International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3016.1

(04/2005)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Telecommunications management network

Security for the management plane: Security requirements

ITU-T Recommendation M.3016.1

ITU-T M-SERIES RECOMMENDATIONS

TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	**M.3000–M.3599**
Integrated services digital networks	M.3600–M.3999
Common channel signalling systems	M.4000–M.4999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation M.3016.1

Security for the management plane: Security requirements

Summary

This Recommendation identifies the security requirements for the management plane in telecommunication management. It focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the telecommunication infrastructure.

Source

ITU-T Recommendation M.3016.1 was approved on 13 April 2005 by ITU-T Study Group 4 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Introduction

Telecommunications is a critical infrastructure for global communication and economy. Appropriate security for the management functions controlling this infrastructure is essential. Many standards for Telecommunication network management security exist. However, compliance is low and implementations are inconsistent across the various telecommunication equipment and software components. This Recommendation identifies the security requirements to allow vendors, agencies, and service providers to implement a secure telecommunication management infrastructure. Although the present set of requirements represents the current understanding of the state of the art, technologies will advance and conditions change. To be successful, this Recommendation must evolve as conditions warrant. This Recommendation is intended as a foundation. Service providers may include additional requirements to meet their specific needs over and above those dealt within this Recommendation.

This Recommendation is part of the M.3016.x series of ITU-T Recommendations intended to provide guidance and recommendations for securing the management plane of evolving networks:

– ITU-T Rec. M.3016.0 – Security for the management plane: Overview.

– ITU-T Rec. M.3016.1 – Security for the management plane: Security requirements.

– ITU-T Rec. M.3016.2 – Security for the management plane: Security services.

– ITU-T Rec. M.3016.3 – Security for the management plane: Security mechanism.

– ITU-T Rec. M.3016.4 – Security for the management plane: Profile proforma.

ITU-T Recommendation M.3016.1

Security for the management plane: Security requirements

1 Scope

ITU-T Recs M.3016.1-3 specify a set of requirements, services and mechanisms for the appropriate security of the management functions necessary to support the telecommunication infrastructure. Because different administrations and organizations require varying levels of security support, ITU-T Recs M.3016.1-3 do not specify whether a requirement, service/or mechanism is mandatory or optional.

This Recommendation identifies the security requirements for the management plane in Telecommunication management. It focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the Telecommunication infrastructure.

This Recommendation is generic in nature and does not identify or address the requirements for a specific Telecommunications Management Network (TMN) interface.

The proforma defined in ITU-T Rec. M.3016.4 is provided to assist organizations, administrations and other national/international organizations, specify the mandatory and optional support of the requirements as well as value ranges, values, etc. to help implement their security policies.

1.1 Purpose

ITU-T Rec. M.3016.0 identifies a number of objectives, for securing the management network and threats that introduce risks with regard to meeting these objectives. This Recommendation derives the requirements from the objectives against threats and identifies the security services that counter them. In defining the services, mechanisms are used based on certain algorithms. The other Recommendations in this series build on the structure set forth in the ITU-T Rec. M.3016.0 overview. It augments the various steps required to secure the management plane.

1.2 Relationship with X.805 security architecture

ITU-T Rec. X.805 defines security architecture for providing end-to-end network security. The X.805 security architecture logically divides a complex set of end-to-end network security-related features into three separate architectural components, namely Security Dimensions, Security Layers and Security Planes (see Figure 2/X.805). A Security Dimension is a set of security measures designed to address a particular aspect of the network security. ITU-T Rec. X.805 defines three Security Layers: the Infrastructure Security Layer, the Services Security Layer, and the Applications Security Layer, which build on one another to provide network-based solutions. A Security Plane is a certain type of network activity protected by Security Dimensions. Three Security Planes are identified in ITU-T Rec. X.805, namely, Management Plane, Control Plane, and End-User Plane. To provide a complete solution, security measures (e.g., access control, authentication) should be applied to each type of network activity (i.e., management plane activity, control plane activity, and end user plane activity) for the network infrastructure, network services, and network applications. This Recommendation focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the network infrastructure.

1.3 Relationship with E.408 telecommunication networks security requirements

ITU-T Rec. E.408 provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile; both voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats. It is generic in nature and does not identify or address requirements for specific networks. The M.3016.x series identifies the security requirements, services, and mechanisms for the telecommunication network, i.e., the management plane in general in telecommunication management.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation

- ITU-T Recommendation E.408 (2004), *Telecommunication networks security requirements*.
- ITU-T Recommendation G.8080/Y.1304 (2001), *Architecture for the automatically switched optical network (ASON),* plus Amendment 2 (2005).
- ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network.*
- ITU-T Recommendation M.3013 (2000), *Considerations for a telecommunications management network.*
- ITU-T Recommendation M.3016.0 (2005), *Security for the management plane: Overview*.
- ITU-T Recommendation M.3016.2 (2005), *Security for the management plane: Security services*.
- ITU-T Recommendation M.3016.3 (2005), *Security for the management plane: Security mechanism*.
- ITU-T Recommendation M.3016.4 (2005), *Security for the management plane: Profile proforma*.
- ITU-T Recommendation X.509 (2000), *Information Technology – Open Systems Interconnection: The Directory: Public-key and attribute certificate frameworks,* plus Technical Cor.1 (2001), Technical Cor.2 (2002) and Technical Cor.3 (2003).
- ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*, plus Amendment 1 (1996), *Layer Two Security Service and Mechanisms for LANs*.
- ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- IETF RFC 1750 (1994), *Randomness Recommendations for Security.*

3 Terms and definitions

This Recommendation uses the following terms from ITU-T Rec. G.8080/Y.1304:

- Control Plane;
- Management Plane;
- Transport Plane.

This Recommendation uses the following terms from ITU-T Rec. M.3010:

- Management System;
- Network Element.

This Recommendation uses the following term from ITU-T Rec. M.3013:

- Element Management System.

This Recommendation uses the following term from ITU-T Rec. X.509:

- Strong Authentication.

This Recommendation uses the following terms from ITU-T Rec. X.800:

- Access Control;
- Authentication.

This Recommendation defines the following term:

3.1 **critical security administration actions**; which include but are not limited to:

a) Defining and assigning user privileges;

b) Adding and deleting user IDs;

c) Disabling the use of specific user IDs as login IDs;

d) Initializing and resetting login passwords;

e) Initializing and changing cryptographic keys;

f) Setting the system's aging threshold for login passwords;

g) Setting the system's limit on the number of failed logins for each login ID;

h) Removing a lockout, or changing the system's lockout timer value;

i) Setting the system's inactivity timer value;

j) Setting system security logging and alarm configuration;

k) Managing the security logging processes;

l) Upgrading security software;

m) Terminating any user or system session.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

AAA	Authentication, Authorization and Accounting
ACS	Access Control Server
ALE	Annualized Loss Expectancy
ANSI	American National Standards Institute
CO	Central Office
CORBA	Common Object Request Broker Architecture
CSI	Common Secure Interoperability
DoS	Denial of Service
EMS	Element Management System
FTP	File Transfer Protocol
HAZMAT	Hazardous Materials

HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LAES	Lawfully Authorized Electronic Surveillance
MS	Management System; any EMS, NMS, or OSS[1]
NE	Network Element
NE/MS	NE or MS
NMS	Network Management System
NTP	Network Time Protocol
OAM&P	Operations, Administration, Maintenance and Provisioning
OASIS	Organization for the Advancement of Structured Information Standards
OEM	Original Equipment Manufacturer
ORB	Object Request Broker
OS	Operating System
OSS	Operations Support System
RFC	Request for Comments
SAML	Security Assertion Markup Language
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMN	Telecommunications Management Network
XML	Extensible Markup Language

5 Conventions

In ITU-T Recs M.3016.1-3, a descriptor is used to identify the different requirements, services and mechanisms. The descriptor consists of one of the following three-letter labels followed by a number:

– REQ for requirement;

[1] OSSs generally can be used in the same context as MSs on any layer of the telecommunication management network hierarchy.

– SER for service;

– MEC for mechanism.

6 Security requirements

This clause contains the security requirements for operations, administration, maintenance and provisioning (OAM&P) and operations support system (OSS) of the **Management Plane**.

Figure 1/M.3016.0 describes the relationships between Security objectives, Threats, Risks, Security requirements, and Services. It describes the process how to derive "Security requirements" from "Threats" and "Security objectives" which in turn will be realized by a set of security services. These "Services", which counteract threats, will make use of "Mechanisms" which themselves make use of "Security algorithms". Table 1 (which is Table 4/M.3106.0) gives the relationship between Security requirements and Security services. The security requirements described in this clause are organized, following Table 1, as follow:

– Verification of identities;

– Controlled access and authorization;

– Protection of confidentiality;

– Protection of data integrity;

– Accountability;

– Security logging and audit;

– Security alarm reporting.

NOTE – Recovery from security breach is an area for further study.

Table 1/M.3016.1 – Mapping of security requirements and security services (Table 4/M.3016.0)

Functional requirement	Security service
Verification of identities	User authentication Peer entity authentication Data origin authentication
Controlled access and authorization	Access control
Protection of confidentiality – stored data	Access control Confidentiality
Protection of confidentiality – transferred data	Confidentiality
Protection of data integrity – stored data	Access control
Protection of data integrity – transferred data	Integrity
Accountability	Non-repudiation
Activity logging	Audit trail
Security alarm reporting	Security alarm
Security audit	Audit trail

6.1 Verification of identities

Authentication has two purposes in securing the **Management Plane**:

1) it ensures the identity of the communicating parties, providing a basis for setting up private communications with full data integrity and confidentiality between two systems; and

2) it provides a basic mechanism for logging into a management system and/or auditing the management activities on any system.

6.1.1 User Authentication, Passwords, and User IDs

User **Authentication** concerns the **Authentication** of clients involved in the management of the network. In this case, **Authentication** proves the identity of the legitimate user and prevents masquerading attacks by illegitimate users. With proper **Authentication**, it is possible to track activities and restrict users to pre-authorized activities or roles as discussed in 6.3.

The minimum requirements for **Authentication** are the use of a user ID and static **Complex 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 strong as that provided by a user ID and static **Complex Password**. Other mechanisms that may be considered include:

– A user ID and **Two-Factor Authentication** using a one-time password generator;[2] and

– **Two-Factor Authentication** using a smart-card with credentials stored on it in a protected manner.

REQ 1: For NE/MS logging in, logging, and auditing, strong authentication should be supported.

REQ 1 presents the security requirement. Description of general authentication mechanism is given in ITU-T Rec. M.3016.3. It is expected that **Authentication** techniques and single sign-on technologies will continue to improve.

In secure single sign-on, the protocol still challenges the entity(s) for credentials; however, a user may not have to enter the credentials because they are securely cached in some way (e.g., Kerberos).

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

REQ 2: Each NE/MS should enforce **Authentication** according to organizational policy.

REQ 3: Each NE/MS should support the Minimum complexity rules for **Authentication** according to the organizational policy.

REQ 4: The NE/MS should prevent another user from changing a logged-on user's password without their knowledge.

REQ 5: Each NE/MS should automatically ensure that each new login password differs from the previous password. The degree of difference should be configurable according to organizational policy.

Because passwords are typically stored via one-way encryption, the entry of the old password is also required to allow the NE/MS to determine the degree of difference between the old and new passwords.

REQ 6: Each NE/MS should support prevention of password reuse. Password use prevention parameters should be configurable according to organizational policy.

REQ 7: Each user ID should have its own settable login password.

REQ 8: Passwords should be user changeable at the user's discretion, following a minimum interval since the last change. The minimum interval should be configurable according to the organizational policy and set by the **System Security Administrator**.

[2] This clause does not discuss dynamic passwords as those are considered to be outside of the scope of this Recommendation.

REQ 9: Each NE/MS should support multi-level password control. Some users can be locked out (e.g., due to password aging or login failure) while some users cannot be.

6.1.2 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.

REQ 10: One of the following should apply:

- The configuration software should create a unique initialization password for each application in the new release or upgrade[3] of the software.
- If a default password is used, the system should require the replacement of the default password with a unique password before the device goes into service.
- If a device is delivered without a password or a null password, a unique password should be assigned during the installation process before the device goes into service.

REQ 11: The system age threshold for login passwords should be configurable if the functionality is also built into the application. At the expiration of the age threshold, the login password for an affected application should be reset to an original default state defined in REQ 10. All password change privileges should be revoked for all users except for the user role, which has the highest level of security authority for a system or application instance.

REQ 12: The system inactivity timer value should be configurable if the functionality is also built into the application. When the system inactivity timer is enabled, an access to the system for a given user ID should be prevented and login process for this user should be disabled.

REQ 13: The system limit on consecutive failed logins for a given user ID should be configurable if the functionality is also built into the application. When the system limit on consecutive failed logins for a given user ID is reached, the system inactivity timer defined in REQ 12 shall be invoked.

6.2 Controlled access and authorization

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 allowed by that role). This clause defines basic requirements for implementing "least privilege" through good system security administration.

6.2.1 Security administration

Each NE/MS must ensure that only authorized users are allowed to manage system security resources. All administrative actions are linked to user roles, and those user roles are assigned to specific individuals. Though only a few types of user roles are discussed, many other types of user roles with varying 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.

REQ 14: Each NE/MS should have support for multiple user-defined types of user roles, and **Management Actions** are assignable to each user role.

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

User roles might result in a hierarchy of roles such that each user role has different or fewer tasks assigned such that it has less authority than the more privileged user role. An example of such a hierarchy is one which a user role has the ability to perform all **Management Actions**, like a computer 'super-user'. Another user role supports only read-only access to support monitoring of the devices, such as an operator.

REQ 15: Each NE/MS should support a default user type, which has minimal or restrictive **Management Actions**.

REQ 16: Each NE/MS should support the following **Critical Security Administration Actions,** but is not limited to:

- Defining and assigning user and group privileges.
- Maintaining a record of all requests for login IDs to the system.
- Adding and deleting user IDs.
- Disabling and enabling the use of specific user IDs as login IDs.
- Initializing and resetting login passwords.
- Initializing and changing cryptographic keys.
- Setting the system's aging threshold for login passwords.
- Setting the system's limit on the number of failed logins for each login ID.
- Removing a lockout or change the system's lockout timer value.
- Setting the system's inactivity timer value.
- Setting system security logging and alarm configuration.
- Monitoring all system security logs.
- Managing system security logging processes.
- Upgrading security software.
- Terminating any user or system session.
- Delegating security authorizations to specific persons in other roles.
- Setting password complexity rules.

REQ 17: Each NE/MS should support the following application security **Management Actions,** but is not limited to:

- Defining and assigning new user and group privileges at the application level.
- Maintaining a record of all requests for login IDs to the application.
- Adding and deleting users at the application level.
- Monitoring all application security logs.
- Configuring application security logging and alarms.
- Managing application security logging processes.
- Terminating user application session.

6.2.2 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 ACS to store user IDs and passwords. The mandatory requirements expressed throughout this Recommendation apply to a NE/MS if it holds user IDs and passwords and the user IDs and passwords stored on the ACS.

REQ 18: NE/MS should synchronize time in an authenticated manner (e.g., NTP Version 3).

REQ 19: For an NE/MS, each **Management Action** should be associated with a single authorized SESSION.

REQ 20: Each SESSION should be established via proper **Authentication** as detailed in requirement REQ 1.

REQ 21: Communications between a NE/MS and an ACS for the purposes of conveying **Authentication** credentials should occur over a **Trusted Path**.

REQ 22: NE/MS should use **Access Control** and partitions to allow, deny, or otherwise control a user, user group, or remote system's access to the NE/MS and should provide functionality restricting users to the data, transactions, and equipment necessary to fulfill their roles. Access permissions should include, and not be limited to, read-only and read-write.

6.2.3 Login process

REQ 23: The NE/MS should support the ability to assign to every individual a unique user ID to login to an application or host computer system.

REQ 24: NE/MS should have the capability, when necessary, to automatically force the user to change their password on the first access after the account has been established and on the first access after the password has been reset.

NOTE – The following requirement (REQ 25) demands that a distinction be made as it pertains to the management of a Network Element (NE) vs a Management System (MS). Management of Network Elements requires the monitoring of a device through several mechanisms, perhaps simultaneously, while making configuration changes. In the case of an MS, this is not necessary.

The intent of this requirement is to manage users capability of consuming all available resources of an NE/MS. Operations staffs should adjust the NE default as needed for individual situations, and should monitor and investigate attempts to exceed these limits, as they may indicate an operational deficiency or an attempt at mischievous activities.

REQ 25: NE/MS should prevent, control, or limit the simultaneous active usage of the same user ID, when appropriate. The number of simultaneous active sessions should be configurable on a user ID basis.

REQ 26: The NE/MS application should note require **Superuser** access privileges in order to work properly.

REQ 27: NE/MS should have the capability of displaying to the user, when appropriate, during the logon process, the time and date of that user's last successful **Authentication**.

REQ 28: A customizable proprietary information statement and no trespassing warning should be displayed on the initial entry screen before any logical access is allowed. Equipment should support a minimum length of 1600 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.

REQ 29: Any failed login attempt should report to the user only that the login process has failed or is invalid. Information such as "invalid user ID" or "invalid password" should not be reported.

REQ 30: NE/MS should **Lockout** a user account from logging in after a configurable threshold number of login failures has been reached. The **Lockout** should include the console interface. The **Lockout** should NOT include the original default account that supports all the management actions.

REQ 31: NE/MS should NOT have a mechanism for bypassing the login **Authentication** and logging in processes.

REQ 32: No NE/MS should ever display a plaintext credential, such as password, in any media, including displays on terminal screens, printouts, and storing in log records.

REQ 33: NE/MS should enforce password aging with a configurable threshold.

A common and acceptable implementation of REQ 33 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 an administrator to properly change the password. If an account has not been used for a period of time, it will be considered dormant.

REQ 34: If a login password has surpassed the age limit for that system, then the NE/MS should **Lockout** the login for that user ID until the password is properly changed.

REQ 35: If an account has been dormant for a configurable threshold period of time, each NE/MS should generate an alert.

REQ 36: If an account has been dormant for a configurable threshold period of time, the NE/MS should disable the account after generating a Disable alert. The DISABLE process should NOT include the **System Administrator** account, the **System Security Administrator** account, and the **Superuser** account.

REQ 37: To re-enable a **Disabled** login ID, a properly logged in administrator, with the assigned Critical Security Administration Action to initialize and reset login passwords, is required.

The options to re-enable login IDs can be configured as a system-wide parameter at the role level.

REQ 38: To reset a LOCKED OUT login ID and to remove the **Lockout** condition, a properly logged in administrator with the assigned Critical Security Administration Action to remove a lockout or change the system's Lockout timer value is required.

The options to remove a **Lockout** from login IDs can be configured as a system-wide parameter at the role level.

6.2.4 Logout process

REQ 39: Each properly logged-in **Session** should be logged out by the user or by system inactivity.

REQ 40: NE/MS should log out a properly logged-in **Session** when the time, since the last activity for that **Session**, exceeds the system's configurable inactivity timer value.

6.2.5 Applications

REQ 41: A user's role type should remain unchanged during the execution of and exit from any NE/MS application.

The user should not be able to use a control sequence mechanism, for example, 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 re-authenticate (relogin) in order to assume a different role.

6.3 Protection of confidentiality

This clause specifies requirements for cryptographic algorithms and key management to help ensure system and network security. Symmetric algorithms are normally used for both confidentiality and integrity services. The keys for symmetric algorithms should normally be exchanged in a process tightly bound to authentication. Asymmetric algorithms may also be used in support of authentication and key exchange services. The methods used to generate, store, distribute, destroy, and revoke these keys are of paramount importance. In addition, factors such as key length, key selection, and algorithm selection have a direct bearing on the security strength of a specific cryptosystem.

Protected Authentication and data confidentiality are based on a cryptographic foundation. Cryptography uses special algorithms that are standards-based and publicly available, thereby allowing for widespread scrutiny and ease of implementation. Cryptographic "strength" is based on the cryptographic algorithm used, as well as the key size used (i.e., 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).

Security protocols (e.g., IPsec, SSL, SSH) typically provide **Authentication**, integrity, and confidentiality. Security extensions to other protocols such as Simple Network Management Protocol Version 3 (SNMPv3)[4], 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.

6.3.1 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 (e.g., the encryption key). The key must be distributed to the individuals via a secure means, or internally generated (e.g., based on a shared secret root key) because knowledge of the enciphering key implies knowledge of the deciphering key and vice versa.

REQ 42: For all symmetric encryption applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.

[4] SNMPv3 may also provide confidentiality.

6.3.2 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 is known for deriving the private key from the public key. Public keys are distributed widely; however, the private key is always kept secret. The use of asymmetric encryption is usually limited to the encryption of symmetric keys for key exchange and the signing of message digests for digital signatures. In key exchange, the recipient's public key is used and, in the signing of message digests, the signer's private key is used.

REQ 43: For all asymmetric encryption applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.

REQ 44: For all key exchange applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.

6.3.3 Cryptographic key management

Properly managing cryptographic key material is difficult and often complex because key management involves expiration, secure exchange, and secure publication, in addition to key generation. IETF RFC 1750, *Randomness Recommendations for Security*, provides additional guidance.

6.3.4 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 apply to all interfaces of a TMN as described in the ITU-T Rec. M.3010, *Principles for a Telecommunications Management Network*.

REQ 45: For each physical or logical interface that carries any **Management Traffic** in an NE/MS, the NE/MS should be configurable to secure **Management Traffic** with **Strong Authentication** and cryptographic protection in order to provide confidentiality, integrity and replay protection.

REQ 46: Any password transmitted in clear text should only be transmitted across a **Trusted Path** unless a one-time password mechanism is used. If one-time passwords are used, then they may be sent in clear text as long as there is no intermediate host.

6.4 Protection of data integrity

6.4.1 Data integrity algorithms

Keyed message digest algorithms combined with hashing functions could be used to ensure data integrity for arbitrary length messages.

REQ 47: For all symmetric secure data integrity applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.

REQ 48: For all asymmetric secure data integrity applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.

6.4.2 NE/MS development and delivery

Security of an NE/MS is dependent on the complete lifecycle 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 lifecycle process are critical to providing acceptable levels of security. Clauses I.5.2 and I.5.3, discuss additional lifecycle considerations.

REQ 49: All software delivered to a service provider or other customer should include, when appropriate, cryptographic **Authentication** and integrity protection mechanisms such as digital signatures or symmetric message **Authentication** as specified in ITU-T M.3016.3.

REQ 50: 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, when appropriate.

REQ 51: All software updates, including patches, should be transmitted to the receiving NE/MS over a **Trusted Path**.

NE/MS should be able to electronically determine their current software and hardware revision levels and validate appropriate software/firmware configurations.

6.5 Accountability

The objective of accountability is to ensure that any entity should be responsible for any actions it initiates.

REQ 52: All NE/MS should provide the capability that an entity cannot deny the responsibility of any of its performed actions as well as their effects.

Also see REQ 49 and REQ 50 for accountability requirements related to NE/MS development and delivery.

6.6 Security logging and audit

It is important that each NE/MS provide adequate capabilities to allow investigation, audit, real-time detection, analysis, and protection 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 Recommendation.

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 clause. Logging of non-security related OAM&P messages, sometimes referred to as "recent change" messages, is required for any actions that are auditable.

REQ 53: NE/MS should be able to log any action that changes the security attributes and services, access controls, configuration parameters of the devices.

REQ 54: NE/MS should provide the capability to configure those **Critical Security Administration Actions** that are to be included in the security log.

REQ 55: The NE/MS should be able to log each login attempt and its result; each logout or Session termination (whether remote or console) and each login attempt and its result that caused invocation of the system inactivity timer defined in REQ 12.

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.

REQ 56: NE/MS should be capable of remote logging over a **Trusted Path**.

REQ 57: Each log entry should contain the following information:

- A description of the action or the actual action that is being logged;
- The identity and security level of the user or process 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.

6.7 Security alarm reporting

Certain events need to be reported as security alarms, e.g., see REQ 35. However, it is beyond the scope of this Recommendation to identify the specific events that need to be reported.

REQ 58: All NE/MS should provide the capability to generate alarm notifications on selected events.

REQ 59: All NE/MS should provide the capability to allow the user to define the selection criteria for events that generate alarm notifications.

6.8 Protection of the DCN

To protect the management infrastructure, and the DCN in general, it is useful for the network operator to inspect and take action on certain traffic received from or destined to outside the DCN (e.g., from peer networks and customers). For example, packets with source IP addresses that match the address space of the DCN should not be permitted into the DCN from outside networks.

REQ 60: All NE/MS with packet-based connectivity should prevent traffic that does not meet the DCN security policy.

Annex A

Mapping of security requirements, services and mechanisms

This annex provides the mapping from the security requirements to the security services defined in ITU-T Rec. M.3016.2 and the security mechanisms defined in ITU-T Rec. M.3016.3.

M.3016.1 security requirements		M.3016.2 security services	M.3016.3 security mechanisms
REQ 1:	For NE/MS logging in, logging, and auditing, strong authentication should be supported.	**SER 1, SER 2, SER 3, SER 8**	**MEC 1-MEC 13**
REQ 2:	Each NE/MS should enforce **Authentication** according to organizational policy.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 3:	Each NE/MS should support the Minimum complexity rules for **Authentication** according to the organizational policy.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 4:	The NE/MS should prevent another user from changing a logged-on user's password without their knowledge.	**SER 8**	**MEC 7-MEC 11**
REQ 5:	Each NE/MS should automatically ensure that each new login password differs from the previous password. The degree of difference should be configurable according to organizational policy.	**SER 1**	**MEC 7-MEC 11**
REQ 6:	Each NE/MS should support prevention of password reuse. Password use prevention parameters should be configurable according to organizational policy.	**SER 1**	**MEC 7-MEC 11**
REQ 7:	Each user ID should have its own settable login password.	**SER 1**	**MEC 7-MEC 11**

M.3016.1 security requirements		M.3016.2 security services	M.3016.3 security mechanisms
REQ 8:	Passwords should be user changeable at the user's discretion, following a minimum interval since the last change. The minimum interval should be configurable according to the organizational policy and set by the **System Security Administrator**.	**SER 1**	**MEC 7-MEC 11**
REQ 9:	Each NE/MS should support multi-level password control. Some users can be locked out (e.g., due to password aging or login failure) while some users cannot be.	**SER 1, SER 2, SER 3, SER 4**	**MEC 20-MEC 23**
REQ 10:	One of the following should apply: • The configuration software should create a unique initialization password for each application in the new release or upgrade of the software. • If a default password is used, the system should require the replacement of the default password with a unique password before the device goes into service. • If a device is delivered without a password or a null password, a unique password should be assigned during the installation process before the device goes into service.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 11:	The system age threshold for login passwords should be configurable if the functionality is also built into the application. At the expiration of the age threshold, the login password for an affected application should be reset to an original default state defined in REQ 10. All password change privileges should be revoked for all users except for the user role, which has the highest level of security authority for a system or application instance.	**SER 4**	**MEC 7-MEC 11**
REQ 12:	The system inactivity timer value should be configurable if the functionality is also built into the application. When the system inactivity timer is enabled, an access to the system for a given user ID should be prevented and login process for this user should be disabled.	**SER 4**	**MEC 7-MEC 11**
REQ 13:	The system limit on consecutive failed logins for a given user ID should be configurable if the functionality is also built into the application. When the system limit on consecutive failed logins for a given user ID is reached, the system inactivity timer defined in REQ 12 should be invoked.	**SER 4**	**MEC 7-MEC 11**
REQ 14:	Each NE/MS should have support for multiple user-defined types of user roles, and **Management Actions** are assignable to each user role.	**SER 4**	**MEC 20-MEC 23**
REQ 15:	Each NE/MS should support a default user type, which has minimal or restrictive **Management Actions**.	**SER 4**	**MEC 20-MEC 23**

M.3016.1 security requirements	M.3016.2 security services	M.3016.3 security mechanisms
REQ 16: Each NE/MS should support the following **Critical Security Administration Actions,** but is not limited to: • Define and assign user and group privileges. • Maintain a record of all requests for login IDs to the system. • Add and delete user IDs. • Disable and 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. • Monitor all system security logs. • Manage system security logging processes. • Upgrade security software. • Terminate any user or system session. • Delegate security authorizations to specific persons in other roles. • Set password complexity rules.	**SER 4, SER 8**	**MEC 20-MEC 23**
REQ 17: Each NE/MS should support the following application security **Management Actions,** but is not limited to: • 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. • Terminate user application session.	**SER 4, SER 8**	**MEC 20-MEC 23**
REQ 18: NE/MS should synchronize time in an authenticated manner (e.g., NTP Version 3).	**SER 8**	**N/A**
REQ 19: For an NE/MS, each **Management Action** should be associated with a single authorized SESSION.	**SER 4**	**MEC 20-MEC 23**
REQ 20: Each SESSION should be established via proper **Authentication** as detailed in requirement REQ 1.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 12**
REQ 21: Communications between a NE/MS and an ACS for the purposes of conveying **Authentication** credentials should occur over a **Trusted Path**.	**SER 5, SER 6**	**MEC 19**

M.3016.1 security requirements	M.3016.2 security services	M.3016.3 security mechanisms
REQ 22: NE/MS should use **Access Control** and partitions to allow, deny, or otherwise control a user, user group, or remote system's access to the NE/MS, and should provide functionality restricting users to the data, transactions, and equipment necessary to fulfill their roles. Access permissions should include, and not be limited to, read-only and read-write.	**SER 4**	**MEC 20-MEC 23**
REQ 23: The NE/MS should support the ability to assign to every individual a unique user ID to log in to an application or host computer system.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 24: NE/MS should have the capability, when necessary, to automatically force the user to change their password on the first access after the account has been established and on the first access after the password has been reset.	**SER 4**	**MEC 7-MEC 11**
REQ 25: NE/MS should prevent, control, or limit the simultaneous active usage of the same user ID, when appropriate. The number of simultaneous active sessions should be configurable on a user ID basis.	**SER 1, SER 2, SER 3, SER 4**	**MEC 7-MEC 11**
REQ 26: The NE/MS application should not require **Superuser** access privileges in order to work properly.	**SER 4**	**MEC 20-MEC 23**
REQ 27: NE/MS should have the capability of displaying to the user, when appropriate during the logon process, the time and date of that user's last successful **Authentication**.	**SER 4, SER 8**	**MEC 7-MEC 11**
REQ 28: A customizable proprietary information statement and no trespassing warning should be displayed on the initial entry screen before any logical access is allowed. Equipment should support a minimum length of 1600 characters. A default message should be provided.	**SER 4**	**N/A**
REQ 29: Any failed login attempt should report to the user only that the login process has failed or is invalid. Information such as "invalid user ID" or "invalid password" should not be reported.	**SER 8**	**MEC 7-MEC 11**
REQ 30: NE/MS should **Lockout** a user account from logging in after a configurable threshold number of login failures has been reached. The **Lockout** should include the console interface. The **Lockout** should NOT include the original default account that supports all the Management Actions.	**SER 4**	**MEC 7-MEC 11**
REQ 31: NE/MS should NOT have a mechanism for bypassing the login **Authentication** and logging in processes.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 32: No NE/MS should ever display a plaintext credential, such as password, in any media, including displays on terminal screens, printouts, and storing in log records.	**SER 8**	**MEC 7-MEC 11**
REQ 33: NE/MS should enforce password aging with a configurable threshold.	**SER 4**	**MEC 7-MEC 11**
REQ 34: If a login password has surpassed the age limit for that system, then the NE/MS should **Lockout** the login for that user ID until the password is properly changed.	**SER 4**	**MEC 7-MEC 11**
REQ 35: If an account has been dormant for a configurable threshold period of time, each NE/MS should generate an alert.	**SER 4, SER 8, SER 9**	**MEC 7-MEC 11** **MEC 33-MEC 37**

M.3016.1 security requirements	M.3016.2 security services	M.3016.3 security mechanisms
REQ 36: If an account has been dormant for a configurable threshold period of time, the NE/MS should Disable the account after generating a Disable alert. The DISABLE process should NOT include the **System Administrator** account, the **System Security Administrator** account, and the **Superuser** account.	**SER 4, SER 8**	**MEC 7-MEC 11** **MEC 20-MEC 23**
REQ 37: To re-enable a Disabled login ID, a properly logged-in administrator with the assigned Critical Security Administration Action to initialize and reset login passwords is required.	**SER 4**	**MEC 7-MEC 11** **MEC 20-MEC 23**
REQ 38: To reset a LOCKED OUT login ID and to remove the Lockout condition, a properly logged-in administrator with the assigned Critical Security Administration Action to remove a lockout or change the system's Lockout timer value is required.	**SER 4**	**MEC 7-MEC 11** **MEC 20-MEC 23**
REQ 39: Each properly logged-in **Session** should be logged out by the user or by system inactivity.	**SER 4**	**MEC 33-MEC 37**
REQ 40: NE/MS should log out a properly logged-in **Session** when the time, since the last activity for that **Session**, exceeds the system's configurable inactivity timer value.	**SER 4**	**MEC 7-MEC 11**
REQ 41: A user's role type should remain unchanged during the execution of and exit from any NE/MS application.	**SER 4**	**MEC 20-MEC 23**
REQ 42: For all symmetric encryption applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.	**SER 5, SER 6**	**MEC 24-MEC 26**
REQ 43: For all asymmetric encryption applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.	**SER 5, SER 6**	**MEC 27-MEC 28**
REQ 44: For all key exchange applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.	**SER 5, SER 6**	**MEC 38-MEC 40**
REQ 45: For each physical or logical interface that carries any **Management Traffic** in an NE/MS, the NE/MS should be configurable to secure **Management Traffic** with **Strong Authentication** and cryptographic protection in order to provide confidentiality, integrity, and replay protection.	**SER 2, SER 3, SER 5, SER 6**	**MEC 24-MEC 32**
REQ 46: Any password transmitted in clear text should only be transmitted across a **Trusted Path** unless a one-time password mechanism is used. If one-time passwords are used, then they may be sent in clear text as long as there is no intermediate host.	**SER 1, SER 2, SER 3, SER 5, SER 6**	**MEC 19**
REQ 47: For all symmetric secure data integrity applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.	**SER 5**	**MEC 29-MEC 30**
REQ 48: For all asymmetric secure data integrity applications, the strength of the algorithms should be consistent with the national, industrial, or organizational policy.	**SER 5**	**MEC 31-MEC 32**
REQ 49: All software delivered to a service provider or other customer should include, when appropriate, cryptographic **Authentication** and integrity protection mechanisms such as digital signatures or symmetric message **Authentication** as specified in ITU-T Rec. M.3016.3.	**SER 7**	**MEC 29-MEC 32**

M.3016.1 security requirements	M.3016.2 security services	M.3016.3 security mechanisms
REQ 50: 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, when appropriate.	**SER 7**	**MEC 29-MEC 32**
REQ 51: All software updates, including patches, should be transmitted to the receiving NE/MS over a **Trusted Path**.	**SER 5, SER 6**	**MEC 19**
REQ 52: All NE/MS should provide the capability that an entity cannot deny the responsibility of any of its performed actions, as well as their effects.	**SER 7**	**MEC 29-MEC 32**
REQ 53: NE/MS should be able to log any action that changes the security attributes and services, access controls, configuration parameters of the devices, and each login attempt and its result that caused invocation of the system inactivity timer defined in REQ 12.	**SER 8**	**MEC 33-MEC 37**
REQ 54: NE/MS should provide the capability to configure those **Critical Security Administration Actions** that are to be included in the security log.	**SER 4**	**MEC 33-MEC 37**
REQ 55: The NE/MS should be able to log each login attempt and its result; and each logout or Session termination (whether remote or console).	**SER 8**	**MEC 33-MEC 37**
REQ 56: NE/MS should be capable of remote logging over a **Trusted Path**.	**SER 5, SER 6,** **SER 8**	**MEC 33-MEC 37** **MEC 19**
REQ 57: Each log entry should contain the following information: • A description of the action or the actual action that is being logged. • The identity and security level of the user or process 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.	**SER 8**	**MEC 33-MEC 37**
REQ 58: All NE/MS should provide the capability to generate alarm notifications on selected events.	**SER 9**	**MEC 41**
REQ 59: All NE/MS should provide the capability to allow the user to define the selection criteria for events that generate alarm notifications.	**SER 9**	**MEC 41**
REQ 60: All NE/MS with packet-based connectivity should prevent traffic that does not meet the DCN security policy.	**SER 10**	**MEC 42**

Appendix I

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 Recommendation, 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 appendix are subject to future discussions and contributions. They do not represent any intent to include or exclude content in existing or emerging standards.

I.1 Applicability to enterprise operations, administration, maintenance and provisioning

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.

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 telecommunication infrastructure. In summary, the security requirements for operations, administration, maintenance, and provisioning traffic outlined in this appendix are fully applicable to enterprises and service provider/carrier networks.

I.2 Common object request broker architecture, simple network management protocol, extensible markup language, and simple object access protocol

The following considerations should be taken into account with regard to security for common object request broker architecture (CORBA), simple network management protocol (SNMP), extensible markup language (XML), and simple object access protocol (SOAP). In addition, there are other protocols that may be equally applicable such as the blocks extensible exchange protocol. Although no changes to these evolving protocols are proposed, the following discussion could be used to enhance security.

I.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, secure socket layer (SSL)) for availability and simplicity reasons. Finally, some applications might require no security. The optional requirements below, therefore, reflect three possible choices:

- No security;
- Object request brokers (ORB) use TLS (or 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 ITU-T Rec. Q.816, *CORBA-based TMN services* and ITU-T Rec. Q.816.1, *CORBA-based TMN services: Extensions to support course-grained interfaces*.

If CORBA is used in the network element/management system (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-ORB Protocol/Internet Inter-ORB 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 ORB technology selected;
- Ensure it meets the requirements for security outlined elsewhere in this Recommendation.

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 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 administration costs, 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 Recommendation. 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.

I.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-T Study Group 4 is considering the establishment of two new protocol stacks:

- SNMPv3 or V2C with TLS over transmission control protocol (no access control); and
- SNMPv3 with user security model over user datagram protocol (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.
- Access controls should be used to allow SNMP messages only from an authorized manager. SNMP messages from all other sources should be denied and treated according to appropriate security policies. It may be desirable to block unauthorized requests at the device and at a network perimeter.
- The default community string should not be used.
- Access violations and access errors should be logged.
- SNMPv3 uses the data encryption standard 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.
- Any service or capability not explicitly required should be disabled, including SNMP if it is enabled.

I.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.

I.2.4 SOAP

SOAP 1.1 is the current Recommendation form the World Wide Web Consortium. SOAP is a message format not tied to a specific protocol. It most commonly uses hypertext transfer protocol (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).

I.3 Lawfully authorized electronic surveillance

Telecommunication carriers should take the following security considerations into account with respect to the implementation of Lawfully Authorized Electronic Surveillance (LAES).

Security practices for LAES activities should be robust and the same as for any critical NE, operations support system (OSS), or MS with some exceptions as listed below. 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 LAES requests.

I.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. Wireless equipment tends to be installed outdoors in an insecure environment. Also, 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, 24/7 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, and remote video monitoring of 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, *Public Switched Network Security Assessment Guidelines*, September 2000.

I.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.

I.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.

I.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".[5] 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.
- 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 so 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 so that the guard can 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.

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

- 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.

I.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 precautions are important:

- Procedures should exist for authorizing distribution of keys to individuals, including key control and logging of access and distribution;
- Keys should be individually numbered;
- A complete inventory of keys and their owners should be maintained and audited;
- Criteria for replacing locks when keys are lost should be in place;
- Periodic audits of the key inventory should be enforced, and procedures for reconciling discrepancies should 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.

I.4.1.4 Functional separation of facilities and multilevel access control

Physical security applies to internal portions of a building as well as to 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 centres) 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.

I.4.2 Building services

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

I.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.

I.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.

I.4.2.3 Transport redundancy and physical protection of critical facilities

Critical computer and communication systems facilities should be geographically dispersed to the extent possible without unduly affecting operational costs, performance, and security. In addition, routing of critical communication links (e.g., important interoffice trunks, signalling 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 communication 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.

I.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, gasline 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 communication 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.

I.4.4 Co-location procedures

Co-location 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 host provider. 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"[6]) becomes a potential hazard in an open environment and should be avoided.

I.5 Development process

I.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 T1.233-2004, *Operations, Administration, Maintenance, and Provisioning – Security framework for Telecommunications Management Network Interfaces*, and ISO/IEC 10181, *Open Systems Interconnection – Security frameworks for open systems* standards documents. General connectivity to open systems broadens threats such as:

- Bootstrap viruses;
- Unauthorized access;
- Masquerade;
- Threats to data integrity;
- Threats to confidentiality;
- Denial of service (DoS); and
- Repudiation.

I.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 operating system (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

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

the provider to verify with the application vendor that the OS patch released will not adversely affect the running of the/an application.

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 service provider 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 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, subsequently, to 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.
– OS 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 should not be constrained by periodic 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.

I.5.3 Development lifecycle security

Security of a product or service is dependent on the complete lifecycle 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 lifecycle process are critical to providing acceptable levels of security.

I.5.3.1 Personnel management

A fundamental issue of security that is often overlooked is the trustworthiness of the staff. All staff with 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.

I.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.

I.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 not only involves 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 lifecycle 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, Internet service provider), 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.

I.5.3.4 Requirements

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

I.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.

I.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.

I.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 on 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.

I.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.

I.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. If the OS does not meet the security provider's security needs, then the software may need to be installed in 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. There are several documents and Web sites that discuss OS

security. Although it is beyond the scope of this Recommendation to list them, some examples include the Common Criteria, and OS Protection Profiles.[7, 8, 9]

– Only a minimum of services will be enabled that are required for operation by default.

I.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.

I.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.

I.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. Testing should be conducted to provide assurance that components and security features have been robustly implemented and correctly configured.

– 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.

I.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 system-to-system.

I.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.

I.5.3.15 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.

[7] The Common Criteria is becoming an internationally recognized standard for formal security evaluation (http://www.commoncriteria.org/).

[8] Information Assurance Technical Framework Forum Operating System Protection Profiles, http://www.iatf.net/protection_profiles/operating_systems.cfm

[9] National Institute of Standards and Technology, Computer Security Resource Center, http://csrc.nist.gov/

- 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.

I.5.3.16 Packaging and delivery

A software configuration management system must be used throughout the lifecycle 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 that 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.

I.5.3.17 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).

Appendix II

Framework and design guidelines

II.1 Framework and model

In the context of this Recommendation, to secure something means to protect it (i.e., computers, networks, data, or other resources) from unauthorized access, use, or activity. Loss of data, denial of service (DoS), and theft of service are only some of the results of security incidents. System and network administrators need to protect systems and their component elements from internal and external 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. A threat consists of, but is not limited to, disclosure, unauthorized use, information element modifications, and denial of service. Table II.1 lists some security threats.

Table II.1/M.3016.1 – Threats

Threat category (Note)	Examples of threats
Unauthorized access	Hacking Unauthorized system access to carry out attacks Theft of service
Masquerade	Session replay Session hijacking Man-in-the-middle attacks
Threats to system integrity	Unauthorized manipulation of system configuration files Unauthorized manipulation of system data
Threats to communication integrity	Unauthorized manipulation of data in transit
Threats to confidentiality	Eavesdropping Session recording and disclosure Privacy violations
Denial of service	Transmission control protocol (TCP) SYN flood Malformed packet attacks Distributed DoS
NOTE – Derived from American National Standards Institute T1.233-1993 (R1999), *Operations, Administration, Maintenance, and Provisioning – Security Framework for Telecommunications Management Network Interfaces* and International Organization for Standardization (ISO) 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*	

These security threats may be minimized or mitigated within a network system or NE platform or application by inclusion of security services (as defined in ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*) to enforce the following:

– Identification and **Authentication**;

– Authorization and **Access Control** Level;

– Data Integrity;

– Privacy and Confidentiality;

– Nonrepudiation.

This Recommendation 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 Recommendation. The following risks are among those with the capability to compromise the management plane:

– Inappropriate actions by authorized users or attackers. These actions can be either malevolent or accidental.

– Bridge of the control plane security (e.g., signalling, routing, naming, and discovery protocols).

– The effects of vulnerabilities in specific protocols.

– Malware (e.g., viruses, Trojan horses, worms, or other embedded code). Once malware successfully compromises any NE/MS, the malware may use the secure network communication links to transmit attacks to other NE/MS components. These attacks may continue until network managers detect the attack and take action to eliminate it.

This Recommendation is concerned with the security of management traffic, especially when it traverses networks mixed with end-user traffic. Figure II.1 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 II.1. EMSs 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.

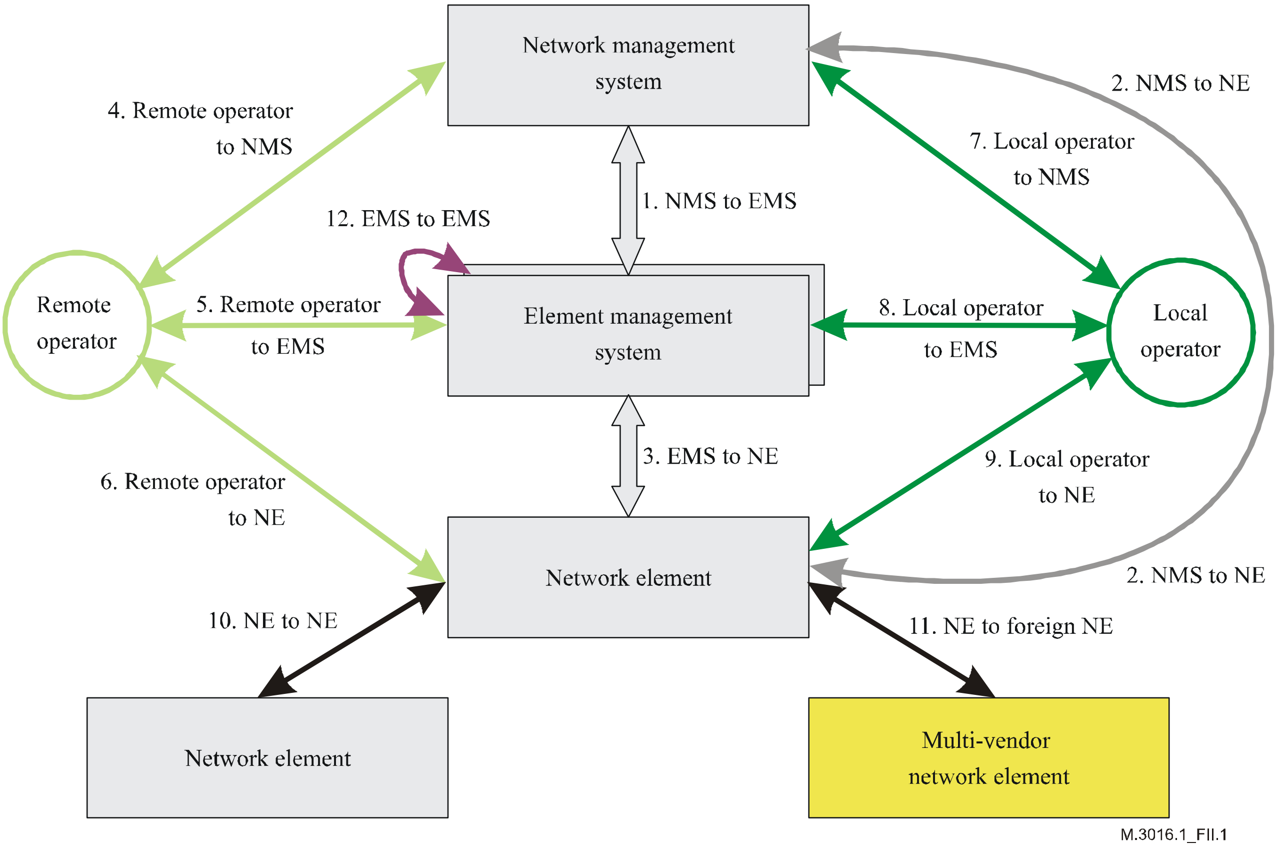

Figure II.1/M.3016.1 – Network management security reference model

The security reference model (Figure II.1) may also be useful in correlating telecommunication management network (TMN)-defined interfaces to the security model. The TMN is defined in ITU-T Rec. M.3010, *Principles for a Telecommunications Management Network*. It is defined as an architecture for management, including planning, provisioning, installation, maintenance, operations, and administration of telecommunication equipment, networks and services.

II.2 Design guidelines

Table II.2 presents design guideline objectives that attempt to satisfy the requirements in clause 6 to mitigate the threats proposed in Table II.1.

Table II.2/M.3016.1 – 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)	Reliable accounting of properly authorizes sessions between authenticated entities.
Highest benefit for a given cost	Improve security by implementing security mechanisms that are standardized, have widely available implementations, and widespread deployment, so that use histories allow security mechanisms to be evaluated.
Path for improvement	Consider next steps for enhancing and improving network management security to further satisfy given requirements with evolving technology and mechanisms or to satisfy newly defined security requirements.

Guideline	Description
Technical feasibility	Requirements must be satisfied with products, solutions, and/or 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 or are being standardized by the standards organizations (e.g., IP security (IPsec), digital signatures). All aspects of the open standards should be considered, including system, protocols, modes, algorithm, option, key size and encoding

Appendix III

Semantics of terms used in the M.3016.x series

The following terms appear in **bold** when they are used in a requirement statement.

III.1 access control: The prevention of unauthorized use of a resource including the prevention of use of a resource in an unauthorized manner.[10]

III.2 access control server (ACS): An auxiliary network element that is deployed to enforce and authenticate access to an MS based on **Complex Passwords**, if an NE cannot directly enforce this functionality.

III.3 application administrator: A role that is responsible for the proper activation, maintenance, and usage of an NE/MS application. Application administration tasks include upgrading application software.[11]

III.4 application security administrator: A role that is responsible for the proper activation, maintenance, and usage of the application layer security features of a NE/MS. Represents the highest level of security authority for a NE/MS application instance. Tasks may include:

- Defining and assigning new user and group privileges at the application level;
- Maintaining a record of all requests for login IDs to the application;
- Adding and deleting users at the application level;
- Monitoring all application security logs;
- Configuring application security logging and alarms;
- Managing application security logging processes;
- Terminating user application session.

III.5 authentication: **Authentication** is the act of verifying a claimed identity.

III.6 complex passwords: A password is characterized as "complex" when it has some combination of alphabetic, numeric, and special characters, which should make guessing the password through social engineering or automated means difficult or unlikely.

[10] Taken from ANSI T1.233-1993 (R1999), *Operations, Administration, Maintenance, and Provisioning – Security Framework for Telecommunications Management Network Interfaces*, clause 3.1.

[11] This task may be a function of the **System Administrator**, if **Superuser** authority is necessary to complete this task. Processes may be developed to control access to the **Superuser** account.

III.7 control plane: The **Control Plane** performs call control and connection control functions. Through signalling, the **Control Plane** sets up and releases connections, and may restore a connection in case of a failure.[12]

III.8 critical security administration actions: A **System Security Administrator** is responsible for critical security administration actions, which allow the proper activation, maintenance, and usage of the security features of a system (NE/MS). **Critical Security Administration Actions** include, but are not limited to:

- Defining and assigning user privileges;
- Adding and deleting user IDs;
- Disabling the use of specific user IDs as login IDs;
- Initializing and resetting login passwords;
- Initializing and changing cryptographic keys;
- Setting the system's aging threshold for login passwords;
- Setting the system's limit on the number of failed logins for each login ID;
- Removing a lockout, or change the system's lockout timer value;
- Setting the system's inactivity timer value;
- Setting system security logging and alarm configuration;
- Managing the security logging processes;
- Upgrading security software;
- Terminating any user or system session.

III.9 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**).

III.10 element management system (EMS): The system that performs the OS function in the element management layer.

III.11 key strength: Different cryptographic algorithms have varying 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 within a "reasonable" amount of time 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 and memory space 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 impossible 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.

III.12 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 resetting after a threshold period of time has elapsed (e.g., after 60 minutes);

[12] ITU-T Rec. G.8080/Y.1304, *Architecture for the automatically switched optical network (ASON)*, November 2001 (available at ITU Electronic Bookshop).

– Automatic resetting after successful completion of a predefined reset process (e.g., after the owner correctly answers a scripted set of questions); or

– Resetting by specific action from another user ID with the appropriate authorization privileges (e.g., **System Security Administrator** or **Application Security Administrator**).

III.13 management action: Actions that are undertaken by or on behalf of the **System Administrator**.

III.14 management communication: Any communication of a **Management Action**.

III.15 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 ITU-T Rec. M.3010, *Principles for a Telecommunications Management Network,* are performed in the **Management Plane**.[13]

III.16 network element (NE): See ITU-T Rec. M.3010.

III.17 network management system (NMS): The system that performs the OS function in the network management layer.

III.18 network element/management system (NE/MS): A collective term used to describe the entirety of elements within a telecommunications network including NEs, EMSs, NMSs and OSSs.

III.19 protected authentication: Includes **Strong Authentication**, **Two-Factor Authentication**, **Trusted Path Authentication**, cryptographic third-party authentication (e.g., Kerberos), or one-time password authentication.

III.20 session: A sequence of operations, either machine-to-machine or human-to-machine, that are associated with a unique process or user ID.

III.21 strong authentication: **Strong Authentication** is **Authentication** that relies on the use of cryptographic techniques (e.g., public key encryption, symmetric key encryption, digital signatures, and digital hashing techniques). **Strong Authentication** should include two-way authentication, which can be used to prevent active attacks.

III.22 strong encryption: A brute force attack occurs when an attacker tries all possible key combinations using available computing resources to uncover an encrypted message. 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 it would take any attacker more than 2 years to break with current technology.

III.23 system administrator: A role that is responsible for OS level processes and procedures pertaining to installation, operations, maintenance of the operating platform, installation of software on the platform, and control of **Super user** authority. Tasks may include:

– Coordinating the installation of a new platform;

– Defining and assigning new user and group privileges at the OS level;

– Maintaining a record of all requests for login IDs to the OS;

– Adding and deleting users at the OS level;

[13] The TMN architecture is described in ITU-T Rec. M.3010, *Principles for a Telecommunication Management Network* and additional details regarding the MANAGEMENT PLANE are provided in the M-series Recommendations. ITU-T Rec. G.8080/Y.1304, *Architecture for the automatically switched optical network (ASON)*, November 2001 (available at ITU Electronic Bookshop).

- Disabling the use of specific IDs as login IDs (bin, sys, uucp);
- Installing OS upgrades and patches;
- Installing application and database software to the OS;
- Monitoring all system logs;
- Maintaining and monitoring access and changes to **Super user** password;
- Control access to the **Super user** account, allowing appropriate access as the business requires;
- Managing system logging processes;
- Delegating administration authorizations to specific persons in other roles, including **Application Administrators**;
- Terminating any user or system session.

III.24 System Security Administrator: A role that is responsible for the proper activation, maintenance, and usage of the system security features of a NE/MS. Represents the highest level of security authority for a system/application instance. Tasks may include:

- Defining and assigning new user and group privileges at the OS level;
- Maintaining a record of all requests for login IDs to the OS;
- Adding and deleting users at the OS level;
- Disabling the use of specific IDs as login IDs (bin, sys, uucp);
- Monitoring all system security logs;
- Initializing and changing cryptographic keys;
- Setting the system's aging threshold for login passwords;
- Setting the system's limit on the number of failed logins for each login ID;
- Removing a lockout or changing the system's lockout timer value;
- Setting the system's inactivity timer value;
- Configuring system logging and alarms;
- Managing system security logging processes;
- Delegating security authorizations to specific persons in other roles, including **Application Security Administrators**;
- Terminating any user or system session.

III.25 transport plane: The **Transport Plane** provides bidirectional or unidirectional transfer of user information from one network element 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 ITU-T Rec. G.8080/Y.1304, *Architecture for the automatically switched optical network (ASON)*.[12]

III.26 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, which includes integrity and replay protection (e.g., "secured" virtual private network, Secure Socket Layer (SSL) tunnel, Secure Shell (SSH)).[14]

[14] Adapted from National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms*, October 1998 (available at http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

III.27 two-factor authentication: **Two-Factor Authentication** is a term commonly used to describe an **Authentication** process that requires the possession of a physical entity (e.g., token or card), and knowledge of a secret (e.g., password or passphrase).

BIBLIOGRAPHY

The items in this bibliography provide additional information on many of the topics addressed in Appendices I and II.

- ANSI J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance.*
- ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation,* (available from the ANSI X9 Electronic Standards Store, http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=80).
- ANSI X9.62-1998, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),* (available from the ANSI X9 Electronic Standards Store, http://webstore. ansi.org/ansidocstore/dept.asp?dept_id=80).
- ANSI T1.210-2004, *OAM&P – Principles of Functions, Architectures, and Protocols for Telecommunications Management Network (TMN) Interfaces.*
- ANSI T1.233-2004, *OAM&P – Security Framework for Telecommunications Management Network (TMN) Interfaces*.
- ANSI T1.252-1996 (R2002), *Operations, Administration, Maintenance and Provisioning OAM&P – Security for the Telecommunications Management Network (TMN) Directory.*
- ANSI T1.261-1998 (R2004), *OAM&P – Security for TMN Management Transactions over the TMN Q3 Interface.*
- ANSI T1.268-2000, *TMN – PKI – Digital Certificates and Certificate Revocation Lists Profile*.
- ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).*
- ATM Forum. AF-SEC-0179.000 (April 2002), *Methods of Securely Managing ATM Network Elements – Implementation Agreements Version 1.1,* (available at ftp://ftp.atmforum.com/pub/approved-specs/af-sec-0179.000.pdf).
- BARRETT (D.), SILVERMAN (R.): SSH, The Secure Shell: The Definitive Guide, *O'Reilly*, January 2001.
- BELLOVIN (S.): An Issue With DES-CBC When Used Without Strong Integrity, *Proceedings of the 32nd Internet Engineering Task Force*, Danvers, MA, April 1995.
- BLEICHENBACHER (D.): Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, *Advances in Cryptology-Crypto '98*, Springer LNCS Vol. 1462, pp. 1-12, 1998.
- BONEH (D.): Twenty Years of Attacks on the RSA Cryptosystem, *Notices of the American Mathematical Society (AMS)*, Vol. 46, No. 2, pp. 203-213, February 1999, (available at http://www.ams.org/notices/199902/boneh.pdf).
- BONEH (D.), JOUX (A.), NGUYEN (P.): Why Textbook RSA and ElGamal Encryption Are Insecure, *Advances in Cryptology-Asiacrypt 2000*, Springer LNCS Vol. 1976, pp. 30-43, 2000.
- Federal Communications Commission Docket Number 97-213 *Implementation of the Communications Assistance for Law Enforcement Act*, September 1999.
- General Requirements (GR)-815, *Generic Requirements for Network Element/Network System Security*, March 2002 (available at Telcordia Information SuperStore, http://telecom-info.telcordia.com/site-cgi/ido/index.html).

- GR-1194, *Bellcore Operations Systems Security Requirements*, December 1998, (available at Telcordia Information SuperStore, http://telecom-info.telcordia.com/site-cgi/ido/index.html).
- GUTMANN (P.): Software Generation of Practically Strong Random Numbers, *Seventh USENIX Security Symposium Proceedings*, The USENIX Association, pp. 243-257, 1998, (available at http://www.usenix.org/publications/library/proceedings/sec98/full_papers/gutmann/gutmann.pdf).
- Information Assurance Technical Framework Forum (IATF), http://www.commoncriteria.org/ and http://www.iatf.net/protection_profiles/profiles.cfm.
- IEEE 1363-2000, *IEEE Standard Specifications for Public Key Cryptography*, (available at IEEE Standards Online, http://standards.ieee.org/catalog/olis/ busarch.html).
- IETF RFC 768, *User Datagram Protocol*, J. Postel, August 1980 (available at http://www.ietf.org/rfc/rfc0768.txt?number=768).
- IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification*, (available at http://www.ietf.org/rfc/ rfc0791.txt?number=791).
- IETF RFC 792 (1981), *Internet Control Message Protocol – DARPA Internet Program Protocol Specification*, (available at http://www.ietf.org/rfc/rfc0792.txt?number=792).
- IETF RFC 793 (1981), *Transmission Control Protocol – DARPA Internet Program Protocol Specification*, (available at http://www.ietf.org/rfc/rfc0793.txt?number=793).
- IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol – or – Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*, (available at http://www.ietf.org/rfc/rfc0826.txt?number=826).
- IETF RFC 859 (1983), *Telnet Status Option,* (available at http://www.ietf.org/rfc/rfc0859.txt?number=859).
- IETF RFC 959 (1985), *File Transfer Protocol (FTP),* (available at http://www.ietf.org/rfc/rfc0959.txt?number=959).
- IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP),* (available at http://www.ietf.org/rfc/rfc1157.txt?number=1157).
- IETF RFC 1288 (1991), *The Finger User Information Protocol,* (available at http://www.ietf.org/rfc/rfc1288.txt?number=1288).
- IETF RFC 1905 (1996), *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2),* (available at http://www.ietf.org/rfc/rfc1905.txt?number=1905).
- IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies,* (available at http://www.ietf.org/rfc/rfc2045.txt?number=2045).
- IETF RFC 2202 (1997), *Test Cases for HMAC-MD5 and HMAC-SHA-1,* (available at http://www.ietf.org/rfc/rfc2202.txt?number=2202).
- IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL),* (available at http://www.ietf.org/rfc/rfc2222.txt?number=2222).
- IETF RFC 2246 (1999), *The TLS Protocol Version 1.0,* (available at http://www.ietf.org/rfc/rfc2246.txt?number=2246).

- IETF RFC 2271 (1998), *An Architecture for Describing SNMP Management Frameworks,* (available at http://www.ietf.org/rfc/rfc2271.txt?number=2271).
- IETF RFC 2272 (1998), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP),* (available at http://www.ietf.org/rfc/rfc2272.txt?number=2272).
- IETF RFC 2273 (1998), *SNMPv3 Applications,* (available at http://www.ietf.org/rfc/rfc2273.txt?number=2273).
- IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, (available at http://www.ietf.org/rfc/rfc3414.txt?number=3414).
- IETF RFC 2275 (1998), *View-based Access Control Model for the Simple Network Management Protocol* (*SNMP)*, (available at http://www.ietf.org/rfc/rfc2275.txt?number=2275).
- IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, (available at http://www.ietf.org/rfc/rfc2401.txt?number=2401).
- IETF RFC 2402 (1998), *IP Authentication Header,* (available at http://www.ietf.org/rfc/rfc2402.txt?number=2402).
- IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*, (available at http://www.ietf.org/rfc/rfc2406.txt?number=2406).
- IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms,* (available at http://www.ietf.org/rfc/rfc2451.txt?number=2451).
- IETF RFC 2616 (1999), *Hypertext Transfer Protocol (HTTP) – HTTP/1.1,* (available at http://www.ietf.org/rfc/rfc2616.txt?number=2616).
- IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method,* (available at http://www.ietf.org/rfc/rfc2631.txt?number=2631).
- IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core,* (available at http://www.ietf.org/rfc/rfc3080.txt?number=3080).
- IETF RFC 3081 (2001), *Mapping the BEEP Core onto TCP,* (available at http://www.ietf.org/rfc/rfc3081.txt?number=3081).
- ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture,* (available at ISO Online Store, http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14256&ICS1 =35&ICS2=100&ICS3=1).
- ITU-T Recommendation M.3010 (2000), *Principles for a Telecommunications Management Network,* (available at ITU Electronic Bookshop).
- ITU-T Recommendation M.3013 (2000), *Considerations for a Telecommunications Management Network,* (available at ITU Electronic Bookshop).
- JANSEN (W.A.): A Revised Model for Role Based Access Control, *NIST-IR 6192*, July 1998, (available at http://csrc.nist.gov/rbac/jansen-ir-rbac.pdf).
- JONSSON (J.), KALISKI (B.): On the Security of RSA Encryption in TLS, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 127-142, August 2002.
- KELSEY (J.), SCHNEIER (B.), FERGUSON (N.): Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator, *Sixth Annual*

Workshop on Selected Areas in Cryptography, Springer-Verlag, August 1999, (available at http://www.counterpane.com/yarrow-notes.html).

– KRAWCZYK (H.): Security Analysis of the Internet Key Exchange's Signature-Based Key Exchange Protocol, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 143-161, August 2002.

– LENSTRA (A.), VERHEUL (E.): Selecting Cryptographic Key Sizes, *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293, 2001.

– National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms.* October 1988, (available at http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

– National Communications System, *Public Switched Network Security Assessment Guidelines*, September 2000, (available at http://www.ncs.gov/ncs/Reports/NCS_Security_Assessment_Guidelines_Version1_sep00.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification*, *Version 1.8*, March 2002, (available at http://cgi.omg.org/docs/formal/02-03-11.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification, Version 1.7,* March 2001, (available at http://cgi.omg.org/docs/formal/01-03-08.pdf).

– Partnership for Critical Infrastructure Security, *Partnership for Critical Infrastructure Security Common Reference Glossary of Terms, Version 2001-09*, September 2001, (available at http://www.pcis.org/library.cfm?urlSection=WG).

– RESCORLA (E.): SSL and TLS, Addison-Wesley, 2001.

– SCHNEIER (Bruce.): Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

– SILVERMAN (R.): The Mythical MIPS Year, *IEEE Computer*, August 1999.

– SILVERMAN (R.): A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, *RSA Laboratories Bulletin*, No. 13, April 2000.

– VAUDENAY (S.): Security Flaws Induced by CBC Padding – Applications to SSL, IPsec, WTLS, *Advances in Cryptology-Eurocrypt 2002*, Springer LNCS Vol. 2332, pp. 534-545, April-May 2002.

– World Wide Web Consortium, *Extensible Markup Language (XML) 1.0*, February 1998, (available at http://www.w3.org/TR/1998/REC-xml-19980210).

– World Wide Web Consortium, *Simple Object Access Protocol 1.1*, D. Box et al, May 2000, (available at http://www.w3.org/TR/SOAP/).

– WU (T.): The Secure Remote Password Protocol, *Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security*, San Diego, California, pp. 97-111, March 1998, (available at http://www.isoc.org/isoc/conferences/ndss/98/wu.pdf)

– YLÖNEN, T.: SSH – Secure Login Connections Over the Internet, *Sixth USENIX Security Symposium Proceedings*, pp. 37-42, July 1996, (available at http://www.usenix.org/publications/library/proceedings/sec96/full_papers/ylonen/index.html).

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	**Telecommunication management, including TMN and network maintenance**
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2005