International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3016.0

(05/2005)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Telecommunications management network

Security for the management plane: Overview

ITU-T Recommendation M.3016.0

International Telecommunication Union

ITU-T M-SERIES RECOMMENDATIONS

TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

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

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

ITU-T Recommendation M.3016.0

Security for the management plane: Overview

Summary

This Recommendation provides an overview and framework that identifies security threats to a TMN and outlines how available security services can be applied within the context of the TMN functional architecture.

Source

ITU-T Recommendation M.3016.0 was approved on 22 May 2005 by ITU-T Study Group 4 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

CONTENTS

Page

ITU-T Recommendation M.3016.0

Security for the management plane: Overview

1 Scope

This Recommendation provides an overview and framework that identifies security threats to a TMN and outlines how available security services can be applied within the context of the TMN functional architecture, as described in ITU-T Rec. M.3010.

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

This Recommendation does not seek to define new security services but uses existing security services defined in other ITU-T Recommendations and ISO Standards.

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 Recs M.3016.1, M.3016.2 and M.3016.3 specify a set of requirements, services and mechanisms for the appropriate security of the management functions necessary to support the telecommunications infrastructure. Because different administrations and organizations require varying levels of security support, ITU-T Recs M.3016.1, M.3016.2 and M.3016.3 do not specify whether a requirement/service/mechanism is mandatory or optional.

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

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 M.3010 (2000), *Principles for a telecommunications management network*.
- ITU-T Recommendation M.3400 (2000), *TMN management functions*.
- ITU-T Recommendation X.509 (2000), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

- ITU-T Recommendation X.741 (1995), *Information technology – Open Systems Interconnection – Systems management: Objects and attributes for access control.*
- ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*
- 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 framework.*
- 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/IEC 9979:1999, *Information technology – Security techniques – Procedures for the registration of cryptographic algorithms.*

3 Definitions

This Recommendation does not define any new terms.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

CCITT	International Telegraph and Telephone Consultative Committee
DCN	Data Communication Network
FC	Functional classes
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LLA	Logical Layered Architecture
MF	Mediation Function
NEF	Network Element Function
OSF	Operation System Function
OSI	Open System Interconnection
PIN	Personal Identification Number
TF	Transformation Function

TMN	Telecommunications Management Network
TTP	Trusted Third Party
WSF	WorkStation Function

5 Rationale

The requirement for security in TMN has originated from different sources:

– **Customers/subscribers** need confidence in the network and the services offered, including correct billing.

– **The Public Community/Authorities** demand security by Directives and Legislation, in order to ensure availability of services and privacy protection.

– **Network Operators/Service Providers** themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the public.

A TMN is intended to manage the underlying telecommunications network; therefore, the security of the TMN is essential to the proper functioning of the telecommunications network. Furthermore, the telecommunications network may incorporate security features that need to be managed by the TMN. ITU-T Rec. M.3400 enumerates those security management functions.

TMN Security Standards should preferably be based upon internationally agreed security standards as it is beneficial to reuse rather than create new ones. The provisioning and usage of security services and mechanisms can be quite expensive relative to the value of the transactions being protected. It is, therefore, important to be able to customize the security provided to the TMN transactions being protected. The security services and mechanisms that are used for securing TMN transactions should be provided in a way that allows such customization. Due to the large number of possible combinations of security features, it is desirable to have **security profiles** (see Appendix I) that cover a broad range of TMN security applications.

Standardization will facilitate **reuse of solutions and products**, meaning that security can be introduced faster and at lower cost.

Important benefits of standardized solutions for vendors and users of the systems alike are the economy of scale in product development and component interoperation within a TMN system with regard to security.

It is necessary to provide security services and mechanisms to protect TMN transactions among TMN entities (as defined in ITU-T Rec. M.3010) against malicious attacks such as eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting, or re-ordering of messages), repudiation or forgery. Protection includes prevention, detection and recovery from attacks, as well as management of security-related information. Standards should cover both intra-domain (Q and F) and inter-domain (X) interfaces.

6 System description

The objective of this Recommendation is an abstraction which makes it possible to avoid the many implementation details and to agree upon results that may be useful when later mapped on to specific implementations.

The TMN is described in terms of a functional architecture, an information architecture and a physical architecture (ITU-T Rec. M.3010).

It is recognized in ITU-T Rec. M.3010 that TMN building blocks may support other interfaces in addition to those of Q, X and F. Similarly, the physical equipment may have other functionality in addition to that associated with information received via Q, X and F. These additional interfaces and related functionality are outside the scope of the TMN and, therefore, outside the scope of TMN security standardization.

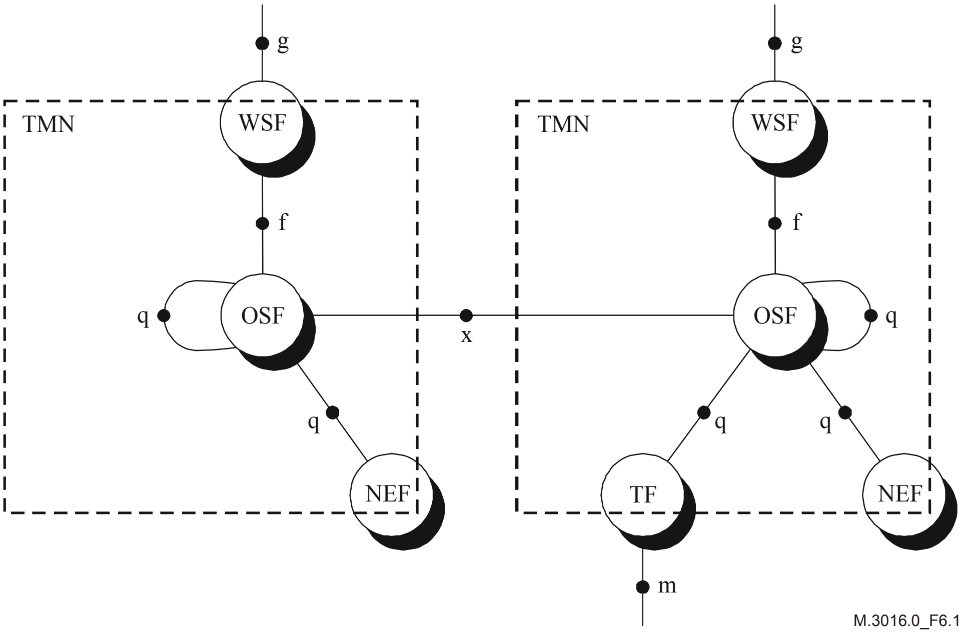

Figure 1/M.3016.0 – TMN functional architecture

6.1 Actors and roles

For the purpose of TMN security standardization, only technical security will be considered, which means that the relevant actors to consider are *TMN users*. A TMN user is a person or process applying TMN Management Services for the purpose of fulfilling management operations. TMN users can further be categorized dependent on whether they belong to the organization running the TMN (internal users) or whether they access the TMN as external users.

Each time a TMN user accesses a Management Service, the TMN user will take on a role. In some cases there will be a one-to-one relationship between a TMN user and a role, i.e., the TMN user will always stay in the same role. In other cases, there will be a one-to-many relationship between a specific TMN user and the possible roles the TMN user can play.

The following gives a high-level classification of some common roles:

- Network Operators (*private or public*);
- Service Providers (*Bearer Service Providers or Value Added Service Providers*);
- Service Subscribers/Service Customers;
- Service End Users;
- Equipment/Software Vendors;
- Trusted Third Party (that is, a third party who is trusted by both parties and operates in accordance with relevant national laws and regulations to provide certification, authentication, and related services).

When securing the TMN, it is not enough to control the behaviour of known TMN users. One must also consider the possibility of an intruder attempting illegal access to the TMN.

Some security measures require actors playing the role of a Trusted Third Party (TTP). An important security issue is how these actors should be allowed to interact with the TMN.

6.2 Security domains

ITU-T Rec. M.3010 introduces the concept of a Logical Layered Architecture (LLA) in which the management functionality is partitioned into layers. Each layer is concerned with a clearly bound subset of the total management activity. Each functional layer will be a separate *management domain* under the control of an Operation System Function (OSF), called an OSF-domain. Network Element Functions (NEFs) controlled by the OSF will be part of the OSF-domain. A TMN will as such be composed of one or several OSF domains, where the different OSF-domains can be either disjoint, interacting, overlapping or contained.

A *security domain* is defined as a set of entities and parties that are subject to a single security policy and a single security administration. A normal assumption has been to consider a TMN as a single security domain. This will often be the case, but it might not be valid to make it a general assumption. In larger TMNs, consisting of many different management systems, different parts of the TMN might be subject to different security policies and security requirements. Therefore, it seems more appropriate to say that a TMN security domain encompasses one single OSF-domain or a set of OSF-domains.

Using this assumption, the following inter-security domain and intra-security domain relationships will apply:

Possible intra-security domain relationships:

– q (OSF-NEF, OSF-OSF).

Possible inter-security domain relationships:

– x (OSF-OSF);

– f (WSF-OSF, WSF-MF);

– q (OSF-OSF, OSF-TF).

Note that the above relationships refer to security domains and not to management domains. An important thing to note is that a q reference point may be involved in both intra-security domain and inter-security domain relationships. One main difference between intra-domain and inter-domain relationships is the degree of trust that exists between the involved entities.

7 Generic security objectives for TMN

The purpose of this clause is to describe the ultimate aim of the security measures taken in a TMN compliant environment. The focus is on what security will achieve rather than on how it is done.

Security objectives should be derived from the operator's; and other actors', interests, business relations, legal and regulatory constraints, contractual constraints, etc.

The security objectives for the TMN are:

– Only legitimate actors should be able to access and operate on assets in a TMN.

– Legitimate actors should be able to access and operate on assets they are authorized to access.

– All actors should be held accountable for their own but only their own actions in the TMN.

– Availability of the TMN should be protected against unsolicited access or operations.

– It should be possible to retrieve security-related information from the TMN.

– If security violations are detected, they should be handled in a controlled way, thus minimizing the damage caused.

– After a security breach is detected, it should be possible to restore normal security levels.

– The security architecture of the TMN should provide a certain flexibility in order to support different security policies, e.g., different strength of security mechanisms.

The term "to access assets" is understood not only to be the possibility to perform functions but also to read information.

The generic objectives are phrased according to the view and language of enterprise management. The following clauses need to be expressed in more technical terms leading to implementable security services and functions. The mapping between the two languages is not always obvious.

It can be shown that by meeting the following set of security objectives the first five of the above-mentioned security objectives for TMN of this clause will be met:

– confidentiality;

– data integrity;

– accountability;

– availability.

Threats and risks identified in clause 9 and functional requirements in clause 6 will be based on these more formal terms. For definitions, see clause 9.

8 Legislation issues

The security infrastructure of a TMN must be able to accommodate constraints imposed by government laws, contractual legislation, treaties, and regulations. These constraints may include mandatory security services (such as assuring the privacy of customer information), the exclusion of certain security mechanisms (such as some types of encryption) and/or support for secret wiretapping by law enforcement agencies.

9 Threats and risks

The intention of this clause is to explore the threats and risks to a TMN. It is not the intention to specify risk assessment or threat analysis for individual TMN instances. These are local matters that can be handled differently by each provider without affecting interoperability.

A threat is a potential violation of security. According to the identified generic security objectives in TMN, threats may be directed at four different kinds of objectives:

– **confidentiality** (confidentiality of stored and transferred information);

– **data integrity** (protection of stored and transferred information);

– **accountability** (any entity should be responsible for any actions initiated); and

– **availability** (all legitimate entities should experience correct access to TMN facilities).

This Recommendation distinguishes between three kinds of threats:

– accidental threat: a threat whose origin does not involve any malicious intent;

– administrative threat: a threat that arises from a lack of administration of security; and

– intentional threat: a threat that involves a malicious entity which may attack either the communication itself or network resources.

Accidental and administrative threats may be taken into account by TMN standardization work as long as their consequences are the same as intentional threats. In order to give a more accurate analysis of threats, taking into account the TMN architecture, this Recommendation focuses on intentional threats involving communication between different actors of the TMN. The aim of this approach is to give a shorter list of threats that may be used directly in the standardization work of TMN. A threat analysis of TMN should thus address the following items based on ITU-T Rec. X.800:

– **masquerade ("spoofing")**: the pretence by an entity to be a different entity;

- **eavesdropping**: a breach of confidentiality by monitoring communication;
- **unauthorized access**: an entity attempts to access data in violation of the security policy in force;
- **loss or corruption of information**: the integrity of data transferred is compromised by unauthorized deletion, insertion, modification, re-ordering, replay or delay;
- **repudiation**: an entity involved in a communication exchange subsequently denies the fact;
- **forgery**: an entity fabricates information and claims that such information was received from another entity or sent to another entity;
- **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 and 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 by delaying the traffic of others.

Table 1 gives a map of threats and objectives.

Table 1/M.3016.0 – Mapping of threats and objectives

Threat	Confidentiality	Data Integrity	Accountability	Availability
Masquerade	x	x	x	x
Eavesdropping	x			
Unauthorized access	x	x	x	x
Loss or corruption of information (transferred)		x		x
Repudiation			x	
Forgery		x	x	
Denial of service				x

A potential threat to a system is of no harm unless there is a corresponding weakness in the system and a point in time when that weakness is exploited. Each threat will imply a risk. Evaluation of the risk may be split into the evaluation of the likelihood of each threat and an evaluation of the impact the threat may have. Threat and risk evaluation must be part of an iterative process: new threats may emerge when countermeasures are established, e.g., threats to cryptography keys when cryptographic measures are used.

10 Security requirements and services

Figure 2 describes the relationships between Security objectives, Threats, 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".

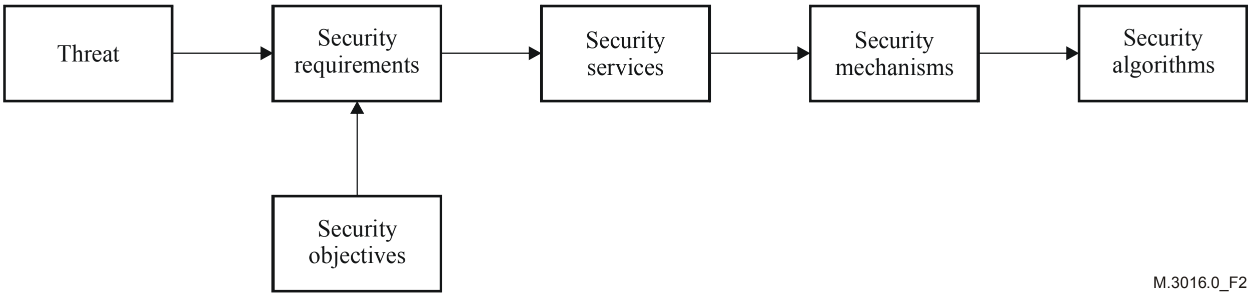

Figure 2/M.3016.0 – Security framework

Clause 10.1 lists such security requirements. Unless otherwise specified, the word "requirement" in this Recommendation does not mean that some functionality is always mandatory in each TMN; rather, it means that a functionality can be made mandatory by a TMN administration for some specific applications and/or interfaces of that TMN. The actual choice will depend on the security objectives stated in the security policy of the operator.

In addition to security requirements and services, this clause also states some generic requirements for the management of the security services (see 10.2) and architectural requirements governing the integration of security services into the TMN architecture (see 10.3). Administrative and life-cycle requirements are important but will not affect the architecture and are not included in this clause.

10.1 Security requirements and corresponding services

This clause describes a set of generic functional requirements and the corresponding services which can be used to counteract threats to a TMN.

10.1.1 Mapping functional requirements, threats and security objectives

This clause will identify functional security requirements to cover the threats listed in clause 9. This has been done in Table 2. From this, the security requirements have been mapped (Table 3) to the security objectives stated in clause 7. The list is limited to requirements which are generic in nature and have substantial impact on components and architecture.

Table 2/M.3016.0 – Mapping of functional requirements and threats

Functional requirement	Masquerade	Eavesdropping	Unauthorized access	Loss or corruption of information	Repudiation	Forgery	Denial of service
Verification of identities	x		x				
Controlled access and authorization			x				x
Protection of confidentiality		x	x				
Protection of data integrity				x			
Accountability					x	x	
Activity logging	x		x		x	x	x
Alarm reporting	x		x	x			x
Audit	x		x		x	x	x

The objectives used are the four formal ones defined in clause 3, each with a column in Table 3, indicating the set of functional requirements to meet the objective in question.

10.1.2 Description of functional requirements and the corresponding services

The functional requirements of Tables 2 and 3 are further discussed in the text which follows and, to each of the requirements, the corresponding security services are identified. Observe that the requirements for any of these functions do not automatically invoke a security service as defined by ISO. In practice, however, there is a coincidence in some of the cases.

Table 3/M.3016.0 – Mapping of security objectives and functional requirements

Functional requirement	Confidentiality	Data integrity	Accountability	Availability
Verification of identities	x	x	x	
Controlled access and authorization	x	x	x	x
Protection of confidentiality	x			
Protection of data integrity		x		
Accountability			x	
Activity logging			x	x
Alarm reporting	x	x	x	x
Audit			x	x

10.1.2.1 Verification of identities

A TMN should provide capabilities to establish and verify the claimed identity of any actor in the TMN.

Actors can be human users or entities within the TMN. Verified identities provide the basis of accountability and are fundamental to meet most of the security requirements listed in this clause.

The security service to support the requirement is **authentication**. The authentication service delivers proof that the identity of an object or subject has indeed the identity it claims to have. Depending on the type of actor and on the purpose of identification, the following kinds of authentication may be required:

– user authentication, establishing proof of the identity of the human user or application process;

– peer entity authentication, establishing the proof of the identity of the peer entity during a communication relationship;

– data origin authentication, establishing the proof of identity responsible for a specific data unit.

Usage of an authentication service establishes the proof for a particular instance of time. To ensure continued proof, the authentication has to be repeated or linked to an integrity service.

Examples of mechanisms used to implement the authentication service are passwords and Personal Identification Numbers (PINs) (simple authentication) and cryptographic-based methods (strong authentication).

10.1.2.2 Controlled access and authorization

A TMN should provide capabilities to ensure that actors are prevented from gaining access to information or resources that they are not authorized to access.

The security service to meet this requirement is **access control**. The access control service provides means to ensure that resources are accessed by subjects only in an authorized manner. Resources concerned may be the physical system, the system software, applications and data. The access control service can be defined and implemented at different levels of granularity in the TMN: at agent level, object level or attribute level. The limitations of access are laid out in access control information, which specify:

– the means to determine which entities are authorized to have access;

– what kind of access is allowed (reading, writing, modifying, creating, deleting).

More specific TMN access control can be divided into three types:

– *Management association access control*

  This service enables access control at the management association level, meaning that the access rights are related to the association itself, i.e., the right to establish the association.

– *Management notification access control*

  This service enables access control with respect to notifications, i.e., to ensure that notifications are only disclosed to entities authorized to receive them.

– *Managed resource access control*

  This service provides access control with respect to the resources themselves.

The identity of the entity trying to gain access needs to be checked before access to the resource is granted. This means that usage of access control is always linked to the usage of an authentication service.

10.1.2.3 Protection of confidentiality

A TMN should provide capabilities to ensure the confidentiality of stored and communicated data.

The security services to support the requirement are: **access control** for stored data and **data confidentiality** for communicated data. **Data confidentiality** may also be required for certain kinds of stored data such as passwords.

The confidentiality service provides protection against unauthorized disclosure of exchanged data. The following kinds of confidentiality services are distinguished:

– selective field confidentiality;

– connection confidentiality;

– data flow confidentiality.

10.1.2.4 Protection of data integrity

A TMN should be able to guarantee the integrity of stored and communicated data.

The security services to support the requirement are: **access control** and **data integrity** for stored data and **data integrity** for communicated data.

The integrity service provides means to ensure the correctness of exchanged data, protecting against modification, deletion, creation (insertion) and replay of exchanged data. The following kinds of integrity services are distinguished:

– selective field integrity;

– connection integrity without recovery;

– connection integrity with recovery.

10.1.2.5 Accountability

A TMN should provide the capability that an entity cannot deny the responsibility for any of its performed actions as well as their effects.

The requirement is supported by the **non-repudiation** service binding the individual (or entity) to the operation performed. The non-repudiation services provide means to prove that exchange of data actually took place. It comes in two forms:

– non-repudiation: proof of origin;

– non-repudiation: proof of delivery.

Another more general, and possibly weaker, realization of accountability is achieved by the appropriate combinations of the **authentication**, **access control** and **audit trail** services.

10.1.2.6 Activity logging, alarm reporting and audit

These requirements cover the needs to store and analyze information about security-relevant activities within the TMN. In addition, alarm notifications should be generated on certain adjustable events. The appropriate services are **audit trail** and **alarm reporting**. Each of the requirements is discussed below in some detail.

10.1.2.6.1 Activity logging

A TMN should provide the capability of storing information about activities on the system with the possibility of tracing this information to individuals or entities.

A log is a repository for records: it is the OSI abstraction of logging resources in real open systems. Records contain the information that is logged.

For the purpose of many management functions, it is necessary to be able to preserve information about events that have occurred or operations that have been performed or attempted by, or on, various resources.

Furthermore, when such information is retrieved from a log, the manager should be able to determine whether any records were lost or whether the characteristics of the records stored in the log were modified at any time.

10.1.2.6.2 Security alarm reporting

A TMN should provide the capability to generate alarm notifications on selected events. The user should be able to define the selection criteria.

The security audit control function is a systems management function describing the notification for collection of security events. The security alarm notification defined by this systems management function provides information regarding the operational condition pertaining to security.

10.1.2.6.3 Security audit

A TMN should provide the capability to analyze logged data on security relevant events in order to check them for violations of the security policy.

An audit should be seen as an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with the established security policy and operational procedures and to detect breaches in security. The result of the Audit would identify changes in control, policy and procedures.

Table 4 gives an overview of the relationship between Requirements and Security services. This clause only defines the security services which are covered by standard solutions; other possible services (e.g., detection of denial of service) are left out.

Table 4/M.3016.0 – Mapping of security requirements and security services

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
Protection of the DCN	packet inspection

NOTE – The following requirements are not the same type as those expressed before Table 4 and may not be seen as obvious candidates for standardization. Nevertheless, they should be taken into account during the design phase along with the implementation of the Core TMN requirements expressed above.

10.1.2.6.4 System integrity

It is essential that the software and hardware environment of the implemented security functions maintain the requested level of security.

This includes the correct configuration of operating systems and the elimination of system defects.

These aspects do not form part of the functional security profile itself, but they have to be stated together with those specifications in order to guarantee the strength of the functions in the real-world environment.

10.1.2.6.5 Remarks on availability

A requirement on availability does not have a single or a limited set of security services which are able to fulfill this requirement. All the security services listed here should form a coherent set which together is able to maintain availability. Security services alone, however, will never be able to ensure availability: this is also a matter of reliability of hardware and software (both from a design and from an implementation point of view).

10.1.2.7 Protection of the DCN

A TMN should provide protection of the DCN from customer and peer network traffic.

A TMN should provide isolation of DCN traffic from other types of traffic, especially in a packet-based DCN.

10.2 Requirements on the management of security

A TMN should contain information models and management capabilities for the services used to secure the TMN.

Detailed requirements on security management state what management applications should be introduced and how they should be designed. This is done in order to provide the security manager with the proper tools to monitor and to control security services in an effective and correct way. Objectives for and targets of security management are presented at three different levels of a telecom system, which corresponds to the management of systems security, security services and security mechanisms, respectively.

Operations and information related to the management of security services in TMN need special consideration from a security point of view. Secret encryption keys, authentication information and access control lists are examples where the required strength of protection may be higher than for network management.

The management of Security should be consistent with the security management functions defined in ITU-T Rec. M.3400.

Recovery to a secure state of the system after a security breach should be supported.

Whenever a breach of security occurs, the TMN should be able to handle this attempt in a controlled manner, meaning that the attempt should not result in a severe degradation of the TMN in terms of availability.

10.3 Architectural requirements

The most important requirements that have to be satisfied by the security measures taken to fit into the TMN framework are:

- Measures should be based on the principles of the TMN functional model.
- Measures should conform to the object-oriented data and information model of TMN.
- Measures should be applicable to all TMN domains in the public and private sector.
- Solutions should be scaleable to fit small and large TMNs.
- Solutions should be compatible with the internal architecture of the TMN reference points considered.
- Solutions should address the concerns of all internal and external TMN users.
- Solutions should consider robustness aspects.
- Solutions should support reconfiguration through the addition or removal of users or applications.

Conflicts are bound to appear between the security area and other functional areas. For example, integrity and confidentiality of charging data have to be balanced with requirements on throughput of the vast amount of information needed for toll-ticketing. A trustworthy set of security requirements needs to take the effects on characteristics of other functional areas into consideration.

Further architectural requirements may arise when specific TMN scenarios are being analyzed.

10.4 Security services and OSI layers

This clause describes which OSI layers are used to provide the security services and, therefore, shows how they can be provided for TMN in a meaningful way.

It is assumed that if a layer provides a security service, that service is provided to the layer above the considered layer. The provision of services by layers laid out in ITU-T Rec. X.800 is used as a basis to limit the possibilities.

10.4.1 User authentication

This service is dependent on interaction with the user. It is, therefore, outside the scope of the OSI model.

10.4.2 Authentication (peer entity and data origin)

The following layers can provide this service (according to ITU-T Rec. X.800):

- Network layer (corroboration of the identity of transport layer peers);
- Transport layer (corroboration of the identity of session layer peers);
- Application layer (corroboration of the identity of application processes);
- Outside OSI: in the application process itself.

Considering that the requirement for the TMN will be to identify and authenticate managers and agents and the link of authentication with access control, recommended positions with respect to the OSI stack are the application layer and the application process.

10.4.3 Access control

- *Management association access control*

  This service is usable at those levels at which an association exists; this will be at Application layer (access control for application processes) or in the application process itself.

  Association access control can be provided at the Network layer, e.g., using X.25 closed user group service. Furthermore, association access control can be provided at the Application layer or in the application process itself.

- *Management notification access control*

  This service can be used in the Application layer or in the application process itself, since it is the application process itself which can discriminate between (application process) entities like managers and agents.

- *Managed resource access control*

  This service can be used in the Application layer or in the application process itself, since it is the application process itself which can discriminate between (application process) entities like managers and agents.

10.4.4 Security alarm, audit trail and recovery

These services are linked to other services and are therefore present in those layers where the other services are present.

10.4.5 Integrity

- *Selective field integrity*

  This service can be used in the Application layer or in the application process itself, since it is the application process which can discriminate between fields.

- *Connection integrity with recovery*

  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.

10.4.6 Confidentiality

- *Selective field confidentiality*

  This service can be used in the Application layer or in the application process itself, since it is the application process which can discriminate between fields.

– *Connection and connectionless confidentiality*

Considering that end-to-end confidentiality is needed, which excludes the Physical layer and the Data link layer, confidentiality can be provided at the Network layer, the Transport layer, the Presentation layer, the Application layer or in the application process.

– *Traffic flow confidentiality*

This service can be provided in the Network, Transport, or Application layers, or in the application process.

10.4.7 Non-repudiation

– non-repudiation – proof of sending;

– non-repudiation – proof of delivery.

This service can be used in the Presentation layer, the Application layer or in the application process itself.

This is summarized in Table 5.

Table 5/M.3016.0 – Linking security services and OSI reference model

	Layer						
Service	**1**	**2**	**3**	**4**	**5**	**6**	**7**
User authentication	–	–	–	–	–	–	+
Peer entity authentication	–	–	+	+	–	–	+
Data origin authentication	–	–	+	+	–	–	+
Management association access control	–	–	+	–	–	–	+
Management notification access control	–	–	–	–	–	–	+
Managed resource access control	–	–	–	–	–	–	+
Security alarm, audit trail and recovery	+	+	+	+	+	+	+
Selective field integrity	–	–	–	–	–	–	+
Connection integrity with recovery	–	–	–	+	–	–	+
Connection integrity without recovery	–	–	+	+	–	–	+
Selective field confidentiality	–	–	–	–	–	–	+
Connection/connectionless confidentiality	–	–	+	+	–	+	+
Traffic flow confidentiality	–	–	+	+	–	+	+
Non-repudiation – proof of sending	–	–	–	–	–	+	+
Non-repudiation – proof of delivery	–	–	–	–	–	+	+

10.5 Security management

Security management comprises all activities to establish, maintain and terminate the security aspects of a system.

Topics covered are:

– management of security services;

– installation of security mechanisms;

– key management (management part);

– establishment of identities, keys, access control information, etc.;

– management of security audit trail and security alarms.

Appendix I

Functional classes and security subprofiles

I.1 Grouping of security measures

Security measures can be grouped into "Functional Classes" (FC). The following definition does not include the strength of security measure:

A functional class is a consistent set of security measures to meet requirements of varying functional levels.

I.1.1 The use of FCs in the inter-domain case

The security of a TMN should not be negatively affected as a result of inter-domain activities. The rules for domain interaction should be defined in an inter-domain security policy. These rules will define which security measures should be used in which case. To facilitate agreement between interacting domains, these security measures can be referred to as a particular functional class.

I.1.2 The use of FCs in the intra-domain case

In the intra-domain case, functional classes can facilitate the definition of security. FCs can also be used for the purpose of security assurance. To achieve this, the functional classes should be associated with a level of assurance claimed by the manufacturer of management products. This topic has strong relations with formal evaluation criteria.

It may be possible that, for the purpose of inter-domain interaction, one operator could require the application of a particular FC for the intra-domain case of the other operator. A reason for this might be that not all threats can be efficiently dealt with at the interface between the two domains. Ensuring that a minimum internal security level exists for interacting TMNs could be a solution for this. A TMN security standard should not prescribe that FCs are required, but should enable the possibility to require certain FCs, by defining appropriate items for selection.

I.2 Functional classes

Functional classes are used to define a concise group of security services aimed at meeting a certain security level. This clause works out a set of functional classes which serves as an example of how functional classes can be defined. Functional classes *for the X-interface* are proposed at three distinct security levels:

1) minimal functional class: (FC 1);
2) basic functional class: (FC 2);
3) advanced functional class: (FC 3).

For practical purposes, the number of FCs should not be too high. On the other hand, it should be possible to match the requirements of many different organizations. The functional classes may be changed in the following ways:

– Functional classes defined only for the X-interface may also include the Q interfaces.
– Confidentiality is supposed to be an optional feature for all classes for two reasons:
  • it is a less severe requirement;
  • mandatory inclusion in a functional class may have legal implications for the usability of the class.

Table I.1 provides an overview of the functional classes.

Table I.1/M.3016.0 – Functional classes of security services

FC 1	FC 2	FC 3
Emphasis on the integrity of stored managed resources	Emphasis on the integrity of stored managed resources and on integrity of transferred data	FC 2 plus accountability of management operations
• Authentication (peer entity and user) • Management association access control • Managed resource access control • Security alarm, audit and recovery	• Authentication (peer entity and user) • Management association access control • Managed resource access control • Data origin authentication • Selective field integrity • Connection integrity • Security alarm, audit and recovery	• Authentication (peer entity and user) • Management association access control • Managed resource access control • Data origin authentication • Selective field integrity • Connection integrity • Source non-repudiation • Destination non-repudiation • Security alarm, audit and recovery
Optional: • Connection integrity • Connection confidentiality	Optional: • Connection confidentiality • Selective field confidentiality	Optional: • Connection confidentiality • Selective field confidentiality

In addition, a distinction should be made between FCs applicable for the inter-domain case and FCs for the intra-domain case. The requirements will be different in both cases and, for that reason, also the security measures might be different.

The next part gives an overview of the different cases so that one can find out which FCs are needed and which are relevant.

Assumption

For each domain, an authority exists that is responsible for the decision which security measures should be applied in the domain.

Three cases are distinguished:

1) FCs defined by a domain authority and applicable to the own domain (intra-domain);

2) FCs defined by a domain authority and applicable to the domain interactions (inter-domain). These FCs will be the result of an agreement between the authorities of the interacting domains;

3) FCs defined by a domain authority as requirements to the internal security of the other domain.

In each case, the number of FCs for different security levels can be identified.

The number of security levels is for further study.

The set of security measures that form an FC is for further study.

FCs in the different cases might be equal, thus reducing the total number of FCs.

One could also consider a trade-off between the different cases, e.g., when the inter-domain security is at a high level, the requirements for internal security in the other domain might be low and vice versa. Another possibility might be that an FC represents a minimum set of security measures that can be extended with additional measures as is appropriate.

I.3 Security profiles

Functional classes do not require the use of standardized security mechanisms; any mechanisms that fulfill the requirements can be applied.

To enable interaction between security measures in different domains, the measures should conform to standards. A prescription of the use of particular standards that together provide a functional class is called a security profile.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2005