INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3320

(04/97)

SERIES M: TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS

Telecommunications management network

Management requirements framework for the TMN X-interface

ITU-T Recommendation M.3320

(Previously CCITT Recommendation)

ITU-T M-SERIES RECOMMENDATIONS

TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS

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 ITU-T List of Recommendations.

ITU-T RECOMMENDATION M.3320

MANAGEMENT REQUIREMENTS FRAMEWORK FOR THE TMN X-INTERFACE

Summary

This Recommendation describes a general framework and a set of basic management requirements for the development and use of the TMN X-interface.

Source

ITU-T Recommendation M.3320 was prepared by ITU-T Study Group 4 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 19th of April 1997.

Keywords

International Aspects, Management Information Exchange, Security consideration, TMN X-interface.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The 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 Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 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.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The 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, the ITU had/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

Recommendation M.3320

MANAGEMENT REQUIREMENTS FRAMEWORK FOR THE TMN X-INTERFACE

(Geneva, 1997)

1 Introduction

This set of requirements identify what is applicable for information exchange, via an automated TMN X-interface, between Administrations for joint end-to-end service and network management. This may be expanded to include Customer Network Management requirements that may add new information for exchange between Administrations. This Recommendation is based on the X-interface definition in Recommendation M.3010.

1.1 Scope

This Recommendation is part of a series dealing with the transfer of information for the management of telecommunication networks and services. The purpose of this Recommendation is to define a requirements framework for all functional, service and network-level requirements for the TMN exchange of information between Administrations. This Recommendation also provides for the general framework of using the TMN X-interface for the exchange of information between Administrations, Recognized Operating Agencies, other Network Operators, Service Providers, Customers and other entities.

1.2 References

1.2.1 Normative 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; all 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.

– ITU-T Recommendation M.3010 (1996), *Principles for a telecommunications management network.*

– ITU-T Recommendation M.3020 (1995), *TMN interface specification methodology*.

– ITU-T Recommendation M.3200 (1997), *TMN management services and telecommunications managed areas: Overview.*

– ITU-T Recommendation M.3400 (1997), *TMN management functions*.

– ITU-T Recommendation Q.811 (1997), *Lower layer protocol profiles for the Q3 and X-interface*.

– ITU-T Recommendation Q.812 (1997), *Upper layer protocol profiles for the Q3 and X-interface*.

– ITU-T Recommendation X.160 (1996), *Architecture for customer network management service for public data networks*.

- ITU-T Recommendation X.161 (1997), *Customer network management services for public data networks*.
- ITU-T Recommendation X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.*
- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- ITU-T Recommendation X.811 (1995), *Information Technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

1.2.2 Other references

- CCITT Recommendation F.435 (1991), *Electronic data interchange messaging service.*
- CCITT Recommendation M.1520 (1992), *Standardized information exchange between Administrations.*
- ITU-T Recommendation M.3000 (1994), *Overview of TMN Recommendations.*
- ITU-T Recommendation M.3100 (1995), *Generic network information model.*
- ITU-T Recommendation X.162 (1997), *Definition of management information for customer network management service for public data networks to be used with the CNMc interface.*
- ITU-T Recommendation X.163 (1995), *Definition of management information for customer network management service for public data networks to be used with the CNMe interface.*
- ITU-T Recommendation X.509 (1997), *Information technology – Open Systems Interconnection – The Directory: Authentication framework.*
- ITU-T Recommendation X.741 (1995), *Information technology – Open Systems Interconnection – Systems Management: Objects and attributes for access control.*
- ITU-T Recommendation X.802 (1995), *Information technology – Lower layers security model*.
- ITU-T Recommendation X.803 (1994), *Information technology – Open Systems Interconnection – Upper layers security model.*
- ITU-T Recommendation X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*
- ITU-T Recommendation X.812 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*
- ITU-T Recommendation X.813 (1996), *Information technology – Open Systems Interconnection –Security frameworks for open systems: Non-repudiation.*
- ITU-T Recommendation X.814 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework.*
- ITU-T Recommendation X.815 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework.*
- ITU-T Recommendation X.816 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework*.
- ISO 9735:1988, *Electronic data interchange for administration, commerce and transport (EDIFACT) – Application level syntax rules.*

- ISO 11166-1:(1994), *Banking – Key management by means of asymmetric algorithms – Part 1: Principles, procedures and formats*.
- ISO 9979:(1991), *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms*.

1.3 Abbreviations

This Recommendation uses the following abbreviations:

AI	Authentication Information
CMISE	Common Management Information Service Element
CNM	Customer Network Management
CPE	Customer Premises Equipment
DAF	Directory Access Function
DCN	Data Communication Network
DSF	Directory System Function
ICF	Information Conversion Function
LAN	Local Area Network
LLA	Logical Layered Architecture
MAF	Management Application Function
MCF	Message Communication Function
OSF	Operations System Function
OSI	Open System Interconnection
ROA	Recognized Operating Agency
SF	Security Function
SMK	Shared Management Knowledge
TMN	Telecommunications Management Network
WAN	Wide Area Network

1.4 Definitions

This Recommendation defines the following terms:

1.4.1 TMN X-interface: Physical interface applied at selected x-reference points (see Recommendation M.3010). The x-reference point is defined as being located between two Operation System Functions found on different TMNs.

1.4.2 Administration: An agency of a government designated to represent that government and its various interests in the ITU. Note, sometimes it is the PTT; sometimes the Administration is another agency. The government entity then acts to nationally administrate the ITU international designations, numbering, addressing, accounting, etc. in coordination with the ITU.

1.4.3 administration: Can be used to generally refer to entities who may own or operate TMNs either for public service or private network purposes.

1.4.4 network operator: An organization which operates a telecommunications network. A Network Operator may be a Service Provider and vice versa. A Network Operator may or may not provide particular telecommunications services.

1.4.5 TMN user: An entity who fulfils at least the role of a Manager in relation to a TMN. In TMN context, a user may interface with a Service Provider or Network Operator's TMN via the X-interface providing the user has a TMN or TMN-like management network or system (see also Recommendation M.3020).

1.4.6 service provider: A general reference to an entity who provides telecommunication services to Customers and other users either on a tariff or contract basis. A Service Provider may or may not operate a network. A Service Provider may or may not be a Customer of another Service Provider.

1.4.7 customer: The Customer is an organization which has a business relationship with a Service Provider for the provision of network services. A Customer may encompass one or more end users of telecommunications services.

1.4.8 management requirement: A specific task associated with identifiable entities. In the ITU sense, it applies to ITU members who through consensus agree to accept the principles and provisions outlined in the ITU Recommendation.

1.4.9 management service: (See Recommendation M.3020.)

1.4.10 access case: In the X-interface context, it is a set of conditions, policies and business environment factors in which the X-interface is to be applied.

2 Architecture and communication requirements

This clause provides detailed requirement specifications to complement and supplement TMN X-interface architectural and protocol profiles found in M.3000 and Q.800-Series Recommendations.

A non-TMN system may interwork with a TMN system over an X-interface if it provides TMN functionality and messages for that interface.

2.1 Organizational requirements

The different Access Cases of the TMN X-interface can be described in terms of the set of conditions, policies and business environment factors in which the X-interface is to be applied. Largely, this set of conditions or requirements can be viewed in terms of the organizations which would consider using the TMN X-interface.

The organizational requirements for managing a collection of resources across or between TMNs includes partitioning the management environment according to: jurisdictions, geographical criteria, technological criteria, policies, organizational reasons and for different functional areas. The characteristics of an X-interface are primarily defined by the TMN management services provided over it. However, the considerations discussed in this subclause may influence these management services provided over an X-interface and the means by which they are provided.

Different types of TMN ownership exist as follows:

- national Administrations;
- administrations who are International Network Operators;
- Recognized Operating Agencies of the ITU;
- Value-Added Service Providers, industrial organizations with limited access to local/national Network Operators;
- Customers and non-subscribing users.

Administratively, the X-interface may vary depending upon geographical or jurisdictional boundaries as follows:

- Intra-company;
- Inter-company;
- Intra-national;
- Inter-national.

2.2 Organizational interworking requirements

The different Access Cases where the TMN X-interface may be applied can also be described in terms of:

- the actual requirements for interworking between TMNs;
- the business or pairing relation between TMN owners;
- and the type and function of the Management Model which may be used.

The TMN X-interface requirement set must cater for TMNs interworking in support of the following various inter-administrative applications and various commercial services provided to Customers:

- public TMN to public TMN interworking in support of various inter-administrative applications;
- public TMN to private TMN interworking in support of various commercial services;
- public TMN to public/private "TMN-like" management networks.

The different uses of the TMN X-interface have been grouped into the following models. Each configuration is regarded as a unique management model.

Table 1/M.3320 – Classification of X-interface Management Models

Management Model	Pairing Relation
Cooperative Management Model	Peer-to-Peer
Joint Management Model	Manager-Agents
Customer Network Management Model	Manager-Agent, Customer-Service Provider

The differences between these concepts affect the handling of administrative, control, and security/-profiling aspects. Differences between models also provide a basis for the functional and management service requirements to vary.

2.2.1 Cooperative Management Model

When two or more Network Operators are required to share in a peer-to-peer relationship, the type of TMN interworking used over the X-interface should be referred to as the Cooperative Management Model.

Since the TMN concept is designed to support telecommunications networks, the owner or operator of the network is the principal actor for that network within a Pairing Relation. In this management model, a Network Operator requires a TMN X-interface association with another Network Operator. This will generally necessitate a bilateral agreement which allows both parties to clearly understand and limit the functions performed over the X-interface.

The cooperative management requirements on the X-interface used between peer entities are:

- Two or more Network Operators take part and one or more Network Operators may or may not perform the role of a Service Provider, too.

- A contractual agreement is required for the establishment of the X-interface and the TMN interworking functions to be performed.
- A contractual agreement is required for each telecommunication service and its respective management.
- Bilateral agreements may differ between different parties, for example every two parties in a larger group may negotiate individual contracts for management information exchange via the X-interface.
- A management view of the service is provided by the Network Operator when the service is requested from one or more Network Operators.
- Each party retains control of its resources but provides means for its usage to other parties according to bilateral agreement.
- Two or more Network Operators support reciprocal Manager and Agent roles.

Figure 1 depicts an example for the Cooperative Management Model.

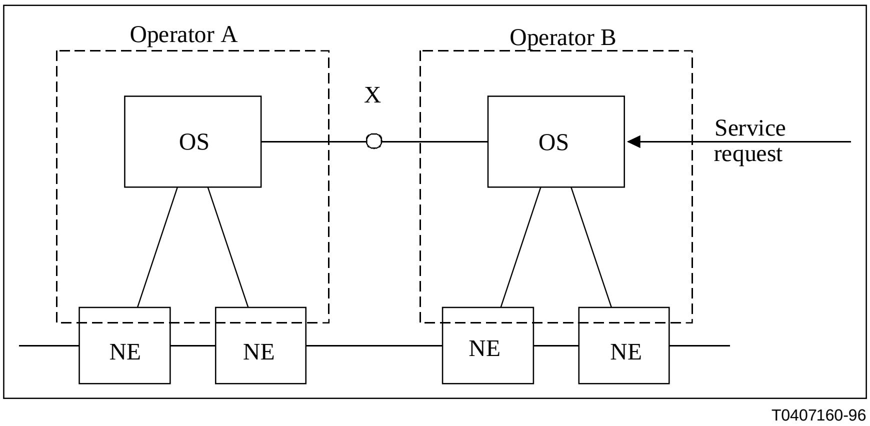


Figure 1/M.3320 – Example for cooperative management via X-interface

2.2.2 Joint Management Model

In this management model, a group of Network Operators may agree to centralize functions to a single location or a single operational entity. This functional grouping between Network Operators can be referred to as Joint Management. Other pairing relations between the operators may or may not remain in the same form as in the cooperative model depending upon the functions which have been centralized. The actual TMN interworking functions may resemble a configuration of a single manager and multiple agents.

The joint management arrangements made possible by use of the TMN X-interface may be described along the following lines:

- A cooperative venture under one jurisdiction is set up by two or more operators.
- Partners contribute and benefit with an agreed share of the resources involved.
- A service's management view is provided to a Customer by a Service Provider of some sort.
- The Service Provider handles external affairs (agreements with non-party owners) on the agreed-upon telecommunication services.
- Management matters between the central entity and the partners' contracted resources are handled via the X-interface.

Figure 2 depicts an example for the Joint Management Model.

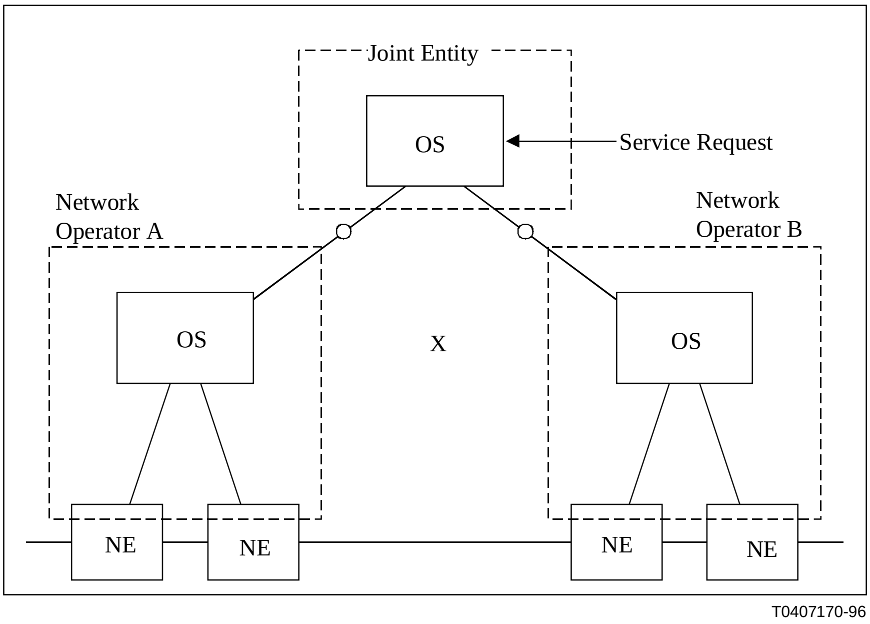


Figure 2/M.3320 – Example for joint management via X-interface

2.2.3 Customer Network Management Model

A Service Provider may provide management services to a Customer on the basis of a tariff or in conjunction with a tariff, or other commercial arrangement. The user in this case enumerates the Service Provider and thus can be referred to as a Customer. This concept, in association with the TMN X-interface, can be referred to as Customer Network Management. The pairing relation can thus be referred to as a provider to Customer association.

The Service Provider-Customer type relation realized using the TMN Customer Network Management Model can be described along the following lines:

- Service Provider and Customer involved;
- on a subscription, tariff or on a contractual basis, the Service Provider grants certain management rights (information, access, features, etc.) to a Customer;
- the amount of information provided and rights granted via the X-interface may vary for each service agreement between one Service Provider and each of its Customers;
- Customers normally communicate at least as a manager and may provide agent functionality depending on the scope of the particular service agreement with the Service Provider.

Figure 3 depicts an example of the Customer Network Management Model.

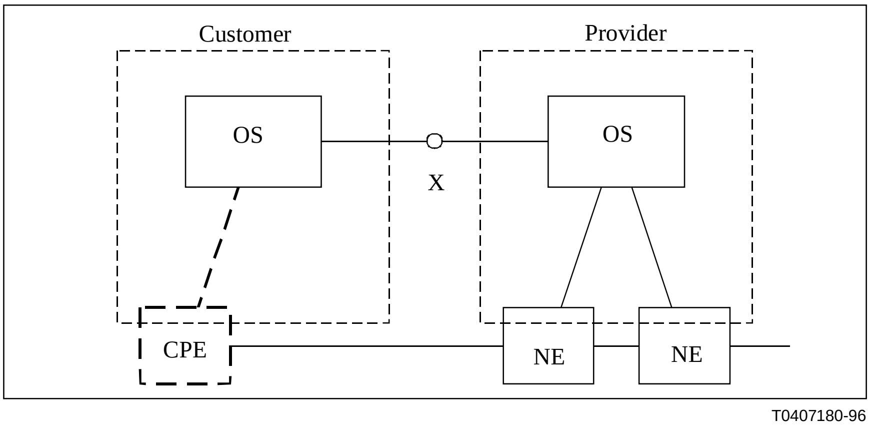


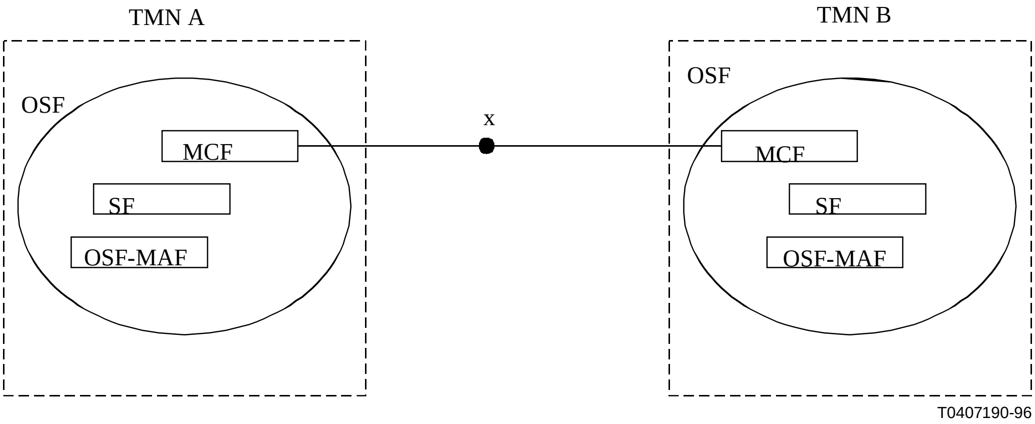
Figure 3/M.3320 – Example for Customer-Network-Management type of X-interface

Note that a Customer may operate his own equipment (CPE) in his TMN or "TMN-like" environment.

When the x-reference point is located between a TMN and a non-TMN management system, it will be invisible at the TMN side, i.e. the non-TMN system will present TMN-like functionality and support TMN protocols and messages.

2.3 Function Block Aspects

The Operations System Function Block at the TMN x-reference point will include both mandatory and optional functional components as shown in Figure 4.



OSF-MAF	Operations System Function – Management Application Function
MCF	Message Communication Function
SF	Security Function

Figure 4/M.3320 – Basic TMN function blocks at TMN x-reference points

2.4 Naming and Addressing requirements

Considering that any single TMN may interwork with several other TMNs, there is a need for identifying any single manageable entity, regardless of its location in terms of TMNs. The assignment of globally unique names to entities that are manageable in inter-TMN relationships is required.

TMN entities participating in X-interface communications are required to be able to accept globally unique names.

Network Operators and users who use Global Naming will need to ensure that their root-name is unique world-wide.

The requirements for the structure of the Global Naming format for the TMN X-interface are as follows:

– country which would receive the TMN message;

– organizational name/code which identifies the international Network Operator;

– the resource or service as identified within the organization.

To support data communications between TMNs, Network Service Access Point (NSAP) or other Network layer addresses can be used to uniquely identify the communicating end system entities (i.e. OSs and NEs). Network layer addresses are allocated on a hierarchical basis by ISO/ITU-T, and may be structured differently in the communicating TMNs.

TMN may (e.g. via directory) translate the Global Name to network layer addressing.

2.5 Communication Services

2.5.1 Interactive Service Aspects

Recommendation Q.812 defines the interactive services for the TMN X-interface as being provided by the Common Management Information Service Element (CMISE: X.710).

CMISE is organized around two types of services:

– The management notification services can be used to report any event about a managed object that the CMISE user reports.

– The management operation services define the operations to create, retrieve, modify, delete or perform other actions on a managed object.

2.5.2 File Transfer Service Aspects

Recommendation Q.812 defines the file transfer services for the TMN X-interface as being provided by Parts 1 through 4, File Transfer, Access and Management (ISO 8571).

The supported file structures involve the use of the following four document types:

– unstructured binary files;

– structured text files;

– unstructured text files;

– sequentially ordered files (these files are made of a sequence of records without any possibility of having direct access to a given record, each record is made of fields of different type).

2.5.3 Directory Service Aspects

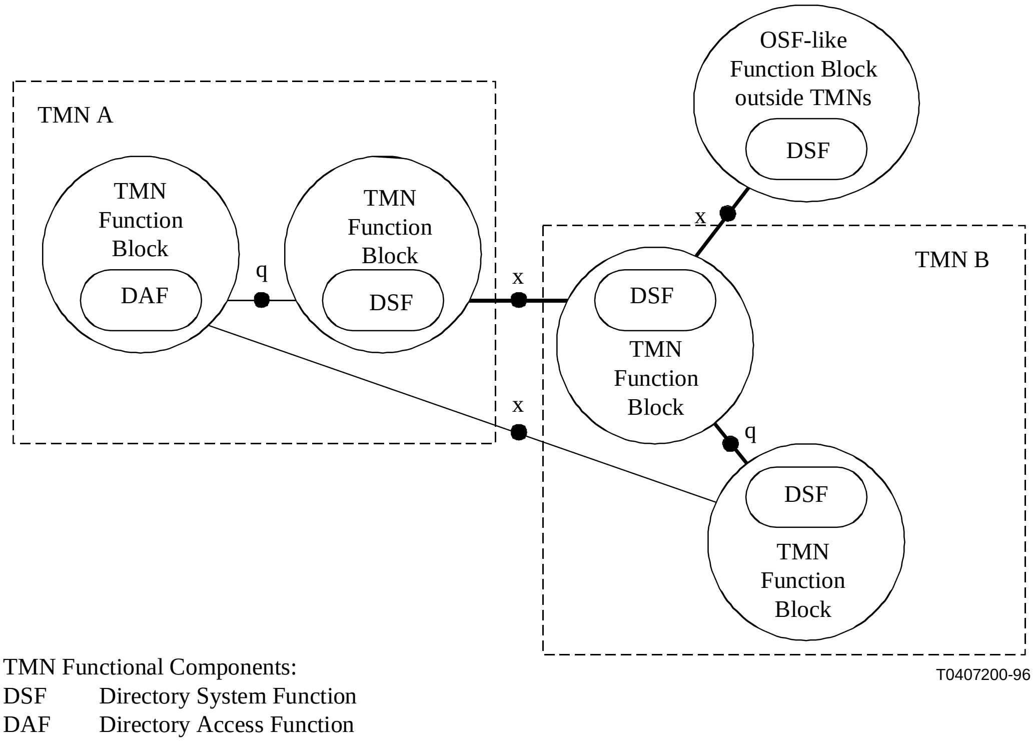
Recommendation Q.812 defines the Directory Services for the TMN X-interface as being provided by the X.500 series of Recommendations. Directory systems can define an architecture that allows the distribution of the Directory’s database over a potentially unlimited number of OSI end systems. Despite its physical distribution, the end user or application invoking the directory service should perceive the Directory as a single logical unit.

Directory Services may be applied via the x-reference point. Recommendation M.3010 describes the general relationship of Directory Functional Components within the TMN framework. Directory

Services stretching beyond the boundaries of a TMN will use the x-reference point. These services can be employed whenever the global availability of information may be essential for a system or service to operate or beneficial for system or service performance.

TMN function blocks may optionally use Directory Functional Components to implement the required Directory function. This is modelled in the TMN functional architecture as TMN functional components which may be contained in specific TMN function blocks requiring Directory functionality. Figure 5 depicts the Integration of Directory and TMN.

Depending on the chosen architecture, DSF-DSF or DAF-DSF (DSF: Directory System Function, DAF: Directory Access Function) associations may be set up via the x-reference point. The association may either be set up between DSF/DAF of TMN function blocks of different TMNs or between DSF/DAF of a TMN function block and a TMN-like function block outside one specific TMN.



TMN Functional Components:
DSF Directory System Function
DAF Directory Access Function

Figure 5/M.3320 – Architecture of Directory application at TMN X-interface

2.5.4 Store/Forward Service Aspects

For further study.

2.6 Data Communication Network Aspects

The different DCNs currently recognized for supporting TMN X-interfaces are defined in Recommendation Q.811, Lower Layer TMN Protocols for Q3 and X-interfaces. DCN type and the network topology will be decided upon agreement of TMN owners on a bilateral or multilateral basis, taking into account the security, network redundancy and other conditions. However, TMN designers may benefit by following the guidelines outlined in this subclause.

TMN X-interface applications may use one or more TMN Lower-Layer protocol stacks/profiles based on selection criteria such as performance and security.

The following DCN Requirements have been identified for the TMN X-interface:

a) TMNs may interwork via a variety of networking technologies including WAN and LAN.

b) The Q.811 lower layer profiles may be used at the X-interfaces.

c) Point-to-Point communication should be supported for interactive and bulk file transfer.

d) Point-to-Multipoint communication may be needed to satisfy certain requirements associated with Management Services for some Managed Areas.

e) Local, national and international communications should be supported.

f) Inter-networking allows DCNs using different lower layer protocols to communicate. The DCN inter-networking methods defined in Recommendation Q.811 are applicable to the X-interface.

3 Management Service Requirements

This clause presents the management requirements for using the TMN X-interface. Management Requirements will need to be properly organized to ensure that the needs of the TMN users are properly interpreted. The following subclauses are organized to serve the TMN Users. International and User Aspects are provided to further qualify the various needs specific to various relationships.

3.1 Telecommunications Managed Areas

The X-interface may support the exchange of management information for the Telecommunications Managed Areas (as defined in Recommendation M.3200).

3.2 Relationship to TMN Methodology

This subclause should be loosely regarded as the framework for the TMN X-interface activities outlined under M.3020 TMN Methodology Tasks 0, 1 and 2. General requirements for the TMN X-interface will be outlined in this subclause. Specific requirements for management services are included in the Guidelines for the Definition of Management Services (GDMS) template format in the M.3200 series of Recommendations. Annexes to this Recommendation that may address considerations specific to the reference point are for further study. These requirements are merged with others into TMN Management Service descriptions which then are used to drive the TIB-X planning steps.

3.3 Management Requirement Categories

This Recommendation recognizes Service Providers who may offer end-user services as defined in ITU-T Recommendations. This Recommendation recognizes Network Operators who may operate networks as defined in ITU-Recommendations. Service Providers provide services to Customers and interact with Network Operators to support their services. (NOTE – The same organization may function as both a Network Operator and a Service Provider.)

Management supported by the X-interface can be grouped into those applicable between and within the roles. That is, a set of management services may be defined as applicable between Network Operator, between Service Providers, between Service Providers and Customers, and between Network Operators and the Vendors of their equipment.

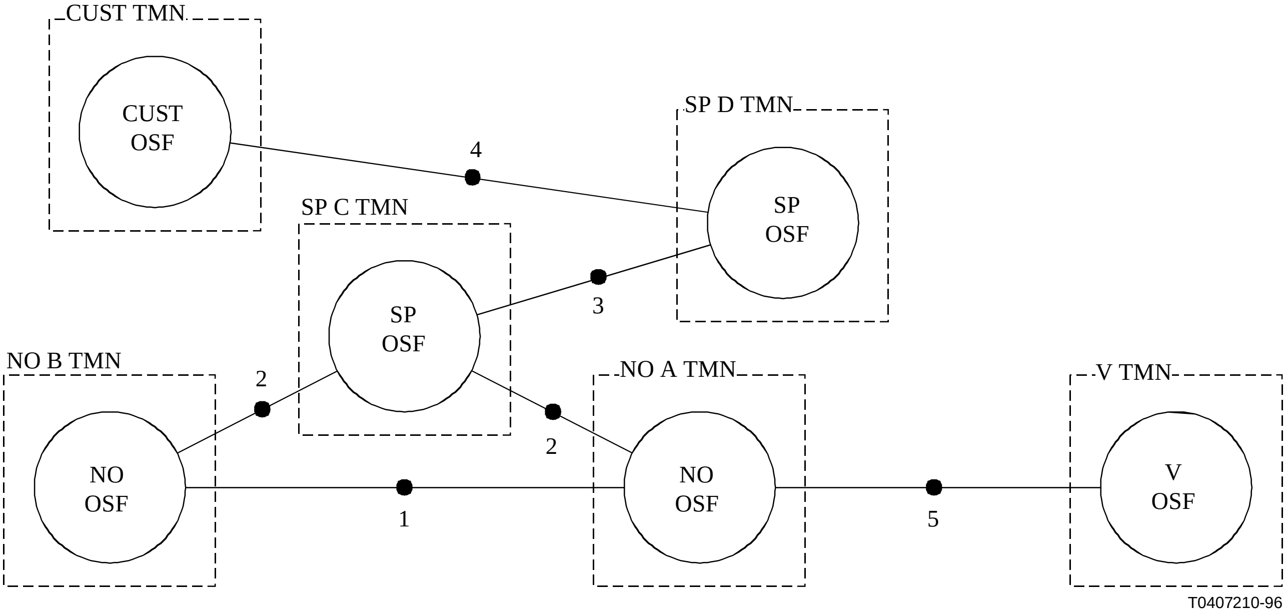
The interaction between the participants in these management services are characterized by the different management models defined in clause 2 and shown in Table 2 with examples in Figure 6.

A given organization (TMN owner) may act in more than one of the categories, i.e. a Network Operator may also act as a Service Provider. Management requirements can also be specified in terms of specific categories. The reason for introducing the management requirement categories: Information exchange via the X-interface can be best thought of in terms of these categories.

Note that for a given Management Requirement Category, more than one Management Model may be applicable. The assignment as primary or secondary assumptions are assumed and not binding.

Table 2/M.3320 – Examples of Relationship Pairings

	Management Requirement	**Management Models**		
No.	**Category**	**cooperative**	**joint**	**CNM**
1	Network Operator – Network Operator	P	S	S
2	Network Operator – Service Provider	S	S	P
3	Service Provider – Service Provider	S	S	P
4	Service Provider – Customer	S	S	P
5	Network Operator – Equipment Vendor	S	S	P*
P Primary option P* Primary option but reverse direction S Secondary option				



NO	Network Operator
SP	Service Provider
CUST	Customer
V	Vendor (to Network Operator)
OSF	Operations System Function

Figure 6/M.3320 – Relationship Pairing Examples of Management Requirements Categories

3.3.1 Network Operator-to-Network Operator Management Requirement Category

The following non-exhaustive list contains services related to information that Network Operators may want to exchange via an X-interface in order to accommodate existing inter-Network Operator procedures by means of an automated TMN X-interface.

FM: Alarm Management;
Trouble Ticketing;
Traffic Management (FM part);
Escalation procedure;
Testing.

CM: Traffic Management (CM part);
Single point of contact;
Customer Administration;
Circuit/system set-up/bringing-into-service/network provisioning;
Restoration.

AM: Accounting;
Billing exchange.

PM: Network performance;
Traffic management (PM part);
Quality of Service Management.

SM: Authorized users.

Priorities have been given to identify the most urgent need for inter-Network Operator information exchange support via an X-interface. Highest priority is given to X-interface specification for inter-Network Operator use; second priority will be given to the needs of a Customer-Network Operator version of the X-interface.

a) fault management for switch and transmission;

b) maintenance, FM, PM for leased lines (international private lines);

c) single point of contact;

d) bringing-into-service;

e) electronic billing.

Currently, for a pre-TMN environment, other ITU-T Recommendations identify information exchanged between Network Operators. Among them, Recommendation M.1520 summarizes relevant M- and E-Series Recommendations requiring information exchange between Network Operators. The TMN X-interface should satisfy these potential requirements of information exchange that are currently defined, and it may support future additional requirements with management requirements categories being expanded.

3.3.2 Network Operator-Service Provider Management Requirement Category

Network Operators may provide an interface to Service Providers to:

- allow Service Providers access to information on network resources in the areas of Fault and Performance Management;
- allow Service Providers to request the Network Operator to support a service with network resources in the area of Configuration Management and to provide information on such configurations;
- support Accounting Management functions;
- support Security Management functions.

3.3.3 Service Provider-Service Provider Management Requirement Category

The Service Provider-to-Service Provider management requirement category is required to provide for service management information exchange among Service Providers to support a given business environment.

3.3.4 Customer-to-Service Provider Management Requirement Category

Customers desire to utilize the management capability in a common manner under the multicarriers and multiservices environment for extracting management information and achieving management operations. An example of this is the exchange of Customer-related data including service and management information.

3.3.5 Network Operator-Vendor Management Requirement Category

Sometimes, the Network Operator is capable of providing Management Services as an Operator to other entities who do not own or operate a telecom network. These entities can be referred to as Users and may be Vendor Maintenance personnel, contracted entities, etc. Often, a Service Contract between the Vendor and the Operator will govern the rights and privileges which the Vendor's personnel may have with the property of the Network Operator. In this case, the Network Operator would be expected to perform the Agent or serving Role and the User would function in the Manager or requesting Role. It should be noted that this Model may apply more to Network Maintenance as opposed to End-User Service Provisioning.

3.4 Shared Management Knowledge (SMK) for the X-interface

Each TMN interface can be classified depending on the information model upon which the manager/agent relationship is based (in particular, see shared Management Knowledge 3.3, Recommendation M.3010). Many different information models will be specified in case of the X-interface, corresponding to different functional requirements.

The availability of such an SMK is a pre-requisite to the functioning of the X-interface, and thus TMN must provide or identify the means for establishing it.

4 Security considerations

This clause identifies the Security requirements for the exchange of management information as well as the management of the Security mechanisms which will support the exchange of management information. This clause:

- describes the conditions which will strongly influence to what degree security should or can be applied in a given instance of using the TMN X-interface;
- identifies Security Threats and related risks to information exchanged at the TMN X-interface as well as risks against the TMN itself;
- identifies the functional requirements and optional security capabilities specific to the TMN X-interface;
- explains the security services that will be used on the TMN X-interface to address those threats, risks and requirements identified;
- identifies the additional requirements, features and functions for managing the security services supporting the TMN X-interface;
- focuses on using the TMN X-interface for exchanging keying material without compromising the integrity of the TMN X-interface itself;
- documents the procedures for using the ISO Registry of Cryptographic Algorithms.

4.1 Security Scope and Objectives

This subclause deals solely with those security aspects specific to the use, maintenance and support of the TMN X-interface. This Recommendation does not define security requirements for either OS-OS or OS-NE Q3-interface or for F-interface applications or configurations.

These security aspects relate to the specification of the TMN Functional Component called Security Function that is included within the supporting OSF function block as described in Recommendation M.3010.

These security aspects also relate to those TMN Management Services that involve exchanging information between TMNs. These aspects also should form the basis for the Security Functions outlined in Recommendation M.3400, TMN Management Functions. These security aspects should also be considered a requirement for the TMN Management Service, "Management of TMN Security".

This subclause further outlines requirements applicable to the TMN Protocol set for the X-interface as found in both Recommendations Q.811 and Q.812. The generic security objectives considered for the TMN X-interface include Authentication, Access Control, Confidentiality, Integrity, Non-repudiation, and Security audits.

4.1.1 Application considerations

Each application of the X-interface should be studied in detail as part of the TMN Interface Methodology to best determine how the Security Threats, Risks and Security Requirements can best be resolved.

Not all security mechanisms are required for every application. An application may use a particular TMN X-interface Management Model. The application may include one or more TMN Management Services, Management Function Sets, and TMN Management Functions. Communications services and environmental conditions need to be factored into the decisions for using security for the X-interface. Each Management Services provided by an application of the TMN X-interface should be broken down to the functional level before deciding on Security requirements.

4.1.2 Implementation considerations

Security Policies may differ between Administrations in different countries. Moreover, one Administration may not have the same security practices as other Administrations. Therefore, it should not be assumed that security requirements can be mandated across different countries that will seek to use the TMN X-interface.

Security Policies that may differ from country to country could include permissible authentication mechanisms, type or strength of encryption or cryptographic techniques used, length of encryption keys, etc.

Additional interworking procedures may be needed to overcome practical and other limitations which may result from differences in Security Policies, Security System technologies and Data Communication Networks. Additional security requirements may be needed in a particular implementation.

Implementation security considerations which should be factored into the security solution for a particular implementation of the X-interface include:

- national security policies;
- security technology available to different countries;
- DCN configuration; Dedicated versus Switched Network;
- public switched data network versus privately switched networks;

- number of intermediate networks or nodes used in DCN configuration;
- type and configuration of DCN such as SS7, OSI/X.25, TCP/IP, LAN/WAN, ISDN, etc.

4.2 Security threats

A careful analysis of all threats that can be identified should be performed.

Security threats identified in this Recommendation are based on the concepts defined in ISO 7498-2 and ISO/IEC 10181. Threats which may impose security risks include the following.

4.2.1 Disclosure of information

Threats to confidentiality of information are the observation of information by an unauthorized entity. Information could be acquired by an unauthorized entity in an illegitimate manner such as capturing messages in transit and unauthorized access to information in systems. For example:

- the disclosure of CMIP or other protocol data units either without proper authorization or to unauthorized parties.

4.2.2 Unauthorized access

This threat includes unauthorized access to systems and resources within systems such as data and software. Once unauthorized access is gained through the X-interface, damage could be done to disrupt a system's normal operation. Sensitive and valuable information could be lost, modified, or disclosed that may ultimately jeopardize business operations.

4.2.3 Masquerade

This threat is the pretence by an entity to be a different entity in order to gain access to information or to acquire additional privileges.

4.2.4 Threats to integrity of information

Threats to the integrity of information include the unauthorized fabrication or modification of information residing in systems as well as information in transit. For example, the replay, reflection, reordering, insertion, deletion, fabrication, modification of data either prior to or during transmission.

4.2.5 Denial of service

This occurs when an entity fails to perform its function or prevents other entities from performing their functions. This may include denial of access to TMN denial of communication by flooding the TMN. In a shared network, this threat can be recognized as a fabrication of extra traffic that floods the network, preventing others from using the network or delaying the traffic.

4.2.6 Repudiation

Denial by one of the entities involved in a communication of having participated in all or part of the communication.

4.2.7 Fraud

An unauthorized party using or misdirecting a resource or service causing a loss of one or more TMN users is called fraud. In the case of Customer Management, this is especially critical as it complicates the accuracy of billing and delivery of service.

4.3 Security requirements

Security Risks exist when one or both TMNs or the DCN providing the X-interface are exposed to one or more security threats. The first step to counter security threats is to perform a security risk assessment. Appendix I illustrates a method for performing security assessment.

4.3.1 Identification requirements

TMNs should provide adequate capabilities for the identification of users in the TMN environment. These capabilities may be required to support auditability of all user actions and activities in the network, and to provide input into authentication and access control.

The baseline security requirements for identification could include:

– Network users shall have globally unambiguous names (or user-IDs) for identification purposes to support individual accountability and auditability.

– A TMN shall forward (pass along) the user name in communications across domains or jurisdictional boundaries as well as a TMN identifier.

4.3.2 Privacy requirements

Privacy requirements should be supported to ensure that confidential information is not compromised. The baseline privacy requirements could include:

– a TMN capability to encrypt sensitive information communicated within or across TMNs, as well as sensitive information stored internally to a TMN;

– a TMN capable of providing end-to-end confidentiality of data communicated within or across TMNs;

– a TMN to encrypt sensitive information, when broadcast technology is used;

– a TMN capability for secure distribution and management of keying material.

4.3.3 Authentication requirements

TMNs should provide adequate capabilities to allow the corroboration of users. Some of these capabilities are generic in nature and are independent of the type of authentication mechanism in use while others are not.

Authentication is a mandatory requirement when switch network arrangements are used in whole or in part to realize a TMN X-interface. For dedicated end-to-end network arrangements where the identities of both TMN parties is certain, authentication may be considered optional.

The requirements for authentication may include:

– A TMN shall have the capability to authenticate users.

– A TMN shall not support ways to bypass the authentication mechanism.

– The confidentiality of all secret authentication information (AI) shall be preserved by a TMN. When internally-stored by a TMN, this AI shall be protected from unauthorized access. Certain AI (e.g. encrypted password) should not be available in clear text even to highly privileged users.

– Each user of the TMN should have a unique AI.

– This authentication information shall not be sent in clear text form within or across TMNs, except when dictated by the particular authentication-mechanism in use; e.g. one-time passwords and some challenge-response mechanisms.

– The integrity of all internally-stored authentication information shall be preserved by a TMN.

- A TMN shall have the capability to provide strong authentication of users wishing to perform "critical" administrative and other OAM&P functions.
- A TMN shall be able to incorporate and support authentication schemes including those based on simple bilateral agreements, trusted-third party servers and those that are based on simple passwords.

It should be noted that Trust Systems and configurations are considered an implementation issue and subject to bilateral negotiation. Some Management Models may require use of Trusted Third Parties. In contrast, the Cooperative Management Model could depend upon agreement of only two parties.

4.3.4 Access Control requirements

TMNs should include capabilities for controlling (grant or deny) access to various telecommunications resources based on properly authenticated user identities. Requirements for using Access Control procedures depend upon the actual Management Service offered. Guidelines for using access control on the TMN X-interface may include:

- A TMN shall not allow users access to any system or network resource unless properly identified and authenticated.
- A TMN shall provide the capability to control access to the TMN resources at all levels of granularity.
- A TMN shall be able to incorporate and support the provision of access control to various classes of users including but not limited to: Individual users, Groups, Roles and Proxies.
- A TMN shall have the capability to screen access to resources based on any combination of originating entity/address of requester, requested operation, destination entity/address as well as authorization profile.
- A TMN shall be able to incorporate and support mechanisms to grant or deny accesses to any user based on contextual information (e.g. time).
- A TMN shall be able to control access to applications that effect routing, configuration and flow control.

4.3.5 Integrity requirements

The baseline requirements for network, data and system integrity may include:

- A TMN shall be able to reliably associate any network resource (data, processes) with its original creator/owner. Specific provisions should be made to support user anonymity.
- A TMN shall reliably associate communicated data with its origin.
- A TMN shall be capable of providing end-to-end integrity of data communicated within or across TMNs.
- A TMN shall provide mechanisms to protect against replay attacks.
- A TMN shall preserve the integrity of TMN data.

4.3.6 Security audit requirements

The baseline requirements for security audit may include:

- A TMN shall provide the means to validate the correct operation of the security mechanisms (e.g. activation of security log).
- The security log, audit control as well as other security functions provided within the TMN shall survive restarts.

4.4 Security services

The security approach for a particular TMN X-interface application should include a Security Profile. The Profile encompasses the set of requirements which have been deemed relevant and necessary to counter threats and to minimize risks. Security services will be determined from the application requirements as follows:

Table 3/M.3320 – Requirements and security services

Requirement	Security service
Identification and authentication	User authentication Peer entity authentication Data origin authentication
Access control and authentication	Access control Data origin authentication
Access control and authentication	Access control
Integrity – Stored data	Access control Detection of denial of service
Integrity – Transferred data	Integrity Detection of denial of service
Confidentiality – Stored data	Access control Object reuse[a)]
Confidentiality – Transferred data	Confidentiality Object reuse
Non-repudiation	Non-repudiation
(All)	Security Alarm, Audit Trail, Recovery

[a)] The term "Object reuse" refers to a security service that ensures that storage media (memory, disk, tape, etc.) retain no residual information after completion of their use.

4.4.1 Authentication services

Authentication usually refers to Peer-Entity Authentication at the association establishment time but also can refer to either User and/or Data-Origin Authentication. User Authentication delivers only corroboration of the identity of the user who is most likely the association initiator.

Peer Entity authentication during association establishment can be one-way or two-way. One-way authentication indicates only the identity of the association initiator, while two-way authentication authenticates the identities of both the association initiator and the association receiver.

Data Origin Authentication service provides the corroboration of the source of a data unit. Service does not provide protection against duplication or modification of the data units.

4.4.2 Access Control services

This service provides protection against unauthorized access, use, reading, writing and deletion of information and authorized execution of a processing resource or to all accesses to a resource.

Use will depend upon specifics identified in TMN Management Services since both information and resources will vary by functions performed. Access Control mechanisms which may be used include:

– access Control Lists stating the access rights of peer entities;

- exchanging information which identifies what information and resources can be authorized;
- exchanging Authentication Information such as passwords;
- security labels indicating sensitivity levels of data items may be used to grant or deny access (it is often necessary to convey the security label with data in transit);
- logging of time of access, route of attempted access, duration of access and tracking of use of resources.

4.4.3 Confidentiality services

Of the existing forms of confidentiality services, two can be used to ensure the privacy of the X-interface transactions:

- Connection Confidentiality will provide total encipherment of the data stream.
- Message Data Confidentiality, including Selective Field Confidentiality, can be used to protect the confidentiality of data involved in X-interface transactions.

Use of Confidentiality should be considered optional and subject to bilateral agreement and adherence to Security Policies.

4.4.4 Data Integrity

Data Integrity counters active threats by providing for integrity of all selected data fields and detects any modification, insertion, deletion, or replay of any data within the entire sequence.

Data Integrity services include:

- *Selective Field Integrity*: This service can be used in the application layer or in the application process itself, since it is only the application process itself which can discriminate between fields.
- *Connection Integrity*: Can be provided at the transport layer, at the application layer or in the application process.
- *Connection integrity without recovery*: Can be provided at the network layer, the transport layer, the application layer or in the application process.

4.4.5 Non-repudiation

Provides receiver of data with proof of data-origin and the sender with proof of data delivery.

4.5 Management of security

4.5.1 Audit requirement

TMNs need to provide adequate capabilities to allow the investigation, audit and real-time detection and analysis activities so that proper remedial actions can be taken.

4.5.2 Audit Trail

The security audit trail enables the logging of security-related events that are of potential use in a security audit. The security audit trail should be realized using Security Logs as follows:

- Security logs shall be generated and maintained (e.g. safeguarded after system failure) within the TMN.
- Security logs shall be protected from unauthorized access and no modification should be allowed.
- Security logs shall record at least the following events: invalid user authentication attempts, unauthorized attempts to access TMN resources of any type, changes to a user's access

rights, shutdown restart, log deletions, changes to the security attributes associated with a TMN resource.

- For each recorded event, the security log shall include at least the following parameters: date and time of event using Universal Time Coordinated (UTC), user-ID including network address (if applicable), type of event, names of TMN resources accessed, success or failure of the event.
- Logging of apparent violations of security and logging of "normal" events, such as a log-on. Further information can be found in Recommendations X.816, X.735, X.736, X.740.

Recommendation X.740 defines a model for generating security audit trail reports. The requirements as listed above are consistent with Recommendation X.740.

4.5.3 Alarm reporting

Security alarms are a particular type of event report which should always be logged. Security alarm reporting is used to notify an entity of a violation or suspected violation of security. The following Recommendations apply:

- CCITT Recommendation X.734 (1992), *Information technology – Open Systems Interconnection – Systems Management: Event report management function.*
- CCITT Recommendation X.736 (1992), *Information technology – Open Systems Interconnection – Systems Management: Security alarm reporting function.*

A TMN shall provide a mechanism to notify (e.g. alarm, on-line report) the administrator, in real time if possible, if the security log fails to record the events that are required to be recorded.

A TMN shall provide the capability for off loading audit information onto storage media for longer retention: writeover should be prevented.

4.5.4 Administrative requirements

There are a number of administrative functions that the TMN should support separate from other user functions.

Since many security incidents could involve several interconnected TMNs, it may be desirable for TMN to exchange pertinent information concerning these events. Otherwise, requirements stated below can simply apply to the TMN itself as opposed to being limited to the TMN X-interface only:

a) A TMN shall provide a mechanism for a security administrator to display at any time all currently active users.

b) A TMN shall provide a mechanism for the security administrator to be able to independently and selectively review the actions of any user, including privileged users, based on individual user identity.

c) A TMN shall provide a mechanism for the security administrator to block a specific communication path by controlling ports at a gateway and at intermediate relay systems.

d) A TMN should provide both automatic and manual congestion controls to counter denial of service attacks; e.g. intentional flooding attacks that may affect the TMN from timely actions and responses.

e) A TMN shall in the event of a security failure provide the capability to maintain and or restore the OAM&P functionality network services on a timely basis; e.g. by providing the capability to recover and reinitialize the system.

f) A TMN shall provide the capability for the security administrator to disable user-IDs, that have not been used for a specifiable period or other specific administrative purpose.

g) A TMN shall provide a mechanism for the security administrator to reset authentication information for users or delete user accounts.

h) A TMN shall provide the capability to generate alarms for specifiable security events including integrity violations (e.g. replays), and physical violations (e.g. cable tampering and intrusion elements).

i) A TMN shall provide the security administrator with post-collection audit analysis tools that can produce exception reports, summary reports, and detailed reports on specific network data items and users.

j) A TMN shall also protect operational tools from unauthorized access.

4.5.5 Key Management

Security begins with the availability and use of data encryption keying material. Key Management refers to the generation, storage, distribution, deletion, archiving and application of keying material in accordance with a security policy. Security policy can be defined by the set of criteria for the provision of security services. Thus Key Management represents a critical first step in providing and ensuring reliable Security Services.

Recommendation Q.812, TMN Upper-Layer Protocol, identifies the specific Security Protocol Mechanisms to be applied on the TMN X-interface. In contrast, this Recommendation specifies only management requirements for handling of keying material for the TMN X-interface. In addition, this Recommendation specifies the requirements for using the TMN X-interface itself, on an optional basis, for distributing or exchanging encryption keying material.

4.5.6 Requirements

The two TMN X-interface parties shall be capable of supporting Key Management because Encryption Keys will be needed to perform the various Security Services previously outlined.
The minimum requirements for managing keying material are:

– control of the keying material during its lifetime to prevent an unauthorized disclosure, modification or substitution;

– distribution of the keying material in order to permit the interoperability between cryptographic equipment or facilities;

– ensuring the integrity of keying material during all phases of its life, including its generation, distribution, storage, entry, use and destruction; and

– recovery in the event of a failure of the key management processes when the integrity of the keying material is questioned.

Key Management can be performed either manually or automatically. Manual Key Management generally refers to distributing the keying material to the locations where it is needed by using some manual procedures (Registered Mail, Bonded Courier, MagTape, etc.). In contrast, automated Key Management enables the keying material to be electronically transmitted over some secure communications channel to the appropriate locations. However, note that even when automated key management is agreed upon, there is still need to support manual procedures for the "bootstrap" effort to establish the first and most important secure connection.

Key management also varies by the type of encryption system being used in a particular TMN X-interface application. There are two types of encryption systems: Private-Key and Public-Key as described below.

4.5.7 Private-Key Management

The first type of Key Management is to support Private-Key Cryptographic systems which use a secret transformation (key) to encrypt data that is sent over a communications channel. At the receiving TMN, the same key is used to convert the enciphered data back into the original form. The transformation key is sent to the authorized receiver over a secure channel and is therefore unavailable to other parties.

Private-Key systems depend upon distribution of the private-keying material over a secure channel which may be manual or automated. The channel may or may not be a TMN X-interface. The Private-Key system approach enables the security to be limited to only the two TMNs engaged in exchanging information independently from information exchanged with other TMNs. This bilateral nature of Private-key systems is attractive for applications involving the Cooperative Management Model.

See Appendix II for further information.

4.5.8 Public-Key Management

The second type of encryption involves the use of Public-Key Crypto-systems which use separate keys at the transmitting and receiving stations. One of the keys is made public and the other is kept private. The private key can not be obtained from the public key. Each TMN in a pairing relation or group will need to keep its private key secret while publishing the other. These keys can then be used in various security transforms.

4.5.9 Trust Systems

The X-interface shall be capable of supporting interactions with trusted third parties for the authentication, certification and distribution of keys.

4.6 Data Cryptography

Participants in X-interface interactions must be able to use a cryptographic registry such as ISO 9979. An example of a cryptographic registry is discussed in Appendix III.

APPENDIX I

Additional information on Security Risk Assessment

To counter security threats, the participants in an X-interface services may perform a security risk analysis with the purpose of:

- providing evaluation of different threats;
- identifying potential risks according to relevant security threats;
- prioritizing which risks need to be addressed and how often;
- and concluding a Risk Assessment Report.

The Risk Assessment Report becomes the basis for subsequent Security Risk Analysis where each Risk is studied further for determining:

- the probability that a weakness will be detected;
- the cost and effort involved in exploiting the weakness;
- the potential benefit gained by the intruder in exploiting the weakness;
- the potential damage for the operating company business or for the company's subscribers.

The output of the Risk Analysis should provide enough information so that TMN X-interface Planners will be able to develop a Security Approach to counter the threats and minimize the risks. The Security Approach should include a Security Profile for that particular application of the TMN X-interface taking into account both the Application and Implementation Considerations outlined earlier.

APPENDIX II

Additional information on Private Key Management

This appendix provides an illustrative example of a possible set of minimum requirements for providing a private-key management system which uses the TMN X-interface as the secure channel:

– Manually, a Master Key is shared between both TMN Administrators and represents the first step of a three-step process. The Master Key is also referred to as Key Encrypting Key or KEK.

– This Master Key is used to encrypt a second level of keying material known as Session Keys or Data Encrypting Keys (DEKs).

– Session Keys are disseminated electronically over the secure communication channel, such as the TMN X-interface. The Keys may be disseminated using one the TMN X-interface Communication Services. However, in most cases, the exchange will simply be File Transfer.

– The DEKs are used by both TMNs to encrypt either the selective fields or data messages according to the Security Services required on that particular TMN X-interface application.

– In some installations, there may be additional need to encrypt files containing Session Keys using a third set of keys known as Facility Keys. However, if no apparent risk exist when DEKs are stored on computers at each TMN, then there is no requirement to use Facility Keys to encrypt the DEKs.

The use of a two-tier hierarchy of Encryption Keys is called "Key Hierarchy" Concept. Additionally, the "Key Separation Concept" needs to also be supported in Private-Key Management Systems as well. The Key Separation dictates that keying material used for Authentication should not be used for Access Control, Data Confidentiality, etc. Therefore, Keys for each OSI Security Service that is required for a particular TMN X-interface application should have separate procedures for creation, storage, distribution, use and deletion. Following this concept rigorously allows the TMN party to be able to recover from a security break and minimize the total impact on the various communications supporting across the TMN X-interface.

For transmitting large volumes of keying material over the TMN X-interface, the keys themselves should be organized into Security Key Files. This will permit use of the File Transfer service and the Security protocol mechanisms outlined in Recommendation Q.812. Both TMN parties should regularly provide an encrypted text file containing a list of 1000 keys. This may provide a supply for up to a year. From that set, the TMN Administrator will indicate which member is the valid key used for the next session on the TMN X-interface. The actual key will be randomly selected at random intervals by one or both TMN parties. The initiation of a new key will need to commence at an agreed upon time by both parties.

Backup Security Files should contain indices that are multiples of 10 000 for reserve purposes. The naming convention for backup security key files is: keys.networkid.bk, where networkid is the network identification name for the Administration/ROA and bk is the sequential number of the file, beginning with 10 000. Backup files are used when:

1) current file has been compromised;

2) current file has used up all keys; or

3) current file has been corrupted.

Once a backup file has been used, the Agent should provide a new backup file with a new set of backup keys and indices. The new indices will begin at the next sequential multiple of 10 000.

APPENDIX III

Additional information on Data Cryptography

The ISO Registry for Cryptographic Techniques will provide much of the basis for using security for the international applications. The choice or selection of a particular Cryptographic Algorithm is well beyond the scope of this and other ITU TMN Recommendations; however, two TMN parties may reference the ISO Register for Cryptographic Algorithms and agree on which, if any, may be suitable to meet their mutual needs.

ISO 9979 defines the procedures for registering the information associated with Cryptographic Algorithms as follows:

a) a formal ISO-entry name for the algorithm;

b) the proprietary name (or names) given to the algorithm by its originator or owner;

c) intended range of applications for the algorithms;

d) cryptographic interface requirements;

e) a set of test words to check basic functionality;

f) the identity of the organization that requested registration of the algorithm;

g) the dates of registration and modifications;

h) whether it is the subject of a national standard;

i) patent license restriction information.

On an optional basis, the ISO Register for Cryptographic Algorithms may also contain:

j) a list of references to any associated algorithms;

k) description of the algorithm;

l) modes of operation;

m) other information.

For further details, please reference ISO 9979.

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
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	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	**TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits**
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 and open system communication
Series Z	Programming languages