

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

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.

Copyright © 2005 ITU-T. All rights reserved.

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.

© ITU 2005

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
1.1	Purpose	1
1.2	Relationship with X.805 Security Architecture.....	1
1.3	Relationship with E.408 telecommunication networks security requirements	1
2	References.....	2
3	Terms and definitions	2
4	Abbreviations and acronyms	3
5	Conventions	4
6	Security requirements	5
6.1	Verification of identities.....	5
6.2	Controlled access and authorization	7
6.3	Protection of confidentiality	11
6.4	Protection of data integrity	12
6.5	Accountability	13
6.6	Security logging and audit.....	13
6.7	Security alarm reporting	14
6.8	Protection of the DCN	14
Annex A – Mapping of security requirements, services and mechanisms		14
Appendix I – Additional security considerations.....		20
I.1	Applicability to enterprise operations, administration, maintenance and provisioning	20
I.2	Common object request broker architecture, simple network management protocol, extensible markup language, and simple object access protocol	20
I.3	Lawfully authorized electronic surveillance	23
I.4	Physical security considerations.....	24
I.5	Development process.....	29
Appendix II – Framework and design guidelines		35
II.1	Framework and model	35
II.2	Design guidelines	37
Appendix III – Semantics of terms used in the M.3016.x series		38
BIBLIOGRAPHY		43

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 upgrade³ 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 not 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.