INTERNATIONAL TELECOMMUNICATION UNION

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# E.408

(05/2004)

SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

Network management – International network management

## Telecommunication networks security requirements

ITU-T Recommendation E.408

ITU-T E-SERIES RECOMMENDATIONS

**OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS**

| | |
|---|---|
| INTERNATIONAL OPERATION | |
| Definitions | E.100–E.103 |
| General provisions concerning Administrations | E.104–E.119 |
| General provisions concerning users | E.120–E.139 |
| Operation of international telephone services | E.140–E.159 |
| Numbering plan of the international telephone service | E.160–E.169 |
| International routing plan | E.170–E.179 |
| Tones in national signalling systems | E.180–E.189 |
| Numbering plan of the international telephone service | E.190–E.199 |
| Maritime mobile service and public land mobile service | E.200–E.229 |
| OPERATIONAL PROVISIONS RELATING TO CHARGING AND ACCOUNTING IN THE INTERNATIONAL TELEPHONE SERVICE | |
| Charging in the international telephone service | E.230–E.249 |
| Measuring and recording call durations for accounting purposes | E.260–E.269 |
| UTILIZATION OF THE INTERNATIONAL TELEPHONE NETWORK FOR NON-TELEPHONY APPLICATIONS | |
| General | E.300–E.319 |
| Phototelegraphy | E.320–E.329 |
| ISDN PROVISIONS CONCERNING USERS | E.330–E.349 |
| INTERNATIONAL ROUTING PLAN | E.350–E.399 |
| NETWORK MANAGEMENT | |
| International service statistics | E.400–E.404 |
| **International network management** | **E.405–E.419** |
| Checking the quality of the international telephone service | E.420–E.489 |
| TRAFFIC ENGINEERING | |
| Measurement and recording of traffic | E.490–E.505 |
| Forecasting of traffic | E.506–E.509 |
| Determination of the number of circuits in manual operation | E.510–E.519 |
| Determination of the number of circuits in automatic and semi-automatic operation | E.520–E.539 |
| Grade of service | E.540–E.599 |
| Definitions | E.600–E.649 |
| Traffic engineering for IP-networks | E.650–E.699 |
| ISDN traffic engineering | E.700–E.749 |
| Mobile network traffic engineering | E.750–E.799 |
| QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING | |
| Terms and definitions related to the quality of telecommunication services | E.800–E.809 |
| Models for telecommunication services | E.810–E.844 |
| Objectives for quality of service and related concepts of telecommunication services | E.845–E.859 |
| Use of quality of service objectives for planning of telecommunication networks | E.860–E.879 |
| Field data collection and evaluation on the performance of equipment, networks and services | E.880–E.899 |

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

# ITU-T Recommendation E.408

## Telecommunication networks security requirements

**Summary**

This Recommendation provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile; both voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats.

**Source**

ITU-T Recommendation E.408 was approved on 28 May 2004 by ITU-T Study Group 2 (2001-2004) under the WTSA Resolution 1.

## 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

# ITU-T Recommendation E.408

## Telecommunication networks security requirements

## 1 Introduction

### 1.1 Scope

This Recommendation provides an overview and framework that identifies security threats to telecommunication networks in general (both fixed and mobile; both voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats.

This Recommendation is generic in nature and does not identify or address requirements for specific networks.

This Recommendation does not seek to define new security services but uses existing security services defined in other ITU-T Recommendations and relevant standards from other bodies.

This Recommendation is intended to facilitate international cooperation in the following areas regarding telecommunication network security:

- Information sharing and dissemination;
- Incident coordination and crisis response;
- Recruitment and training of security professionals;
- Law enforcement coordination;
- Protection of critical infrastructure and critical services;
- Development of appropriate legislation.

To succeed in obtaining such cooperation, national implementation of the requirements of this Recommendation for the national components of the network is essential.

### 1.2 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 M.3010 (2000), *Principles for a telecommunications management network*.

– ITU-T Recommendation M.3016 (1998), *TMN security overview*.

– ITU-T Recommendation M.3400 (2000), *TMN management functions*.

– ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

– ITU-T Recommendation X.741 (1995) | ISO/IEC 10164-9:1995, *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) | ISO/IEC TR 13594:1995, *Information technology – Lower layers security model*.

– ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

– ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

– ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

– ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

– ITU-T Recommendation X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

– ITU-T Recommendation X.814 (1995) | ISO/IEC 10181-5:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework*.

– ITU-T Recommendation X.815 (1995) | ISO/IEC 10181-6:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework*.

– ITU-T Recommendation X.816 (1995) | ISO/IEC 10181-7:1996, *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*.

– IETF RFC 2535 (1999), *Domain Name System Security Extensions*.

– IETF RFC 2870 (2000), *Root Name Server Operational Requirements*.

– IETF RFC 3013 (2000), *Recommended Internet Service Provider Security Services and Procedures*.

### 1.3 Use of the term "service"

The word "service" used in this Recommendation does not refer to any defined ITU services. It is used as a generic term when discussing security issues and/or functions and should be defined in the future.

### 1.4 Rationale

The requirement for a generic network security framework for international telecommunications has originated from different sources:

– **Customers/subscribers** need confidence in the network and the services offered, including availability of services (especially emergency services) in case of major catastrophes, including terrorist actions.

– **The public community/authorities** demand security by directives and legislation, in order to ensure availability of services, fair competition 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, at the national and international level.

Telecommunication networks security requirements 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 relatively to the value of the transactions being protected. It is, therefore, important to have the ability to customize the security provided in relation to the services being protected. The security services and mechanisms that are used 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 II) that cover a broad range of telecommunication network services.

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 economies of scale in product development and component interoperation within telecommunication networks with regard to security.

It is necessary to provide security services and mechanisms to protect telecommunication networks against malicious attacks such as denial of service, 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. Protection must also include measures to prevent service outages due to natural events (weather, etc.) or malicious attacks (terrorist actions). Provisions must be made to allow eavesdropping and monitoring as requested by duly authorized legal authorities.

## 2 System description

To effectively secure one network, it is recommended to implement layers of security; the more layers someone puts in place, the more effective its security. This technique of building layers can be analysed from the ground up:


**Figure 1/E.408 – Six layers for network security**

The term "layer" as used in this Recommendation merely constitutes a description of some security considerations that are relevant to organizing network security. Layers in this Recommendation should not be considered as architectural elements and should not be confused with the security layers of ITU-T Rec. X.805.

Like the foundation of a house, the first layer, network administrators, will be an organization's most important asset in network security. Spending extra money each year on a good network administrator is more effective than buying an expensive firewall. Good network administrators understand the operating systems they work with and understand how to lock down every machine

on their network to only allow the ports and processes through that need to get through. Management must give their network administrators ongoing training and time to stay ahead of network bugs and exploitation.

The second layer is physical security. Every attacker in the world knows the easiest way to gain access to a network is from the inside. There are just too many cases of "social engineering", where attackers have simply called the helpdesk and mentioned they have forgotten their password and asked the helpdesk to change it to xxxxx. Physical security includes everything from letting only certain people (system administrators) access the consoles, to policies on what information is given to the public about an organization's network. Good acceptable use policies, password policies, and software installation policies do a lot to help organizations lock down access to their networks.

The third layer is monitoring. It is very rare that an attack succeeds on the first try. Most attacks could be stopped if the system's logs are scrutinized at least once a day. This will not take as much time as initially appears. The human eye is the best device for picking out patterns in log files. Several good software programs exist that will monitor log files, and while these programs can be very helpful, the system administrator should read through the logs of his primary machines every day.

The fourth layer is the telecommunications software. Every piece of software put on the servers should be evaluated with security in mind. The system administrator should know, for example, what TCP and UDP ports the software will be listening to, what user accounts the software interacts with, and the directory permissions the software requires. Also, it is recommended that known security bugs should be looked for before purchasing. This should become part of the evaluation process of all software purchased.

The fifth layer is security tools. After good policies and practices have been established for the previous four layers, it is necessary to start to look at firewalls, intrusion detection software, and proxies. Installing the best firewall in the world with bad firewall policies is worse than having no firewall at all. All too often, it is possible to find network servers with poor security policies depending on the firewall to keep attackers at bay. Once the firewall is compromised, all the servers are laid wide open to attack.

The sixth layer is security auditing. Network security is a moving target. Every day, someone somewhere finds a new method of breaching a network's security. It is important that organizations regularly try to penetrate their own network. An audit should test every aspect of network security. Testing a network's resistance to physical attacks on its security is recommended and a war dialer should be run against all phone numbers to ensure that no modems have been installed on a desktop without the network administrator's knowledge. Audits should be performed on the mail server, DNS, domain, web and FTP servers.

## 2.1 Actors and roles

For the purpose of telecommunication network standardization, only technical security should be considered, which means that the relevant actors to consider are *Telecommunication Actors* (TAs). A TA is a person (physical or legal) or process responsible for certain network operations.

Each time a TA performs an action, it will take on a role. In some cases, there will be a one-to-one relationship between a TA user and a role, i.e., the TA will always stay in the same role. In other cases there will be a one-to-many relationship between a specific TA user and the possible roles the TA can play.

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

– Network operators (*public or private*);

– Service providers (*bearer service providers or value-added service providers*);

– Service subscribers/service customers;

– Service end users;
– Equipment/software vendors;
– Trusted third party.

## 2.2 Security domains for telecommunication networks

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.

The network security design can consider different domains and sub-domains to surround and delimit the responsibilities in network management and security control.

At least, the following aspects must be considered for the network segregation in domains:

- The physical network boundaries.
- The liabilities areas.
- The functionalities fields.
- The criticality of applications and data communicated through the networks.
- Potential geographic limits (premises, regional customs, etc.).
- Traffic and capacity needs/availability.
- Continuity and recovery needs.
- Business application domain.
- Business support domain (billing, human resources management, etc.).
- Development and testing domains.
- Production domains.
- Alarm management domain.
- Managerial and administrative network security responsibilities.

The backbone layer interfaces are typically an area where the liabilities change. The interface between a production environment and the office environment, or the test environment, are typical network functionality boundaries. Each access point to domain and sub-domain needs a gateway which can provide several security services such as traffic control, access control, etc.

# 3 Generic security objectives for telecommunication networks

The purpose of this clause is to describe the ultimate aim of the security measures taken in telecommunication networks. The focus is on what security requirements should achieve rather than on how it is done.

The security objectives for telecommunication networks are:

– Only legitimate actors should be able to access and use telecommunication networks.
– Legitimate actors should be able to access and operate on assets they are authorized to access.
– Telecommunication networks should provide privacy at the level set by the security policies of the network.
– All actors should be held accountable for their own, and only their own, actions in telecommunication networks.
– In order to ensure availability, telecommunication networks should be protected against unsolicited access or operations.

– It should be possible to retrieve security-related information from telecommunication networks (but only legitimate actors should be able to retrieve such information).
– If security violations are detected, they should be handled in a controlled way in accordance with a pre-defined plan to minimize potential damage.
– After a security breach is detected, it should be possible to restore normal security levels.
– The security architecture of telecommunication networks 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 as 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 telecommunication networks of this clause will be met:

– confidentiality;
– data integrity; (surely integrity of system programs is also required, or else you have a DoS attack?)
– accountability, including authentication, non-repudiation and access control;
– availability.

Threats and risks identified later in clause 5, as well as the functional requirements in clause 6, will be based on these more formal terms. For definitions, see clause 5.

The rest of the objectives deal with the monitoring and control of the security state of the system. They will be dealt with in the relevant clauses on recovery, architecture and security management according to security policy implemented.

## 4 Legislation issues

The security infrastructure of a telecommunication network 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.

## 5 Threats and risks

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

A threat is a potential violation of security. According to the identified generic security objectives, 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);
– **system integrity** (Protection of operating system);
– **accountability** (Any entity should be responsible for any actions initiated); and

– **availability** (All legitimate entities should experience correct access to telecommunication networks).

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 telecommunication network itself or network resources.

Accidental and administrative threats may be taken into account by standardization work as long as their consequences are the same as intentional threats. In order to give a more accurate analysis of threats, this Recommendation focuses on intentional threats. The aim of this approach is to give a shorter list of threats that may be used directly in the standardization work. A threat analysis should thus address the following issues 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 telecommunication;

– **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 telecommunication 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 telecommunication networks and denial of telecommunication by flooding telecommunication networks or components of a network. 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/E.408 – Mapping of threats and objectives**

| Threats | Objectives | | | |
|---|---|---|---|---|
| | **Confidentiality** | **System or 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 not necessarily harmful 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.

## 6 Security requirements

Figure 2 describes the relationships among security objectives, Threats, Risks, Security requirements, and Services. It describes the process on 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". This process is shown in Figure 2.

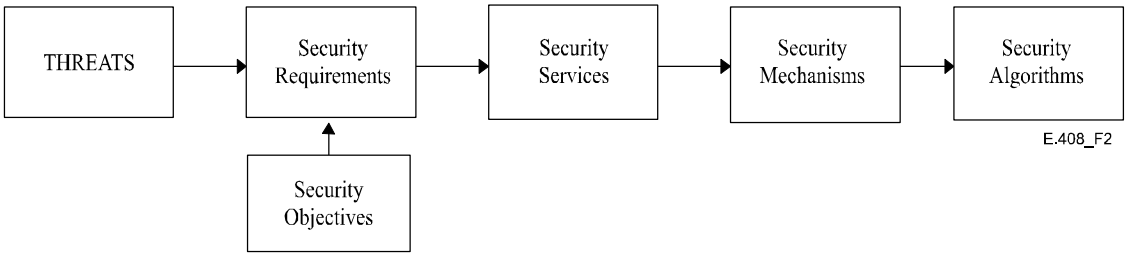


**Figure 2/E.408 – Derived security requirements**

Clause 6.1 lists such security requirements. Unless otherwise specified, the word "requirement" in this Recommendation does not mean that some functionality is always mandatory in each telecommunication network; rather, it means that a functionality can be made mandatory by a network administrator for some specific services, applications and/or interfaces of that network. 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 6.2) and architectural requirements governing the integration of security services into a generic network architecture (see 6.3). Administrative and life-cycle requirements are important but will not affect the architecture and are omitted from this clause.

The security requirements can be applied to every security perspective of the security architecture standardized by ITU-T Rec. X.805. The Security Dimensions (also introduced in ITU-T Rec. X.805) are designed to meet security requirements for each security perspective. The Security Services, Security Mechanisms and Security Algorithms that are discussed in this Recommendation should be viewed as the integral parts of each Security Dimension.

### 6.1 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 telecommunication networks.

#### 6.1.1 Mapping functional requirements, threats and security objectives

This clause will identify functional security requirements to cover the threats listed in clause 5. This has been done in Table 2. From this, the security requirements have been mapped (Table 3) to the security objectives stated in clause 3. The list is limited to requirements which are generic in nature and have substantial impact on components and architecture.

**Table 2/E.408 – Mapping of functional requirements and threats**

| Functional requirements | Threats | | | | | | |
|---|---|---|---|---|---|---|---|
| | 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.

### 6.1.2 Description of functional requirements and the corresponding functions

The functional requirements of Tables 2 and 3 are further discussed in the text which follows and, for each of the requirements, the corresponding security functions 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/E.408 – Mapping of security objectives and functional requirements**

| Functional requirements | Security objectives | | | |
|---|---|---|---|---|
| | Confidentiality | System or data integrity | Accountability | Availability |
| Verification of identities | x | x | x | |
| Controlled access and authorization | x | x | x | x |
| Protection of confidentiality | x | x | | |
| Protection of system or data integrity | | x | | |
| Accountability | | | x | |
| Activity logging | | | x | x |
| Alarm reporting | x | x | x | x |
| Audit | | | x | x |

NOTE – Keeping data confidential is a sufficient condition for maintaining data integrity, i.e., if data can be kept confidential, it will be protected from being altered. However, protection from being altered does not necessarily protect it from being divulged.

#### 6.1.2.1 Verification of identities

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

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

The security service to support the requirement is **authentication**. The authentication function 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 telecommunication relationship;
– data origin authentication, establishing the proof of identity responsible for a specific data unit.

Usage of the authentication function 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).

#### 6.1.2.2 Controlled access and authorization

*A telecommunication network 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 which meets this requirement is **access control**. The access control service provides the means of ensuring 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 function can be defined and implemented at different levels of granularity in the telecommunication network: 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 specifically, telecommunication network access control can be divided into three types:

– *Management association access control*

  This 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 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 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 the authentication service.

#### 6.1.2.3 Protection of confidentiality

*A telecommunication network should provide capabilities to ensure the confidentiality of stored and communicated data*.

The security services which support the requirement are: **access control** for systems, **access control** for stored data and **data confidentiality** for telecommunicated data.

Breach of system confidentiality should not be overlooked as it is often a precursor to attacks on system or data integrity (assists attackers in finding DoS type vulnerabilities).

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

– system confidentiality (includes information as diverse as architectural and configurational information, algorithms used, software version numbers, types of hardware used, etc.);
– selective field confidentiality;
– connection confidentiality;
– data flow confidentiality.

#### 6.1.2.4 Protection of system and data integrity

*A telecommunication network should be able to guarantee the integrity of systems and stored and communicated data*.

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

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

– operating system integrity;
– selective field integrity;
– connection integrity without recovery;
– connection integrity with recovery.

#### 6.1.2.5 Accountability

*A telecommunication network should provide a capability so that an entity cannot deny the responsibility for any of its performed actions as well as their effects. For example, a telecommunication network should provide the means of proof that an entity has performed certain actions*.

The requirement is supported by the **non-repudiation** service binding the individual (or entity) to the operation performed. The non-repudiation services provide means of proving that exchange of data actually took place and that users are aware of the legal environment surrounding use of the service or product (e.g., awareness that usage is monitored etc., typically achieved through use of logon banners). It comes in three forms:

– non-repudiation: proof of origin;
– non-repudiation: proof of delivery.
– non-repudiation: proof of knowledge of legal environment.

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

#### 6.1.2.6 Activity logging, alarm reporting and audit

These requirements cover the needs to store and analyse information about security-relevant activities within the telecommunication network. The appropriate services are **activity logging**, **audit trail**, and **alarm reporting**. Each of the requirements is discussed below in some detail.

##### 6.1.2.6.1 Activity logging

*A telecommunication network 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.

As log files constitute part of the system data, this requirement will also necessitate requirements defined in 6.1.2.4 and possibly 6.1.2.3.

##### 6.1.2.6.2 Security alarm reporting

*A telecommunication network 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.

##### 6.1.2.6.3 Security audit

*A telecommunication network should provide the capability to analyse 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 systems. 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/E.408 – Mapping of security requirements and security services**

| Functional requirement | Security service |
|---|---|
| Verification of identities | user authentication<br>peer entity authentication<br>data origin authentication |
| Controlled access and authorization | access control |
| Protection of system integrity | access control |
| Protection of confidentiality – stored data | access control |
| 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 and recovery |

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

#### 6.1.2.6.4 System integrity

*It is essential that the software and hardware environment of the implemented security functions should 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.

#### 6.1.2.6.5 Remarks on availability

A requirement on availability does not have a single or a limited set of security services which are able to fulfil 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).

### 6.2 Requirements on the management of security

*A telecommunication network should contain information models and management capabilities for the services used to secure the telecommunication network.*

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.

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

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

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

### 6.3 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 telecommunication networks 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.

#### 6.3.1 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.

#### 6.3.2 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. 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.

#### 6.3.3 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.

### 6.3.4 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.

### 6.3.5 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.

### 6.3.6 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 is not identical to Table 2 of ITU-T Rec. X.800 because of the differing scopes of the two Recommendations.

**Table 5/E.408 – 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 | – | – | – | – | – | + | + |

## 6.4 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;
– security awareness and training;
– security strategy;
– security policies and regulations;
– collaborative security management;

# Appendix I

# Legislation issues

## I.1 Introduction

This clause describes the areas of legislation which may influence standardization of security in telecommunication networks and tries to give some consequences of this legislation.

## I.2 Applicable legislation areas

The following areas of legislation which may possibly influence standardization of telecommunication network security have been identified:

**Privacy**

– "privacy of letter": keeping information exchanged between customers away from non-authorized third parties;

– limitations on collection, storage and processing of personal data: personal data may only be collected, stored and processed if there is a relationship between the data and the actual provision of services;

– disclosure: the obligation of a network operator to keep information concerning customers away from non-authorized third parties;

– "inspection and correction": the right of the customer to inspect and correct information about himself stored, if justified, by the network operator.

Privacy legislation will mostly influence security requirements regarding access control, integrity and confidentiality.

**Contractual**

– the possibility of using information concerning the telecommunication between entities in case of a dispute in a court of law;

– the recognition of an electronically delivered contract in a court of law.

Security requirements regarding integrity and non-repudiation will mostly be influenced.

**International security and National public order**

– demands on the proper protection of information and infrastructure: ensuring the availability and integrity of the telecommunication network;

– restrictions on use of cryptographic methods: some countries have laws restricting the usage of encryption;

– the obligation of network operators to cooperate and provide information in case of lawful interception, for criminal investigation.

This legislation may influence security requirements. The influence of legal interception legislation on requirements is somewhat unclear. There is, however, a relationship with privacy, e.g., only information about the person being investigated should be provided.

## I.3 Sources of legislation

In the previous clause, legislation was categorized into subjects. The following identifies some sources of legislation and their possible influence on telecommunication network security.

– *Constitutions*

  Covering secrecy of correspondence, right of privacy, right of personal liberty, etc. Not all constitutions specifically refer to telecommunications.

– *International treaties*

  Two examples are the treaties of Rome and Maastricht. Two areas of legislation are important here for telecommunications: The first area concerning the European market (the so-called "first pillar"), which aims at competition on the (telecommunications) market: important for security are the "essential requirements" on safety and integrity of networks and on the protection of data. The second area (the "third pillar") is concerned with European cooperation in the field of justice: this area's main points for security are the requirements on legal interception. These requirements are for call content, call-associated data and target location. Important aspects for telecommunication network security could be the following: *Specific provisions are needed for confidentiality, integrity, and auditing in the interception process.*

– *Other international conventions*

  Many of these conventions deal with human rights: with regard to telecommunications, privacy and secrecy are the most relevant ones. Copyright laws are considered not to be relevant for telecommunication network security.

– *National laws*

  Applicable laws again deal with privacy, secrecy and legal interception.

– *Rules issued by the National Telecommunications Regulator (NTR)*

  The NTR is the national body (appointed by national law) which is given the authority to issue rules and regulations in the telecommunication area. These rules may include security issues.

– *Codes of practice*

  Agreed policies between telecommunication companies and organizations to deal with security issues. For telecommunication network security, these codes of practice might become an important issue when telecommunication networks are connected together.

### I.4 Possible consequences for telecommunication network security standardization

For telecommunication network security standardization, the following consequences of legislation are envisaged and should be taken into account:

– Legislation may result in requirements with regard to strength and availability of security services. The previous clauses gave some indication concerning these requirements.

– Necessity to provide a certain level of integrity of the telecommunication network.

– Possibility to support legal interception and access to management data for the Justice department. The length of time for which data may need to be stored, and processes to ensure that data is destroyed when required.

– Legislation may result in an inhibition of the usage of encryption in some countries.

– Legislation will not be the same in different countries. This means that for different countries, different requirements might arise.

# Appendix II

# Functional classes and security profiles

## II.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 security requirements at various levels (functional levels).

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

The security of a telecommunication network 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.

### II.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 telecommunication networks could be a solution to this problem. A telecommunication network security standard should not prescribe that FCs are required, but should enable the possibility of requiring certain FCs, by defining appropriate items for selection.

## II.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 II.1 provides an overview of the functional classes.

**Table II.1/E.408 – 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)<br>• Management association access control<br>• Managed resource access control<br>• Security alarm, audit and recovery | • Authentication (peer entity and user)<br>• Management association access control<br>• Managed resource access control<br>• Data origin authentication<br>• Selective field integrity<br>• Connection integrity<br>• Security alarm, audit and recovery | • Authentication (peer entity and user)<br>• Management association access control<br>• Managed resource access control<br>• Data origin authentication<br>• Selective field integrity<br>• Connection integrity<br>• Source non-repudiation<br>• Destination non-repudiation<br>• Security alarm, audit and recovery |
| Optional:<br>• Connection integrity<br>• Connection confidentiality | Optional:<br>• Connection confidentiality<br>• Selective field confidentiality | Optional:<br>• Connection confidentiality<br>• 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, the security measures might also 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.

## II.3 Security profiles

Functional classes do not require the use of standardized security mechanisms; any mechanisms that fulfil 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 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 | 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 | 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 communications |
| 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, 2004