 7498-2) to enforce the following:

- Identification and AUTHENTICATION
- Authorization and Access Control Level
- Data Integrity
- Privacy and Confidentiality
- Nonrepudiation

Figure 1 illustrates the scope of the network security area. Three communication planes are shown: Management Plane, Control Plane, and End User Plane. This document addresses security for the

Management Plane—that is, security features to ensure that the network can be administered and managed in a secure manner.

Some vulnerability may still exist, even after following the recommendations contained in this document. The following residual risks are among those with the capability to compromise the Management Plane:

- The residual risk of inappropriate actions by authorized users remains. These actions can be either malevolent or accidental. Judicious control of the logs generated by the NE/MS can mitigate this risk.
- Security for the Control Plane (e.g., routing protocol security and domain name server) and the End User Plane are not discussed.
- The effects of vulnerabilities in specific protocols are not discussed in this document.
- Once malware (e.g., virus, Trojan horses, and worms, or other embedded code) successfully compromises any NE/MS, the malware may use the secure network communication links to transmit its attacks to other NE/MS components. These attacks may continue until the network managers detect and capture the attack signature, and eliminate the source of the compromising effects from the environment.

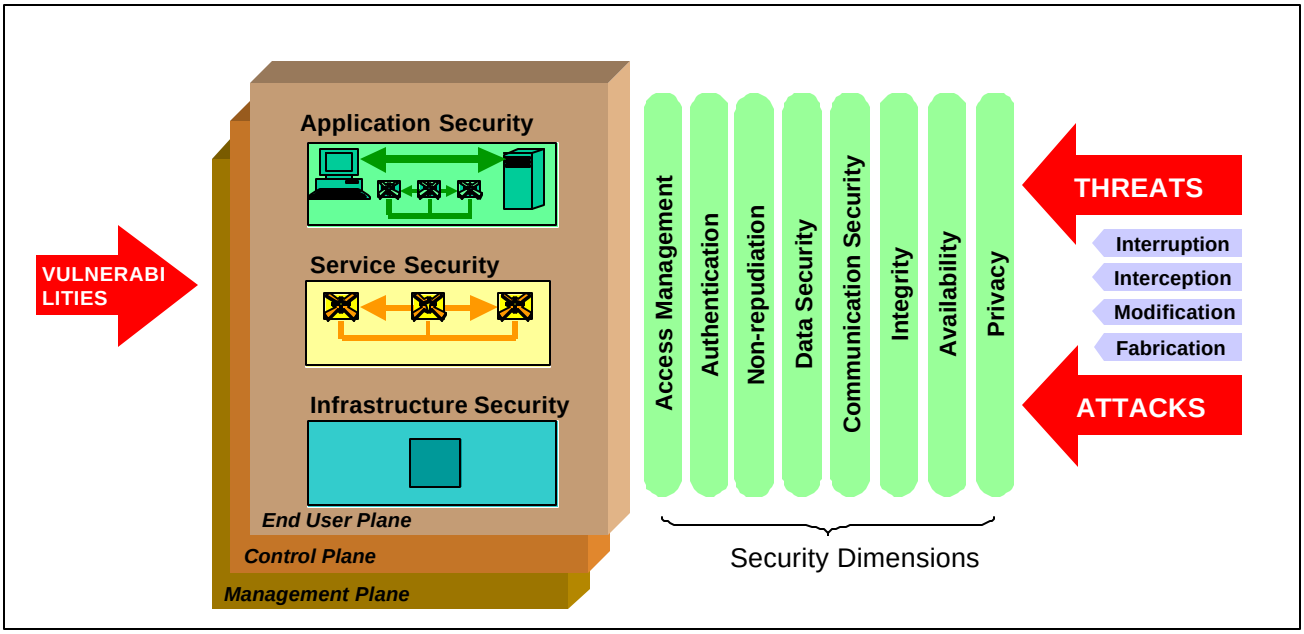



**Figure 1 – Model for Security Framework**

This document is concerned with the security of management traffic, especially when it traverses networks mixed with traffic from the end-user plane. Figure 2 illustrates a reference model that is used to specify network management security solutions. This model is used to examine logical communication paths within the entire network and quantify which protocols are used for communications on each path. Using this model, threats and vulnerabilities can be examined for each path, and appropriate security mechanisms can be applied.

Multivendor NEs are shown at the bottom of the model in figure 2. Element management systems (EMS) that provide specific management functions for the particular NE are illustrated above the NE. The network management system (NMS) itself is at the top of the model. The NMS provides overall management to the NE and EMS, and contains the specific service management applications and the

business management applications, such as configuration and billing systems. Remote and local operators are also shown in the model and communication paths are shown with all other system elements.

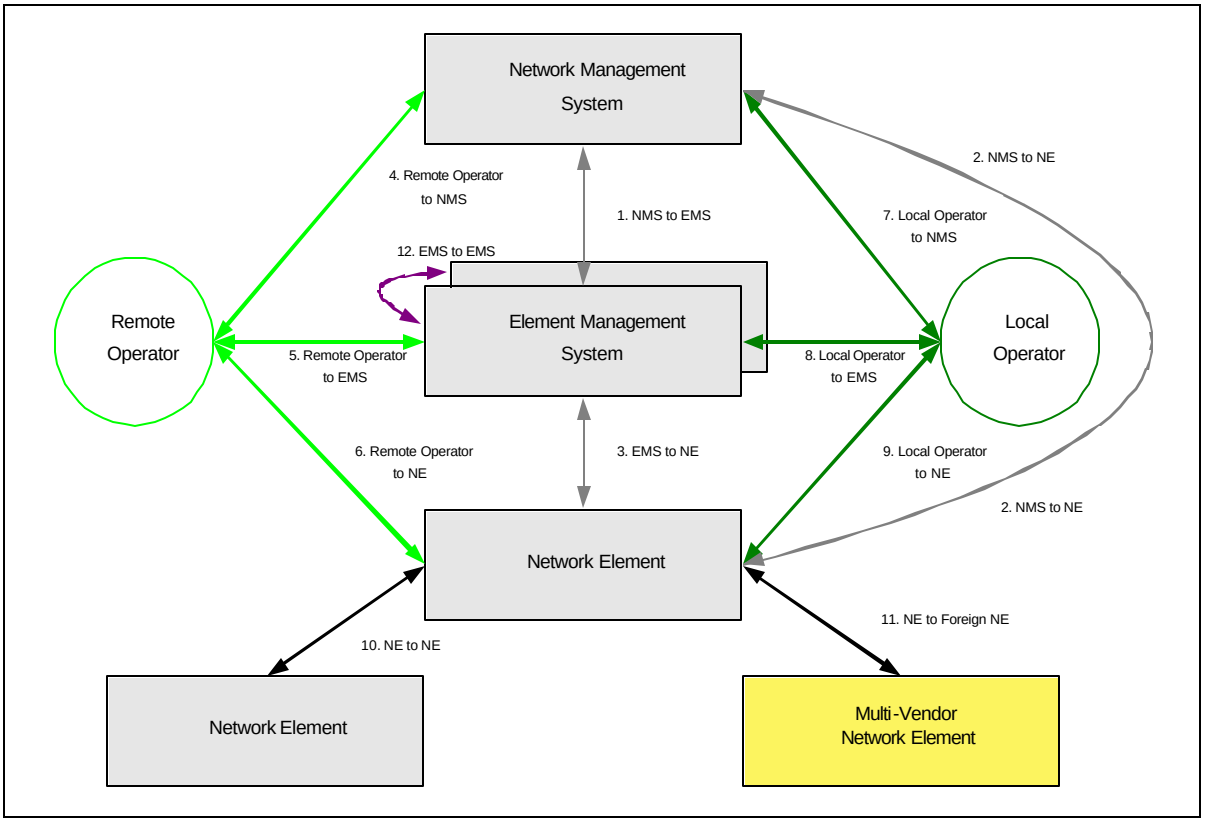



**Figure 2 – Network Management Security Reference Model**

The reference model (figure 2) also takes into account the types of interfaces (X, Q, F,[1] shown in figure 3) used within a communications network. Additional relationships are also identified because mediation devices may exist within a telecommunications management network (TMN). In today's network environment, relationships among TMNs may require different security mechanisms. For example, in the relationship between a telecommunications provider and a customer of wholesale network services (an Internet Service Provider [ISP]) or managed network services (a retail customer), interconnections between various infrastructures owned by different legal entities versus infrastructures owned by the same legal entity may require more stringent security controls. The term "legal entities" refers to different organizations or affiliated organizations. For additional information regarding the relationships shown in figure 2, see International Telecommunication Union (ITU) document M.3010, Clause 5.2.[2].

The following functional relationships exist within and between network infrastructures, as defined by the term "reference point" in American National Standards Institute (ANSI) T1-210-1993:

- Network Element Function to Operating System Function (NEF to OSF)
- Network Element Function to Mediation Function (NEF to MF)

[1] X, Q, and F interfaces are defined in ITU-T M.3010, Principles for a TMN.
[2] This document defines a TMN as "conceptually a separate network that interfaces a telecommunications network at several different points to send/receive information to/from it and to control its operations." The interfaces used between functional components of a TMN are also defined in ITU-M.3010.

- Mediation Function to Mediation Function (MF to MF)
- Mediation Function to Operating System Function (MF to OSF)
- Mediation Function to Network Element Function (MF to NEF)
- Mediation Function to Workstation Function (MF to WSF)
- Operating System Function to Operating System Function (OSF to OSF)
- Operating System Function to Workstation Function (OSF to WSF)
- Q-Adapter Function to Operating System Function (QAF to OSF)
- Q-Adapter Function to Mediation Function (QAF to MF)
- Q-Adapter Function to Network Element Function (QAF to NEF)

Figure 3[3] shows a generalized physical architecture as a single TMN. TMNs may be interconnected, as described above, between different entities. Although entities usually correspond to organizational boundaries (e.g., geographic or national), they may be distinguished by other criteria such as affiliated organizations and business partners.

Figure 2 identifies the logical relationships among NMSs, EMSs, and remote and local operators. The physical embodiment of these logical relationships, as shown in the generalized physical architecture (figure 3) may result in various communication components existing in different data communication networks (DCN). In typical service provider networks, this usually is the case. Although only one TMN is shown in Figure 3, it is possible to extrapolate the relationships between NMSs and EMSs of different TMNs.

[3] See ITU-T M.3010, Principles for a TMN.

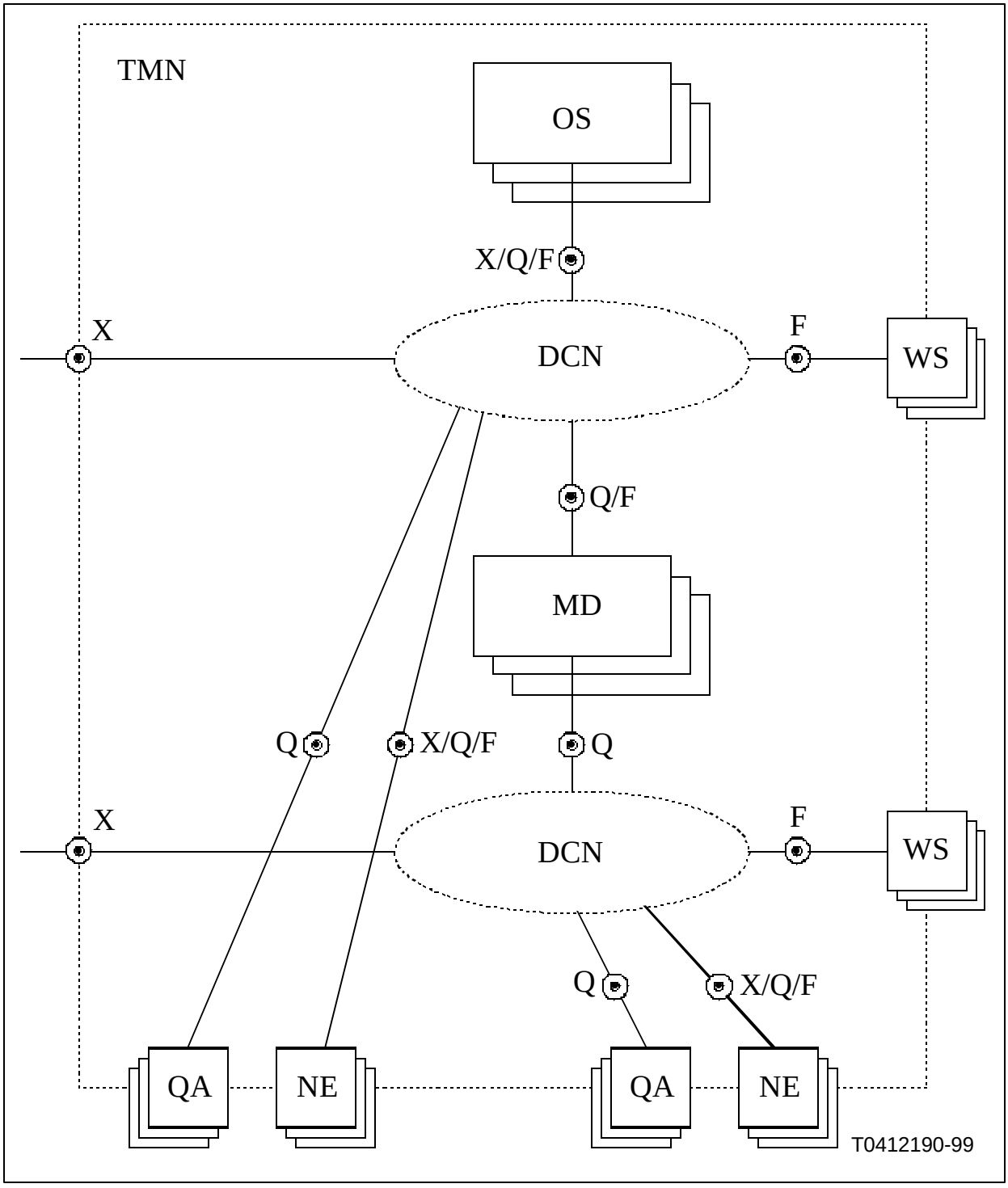



**Figure 3 – Examples of interfaces for the TMN physical infrastructure**[4]

[4] Data Communications Network (DCN), Network Element (NE), Operations System (OS), Workstation (WS), Mediation Device (MD), Q-Adapter (QA). For additional information see ITU-T-M.3010, Section 11.

## 1.2 Design Guidelines

Table 2 presents design guidelines that were considered in developing the requirements in clause 2.

**Table 2 – Design Guidelines Considered**

| Guideline | Description |
|---|---|
| Isolation | Insulation of management traffic from customer traffic |
| Effective Security Policies | Requirements and supporting architectures must allow for policies that are definable, flexible, enforceable, auditable, verifiable, reliable, and usable |
| Strong AUTHENTICATION, Authorization, and Accounting (AAA) | Two-factor and cryptographically secure AAA |
| Low Hanging Fruit | Improve security first with what is easy to implement, obvious, cheap, simple to describe, cost effective, and straightforward to verify |
| Path for Improvement | Consider what the next steps will be to improve network management security |
| Technical Feasibility | Requirements must be satisfied with products/solutions/technologies available today |
| Housekeeping | Requirements should be consistent with standard operating procedures of well-run network management operations |
| Open Standards | Use ideas and concepts that are already standardized (e.g., Internet Protocol security [IPsec], digital signatures) |

## 1.3 Applicability of this document to the TMN

This document applies to the entirety of the TMN covering both the traditional circuit-based NEs as well as new packet-based NEs. Circuit-based NEs provide multiple logical interfaces between switches, transmission elements, signaling elements, and other special-purpose elements that are designed and developed to support traditional telephony services. The new packet based NE model has migrated from the centralized system where all functions were hosted on one platform to a more distributed system where functions may be hosted by multiple platforms coupled together to form a complete system. These functions can be service or operations related. This requirements document provides a security framework to protect all of the facilities of the NE/MS that are exposed to various threats and risks. This includes the platforms, visible interfaces and the associated functions, applications and services. To provide equal protection to all types of NE/MSs, the total overall system security features should be the same for all types of NE/MSs. However, depending on the architecture of the resident and distributed features and the available processing capabilities, the implementation scheme of the security features in NE/MSs may be different in its details.

Some NE/MS will have the capacity to incorporate security features within themselves. They can fully implement all of the mandatory security requirements in this document. Other NE/MS will not have the capacity to incorporate all of the mandatory security features defined in this document within them. It may be unrealistic to ask for all security features to be embedded within the NE/MS operating system or application layers of these devices. For these types of devices that exist in or are placed into a network their security properties should be augmented so that the system meets the requirements of this standard. As an example, if a MS cannot provide STRONG ENCRYPTION for MANAGEMENT ACTIONS over a TRUSTED PATH, then an auxiliary device may be placed in the network path so that MANAGEMENT COMMUNICATIONS will go pass through this device so they may be performed over an encrypted SESSION. As another example, if an NE cannot directly enforce COMPLEX PASSWORDS, then it may utilize an Access Control Server (ACS) which can.

## 2 Normative References

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

IETF RFC 1321. The MD5 Message-Digest Algorithm. Rivest, R. April 1992.

IETF RFC 2104. HMAC: Keyed-Hashing for Message Authentication. Krawczyk, H., Bellare, M., and R. Canetti. February 1997.

IETF RFC 2403. The Use of HMAC-MD5-96 within ESP and AH. Madsen C., Glenn R., November 1998

IETF RFC 2404. The Use of HMAC-SHA-1-96 within ESP and AH. Madsen C., Glenn R., November 1998

IETF RFC 2437. PKCS #1: RSA Cryptography Specifications Version 2.0. B. Kaliski, J. Staddon. October 1998

ITU-T Recommendation X.500. The Directory: Overview of Concepts, Models and Service.

ITU-T Recommendation X.509. Information Technology - Open Systems Interconnection: The Directory: Authentication Framework.

ANSI X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).

ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation

ANSI X9.62-1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

Data Encryption Standard (DES), FIPS Publication 46-3, National Institute of Standards and Technology, October 1999.

Secure Hash Standard (SHS). FIPS Publication 180-1, National Institute of Standards and Technology

Data Signature Standard (DSS), FIPS Publication 186-2, National Institute of Standards and Technology, January 2000.

Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001.

## 3 Definitions

### 3.1 Application Administrator

A role responsible for the proper activation, maintenance, and usage of an NE/MS application. Application administration tasks include upgrading application software. [5]

[5] This task may be a function of the SYSTEM ADMINISTRATOR, if “root” authority is necessary to complete this task. Processes may be developed to control access to the “root” account.

### 3.2 Application Security Administrator

A role responsible for the proper activation, maintenance, and usage of the application layer security features of a NE/MS. The highest level of security authority for a NE/MS application instance. Tasks include the following:

- Define and assign new user and group privileges at the application level
- Maintain a record of all requests for login IDs to the application
- Add and delete users at the application level
- Monitor all application security logs
- Configure application security logging and alarms
- Manage application security logging processes

### 3.3 Application User/Operator

A role that has authorization to access business and management functions provided by the NE/MS but has no authorization to access any system administration or security administration operations within a system other than changing one's own password.

### 3.4 Authentication

AUTHENTICATION is the act of verifying a claimed identity.

### 3.5 Complex Passwords

A password is characterized as "complex" when it has some combination of alphabetic, numeric, or special characters. See clause 5.2.2 for complexity rules for static passwords.

### 3.6 Control Plane

The CONTROL PLANE performs call control and connection control functions. Through signaling, the CONTROL PLANE sets up and releases connections, and may restore a connection in case of a failure.[6]

### 3.7 Critical Security Administration Actions

A SECURITY ADMINISTRATOR is responsible for the proper activation, maintenance, and usage of the security features of a system (NE/MS). CRITICAL SECURITY ADMINISTRATION ACTIONS are as follows:

- Define and assign user privileges
- Add and delete User IDs
- Disable the use of specific User IDs as login IDs

[6] G.8080/Y.1304, "Architecture for the Automatically Switched Optical Network (ASON)," November 2001.

- Initialize and reset login passwords
- Initialize and change cryptographic keys
- Set the system's aging threshold for login passwords
- Set the system's limit on the number of failed logins for each login ID
- Remove a lockout, or change the system's lockout timer value
- Set the system's inactivity timer value
- Set system security logging and alarm configuration
- Manage the security logging processes
- Upgrade security software

### 3.8 Disable/Disabled

When referring to a User ID, a state in which the User ID cannot be used for login until the ID has been enabled by specific action from another User ID with the appropriate authorization privileges, e.g. SYSTEM SECURITY ADMINISTRATOR or APPLICATION SECURITY ADMINISTRATOR.

### 3.9 Key Strength

Different cryptographic algorithms have various degrees of security depending on how difficult they are to break. A cryptographic algorithm is considered strong if it is computationally infeasible to break—that is, it has sufficient complexity that it cannot be broken with available resources either currently or in the foreseeable future. Computational complexity is most often measured in terms of processing complexity, or the amount of time needed to perform an attack. Although the complexity of an attack remains constant for a particular algorithm and key size, computing power is constantly increasing. Good cryptosystems are designed to be infeasible to break with the computing power that is expected to evolve many years in the future. As a result of the rapid development of new technology and cryptanalytic methods, the correct key size for a particular application is continuously changing.

### 3.10 Lockout/Locked Out

When referring to a User ID, a state in which the User ID cannot be used for login until the lockout state has been removed by one or more appropriate actions. Appropriate actions include, but are not limited to:

- Automatic reset after a threshold period of time has elapsed (e.g., after 60 minutes),
- Automatic reset after successful completion of a predefined reset process (e.g., after the owner of the correctly answers a scripted set of questions), or
- Reset by specific action from another User ID with the appropriate authorization privileges, e.g. SYSTEM SECURITY ADMINISTRATOR or APPLICATION SECURITY ADMINISTRATOR.

### 3.11 Management Action

Actions undertaken by or on behalf of the SYSTEM ADMINISTRATOR.

### 3.12 Management Communication

Any communication of a MANAGEMENT ACTION.

### 3.13 Management Plane

The MANAGEMENT PLANE performs management functions for the TRANSPORT PLANE, the CONTROL PLANE, and the system as a whole. It also provides coordination between all the planes. Performance, fault, configuration, accounting, and security management functional areas identified in M.3010 are performed in the MANAGEMENT PLANE.[7]

### 3.14 Network Element/Management System

A collective term used to describe the entirety of elements within a telecommunications network including NEs, EMSs, NMSs, and OSSs.

### 3.15 Network System

Encompasses embedded software and databases including adjuncts, intelligence peripherals, and EMSs. May perform a wide range of functions related to the NE environment.

### 3.16 Protected Authentication

Includes STRONG AUTHENTICATION, TWO-FACTOR AUTHENTICATION, TRUSTED PATH AUTHENTICATION, or one-time passwords.

### 3.17 Session

A sequence of operations, either machine-to-machine or human-to-machine, that is associated with a unique process or User ID.

### 3.18 Strong Authentication

AUTHENTICATION that relies on the use of cryptographic techniques (e.g., public key encryption, symmetric key encryption, digital signatures, digital hashing techniques).[8] (Also refer to ISO/International Electrotechnical Commission [IEC] 9594-8)

### 3.19 Strong Encryption

A brute force attack occurs when an attacker tries all possible key combinations using available computing resources. In this fashion, the correct key can be found on average after one-half of all possible key combinations have been tried. The expected time to test one half of the key combinations is a measure of the strength of the encryption. Therefore, at any given time, STRONG ENCRYPTION mechanisms use algorithms and keys such that a brute force attack would take more than 2 years to break.

---

[7] The TMN architecture is described in M.3010 and additional details regarding the MANAGEMENT PLANE are provided in the M series recommendations. Source: G.8080/Y.1304, "Architecture for the Automatically Switched Optical Network (ASON)," November 2001.

[8] T1.243-1995, OAM&P—Baseline Security Requirements for TMN.

### 3.20 SuperUser

A role, which has complete access to all resources within a system and the applications residing on that system, e.g. “root” for UNIX systems. SUPERUSER roles can be used during installation, but should be used only in emergency situations for operational systems.

### 3.21 System Administrator

A role responsible for operating system (OS) level processes and procedures pertaining to installation, operations, and maintenance of the operating platform; installation of software on the platform; and control of SUPERUSER authority. Tasks include the following:

- Coordinate of installation of a new platform
- Define and assign new user and group privileges at the OS level
- Maintain a record of all requests for login IDs to the OS
- Add and delete users at the OS level
- Disable the use of specific IDs as login IDs (bin, sys, uucp, etc.)
- Install OS upgrades and patches
- Install application and database software to the OS
- Monitor all system logs
- Maintain and monitor access and changes to “root” password
- Control access to the “root” account, allowing appropriate access as the business requires
- Manage system logging processes
- Delegate administration authorizations to specific persons in other roles, including APPLICATION ADMINISTRATORS

### 3.22 System Security Administrator

A role that is responsible for the proper activation, maintenance, and usage of the system security features of a NE/MS. The highest level of security authority for a system/application instance. Tasks include the following:

- Define and assign new user and group privileges at the OS level
- Maintain a record of all requests for login IDs to the OS
- Add and delete users at the OS level
- Disable the use of specific IDs as login IDs (bin, sys, uucp, etc.)
- Monitor all system security logs

- Initialize and change cryptographic keys
- Set the system's aging threshold for login passwords
- Set the system's limit on the number of failed logins for each login ID
- Remove a lockout or changing the system's lockout timer value
- Set the system's inactivity timer value
- Configure system logging and alarms
- Manage system security logging processes
- Delegate security authorizations to specific persons in other roles, including APPLICATION SECURITY ADMINISTRATORS

### 3.23 Transport Plane

The TRANSPORT PLANE provides bi-directional or unidirectional transfer of user information, from one location to another. It can also provide transfer of some control and network management information. The TRANSPORT PLANE is layered; it is equivalent to the transport network defined in G.805. [9]

### 3.24 Trusted Path

A mechanism by which any user/operator-to-system or system-to-system interactions with a system are secured. This mechanism can be activated only by the user/operator or system and cannot be imitated. A TRUSTED PATH can either be a dedicated physical path (i.e., a terminal directly connected to the system) or an encrypted pathway (e.g., virtual private network, Secure Socket Layer [SSL] tunnel, etc.). [10]

### 3.25 Two-Factor Authentication

TWO-FACTOR AUTHENTICATION is a commonly used term to describe an AUTHENTICATION process that requires two components: possession of a physical entity (e.g., token or card), and knowledge of a secret (e.g., password or passphrase).

NOTE: - These terms appear in all capital letters when they are used in a requirement statement. For security definitions, please refer to the Partnership for Critical Infrastructure Security Common Reference Glossary, Version 2001-09.[11]

[9] G.8080/Y.1304, "Architecture for the Automatically Switched Optical Network (ASON)," November 2001.
[10] Adapted from NCSC-TG-004-88.
[11] See http://www.pcis.org.

# 4 Abbreviations, Acronyms, and Symbols

Ad Hoc Group Editor's Note: List will be checked for accuracy to ensure all acronyms used in document appear in list and list will be updated – will take place following ballot process.

| | |
|---|---|
| AAA | Administration, Authorization, and Authentication |
| AES | Advanced Encryption Standard |
| ALE | Annualized Loss Expectancy |
| ANSI | American National Standards Institute |
| CALEA | Communications Assistance to Law Enforcement Act |
| CO | Central Office |
| CORBA | Common Object Request Broker Architecture |
| COTS | Commercial Off-the-Shelf |
| CSI | Common Secure Interoperability |
| DAC | Discretionary Access Control |
| DCN | Data Communication Network |
| DES | Data Encryption Standard |
| DNS | Domain Name Server/Service |
| DoS | Denial of Service |
| DSA | Digital Signature Algorithm |
| DSS | Digital Signature Standard |
| ECC | Elliptic Curve Cryptography |
| EMS | Element Management System |
| FCC | Federal Communications Commission |
| FTP | File Transfer Protocol |
| HAZMAT | Hazardous Materials |
| HMAC-MD5 | Hashed Message Authentication Code with Message Digest 5 |
| HMCA-SHA-1 | HMAC with Secure Hash Algorithm 1 |
| HTTP | Hyper Text Transfer Protocol |
| IETF | Internet Engineering Task Force |

| | |
|---|---|
| IKE | Internet Key Exchange |
| ILEC | Incumbent Local Exchange Carrier |
| IP | Internet Protocol |
| IPsec | Internet Protocol Security |
| ISO/IEC | International Organization for Standardization/International Electrotechnical Commission |
| ISP | Internet Service Provider |
| IT | Information Technology |
| ITU | International Telecommunication Union |
| LAES | Lawfully Authorized Electronic Surveillance |
| MAC | Mandatory Access Control |
| MF | Mediation Function |
| MPLS | Multi Protocol Label Switching |
| MS | Management System |
| MTBF | Mean Time Between Failures |
| NE | Network Element |
| NEF | Network Element Function |
| NE/MS | NE, EMS, NMS, or OSS |
| NFS | Network File System |
| NME | Network and Management Element |
| NML | Network Management Layer |
| NMS | Network Management System |
| NS | Network System |
| NSIEs | Network Security Information Exchanges |
| NSTAC | National Security Telecommunications Advisory Committee |
| OAM&P | Operations, Administration, Maintenance and Provisioning |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OS | Operating System |
| OSF | Operating System Function |

| | |
|---|---|
| OSI | Open Systems Interconnect |
| OSS | Operations Support System |
| PKI | Public Key Infrastructure |
| QAF | Q-Adapter Function |
| RAM | Random Access Memory |
| RBAC | Role Based Access Control |
| RSA | Rivest, Shamir, and Adleman |
| SAML | Security Assertion Markup Language |
| SML | Service Management Layer |
| SMS | Service Management System |
| SNMP | Simple Network Management Protocol |
| SOAP | Simple Object Access Protocol |
| SRWG | Security Requirements Working Group |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| TCP | Transmission Control Protocol |
| TCSEC | Trusted Computer System Evaluation Criteria |
| TLS | Transport Layer Security |
| TMN | Telecommunications Management Network |
| TRA | Telecommunications Reform Act |
| UDP | User Datagram Protocol |
| VAR | Value Added Reseller |
| WSF | Workstation Function |
| XML | Extensible Markup Language |

# 5 Security Requirements

This clause contains the specific baseline requirements for OAM&P and operations support system (OSS) security as they specifically apply to MANAGEMENT PLANE security for infrastructure, services, and applications (see figure 1).

This clause addresses six essential principles of OAM&P security:

- Secure management traffic with STRONG ENCRYPTION and AUTHENTICATION
- Authenticate and attribute all MANAGEMENT ACTIONS.
- Manage security resources and configurations with integrity
- Maintain logs for all of the above
- Support least privilege
- Support security alarms

  NOTE – Security alarms are an area for further study.

The following table outlines the organization of this clause.

| Clause | Contents |
|---|---|
| Clause 5.1 | Discusses required security (cryptographic) algorithms and lays out key length and key management requirements |
| Clause 5.2 | Discusses requirements for AUTHENTICATION |
| Clause 5.3 | Discusses requirements for administration |
| Clause 5.4 | Describes specific security requirements for the management of NE/MSs |
| Clause 5.5 | Lays out requirements for OAM&P communications (physical or virtual management of communications networks, also known as DCN in some companies) |
| Clause 5.6 | Discusses requirements for NE/MS development and delivery |

All requirements outlined in this clause that have a prefix of M-xxx are mandatory and must be met by available components. All requirements that have a prefix of O-xxx are considered to be objectives. Objective requirements need additional examination; however, it is likely that in the future industry will coalesce around them and develop standards to address the requirements.

### 5.1 Cryptographic Algorithms and Keys

This clause specifies requirements for cryptographic algorithms, key lengths, and key management to help ensure system and network security. Requirements are identified for symmetric and asymmetric cryptographic systems, and algorithms used for data integrity and confidentiality. Note that the key lengths recommended in this clause are appropriate at present; however, increases in key lengths will be required in the future.

PROTECTED AUTHENTICATION and data confidentiality can be based on a cryptographic foundation. Cryptography uses special algorithms that are and should be standards based and publicly available thereby allowing for widespread scrutiny and ease of implementation. The “strength” of this concept is in the keys (strength refers to the amount of time required to reverse engineer [i.e., find or guess] the key value(s) being used with a specific algorithm). Consequently, the methods used to generate, store, distribute, destroy, and revoke these keys are of paramount importance. In addition, factors such as key length and key selection have a direct bearing on the amount of security a cryptosystem provides.

Security protocols (e.g., IPsec, SSL, Secure Shell [SSH]) typically provide AUTHENTICATION, integrity, and confidentiality. Security extensions to other protocols such as Simple Network Management Protocol Version 3 [SNMPv3][12], Common Object Request Broker Architecture [CORBA], Border Gateway Protocol, and Open Shortest Path First are designed to provide AUTHENTICATION and integrity. PROTECTED AUTHENTICATION and integrity are essential between NE/MS and, where deemed appropriate, confidentiality is also required.

### 5.1.1 Symmetric Encryption Algorithms

Symmetric, or secret key encryption refers to a cryptographic system where enciphering and deciphering keys are the same. Symmetric cryptosystems require that initial arrangements be made for the individuals to share a unique secret key. The key must be distributed to the individuals via a secure means, because knowledge of the enciphering key implies knowledge of the deciphering key and vice-versa.

For symmetric encryption, 128-bit Advanced Encryption Standard (AES) should be used. AES with greater than 128-bit key length (i.e., 192- or 256-bit key AES) may also be used. Fifty-six (56)-bit Data Encryption Standard (DES) has keys that are considered to be too short to be effective any longer and should not be used for any purpose unless required for export. Three key triple DES (TDES)[13], which has a worst case equivalent strength of 112 bits,[14] is acceptable but is not recommended if AES is available. For clarity, this information is presented in tabular format in Table 3.

**M-1.** For all symmetric encryption applications, algorithms at least as strong as AES or TDES shall be used. DES may be used only when required by law for export purposes.

### 5.1.2 Asymmetric Encryption Algorithms

An asymmetric encryption system is one in which the enciphering and deciphering keys are related but different: one is made public, whereas the other is kept secret. The public key is different from the private key, and no feasible way exists for deriving the private key from the public key. Public keys are distributed widely; however, the private key is always kept secret. Encryption is performed by enciphering data using a user's public key—then only the user possessing the corresponding private key can decipher the message.

For asymmetric encryption, the Rivest, Shamir, Adleman (RSA) algorithm is recommended to be used with a key length of 2,048 bits or greater, which is roughly equivalent in cryptographic strength to the 128-bit symmetric key encryption. The Diffie-Hellman key exchange algorithm with a prime group of 2,048 bits or greater may also be used (e.g., as employed in the Internet Key Exchange [IKE] algorithm). Elliptic Curve Cryptography (ECC) is a new method of performing public-key cryptography (i.e., the existing RSA encryption algorithm). With ECC, an elliptic curve is defined over a certain field; then, the elliptic curve discrete logarithm problem is solved over this field. The main advantage of ECC as compared to other public-key algorithms is the key size. A 160-bit ECC key is approximately equivalent in security to a 1,024-bit RSA key, and a 210-bit ECC key is approximately equivalent to a 2,048-bit RSA. The smaller ECC key results in less computational overhead and a more efficient cryptosystem.[15] For clarity, this information is presented in tabular format in Table 3.

---

[12] SNMPv3 may also provide confidentiality.

[13] TDES is specified in Federal Information Processing Standard (FIPS) Publication 46-3, Appendix 2, Page 22. See http://csirc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[14] TDES can be performed using either two independent 56-bit keys or three independent 56-bit keys, which could be expected to have a strength of 112 bits and 168 bits, respectively. However, TDES is subject to the "meet in the middle" attack, which can reduce two key 3DES strength to only 57 bits rather than the expected 112 bits. The same attack can render three key TDES strength to only 112 bits rather than the expected 168 bits. Thus, TDES should be used with three independent keys and the worst case strength should be assumed to be 112 bits. Source: Bruce Schneier, *Applied Cryptography*, Second Edition, 1996, John Wiley & Sons, Chapter 15.2, p. 358.

[15] See http://csrc.nist.gov/cryptval/dss.htm for more details on RSA, Diffie-Hellman, and ECC.

**M-2.** For all asymmetric encryption applications, algorithms at least as strong as the RSA 2,048-bit key algorithm shall be used.

**M-3.** For all key exchange applications, algorithms at least as strong as 2,048-bit RSA or Diffie-Hellman with a prime group of 2,048 bits shall be used.

### 5.1.3 Data Integrity Algorithms

Keyed message digest algorithms combined with hashing functions are used to ensure data integrity for arbitrary length messages. For symmetric data integrity where the sender and receiver have the same key, the Hashed Message Authentication Code with Message Digest 5 (HMAC-MD5)[16] algorithm or the Hashed Message Authentication Code with Secure Hash Algorithm 1 (HMAC-SHA-1)[17] algorithm is acceptable.

**M-4.** For all symmetric secure data integrity applications, algorithms at least as strong as HMAC-MD5 with 128-bit keys or HMAC-SHA-1 with 160-bit keys shall be used.

The Digital Signature Standard (DSS), with a key length of 1,024 bits or greater in length, and RSA are excellent standards for asymmetric data integrity where public-private key pairs are used.[18]

**M-5.** For all asymmetric secure data integrity applications, an algorithm at least as strong as DSS or RSA shall be used.

### 5.1.4 Keys for Cryptographic Algorithms

According to current best practices for KEY STRENGTH, when a key is chosen, it should be expected that it can not be broken using a brute force attack in less than 2 years. The key length recommendations in this clause are made with this in mind.

**M-6.** Any key for encryption or data integrity shall have a KEY STRENGTH that takes at least 2 years to break the key using known technology when first provided or used. Weaker keys may be used only when required by law for export purposes.

**Table 3 – Cryptographic Algorithm Requirements**

| Category | Algorithm | Minimum Key Length as of October 2002 | Optional Key Lengths | Comments |
|---|---|---|---|---|
| Symmetric Encryption | AES | 128 bits | 192 bits, 256 bits | Standard algorithm chosen by the National Institute of Standards and Technology (NIST) to replace DES |
| | TDES (3 key) | Worst case strength equivalent 112 bits | N/A | Near the end of its useful life |
| | DES | Not allowed | Not allowed | For export use only when required by law |

[16] Internet Engineering Task Force (IETF) Request for Comment (RFC) 2403.
[17] IETF RFC 2404.
[18] See http://csrc.nist.gov/cryptval/dss.htm

| Category | Algorithm | Minimum Key Length as of October 2002 | Optional Key Lengths | Comments |
|---|---|---|---|---|
| Asymmetric Encryption | RSA | 2,048 bits | >2,048 bits | 2048 bits chosen to be roughly equivalent in cryptographic strength to 128 bit symmetric |
| | Elliptic Curve | 210 bits | >210 bits | A set of relatively new algorithms. 210 bits chosen to be roughly equivalent in cryptographic strength to 128-bit symmetric |
| Key Exchange | Diffie-Hellman | 2,048-bit MODP group, 256 bit exponent | >2,048-bit MODP group, >256 bit exponent | 2,048 bits chosen to be roughly equivalent in cryptographic strength to 128-bit symmetric. |
| Message Verification | DSS (asymmetric) | 1024 bits | >1024 bits | Digital Signature Algorithm. 1024 bits mandated by NIST[**)] |
| | HMAC-MD5 (symmetric) | 128 bits | N/A | Hashed message authentication code with message digest 5 |
| | HMAC-SHA-1 (symmetric) | 160 bits | N/A | Hashed message authentication code with secure hash algorithm 1 |

[**)] See http://csrc.nist.gov/cryptval/dss.html

### 5.1.5 Cryptographic Key Management

Properly managing cryptographic key material is difficult and often complex. Below are a few requirements that any effective key management system must satisfy. However, the requirements do not assure the security of the key management system, method, or process.

Secure methods, at a minimum, include not sending keys over a communication medium in the clear and not storing keys in the clear in system memory or storage media. These requirements apply to symmetric encryption keys, symmetrically based digital signature keys, and asymmetric private keys.

**M-7.** The NE/MS supplier shall provide capabilities for secure key generation, distribution, storage, and replacement/recovery, as defined in ITU X.500 and X.509.

**M-8.** Keys used for symmetric encryption and symmetrically based digital signatures shall be distributed out of band or by secure cryptographic processes.

## 5.2 Authentication

AUTHENTICATION has two purposes in securing the MANAGEMENT PLANE: (1) it provides a basis for setting up private communications with full data integrity between two systems; and (2) it provides a basic mechanism for logging and auditing the management activities on any system.

### 5.2.1 Server-to-Server Process Authentication

Process AUTHENTICATION provides AUTHENTICATION during data communications between systems (e.g., server-to-server, application-to-application), and is the basis for setting up private communications with full data integrity. During data communications, AUTHENTICATION of the sending entity allows the receiver of a message to ascertain the origin of the message. Within a secure communication channel, cryptographic AUTHENTICATION should be associated with each message to bind the sending entity's identity to the message. The receiver will check the cryptographic information supplied with the message to verify the true identity of the sending entity.

**M-9.** Server-to-server process AUTHENTICATION for communications shall use certificate-based AUTHENTICATION or PROTECTED AUTHENTICATION.

**M-10.** Certificate-based AUTHENTICATION shall be X.509-based certificate systems.

**M-11.** STRONG AUTHENTICATION exchanges between systems shall be protected in compliance with M-6.

### 5.2.2 User Authentication, Static Passwords, and User IDs[19]

User AUTHENTICATION concerns the AUTHENTICATION of clients involved in the management of the network. In this case, AUTHENTICATION involves proving the true identity of the legitimate user and preventing masquerading by illegitimate imposters. With proper AUTHENTICATION, it is possible to track activities and restrict users to pre-authorized activities or roles as discussed in clause 5.3.

The minimum requirements for AUTHENTICATION for NE/MS are through the use of a user ID and static password. Other mechanisms may be used as long as the administrators of the NE/MS are confident that the security level is at least as great as that of the use of a user ID and static password. Other mechanisms that may be considered include:

- A user ID and TWO-FACTOR AUTHENTICATION using a one-time password generator,
- TWO-FACTOR AUTHENTICATION using a smart-card with credentials stored on it in a protected manner, and
- TWO-FACTOR AUTHENTICATION using credentials stored within a certificate in a protected manner.

**M-12.** Client AUTHENTICATION for logging in, logging, and auditing on each NE/MS shall be at least as strong as a User ID with a COMPLEX PASSWORD over a previously established TRUSTED PATH.

M-12 presents the baseline security requirement. It is expected that AUTHENTICATION techniques and single sign-on technologies will continue to improve.

O-1 represents an objective requirement that anticipates standardization around single sign-on and digital certificates.

**O-1.** Client AUTHENTICATION should support methods for secure single sign-on and X.509 PKI.

The following requirements help maintain password complexity and are useful for auditing and logging.

[19] This clause does not discuss non-static passwords as those are considered to be outside of the scope of defining the minimum security requirements in the document.

**M-13.** Each NE/MS shall automatically enforce COMPLEX PASSWORDS. Minimum complexity rules for static passwords are as follows:

- Passwords must be a minimum of eight characters long.
- Passwords must not be a repeat or the reverse of the associated User ID.

**M-14.** COMPLEX PASSWORDS must contain at least three (3) of the following combinations:

- Alpha characters – at least one (1) lower case alpha character
- Alpha characters – at least one (1) upper case alpha character
- Numeric characters – at least one (1) numeric character
- Special characters – at least one (1) special character
- No more than three (3) of the same characters used consecutively

**M-15.** Each NE/MS shall automatically ensure that each new login password differs from the previous password. The degree of difference shall be configurable, with a default difference of at least two positions.

**M-16.** Each NE/MS will support a password history preventing reuse. The parameters shall be configurable with a default of at least the past five password iterations and at least 180 days.

**M-17.** Each User ID must have its own settable login password.

**M-18.** Each NE/MS shall identify at least one, and not more than two, specific SYSTEM SECURITY ADMINISTRATOR accounts that cannot be LOCKED OUT due to password aging.

A common implementation of M-18 allows the SYSTEM SECURITY ADMINISTRATOR to login from the console with no restrictions on the number of failed logins. Alternatively, that user can have a retry timer (e.g., 60 minutes). If no retry timer is used for non-console attempts, then the password for that User ID is vulnerable to a brute force password attack.

**M-19.** Each NE/MS shall identify at least one, and not more than two, specific SYSTEM SECURITY ADMINISTRATOR account(s) that cannot be LOCKED OUT due to login failures.

**M-20.** Each NE/MS shall store User IDs in a nonvolatile manner.

**M-21.** Each NE/MS shall store login passwords in a nonvolatile and one-way encrypted manner. As an exception to one-way encryption, symmetrically encrypted passwords can be used for passwords that need to be decrypted for internal, transient use in trusted system-to-system communication or single sign-on.[20]

### 5.3 Administration

Each NE/MS must support the concept of "least privilege" (i.e., a person will have a role and will have authorization to view data, modify data, or initiate MANAGEMENT ACTIONS only for those functions required by that role. This clause defines basic requirements for implementing "least privilege" through good system security administration.

[20] See clause 5.1 for a discussion of symmetric encryption.

### 5.3.1 Security Administration

Each NE/MS must ensure that only authorized users are allowed to manage system security resources. Though only five types of users are discussed, many other types of users with various degrees of privileges may exist, especially with respect to critical security MANAGEMENT ACTIONS. The goal is to ensure that only authorized, privileged users can manage critical security resources.

**M-22.** Each NE/MS shall have at least five types of user roles: a SYSTEM SECURITY ADMINISTRATOR, an APPLICATION SECURITY ADMINISTRATOR, a SYSTEM ADMINISTRATOR, an APPLICATION ADMINISTRATOR, and an APPLICATION USER/OPERATOR. In the case of embedded systems without a separation of system and application, the NE shall support at least three types of user roles: a combined SYSTEM SECURITY ADMINISTRATOR and APPLICATION SECURITY ADMINISTRATOR, a combined SYSTEM ADMINISTRATOR and APPLICATION ADMINISTRATOR, and an APPLICATION USER/OPERATOR.

**M-23.** The default user type on each NE/MS shall be the APPLICATION USER/OPERATOR.

**M-24.** Each NE/MS shall support the following CRITICAL SECURITY MANAGEMENT ACTIONS:

- Define and assign user privileges.
- Add and delete User IDs.
- DISABLE/enable the use of specific User IDs as login IDs.
- Initialize and reset login passwords.
- Initialize and change cryptographic keys.
- Set the system's aging threshold for login passwords.
- Set the system's limit on the number of failed logins for each login ID.
- Remove a lockout or change the system's LOCKOUT timer value.
- Set the system's inactivity timer value.
- Set system security logging and alarm configuration.
- Manage system security logging processes
- Upgrade security software.

**M-25.** On each NE/MS, a SYSTEM SECURITY ADMINISTRATOR shall be able to execute all of the CRITICAL SECURITY MANAGEMENT ACTIONS.

**M-26.** On each NE/MS, a role other than the SYSTEM SECURITY ADMINISTRATOR shall NOT be able to execute any of the CRITICAL SECURITY MANAGEMENT ACTIONS unless a SYSTEM SECURITY ADMINISTRATOR has delegated these specific authorizations.

### 5.3.2 Authentication Defaults

The proper use of default passwords has been discussed at length in security literature. Historically, default passwords ranged from hard coded in the program to a default associated with each software release or upgrade. The following are AUTHENTICATION default requirements.

**M-27.** One of the following shall apply:

- The configuration software shall create a unique initialization password for each application in the new release or upgrade[21] of the software.
- If a default password is used, the system shall require the replacement of the default password with a unique password before it goes into service.

**M-28.** The system age threshold for login passwords shall be configurable by the SYSTEM SECURITY ADMINISTRATOR or by the APPLICATION SECURITY ADMINISTRATOR if the functionality is also built into the application. The default shall be 90 days.

**M-29.** The system inactivity timer value shall be configurable by the SYSTEM SECURITY ADMINISTRATOR or by the APPLICATION SECURITY ADMINISTRATOR if the functionality is also built into the application. The default shall be 1 hour.

**M-30.** The system limit on consecutive failed logins for a given User ID shall be configurable by the SYSTEM SECURITY ADMINISTRATOR or by the APPLICATION SECURITY ADMINISTATOR if the functionality is also built into the application. The default shall be five.

### 5.3.3 Security Audit Logging

Each NE/MS shall provide adequate capabilities to allow investigation, audit, and real-time detection and analysis activities, so that proper remedial actions can be taken. This clause considers security audit logs; however, the specific details of the content and format of the security audit logs are beyond the scope of this document.

Note that investigation and forensic analysis activities may include investigation of non-security related OAM&P messages as well as the information stored in the security audit logs described in this section. Logging of non-security related OAM&P messages (sometimes referred to as “Recent Change” messages) is beyond the scope of this document.

**M-31.** Each NE/MS shall be able to log each CRITICAL SECURITY ADMINISTRATION ACTION, each login attempt and its result, and each logout or SESSION termination.

**O-2.** Each NE/MS should provide the capability to configure those CRITICAL SECURITY ADMNISTRATOR ACTIONS that are to be included in the security log.

It is recommended that audit log entries be sent to an unalterable audit server after being sequence labeled and cryptographically authenticated (signed) by the NE/MS.

**M-32.** Each NE/MS shall be capable of remote logging over a TRUSTED PATH.

**M-33.** Each log entry shall contain the following information:

- A description of the action or the actual action that is being logged

[21] This is similar to the practice in which each commercially purchased compact disk carries a unique enabling password.

- The identity and security level of the user that initiated the action
- The date and time the action occurred
- Network source and destination information, if applicable (e.g., when logging in)
- An indication of the success or failure of the activity.

Additional information on logging may be found in T1.243.

### 5.4 NE/MS Use and Operation

The requirements in this clause apply to both remote and console access to a NE/MS. These mandatory requirements represent a baseline for NE/MS that actually store user IDs and passwords. Many NE/MS reference a centralized authentication control server (ACS) to store user IDs and passwords. The mandatory requirements expressed throughout this document shall apply to a NE/MS if it holds user IDs and passwords and shall apply to the user IDs and passwords stored on the ACS.

**M-34.** For each NE/MS, each MANAGEMENT ACTION shall be associated with a single authorized SESSION.

**M-35.** Each SESSION shall be established via proper AUTHENTICATION as detailed in requirement M-12.

**M-36.** Communications between a NE/MS and an ACS for the purposes of conveying AUTHENTICATION credentials shall occur over a TRUSTED PATH.

#### 5.4.1 Login Process

**M-37.** The APPLICATION SECURITY ADMINISTRATION or SYSTEM SECURITY ADMINISTRATOR shall assign each User ID used to log in to an application or host computer system to unique individuals.

**M-38.** Each NE/MS shall automatically force the user to change their password on the first access after the account has been established an on the first access after the password has been reset.

**M-39.** The NE/MS application shall work properly without SUPERUSER access privileges for any application roles (i.e., APPLICATION USER/OPERATOR, APPLICATION ADMINISTRATOR, and Application System Administrator).

**M-40.** Each NE/MS must display the time and date of the last successful AUTHENTICATION by the user during the logon process.

**M-41.** Customizable proprietary information statement and no trespassing warning must be displayed on the initial entry screen before any logical access is allowed. Equipment should support a minimum length of 1,600 characters. A default message should be provided. The following is an example of a warning banner:

> WARNING! This computer system and network is PRIVATE and PROPRIETARY and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network. The owner, or its agents, may retrieve any information stored within the computer system or

network. By accessing and using this computer system or network, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the computer system or network, including information stored locally or remotely on a hard drive or other media in use with this computer system or network.

It is recommended that each entity develop an appropriate warning banner.

**M-42.** Any failed login attempt shall report to the user only that the login process has failed or is invalid. Information such as "invalid User ID" or "invalid password" shall not be reported.

**M-43.** Each NE/MS shall LOCKOUT a user account from logging in after a configurable threshold number of login failures has been reached. The LOCKOUT shall include the console interface. The LOCKOUT shall NOT include the SUPERUSER account. The default value is five logon failures.

**M-44.** Each NE/MS shall have no mechanism for bypassing the login AUTHENTICATION and logging in processes.

**M-45.** No NE/MS shall ever display a password in plaintext or provide any indication of the number of characters in the password, including displays on terminal screens, printouts, and log records.

**M-46.** Each NE/MS shall enforce password aging with a configurable threshold.

A common and acceptable implementation of M-46 is for the system to immediately require the user to set a new password after authenticating the user with the old password. Alternatively, the system may require a SECURITY ADMINISTRATOR to properly change the password. If an account has not been used for a period of time, it will be considered dormant.

**M-47.** If a login password has surpassed the age limit for that system, then the NE/MS shall LOCKOUT the login for that User ID until the password is properly changed. The default age limit is 90 days.

**M-48.** If an account, including the SYSTEM ADMINISTRATOR account has been dormant for a configurable threshold period of time, each NE/MS shall generate an alert. The default value is to alert after 120 days.

**M-49.** If an account has been dormant for a configurable threshold period of time, each NE/MS shall generate an alert and the account shall be DISABLED. The DISABLE process shall NOT include the SYSTEM ADMINISTRATOR account, the SYSTEM SECURITY ADMINISTRATOR account, and the SUPERUSER account. The default value is to alert and DISABLE the account after 180 days.

**M-50.** A DISABLED login ID shall be re-enabled by at least one of the following methods:

- A properly logged-in APPLICATION SECURITY ADMINISTRATOR
- A properly logged-in SYSTEM ADMINISTRATOR
- A properly logged-in SYSTEM SECURITY ADMINISTRATOR

The options to re-enable login IDs can be configured at the system level and at the role level. The default allows Options 1, 2, and 3 for both levels.

**M-51.** A LOCKED OUT login ID shall be reset to remove the LOCKOUT condition by at least one of the following methods:

- A properly logged-in APPLICATION SECURITY ADMINISTRATOR
- A properly logged-in SYSTEM ADMINISTRATOR
- A properly logged-in SYSTEM SECURITY ADMINISTRATOR
- Automatically, following the crossing of a configurable timeframe. The default delay must be at least 60 minutes.

The options to remove a LOCKOUT from login IDs can be configured at the system level and at the role level. The default allows Options 1, 2, and 3 for both levels.

### 5.4.2 Logout Process

**M-52.** Each properly logged-in SESSION shall be logged out by either the user or the system resulting from inactivity.

**M-53.** Each NE/MS shall log out a properly logged-in SESSION when the time since the last activity for that SESSION exceeds the system's inactivity timer value.

### 5.4.3 Applications

**M-54.** A user's role type shall remain unchanged during the execution of and exit from any NE/MS application.

In particular, the user must not be able to "shell escape" to a SUPERUSER mode. Or, if the application fails, it must not leave the user in a different role with more privileges. The user must reauthenticate (relog-in) in order to assume a different role.

## 5.5 Communications

Secure communications are the foundation for securing the MANAGEMENT PLANE in a modern network. Annex A discusses architectures and protocols for implementing secure MANAGEMENT COMMUNICATIONS. The mandatory requirements defined in this clause shall apply to all X, Q, and F interfaces of a TMN as described in the ITU-T recommendation M.3010.

**M-55.** For each physical or logical interface that carries any MANAGEMENT TRAFFIC in an NE/MS, the NE/MS shall be configurable to secure MANAGEMENT TRAFFIC with STRONG AUTHENTICATION and symmetric or asymmetric encryption in order to provide confidentiality and integrity.

## 5.6 NE/MS Development and Delivery

Security of an NE/MS is dependent on the complete life cycle process. Security is an issue during conceptual design and remains an issue through detailed design, development, deployment, and decommissioning of a product. Appropriate controls and testing during the complete life cycle process are critical to providing acceptable levels of security. Clauses B.5.2 and B.5.3 discuss additional life cycle considerations.

**M-56.** All software delivered to a service provider or other customer must include cryptographic AUTHENTICATION and integrity protection mechanisms such as digital signatures or symmetric message AUTHENTICATION as specified in clause 5.1.

**O-3.** All NE/MS receiving software should be capable of interpreting the cryptographic AUTHENTICATION and integrity protection mechanisms and verifying the source and integrity of the software.

**M-57.** All software updates including patches must be transmitted to the receiving NE/MS over a TRUSTED PATH.

**M-58.** All NE/MS receiving software must be capable of interpreting the cryptographic AUTHENTICATION and integrity protection mechanisms and verifying the source and integrity of the software.

**M-59.** All NE/MS must be able to electronically determine their current software and hardware revision levels and to validate appropriate software/firmware configurations.

**Annex A**

(Informative)

# A Architectural Considerations and Examples

This annex describes considerations for providing security at each protocol layer. Table A.1 describes the basic alternatives for secure network architectures based on the open systems interconnect (OSI) layers.

**Table A.1 – Pros and Cons Based on OSI Layers**

| Layer | Protocols | Viability | Pros | Cons |
|---|---|---|---|---|
| 1 | Physical | None | N/A | N/A |
| 2 | Ethernet MAC and LLC, PPP, Frame Relay, LAP(B\|D\|S), and others | Low | N/A | In some cases, encryption is difficult to tie to AAA. |
| 3 | IPsec | High | Available, minimal device impact possible. Works with any application. | Bootstrapping, installation, and full resets can possibly open vulnerabilities. |
| 4 | SSL/TLS | High | Available, well integrated w/PKI. Allows specific port for each type of traffic (HTTP/SSL: 443, LDAP/SSL: 636, etc.) | Nontrivial interface for each element. Provides only security mechanisms for traffic running over TCP. No protection for user datagram protocol (UDP), RTP, or SCTP traffic. |
| 7 | SNMPv3, CORBA, XML | Medium | Specific security solution targeted to particular application. Independent of underlying transport. | Difficult to create a seamless architecture. Difficult to deploy in embedded systems. |

Security can be added at different layers within the OSI seven-layer model. Usually, security exists at the Application Layer (Layer 7), Transport Layer (Layer 4), Network Layer (Layer 3), or Data Link Layer (Layer 2). These layers are described below.

## A.1 Application Layer Security

Application layer security provides a security solution targeted specifically to a particular application, which must be implemented in the end hosts. An example of application level security is an SSH terminal session that may be used as a secure replacement for Telnet.

Application layer security has the advantage of easy access to user credentials because it operates in the context of the user, which makes user AAA services easier to implement. Also, an application can be extended for security without having to depend on the OS to provide these services.

The downside of application level security is that security mechanisms must be designed independently for every application that needs to be secured. Thus, it is very difficult to create seamless and scalable security architectures.

### A.2 Transport Layer Security

TLS provides security services at the TCP layer. SSL, which is being standardized by the Internet Engineering Task Force (IETF) as TLS, is the security protocol that provides security at the transport layer.

As shown in figure A.1, a single SSL/TLS instance can be used to create multiple SSL/TLS sessions through an IP network to provide security for various applications. Modifications are required to each application to allow that application to request SSL/TLS security services. SSL/TLS is the de-facto standard for Web-based HTTP traffic. All standard Web browsers include built-in SSL/TLS technology.

Because SSL/TLS technology does not operate in the context of the user, obtaining user context is difficult, making it harder to implement user AAA services. SSL/TLS is applicable only to TCP traffic and cannot be used to protect UDP traffic.

The significant security advantage of using SSL/TLS over network layer security is that SSL/TLS allows the transport layer protocols to be represented by a TCP port number that are registered by the Internet Assigned Numbers Authority. Consequently, firewalls can be used to enforce access control based on authorized communications types for a variety of users and a variety of functions (e.g., remote access, file transfer, and device management).

### A.3 Network Layer Security

Network layer security provides security services at the IP layer. The IETF IPsec Suite is the security protocol that provides security at the network layer. IPsec is optional for IPv4 and a mandatory component of IPv6.

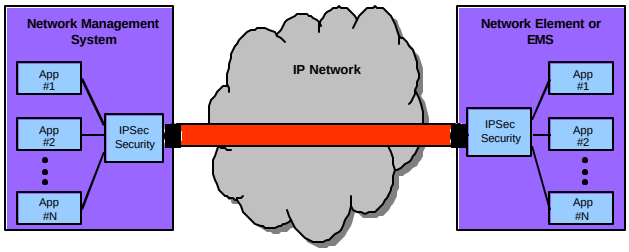
As shown in figure A.1, a single IPsec tunnel can be used to protect data from many different applications or transport protocols, or both. No modifications are required to the applications, and the security services appear transparent to the applications. IPsec is the de-facto standard used for creating network layer virtual private networks.

Because IPsec technology does not operate in the context of the user, obtaining user context is difficult, making it harder to implement user AAA services. A human should authenticate himself or herself to the workstation, and the workstation can then act as AUTHENTICATION proxy for the human to other systems. Authenticated operator IDs can be logged as part of the command execution for nonrepudiation. Use of multiple-user IPsec tunnels weakens attribution to a single individual and acts as a “backdoor” into networks, weakening defense-in-depth measures such as firewalls and intrusion detection systems.

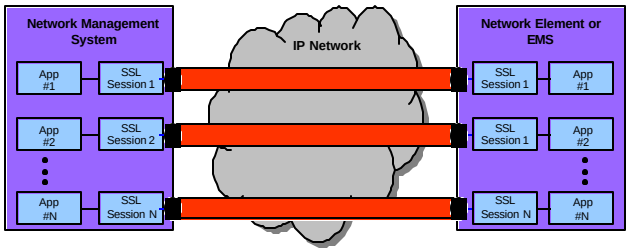
### A.4 Data Link Layer Security

If two devices are connected by a data link (e.g., FR VC, PPP, and Ethernet) and all the traffic between the two devices needs to be encrypted, then data link encryption can be used to provide confidentiality. The data link encryption can be provided by the end devices or by external encryption devices. The advantages to using external data link encryption include speed and lower processing requirements on the end devices; however, the solution is not scalable. This solution only works well for devices connected by a common Layer-2 technology (e.g., Ethernet, PPP, and Frame Relay). A disadvantage of this solution is that each link in the network has to be encrypted separately and the information is not protected once it leaves a link (i.e., enters an X.25 switch, Ethernet switch, IP router, etc.).

### Layer 3 Security (IPSec)




### Layer 4 Security (SSL Session for TCP)




### Layer 7 Security (Specific Application Security)

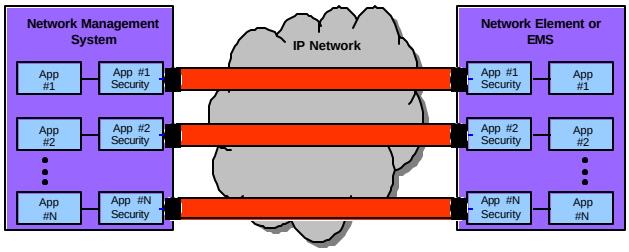



**Figure A.1 – Security at Different Layers in the OSI Model**

**Annex B**

(Informative)

# B Additional Security Considerations

The security procedures detailed in the subsequent clauses are tutorial in nature. They are outside the scope of detailed requirements provided by this document, but should be considered to provide a secure system. In some cases, mandatory language is used; however, this is provided for informational purposes and should serve only as an example. Protocols and recommendations included in this annex are subject to future discussions and contributions. They do not represent any intent to include or exclude content in existing or emerging standards.

## B.1 Applicability to Enterprise OAM&P

Enterprises today have evolved beyond the traditional isolated enterprise networks of the past. Enterprises have grown to multi-site businesses that span large geographical areas requiring extranet network connection to customers and business partners. Enterprises must allow partners and customers to gain access to internal data and make operational business decisions based on this data.

Enterprise networks are developed and administered by the enterprise itself or have been purchased as a managed network from a network provider. Services being developed by providers will allow the enterprise to manage their portion of a larger network environment. These services are based on national and international standards.

As the industry moves forward, requirements for access to fault and performance data, and the ability to configure various components of the network by the contracting enterprise, necessitates that appropriate security mechanisms are in place. These mechanisms must provide adequate control for protecting not only the enterprises' managed network, but also providers' own internal network. The internal network may be interconnected to these enterprise networks and may be a part of the national telecommunications infrastructure.

In summary, the security requirements for OAM&P traffic outlined in this document are fully applicable to enterprises and service provider/carrier networks. In larger enterprises, the line between large enterprise networks and carrier networks continues to blur. In smaller enterprises, the security emphasis is on the authentication, authorization, and logging requirements described in this document. Less emphasis will be placed on encryption technologies resulting from the smaller and more isolated nature of their networks.

## B.2 CORBA, SNMP, XML, and SOAP

The following considerations should be taken into account with regard to security for CORBA, SNMP, Extensible Markup Language (XML), and Simple Object Access Protocol (SOAP). Although no changes to these evolving protocols are proposed, the following discussion could be used to enhance security.

### B.2.1 CORBA

The CORBA Security Service comprises the security functionality of authentication of principals (human users and objects), authorization of access to objects by principals, security auditing, communication security, nonrepudiation, and administration. All of this may be overkill for many applications, though. Instead, applications might require only the communication security and system-level authentication functionality based on Transport Layer Security (TLS) technology (and its precursor, SSL) for availability and simplicity reasons. Finally, some applications might require no security. The optional requirements below, therefore, reflect three possible choices:

- No security

- ORBs use SSL to provide communications security and system-level authentication, which is essentially "session" security

- ORBs use the CORBA Security Service to provide communications security, authentication, nonrepudiation, and access control lists for groups or individuals accessing individual objects and operations

Additional information on security in the CORBA framework may be found in Q.816, CORBA-Based TMN Services and Q.816.1, CORBA-Based TMN Services Extensions to Support Course-Grained Interfaces.

If CORBA is used in the NE/MS interfaces, then CORBA security mechanisms should be applied. Conformance level of the CORBA security implementation should be clear. The following discussion provides guidance regarding CORBA security. No attempt to identify standards should be inferred. When supplying products or systems based on CORBA, the basic security levels are as follows:

- Level 0: No application security is provided, and programs are security unaware. Authentication, encryption, data integrity, object invocation authorization, audit trails, and security domain administration should be provided.

- Level 1: Programs may be security aware, which means that they may call an application programming interface for access to additional services such as verification of signatures, check access to objects, and write audit records.

- Level 2: Provides support for digital signatures permitting signing and nonrepudiation of transactions. This is particularly important when operating across various organizations— for example, in a business-to-business context or network management peering arrangement.

The Common Secure Interoperability (CSI) Specification defines standards by codifying the specification for secure interoperability when using General Inter-Object Request Broker Protocol/Internet Inter-Object Request Broker Protocol:

- CSI Level 1: The identity of the initiating principal is communicated from sender to receiver.

- CSI Level 2: The identity of the initiating principal is communicated from sender to receiver, but the identity can be delegated to other objects so that other objects can impersonate the user.

- CSI Level 3: In addition to identity being passed, the attributes of the initiating principal passed from client to target may include other authorization information, such as membership of roles or groups.

It is incumbent on suppliers to—

- Be fully conversant with the security capabilities of the Object Request Broker technology selected,

- Ensure it meets the requirements for security outlined elsewhere in this document.

As its name implies, CORBA deals with objects. Object security is about preventing the unauthorized use of objects by enforcing a set of access control rules. CORBA security ensures users are accountable for their actions on or with an object and ensures the availability of objects.

Object security differs from many other aspects of security. Frequently, the developer does not need to know security details because security is applied at a later stage as if with a wrapper. Therefore, certain

aspects are vitally important. In CORBA, names may be duplicated or may not exist at all; only reference numbers may exist. It should be possible to define an object's policy without knowing the object's name. Similarly, it must be possible to define an object's policy even on objects with many names, and the policy must be applied regardless of the name used to secure the object.

Typical object-oriented systems have tens of thousands of objects, and it is not reasonable to expect security to be defined for individual objects. Therefore, it should be possible to group together objects and define a policy for the group of objects whose protection needs are similar.

- *End-to-End Authentication:* CORBA can pass the user context to another application. Where a strong trust relationship has been established between these systems, it may be possible to accept this information without further verification. However, where other mechanisms do not exist, it may be necessary for the security of other systems to be tightly coupled with CORBA security. End-to-end authentication is very important, and it is worth checking whether the vendor supports this.

- *Access Control:* CORBA supports the idea of role-based login. Systems should always be developed using this feature because not only does it reduce costs of administration; it simplifies it, which means that the configuration is less likely to have errors.

- *Encryption:* Use of encryption within CORBA must comply with the requirements stated in this document. Full use should be made of CORBA features for integrity, confidentiality, and origin authentication, especially when communicating over a network of any type.

- *Policy Administration:* CORBA policy administration is responsible for setting up information about domains, users, roles object access policy, message protection policy, and audit policy. Clarity should exist throughout the design of all aspects of domain and object naming. Roles should be clearly defined with the aim of ensuring appropriate segregation of duties.

### B.2.2 SNMP Security

SNMP, a widely used method of administering a variety of processor-based equipment, offers the ability to—

- Obtain device configuration parameters

- Set device configuration parameters

- Send alerts from the managed device to a central analysis system.

Many deployed versions of SNMP have significant security vulnerabilities. In Versions 1 and 2, the password (known as the community string) is transmitted in clear text. In addition, although checks may be made to validate the Internet protocol (IP) address of the client, a moderately determined attacker can spoof IP addresses. Versions 1 and 2 of SNMP create significant security exposures in several networks. Therefore, SNMP Versions 1 and 2 should be used only as a last resort. ITU Study Group 4 is considering the establishment of two new protocol stacks:

- SNMPv3 or V2C with TLS over TCP (no access control), and

- SNMPv3 with user security model over UDP (as a forward looking stack).

Where SNMP is deployed, Version 3 is the preferred level. SNMP Version 3 is more secure and should be used in all new systems because it provides protection against modification of data, masquerade, re-ordering of messages, and loss of confidentiality. The following countermeasures should be considered to secure SNMPv3 access to NEs:

- An SNMP agent should send an alert to a manager if it receives a command originating from an unknown source.

- The default community string should not be used.

- Access violations and access errors should be logged to a syslog server.

- SNMPV3 uses DES as default; however, more secure algorithms can be used.

- SNMPV3 should be used at least with AuthNoPriv, which provides authentication but no confidentiality of transactions. Preferably, AuthPriv will be used.

- SNMP agent logging should be enabled.

- Access control lists should be used to only allow SNMP messages from an authorized manager (identified by IP address). SNMP messages from all other sources (i.e., other IP addresses) should be denied and treated according to appropriate security policies.

- Any service or capability not explicitly required should be disabled, including SNMP if it is enabled.

- Unauthorized access to SNMP services should be blocked or filtered at the network perimeter.

- SNMP agent systems should be configured to disallow request messages from unauthorized systems.

- SNMP traffic should be segregated onto a separate management network.

### B.2.3 XML

The XML standard provides language for defining data structures. The current standard is 1.0. Version 1.1 is a candidate recommendation under review. The Organization for the Advancement of Structured Information Standards' (OASIS) Security Services Technical Committee is seeking to broaden security functionality by leveraging XML. OASIS is working on finalizing Security Assertion Markup Language (SAML). SAML is based on four assertions:

- *Authentication*—issuer has authenticated the object,

- *Attribute*—specific uniform resource identifier or extension schema that defines the attribute,

- *Decision*—reports validity of authentication, and

- *Authorization*—subject has permission to access resource(s).

The XML assertions must include the following:

- *Basic information*—unique identifier or name for the assertion and commonly includes date and time of issue and validity time span,

- *Claim*—a document describing the use of the assertion,

- *Condition*—the assertion may be subject to conditions that make it valid or invalid, and

- *Advice*—provides additional information such as assertions used to make a policy decision.

### B.2.4 SOAP

SOAP 1.1 is the current standard. SOAP is a message format not tied to a specific protocol. It most commonly uses HTTP, but can use other protocols such as SMTP or file transfer protocol (FTP). When SOAP is used with HTTP, the firewall views SOAP as HTTP and usually will allow it to pass. SOAP could potentially be filtered by the firewall, even when the firewall is not aware of SOAP. This filtering, however, is not an easy task and is susceptible to errors. Filtering is a challenge because encryption can hide the content and context of the data transported (i.e., XML), and SOAP has no uniform addressing scheme or internal structure (i.e., headers and method names are optional).

SOAP does provide security functionality. It has three main security components:

- *Credential Transfer*—the security credentials supported are flexible and take on almost any form. X.509 and Kerberos credentials are most commonly used.

- *Message integrity*—SOAP supports integrity of the message over the route traversed by the message.

- *Message privacy*—SOAP relies on XML encryption for privacy of the data.

## B.3 Communications Assistance to Law Enforcement Act

Telecommunications carriers should take the following security considerations into account with respect to the implementation of the Communications Assistance for Law Enforcement Act (CALEA). The basic CALEA requirements for systems security and integrity can be found in Title 47 Section 1004 of the US Code [47 USC Sec. 1004]. Further requirements on telecommunications carriers for support of lawfully authorized electronic surveillance (LAES) under CALEA can be found in the relevant rulemaking proceedings of the FCC and the Department of Justice (See http://www.askcalea.net/regulatory/). Related industry safe harbor standards such as TIA/EIA/IS-J-STD-025-A-2000, "Lawfully Authorized Electronic Surveillance," December 1, 2000 define the interface between the carrier and the Law Enforcement Agency but do not provide specific security requirements on the carrier's operation or equipment.

Security requirements and practices required under CALEA are explicitly set forth in "Subpart V-Telecommunications Carrier Systems Security and Integrity Pursuant to the Communications Assistance for Law Enforcement Act (CALEA)", Title 47 of the Code of Federal Regulations [47 CFR §§ 64.2100 et seq.]. Section 2105 [47 CFR § 64.2105] requires submission by carriers of their systems security and integrity policies and procedures to the FCC. Section 2106 [47 CFR §§64.2106] addresses penalties for failure to comply with the requirements set forth in Sections 2103 and 2104. However, Title 47 of the CFR does not specify the technical means for securing the surveillance.

Telecommunications carriers may wish to reference Telcordia Technologies generic requirements specifications GR-2975-CORE "Surveillance Administration System Generic Requirements," September 2000 and GR-2973-CORE "Lawful Access Feature: Switching Generic Requirements," April 2000. These specifications provide practices for identification, authentication, system and resource access control, alarm management, security log (audit), and security administration.

Security practices for LAES activities should be robust and the same as for any critical NE, OSS, or management system with some exceptions as listed below. As required in the FCC regulations, these practices relate to the necessity of keeping LAES activities confidential.

- Only authorized employees will participate in LAES activities.
- LAES information, including target identity, law enforcement agency(ies) involved, call content and call-identifying information will be protected from disclosure to unauthorized personnel.
- Only authorized personnel will have access to LAES commands and processes.

- An up-to-date list of personnel authorized to access, maintain, administer and manage LAES activities, processes, and procedures will be maintained.
- LAES security activities, policies, and procedures will be adequately documented and made available to authorized personnel.
- LAES -related security logs and activity records will be maintained and stored in a secure facility.
- A rigorous documented process will be implemented to identify and authenticate law enforcement agencies and process lawful intercept requests.

### B.4 Physical Security Considerations

The following considerations should be taken into account for physical security. When preparing security requirements, physical security is an important component. Most security architecture's assume that the physical environment is protected. At one time, all NE were contained in Central Office (CO) buildings. These buildings had employees working around the clock to operate, provision, administer, and maintain this equipment. Employees knew each other, and outsiders could not gain access to the sites without someone noticing and challenging them. However, the environment is very different today. Many, if not most, COs are unmanned and dark most of the time. Roving crews and individuals who are dispatched by a central location perform scheduled upgrades and maintenance tasks. Today, 24 X 7 security guards are the rare exception. COs are also used by outside plant personnel as a convenient place to meet and store tools and equipment. The following are characteristics of a secure facility:

- All personnel entry and exit is logged and recorded.
- Vendors and co-located personnel are vetted and their entry/exit is logged and recorded.
- Physical access to NE is limited to authorized employees.
- Co-located personnel are subject to the same access requirements as the incumbent service provider.
- No one who has legitimate physical access to the building has logical access to NEs, consoles, network access device's OSSs without PROTECTED AUTHENTICATION.
- Unauthorized access will be detected and responded to in a timely manner.
- Services such as water, power, and telecommunications will be available.
- Sites are under surveillance by:
- Random roaming security personnel
- Alarm systems that monitor and record door and window openings and closings, motion detectors, and inferred detectors
- Remote video monitoring critical locations
- Retention of surveillance media and logs should be documented. Length of retention would vary depending on risk level.

The following clauses provide additional information regarding physical security. A detailed description of physical security issues can be found in the National Communication System publication "Public Switched Network Security Assessment Guidelines," April 2000.

### B.4.1 Physical Premises Security

Organizations will usually implement various levels of building access controls in accordance with the importance of the assets resident in the facility. Often, large corporations will build separate high-security facilities for critical network components, such as switches or data centers. The importance of the assets resident there determines the level of security. This determination comes during a discovery phase and asset assessment review. The following clauses include assessment items for a facility housing high-value or critical assets. Less strenuous reviews would be undertaken for less sensitive facilities. The overall physical security assessment must determine the level of protection needed and the relative quality of the protective mechanisms in place.

#### B.4.1.1 General Building Security

Although a building's doors and windows are usually considered to be its primary access points, other points (e.g., air vents, entry points for water, gas, communications, and electricity, and drainage conduits) must be considered, depending on the kinds of threats. Additional entry points such as CO cable vaults need to be considered, as do other places where the potential to cause damage exists. Furthermore, the buffer space between the public and the building itself must be considered. Lawns, landscaping, lighting, and fences can contribute to the first layer of perimeter defense because they slow or prevent covert approaches. Physical barriers such as concrete posts or large concrete landscaping planters can be used to prevent approach by cars, trucks, or other vehicles with the potential destructive intent. Outside cameras and other surveillance gear further enhance or enlarge this buffer space.

#### B.4.1.2 Guards, Locks, and Identification Badges

Building guards protect the external perimeter of the building and sometimes protect internal areas. For critical facilities, the review should ensure the following:

- All doors providing access to the facility are either locked or guarded at all times.
- Any doors not normally in use, such as emergency exits, are alarmed. The review should ensure that alarms function properly and procedures exist to respond to alarms.
- Doors are installed properly so that they cannot be removed from the outside (e.g., hinges and bolts are protected from outside tampering).
- During peak periods of ingress and egress, entrances and exits have a guard present. During off-peak times, the door should be monitored, and some other form of access control should exist (e.g., swipe cards, proximity cards, and keys).
- Access through unguarded doors uses a method requiring identification of the entrant.
- Unguarded doors that provide access via keys or other means have mechanisms to prevent "tailgating."[22] Mantraps, revolving doors, and detectors can be used to prevent tailgating or send an alarm that tailgating has occurred.
- The recruitment qualifications, training, and retention methods used for employing guards are adequate and appropriate. This is particularly important for contracted guard services, which are common.
- Employees, onsite vendors, contractors, and other authorized individuals possess and display a badge at all times while in the building.

[22] Tailgating refers to an unauthorized person's act of following through a door opened by an authorized person.

- Non-employee visitors are given a temporary identifier, such as a visitor's pass, and are required to display it clearly.

- Procedures and conditions exist under which visitors can enter and work unescorted, and the conditions under which they must be escorted.

- Employee badges display a color photograph. The photograph should be big enough that the employee need not have to hand the badge to a guard for the guard to see it. It should be constructed so that the photograph cannot be altered or replaced. The photograph should be clear enough that the guard could compare the picture with the face of its wearer.

- The badge displays the employee's name and any other identifying information (e.g., number, bar code) clearly.

- The badge has a mark or indication that distinguishes employees from non-employees with access to buildings.

- The badge is durable and resistant to wear, damage, or alteration as much as possible.

- The badge contains electronic or magnetic information that may be needed by card readers.

- The badge may include a smart chip that embeds additional information, such as biometric data or X.509 certificates.

- Badge authentication and authorization systems should be linked to a central security directory to allow immediate change or removal of access privileges.

- The badge supports a capability to limit access to some areas of the corporate campus, as opposed to full access, when appropriate.

- The badge has an address to which it can be mailed without postage, if lost, if a non-employee were to find it.

- Corporate or building security can disable or invalidate any badge that has been lost or whose wearer is no longer permitted to enter the building or corporate campus.

- When the wearer terminates employment, someone (manager, building guard, corporate security) will retain or destroy the badge so that it cannot be used illicitly.

Guards are not the only personnel responsible for preserving the internal security of a building. Authorized occupants often enhance building security by vigilance and passive monitoring. The assessment should determine whether the staff has been empowered to challenge unauthorized personnel in controlled areas. A penetration test can be valuable for ascertaining the degree to which guards and employees are appropriately trained in the importance of physical security. Reviewers may attempt to sneak past or talk their way past guards or to entice employees to provide admittance through unguarded entrances.

#### B.4.1.3 Physical and Logical Key Administration

Traditional physical keys are rarely used in sensitive facilities because they are difficult to inventory and recover and they do not provide an audit trail of the user. Often, the use of physical keys is restricted to access to internal portions of the building, such as storerooms, custodial rooms, and wire closets. It is still common, however, to find businesses and installations that use key locks as their primary means for ingress to buildings or access to critical areas within buildings. When that is true, the following actions are important:

- Procedures exist for authorizing distribution of keys to individuals, including key control and logging of access and distribution

- Keys be individually numbered

- A complete inventory of keys and their owners be maintained and audited

- Criteria be in place for replacing locks when keys are lost

- Periodic audits of the key inventory be enforced and procedures for reconciling discrepancies be in place

- Procedures are in place for recovering keys when access is no longer needed or authorizations change.

Logical key (e.g., proximity cards) procedures must be evaluated against the same criteria. Key recovery, ingress and egress recording, and authorization procedures are simplified with logical keys because these systems provide central facilities for monitoring use, assigning authorization, and disabling of keys. Still, procedures must be in place to ensure that those responsible for maintaining the key inventory and authorization database are notified when individuals leave or their access requirements change. Combination locks, a special case of logical locks, should be assessed to ensure that combinations are not discernible from wear patterns or from combinations written down. Combinations should be changed if entry authorizations are changed.

#### B.4.1.4 Functional Separation of Facilities and Multilevel Access Control

Physical security applies to internal portions of a building as well as the external perimeter. Access to internal areas that are considered sensitive or operationally critical should be controlled when access to their contents is limited for any reason (e.g., they contain sensitive data, experiments, or equipment). In general—

- Critical computer and network facilities should be contained in areas having separate physical access control mechanisms. Access should be granted only to those having a need.

- Procedures should be in place to ensure that proprietary information is kept in secure facilities when not in use. Offices and file rooms where such material is routinely kept should be locked. The cabinets in which proprietary information is kept should also be locked.

- All potential access points to critical computer and network facilities (e.g., consoles, operations centers) should be controlled in a manner commensurate with the control enforced over the facility itself.

- A record of access to all such controlled spaces should be maintained.

- Storage media holding critical information should be encrypted or housed in locked, limited-access areas.

- A critical system's physical address should not be disclosed to those not having a need to know.

Controlling the internal areas of a building can be enhanced through the use of segregated roles and responsibilities. For example, administrative staff does not require access to an organization's computer rooms. Likewise, engineers do not generally require access to the document control room. The review should assess whether existing functional segregation is appropriate. In addition, dual entry key or combination locks can be used if the degree of risk so indicates.

### B.4.2 Building Services

An organization's operations are critically dependent on the availability of services, such as water, power, telecommunications, and waste disposal.

#### B.4.2.1 Utilities (Water, Power, Telecommunications, and Waste Disposal)

Without water, power, telecommunications, and waste disposal services an organization cannot operate effectively, if at all. Dependency on these services is often undervalued. The assessment should evaluate the organization's planned reactions to service interruptions. For services critical to the continuing function of the business, the following steps are essential:

- Power feeds should be duplicated and geographically separated to prevent accidental loss of power.
- Emergency power should be available to allow the continued operation for greater than the average duration of power outages. Generating capacity should be available for deployment before emergency supplies are exhausted. (Mobile generators may be owned or contracted.)
- Sufficient onsite water storage (or delivery services) should be available to support continued operation of critical components of the facility.
- Outside communications must either have active-standby backups, or must be robust enough to operate in a crisis, as must internal communications. Capacity should be sufficient to handle crisis-level traffic.
- Restroom and sewage facilities must function through crises, or temporary arrangements must be in place (at least contractually) for quick activation.
- Air conditioning for computer rooms and other areas that require controlled environments must be backed up to prevent machine failure or damage from overheating.
- Locked containers for disposal and destruction of proprietary information should be readily available wherever such material is used. The review should trace the disposal path of such material to ensure that it is closed.

Of interest for the assessment is the distribution of these services within buildings. The assessment should evaluate the overall resistance of the facility to service interruption from the origination of the service at the utility provider to the distribution paths inside the building.

#### B.4.2.2 Emergency Facilities

The review should assess the adequacy of emergency facilities such as fire detection and suppression, power conditioning, air conditioning, ventilation, and other environmental protection systems necessary for continued operation of critical systems. These systems must react in ways that allow—

- People to evacuate the premises
- Equipment to be protected (at least long enough for fire companies or others to arrive)
- Facilities to retain structural integrity
- The building's contents to be protected from the outside environment, as much as possible.

Emergency facilities are important as much for the aftermath of a security breach as they are for accidents and natural disasters, as suggested in the previous clause.

#### B.4.2.3 Transport Redundancy and Physical Protection of Critical Facilities

Critical computer and communications systems facilities should be geographically dispersed to the extent possible without unduly affecting operational costs, performance, and security. In addition, routing of critical communications links (e.g., important interoffice trunks, signaling links) should be redundant and geographically dispersed inside and outside the facility so that communications may be immediately rerouted over physically diverse backup routes when necessary. The communications networks required for maintaining service should be designed in such a way that no single point of failure will result in a widespread or serious outage.

### B.4.3 Environmental and Geographical Threats

Critical sites should be reviewed to identify any risks resulting from their location in areas likely to experience natural disasters, serious accidents (e.g., chemical spills, gas line explosions), power interruptions, and related problems. The review should also consider the effects of simple environmental factors, such as extreme heat or cold, damage from salts and pollution, and harsh climate conditions.

Geographical issues include the reactions of the local populous, such as acts of hostility, responsiveness of local emergency services, and the level of safety afforded to staff, on site and en route to the facility. Because human activities and motivations change over time as a result of unrest, political problems, religious views, or other factors, reviews should be repeated periodically according to a predetermined schedule. Although it is often impractical to abandon facilities where such risks exist, it may be appropriate to duplicate or relocate critical systems and resources housed in high-risk facilities.

Business continuity and disaster recovery plans should be developed that address responding to events resulting from these threats and issues. Plans should include command, control, and communications procedures and should be tested on a regular basis. Operations recovery plans should also include provisions and contracts that can be quickly executed in response to hazardous material (HAZMAT) incidents. These plans should also consider that complete restoration to a safe environment might prevent normal access to the facility over an extended period of time. Potential remediation may require relocating to a backup facility or the availability of HAZMAT trained and equipped personnel to operate the facility during the interim.

### B.4.4 Co-location Procedures

The Telecommunications Act of 1996 (also known as the Telecommunications Reform Act [TRA]) mandated that Incumbent Local Exchange Carriers (ILEC) offer various components of their networks to competitors in an unbundled and nondiscriminatory manner. Co-location, a logical result of the mandate, refers to a situation that prevails when plant belonging to multiple providers is present in the same physical location. Of particular concern for the purposes of physical security reviews is that providing such access often means that competitors (sometimes multiple competitors) will require access to physical components and facilities of the ILEC.

For example, physical co-location is the predominant way that ILECs provide facilities for unbundled loops under the TRA. Co-location for the purpose of providing unbundled loops can expose other functional components to misuse or abuse to the extent that their facilities are housed on the same premises. Consequently, extra care must be taken when performing a physical security review of facilities with co-located providers. The review should note that—

- Physical barriers should isolate critical equipment; however, co-located personnel are subject to the same access requirements as the incumbent service provider.

- Key distribution, accounting, and auditing procedures are in place. Processes should be in place to ensure that personnel changes can be monitored across co-located companies.

- Critical equipment and facilities do not draw attention to themselves. The traditional method of clearly marking crucial equipment and transport facilities (so-called "red blocking"[23]) becomes a potential hazard in an open environment and should be avoided.

## B.5 Development Process

### B.5.1 Bootstrapping, Installation, and Failure Modes

The following considerations should be taken into account for bootstrapping, installation, and failure mode security procedures.

Several distinct efforts must be completed to secure an implementation from a "new installation" through the implementation's lifetime. To address these issues it is important to begin by understanding the threats to an implementation. These threats are referenced in ANSI T1.233 and ISO/IEC DIS 10181 standards documents. General connectivity to open systems broadens the threats, which include the following:

- Bootstrap viruses

- Unauthorized access

- Masquerade

- Threats to data integrity

- Threats to confidentiality

- DoS

- Repudiation.

### B.5.2 Patching Process

Service providers contract with vendors who develop and provide both an application and a platform on which an application is installed, or only application software. In the latter case, providers install the software onto a platform they have previously purchased.

Vendors develop patches to correct or modify OS or application software, or both, between general releases. Following appropriate testing, a patch is released to the service provider. In some instances, an application software vendor may release patches in "bundles," perhaps with some contractual regularity. Releases every six months are not uncommon.

An OS patch generally should not affect the manner in which an application runs; however, that is not always the case. Consequently, when a platform vendor releases an OS patch, it is incumbent on the provider to verify with the application vendor that the OS patch released will not adversely affect the running of the/an application.

[23] Red blocking alerts support personnel that the circuit is especially important and that care must be taken not to disturb it accidentally.

In a situation where an application vendor supplies both an application and a hardware platform but is not an original equipment manufacturer (OEM) of the platform, and an OS security patch is released by the OEM of the platform, it is incumbent upon both the application vendor and the SP to be aware that a security patch has been released and to make arrangements for the patch to be tested in a timely manner, in order to verify that the patch will not adversely affect the application.

The application of security patches must be assigned a priority for review by the application vendor (a matter of weeks versus months). As such, a routine must be process must be established such that when a provider communicates a concern regarding a security patch to an application vendor, the vendor will take appropriate action in an expedited manner. In addition, the vendor will ensure that installation of the patch will not corrupt previously installed security patches.

If security patch testing reveals an impact to an application, appropriate corrective actions must be taken in a timely manner to identify the issue and formulate plans to correct the condition causing the application to fail, and to subsequently apply the security patch.

The following security considerations should be taken into account when implementing patches to the OS or application software.

- Equipment vendors or system integrators should provide security reference and training manuals for administrators that include details of OS and application security functions and procedures and user access procedures.

- OS security and other patches should be verified as compatible with NE and MS applications.

- Operating System software: Only patches approved by an OEM should be applied to an operational network element or management platform operating system.

- Management Application software: Only patches approved by an original Management Application vendor should be applied to an operational management application.

- High-impact patches should be distributed in a timely manner and not be constrained by normal patch dissemination processes.

- All downloads or uploads of any software or configuration data must be secured with strong data origin authentication and strong integrity protection. Ideally, both would be provided through the software provider's digital signature. In addition, the software provider may choose to encrypt the software or configuration data.

- A description of the procedure(s) for acquiring and incorporating the latest security patches for the system and application software executing within each element should be provided at time of delivery.

- A description of the process for testing each security patch, before approving release to the service provider, should be provided at time of delivery.

- The level of backward compatibility of the system software releases and security maintenance patch releases should be specified at the time of delivery.

- System software or a process must track applied patches and upgrades. Patch and upgrade status should be auditable.

### B.5.3 Development Life Cycle Security

Security of a product or service is dependent on the complete life cycle process. Security is an issue during conceptual design and remains an issue through detailed design, development, deployment, and decommissioning of a product. For products or services dealing with sensitive information, security may be required even beyond the decommissioning of the product or service. Appropriate controls and testing during the complete life cycle process are critical to providing acceptable levels of security.

#### B.5.3.1 Personnel Management

A fundamental issue of security that is often overlooked is the trustworthiness of the staff. All staff that have access to design, development, and testing must be trustworthy.

- All personnel, contractors, subcontractors, consultants, and employees involved in developing and testing critical software components must pass a background check.

#### B.5.3.2 Security Awareness and Training

All personnel must be aware of security policies and procedures and the need to protect information assets. The weakest link in security is often the people involved. Security awareness and training dramatically strengthens the weakest link. Awareness reduces the number of unauthorized actions attempted by staff; increases the effectiveness of protection controls; and helps avoid fraud, waste, and abuse of computing resources.

- Security awareness and training should be provided to all staff, including contractors, subcontractors, consultants, and employees.

#### B.5.3.3 Risk Management

Risk management is fundamental to information security. Risk management is defined as the identification, analysis, control, and minimization of loss associated with an "event." The primary steps identifying risk include identification of actual threats, consequences of a realized threat, potential frequency of occurrence of a threat, and the likelihood of a realized threat. Risk management involves not only performing risk analysis with a cost benefit analysis of protections but also implementing, reviewing, and maintaining protection.

A risk analysis identifies the risks and provides a cost-benefit justification of countermeasures. This information is used to influence the decision making process of all life-cycle phases, including site selection, building design, and construction decisions. To determine if a safeguard is warranted, the annualized loss expectancy (ALE) is determined. The (ALE before safeguard implementation) – (ALE after safeguard implementation) = value of safeguard. Note that the safeguard implementation should include the annual cost for operation and maintenance.

- A risk analysis should be performed for each new product or service. This analysis should include a formal document outlining the approach used and results of the analysis. At a minimum the report should identify all data accessible and the data owner (i.e., corporate, ISP), quantify or qualify the value of the data or service at risk, and determine potential upstream and downstream impacts of the threat to NEs or OSSs.

#### B.5.3.4 Requirements

- Security requirements should be documented during the requirements gathering phase for the product or service.

#### B.5.3.5 Design

- Security requirements should be addressed at the design phase, not added after development has begun.

- A security design review should be performed to locate design flaws that affect security.

- All access points into the system must be well documented and provide support for identification and authentication.

- Maintenance backdoors or trap doors that violate the security policy must NOT be allowed.

#### B.5.3.6 Separation of Duty

Functions that are harmless in a trusted environment can create security vulnerabilities when used in untrusted environments. For example, a postscript interpreter was designed to view documents. An untrusted document could use the functions within the postscript interpreter in malicious ways, such as making copies or deleting files.

- The system should support at a minimum three user levels: user, SYSTEM ADMINISTRATOR/operator, and security administrator.

- Each function should have the minimum level of privilege required to perform the job function.

#### B.5.3.7 Implementation

- Reused resources should be purged of any information before re-use (i.e., files, memory, and temporary storage).

- Developers should follow best practices for secure programming (i.e., manage buffers so that buffer overflows do not occur).

- Periodic security audits should be performed of the development, test, and support environments.

- Development environments should not be used for non-company business.

- Public domain software should not be imported, used, or distributed for use on development, test, or support systems unless it is available in source code and the source code has been inspected for malicious code.

#### B.5.3.8 Documentation

- Documentation should be marked with proprietary markings, where appropriate.

- The end-user documentation must describe the security functionality that is not transparent to the user, explain its function, and provide guidelines on use.

- The SYSTEM ADMINISTRATOR'S guide should include the following:

    - Cautions regarding functions and privileges that need to be controlled when running in secure mode

    - Document use of audit functions

    - Procedures for examining and maintaining audit logs

    - Detailed audit log structures

    - Procedures for audit log backup and deletion

    - Procedures for checking amount of free space available for audit logs.

#### B.5.3.9 Operating System

The OS must be able to provide effective hardware and software controls to provide protection appropriate to the value of data and resources being managed. For the proposed security architecture, it is assumed that the OS will provide the security level required for the data and resources being managed. This assumption may need to be reviewed for specific service provider needs. For example, the Department of Defense might have stricter OS security requirements. If the OS does not meet the security provider's security needs, then the software may need to be ported to another OS that supports higher levels of security.

- The OS must have relevant security patches installed.
- The OS must be configured securely and must be delivered with a restrictive security access privilege configuration. The Trusted Computer System Evaluation Criteria provides a very extensive discussion of OS security capabilities.[24]
- Only a minimum of services will be enabled that are required for operation by default.

#### B.5.3.10 Software Engineering

Security is an integral part of software engineering. To develop a secure product, secure programming techniques and secure protocols must be used. Non-secure programming techniques can circumvent the best security protocols and mechanisms. For example, if a programmer does not manage buffers properly, a buffer overflow may occur and provide more privilege to a user than is appropriate.

- Vendors should follow formal documented development processes, such as the Capability Maturity Model developed by the Software Engineering Institute. Secure programming best practices must be followed in design, development, testing, and distribution of the software.

#### B.5.3.11 Availability and Performance

Availability and performance are integral to a secure system. Performance can be degraded to the point that the system is no longer usable.

- Design, development, and implementation should minimize the effects of a DoS attack.
- Design, development, and implementation should ensure high availability.
- The network architecture and implementation should have no *single point of failure*.

#### B.5.3.12 System Software

The software used to operate and maintain the computer systems (OSs, utilities, and MSs) must be able to be configured and maintained securely.

- System software and middleware products must be installed and configured securely, including installation of security patches. The software must be delivered with a restrictive security access privilege configuration.

[24] Department of Defense Standard 5200.28, "Department of Defense Trusted Computer Security Evaluation Criteria," December 1985.

#### B.5.3.13 Transmission

- The option to secure data transmissions must be available to be used at the service provider's discretion. Secure transmissions options should be available for both client-to-server and server-to-server.

#### B.5.3.14 Secure Storage

- Service provider configurable options for securely storing data should be provided. The service provider should be able to specify which fields are stored securely.

#### B.5.3.16 Software Assurance

Software assurance should be addressed from two perspectives: testing of security features and testing for potential security policy violations.

- Duties must be segregated between software development groups and software testing groups.
- A security test plan, test procedures, and results should be documented.
- All security features must be tested.
- Tests should include attempts to locate violations of security policy (i.e., vulnerabilities such as access control).
- As part of the test, verification must be done so that the newly developed system or application does not introduce vulnerabilities in existing structures, common networks, and systems.
- Verification of secure programming techniques must be performed. Verification may be done via code reviews or software tools.
- All security flaws must be corrected, removed, or neutralized and the system retested.

#### B.5.3.17 Packaging and Delivery

A software configuration management system must be used throughout the life cycle of a product that maintains control of changes to source code and documentation.

- Developers should not maintain the software configuration management system.
- Developers should not have access to production systems except under controlled emergency provisions that are approved and logged.
- Only authorized code and code modifications should be added to the deliverable source baseline.
- All changes must be documented and reviewed.
- Tools or procedures must exist to generate a new version of the system from source code.
- Tools or procedures must exist to protect the source code from unauthorized modifications.
- Tools or procedures must exist to verify the appropriate versions and levels of component source modules were used.

- The product must contain integrity mechanisms such that it is possible to verify the installed software is consistent with the delivered software (i.e., no unauthorized modifications have been made).

- Where a mechanized scanning tool is available, a vulnerability scan must be completed after upgrades or other significant changes to the OS or application software

- Security flaw remedies or “fixes” must be provided in a timely manner commensurate with the threat.

- A master database must exist that contains copies of all delivered software. The software must have a release number and specifications for appropriate OSs and hardware.

#### B.5.3.19 Secure Installation, Configuration, and Operation

- Secure configuration parameters should be defined for the software.

- Secure operations procedures should be defined and documented for the software.

- All remote support of the software should be performed in a secure manner.

- All default User IDs delivered with the system should be delivered in an inactive state that requires explicit action by the administrator/software installer to be usable.

- All installation processes should be secure and should not rely on trust relationships (i.e., share drives).

## Annex C

(Informative)

### C Informative References

Ad Hoc Group Editor's Note: References will be formatted during ballot process and checked for accuracy.


American National Standards Institute-J-STD-025-A-2000, Lawfully Authorized Electronic Surveillance, December 1, 2000.

ANSI T1.210-1993, *OAM&P—Principles of Functions, Architectures, and Protocols for TMN Interfaces.*

ANSI T1.233-1993 (R1999), OAM&P - Security Framework for Telecommunications Management Network (TMN) Interfaces

ANSI T1.243-1995 (R1999), OAM&P - Baseline Security Requirements for the TMN

ANSI T1.252-1996, *OAM&P—Security for the TMN Directory.*

ANSI T1.261-1998, *OAM&P—Security for TMN Management Transactions Over the TMN Q3 Interface.*

ANSI T1.268-2000, *TMN Public Key Infrastructure (PKI) Digital Certifications and Certificate Revocation Lists Profiles*.

Department of Defense (DoD) 5200.28-STD, DoD Trusted Computer System Evaluation Criteria, December 1985.

Draft Standard RFC-2616, Hyper Text Transfer Protocol (HTTP)—HTTP/1.1, R. Fielding,

J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, June 1999.

Draft Standard RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, January 1996.

“Digital Signature Standard,” http://csrc.nist.gov/cryptval/dss.htm.

Federal Information Processing Standard (FIPS) Publication 197.

Federal Communications Commission (FCC) Docket Number 97-213.

G.8080/Y.1304, “Architecture for the Automatically Switched Optical Network (ASON),” November 2001.

General Requirements (GR)-815, Generic Requirements for NE/NS Security.

GR-1194, Bellcore Operating Systems Security Requirements.

GR-2973-CORE (Central Office Relay Equipment), Lawful Access Feature: Switching Generic Requirements, April 2000.

GR-2975-CORE, Surveillance Administration System Generic Requirements, September 2000.

International Organization for Standardization (ISO) 7498-2, Information Processing Systems—Open Systems Interconnection Basic Reference Model, Part 2: Security Architecture.

International Telecommunications Union (ITU) M.3010, Principles for a TMN.

ITU-T-M3013, *Considerations for a TMN.*

National Communications System, Public Switched Network Security Assessment Guidelines, April 2000.

National Computer Security Center (NCSC), "NCSC-TG-004-88: Glossary of Computer Security Terms."

National Institute of Standards and Technology (NIST), "NISTIR 6192: A Revised Model for Role Based Access Control", Jansen, W.A.

"Partnership for Critical Infrastructure Security Common Reference Glossary, Version 2001-09," http://www.pcis.org.

Proposed Standard RFC-2409, The Internet Key Exchange, D. Harkins, D. Carrel, November 1998.

Proposed Standard RFC-2402, Internet Protocol (IP) Authentication Header, S. Kent, R. Atkinson, November 1998.

Proposed Standard RFC-2406, IP Encapsulating Security Payload, S. Kent, R. Atkinson, November 1998.

Proposed Standard RFC-2401, Security Architecture for IP, S. Kent, R. Atkinson, November 1998.

Proposed Standard RFC-2246, The Transport Layer Security Protocol Version 1.0, T. Dierks, C. Allen, January 1999.

Request for Comment (RFC)-0826, Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48-bit Ethernet Address for Transmission on Ethernet Hardware, D. C. Plummer, November 1982.

RFC-0959, File Transfer Protocol, J. Postel, J. K. Reynolds, October 1985.

RFC-1288, The Finger User Information Protocol, D. Zimmerman, December 1991.

RFC-0792, Internet Control Message Protocol, J. Postel, September 1981.

RFC-0791, IP, J. Postel, September 1981.

RFC-1157, SNMP, J. D. Case, M. Fedor, M. L. Schoffstall, C. Davin, May 1990.

RFC-0859, Telnet Status Option, J. Postel, J. K. Reynolds, May 1983.

RFC-0793, Transmission Control Protocol, J. Postel, September 1981.

RFC-0768, User Datagram Protocol, J. Postel, August 1980.

RFC 2403 and 2404, The Use of HMAC-MD5-96 within ESP and AH, Network Working Group, November 1998

"Security Service Specification," Version1.7, March 2001, Object Management Group, Inc., http://www.omg.org

Schneier, Bruce., *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996.

Telecommunications Industry Association, Lawfully Authorized Electronic Surveillance, TR45 J-STD-025, April 17, 2000.