ETSI TECHNICAL REPORT

ETR 336

January 1997

Source: ETSI TC-NA

Reference: DTR/NA-043208

ICS: 33.020

Key words: TMN, OSI Management, Security

Telecommunication Management Network (TMN); Introduction to standardizing security for TMN

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Foreword

This ETSI Technical Report (ETR) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or the application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or an I-ETS.

This ETR is jointly published with EWOS.

Blank page

1 Scope

The purpose of this ETSI Technical Report (ETR) is:

- to identify the requirements for security of Telecommunications Management Network (TMN);

- to specify the scope and priorities for future work on security of TMN - such future work may include identification of existing standards (formal or industry) and development of new standards.

The ETR is not intended to be a tutorial on security (or on TMN). It is a presumption that the reader has a basic knowledge of both these fields.

One of the basic objectives of this ETR is to support the realization of different security policies, not to impose a specific one.

The scope of the TMN security standardization is Security of Management (SoM), not Management of Security (MoS). The scope of the standards that result from or are identified by future work will, however, include the management of security information that is needed for the security services which are specified. The scope does also not include administrative and physical security.

The OSI management standards (the ITU-T X.700 series of Recommendations, jointly published by ISO) are applicable for the management of any environment, and the standards/recommendations for TMN can be seen as a user of the OSI management standards. It is considered that the requirements for security of the OSI management environment are in most cases identical to those of security of TMN. Thus, this ETR can also be seen as specifying requirements for security in the OSI management environment.

Additionally, although the concepts within the standards that result from or are identified by future work are intended for use within a purist TMN environment, elements may be adopted by network operators for use within pre- and non-standardized TMN environments.

The requirements identified for a secure TMN environment are seen as applicable world-wide. In later phases of work, an important objective is that the solutions identified should also be world-wide.

The ETR covers the following points in approximately the same sequence as they are listed below:

- explain the rationale for standardization of TMN security;
- define the main objectives for TMN security standardization;
- outline a global picture of TMN and TMN security;
- do a threat analysis and risk assessment;
- identification of security requirements and countermeasures (security services);
- define the methodology to apply for standardization;
- make a preliminary identification of existing work; standards and other documents to base the work on;
- define criteria's for prioritization of the standardization work, document the priorities and define the scope for the first phases of the standardization work.

An elaborate description of the approach followed is given in clause 6.

2 References

This ETR incorporates by dated and undated reference, provisions from other publications. These references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] CEC Council Directive of 28 June 1990 on the establishment of the internal market for telecommunications services through the implementation of open network Provisioning (90/387/EEC).

[2] Proposal for a Council Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunication Networks, in particular the Integrated Services Digital Networks (ISDN) and Public Digital Mobile Networks, COM(94)128 def / COD 288 -1994.

[3] ITU-T Recommendation M.3010: "Principles for a Telecommunications Management Network".

[4] RACE CFS H210: "TMN Security Architecture".

[5] ANSI T1.233-1993: "OAM&P, "Security Framework for TMN Interfaces".

[6] ANSI T1.XXX-199X: "OAM&P, Baseline Security Requirements for TMN".

[7] RACE CFS H211: "Security of Service Management".

[8] ITU-T Recommendation X.741 | ISO/IEC 10164-9 (1993): "Information technology - Open Systems Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control".

[9] ITU-T Recommendation X.800 | ISO 7498-2 (1989): "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[10] ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this ETR, the following definitions apply:

Definitions used in this ETR are defined in ETR 232 [10].

actor: An entity that may be authenticated (e.g. humans or processes) performing operations on assets of the TMN.

3.2 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

ACSE	Association Control Service Element
ANSI	American National Standards Institute
API	Application Programming Interface
ASE	Application Service Element
CEC	Commission of the European Community
CFS	Common Functional Specifications
CMIP	Common Management Information Protocol
CMISE	Common Management Information Service Element
DCF	Data Communication Function
DCN	Data Communication Network
ECMA	European Computer Manufacturers Association
EWOS	European Workshop on Open Systems
FTAM	File Transfer Access and Management
IEC	International Electrotechnical Committee
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
LLA	Logical Layered Architecture
MCF	Message Communication Function

MF	Mediation Function
MO	Managed Object
NEF	Network Element Function
OAM&P	Operation, Administration, Maintenance & Provisioning
ONP	Open Network Provisioning
OSF	Operations System Function
PC	Personal Computer
QAF	Q-interface Adapter Function
RACE	Research for Advanced Communications in Europe
ROSE	Remote Operation Service Element
SMASE	Service Management Application Service Element
STAG	Security Techniques Advisory Group
TMN	Telecommunication Management Network
TTP	Trusted Third Party (security definition)
WSF	Work Station Function

4 Rationale

TMN concepts and standards have been worked on for a long period of time and new network management products include a growing share of standardized facilities and interfaces. However, adequate security features to protect management operations and information are still missing in the standards, and consequently in the emerging products.

Awareness is increasing about potential threats and about the need for security measures in the management of a globally interconnected telecommunication environment.

Therefore this ETR answers the following two questions:

1) why security is needed for TMN?
2) why security for TMN should be standardized?

4.1 Why security is needed for TMN?

The requirement for security in TMN is originating from different sources:

- **customers/subscribers** need confidence in the network and the services offered, including correct billing;

- **the public community/authorities** demands 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.

The reason why these interested parties are increasingly aware of security requirements is the fact that there are growing threats and risks caused by changes in the overall regulatory and technological environment.

The global telecommunication market is growing increasingly competitive. One of the incentives for this is for example the CEC Council Directive of 28 June 1990 on the establishment of the internal market for telecommunications services through the implementation of Open Network Provisioning (ONP) (CEC Directive on **Open Network Provisioning**) [1]. The customers will be free to buy their services wherever they like, and a network service may be based on network resources from many different providers. In order to monitor, control and tailor the services and network resources, **customer access to network/service management facilities** will be required. Thus ONPs will impose well defined interfaces also for management facilities. Customer access to management facilities clearly requires security, not only to protect the provider's operation, but equally important to protect the availability, stability and confidentiality of the customer's operation.

Privacy is of increasing importance; there are, for example, strong restrictions in many countries with regard to storage and visibility of charging data. For instance for the European market the draft CEC

directive "Proposal for a Council Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunication Networks, in particular the Integrated Services Digital Networks (ISDN) and Public Digital Mobile Networks", [2] is only one indication of the community's concern.

Technology is another driving force for security. **Open systems**, as TMN is, means that proprietary interfaces and protocols are replaced by standardized and well known ones, which are easier to attack. And technology comes cheap these days, making life easier for hackers and other dishonest people; there are e.g. dozens of protocol analysers available for PCs as public domain software.

The threats are not, however, restricted to coming from external intruders only. There are surveys indicating, that for data communication systems close to half of the crimes are committed by people within the organization, and in telecommunication systems maybe as much as 80 %. This means it is equally important to protect the intra-domain interfaces (Q3 and F) as the inter-domains ones (X). One should also keep in mind that security is useful not only to protect against fraud, but also to ensure correctness of operation. Much harm is done by unintentional mistakes, which can be reduced by applying suitable security services.

4.2 Why security for TMN should be standardized?

The most obvious reason for defining standards is perhaps that many security services are peer to peer. Given that TMN is a very heterogeneous network consisting of nodes from different vendors and based on different technologies, formal standards are clearly needed.

As mentioned above, ONP and the decomposition of monopolies into many diversified providers will cause increasing **management traffic between TMN domains**. This will further emphasize the need for standards, in order to avoid a multitude of bilateral arrangements between TMNs. Given N domains with different security profiles one will need N.(N-1)/2 bilateral arrangements without a standard; standardized solutions implemented by all parties can provide secure interoperation of Information Technology (IT) systems.

There are currently quite a few security standards available; one reasonable question is why these are not sufficient. The answer is that, like for most other areas, there are options, overlaps, divergence's and gaps which need clarification and amendments. In addition, TMN as one specific environment does not necessarily require the same set of security services and mechanisms as other environments. Thus, **development of one or more security profiles is needed.**

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

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

5 Objectives for TMN security standardization

The main objective is the specification of standard(s) which will allow secure interoperation of TMN systems and components in a multi-vendor and multi-operator environment.

Another objective is to build the TMN security standard(s) on available results from standardization within the security area and from international collaborative programs (RACE, Eurescom, etc.).

Activities during the first phase of the action will be confined to meet high-priority requirements.

TMN standards by ETSI and recommendations by ITU form the framework and target of the proposed ETSI security standard development. Legal and regulatory aspects will be taken into account, in particular regarding interworking over domain and national limits.

The impact on relevant TMN standard specifications will be investigated, clearly stated and fed back to ITU.

Ongoing work in **ETSI Security Technical Committee** will result in a **series of guidelines** and reports. The purpose of these documents is to support the development of security standards, starting with the threat analysis of the target system/service and resulting in the specification of security services/mechanisms and their management. Liaison with STAG will be established to gain close support in the use of the guidelines and produce feedback to the authors.

The TMN security architecture and its components should preferably be based on existing or evolving standards, thereby ensuring stability of the specifications and long term support by vendors and users. De-facto or industrial standards will only be used if there is a strong confidence that they will be widely used and supported over a long period of time. Some of the relevant security standards to be taken into consideration are listed in annex A. On the long term the aim is to use only international standards, either by adopting these international or to endorse the adoption of the defacto standard as an international standard.

Another aspect of lifetime arises from the fact that product development and operation cycles of network management products are relatively long. This calls for **flexible, modular solutions** which in the long run can cope with evolving technology, support different security levels and can be re-used.

Effective use will be made of **results provided by European Commission research programmes, Eurescom, and other projects**. Valuable contributions are available considering threat analysis, security requirements, security management and security concepts/prototypes for management.

The specifications to be developed will comprise a **complete set of components** for each security service in order to facilitate early implementation and evaluation. This means that following the overall requirements and architecture phase, activities should be concerned with the completion of implementable subsets rather than working in parallel on all items simultaneously.

6 Methodology applied

The process of assessing and specifying the subjects for TMN security standardization requires a good understanding of the TMN architecture, its functionality and the communication among its components. To make this process as efficient as possible, it will be beneficial to follow a methodology to guide one through this process in a step-wise manner.

Therefore, the following subclauses describe such a step-wise method used in the elaboration of this ETR. Figure 1 illustrates the main steps in this process.

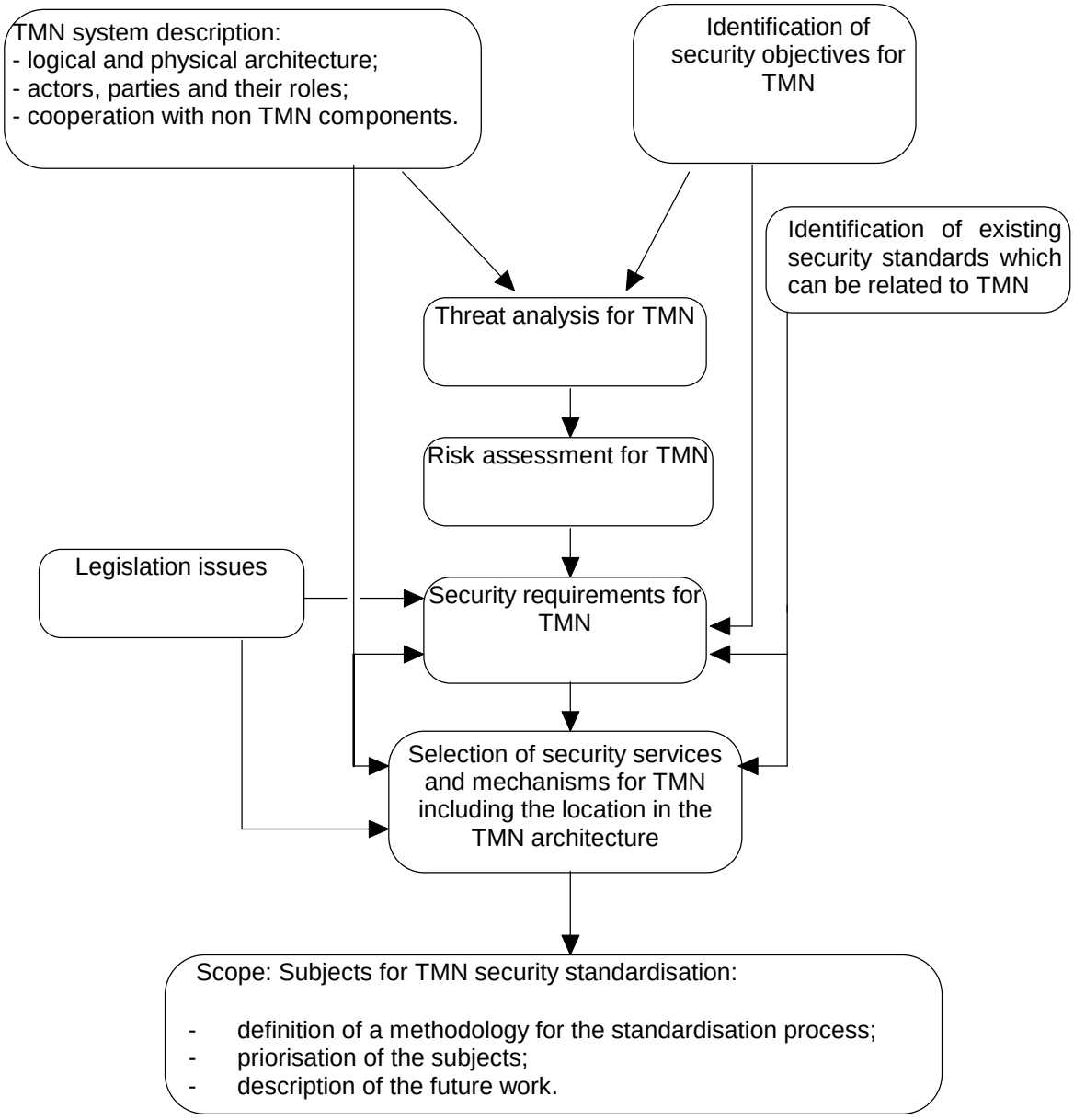

Figure 1: The stepwise process of defining the standardization subject for TMN security

6.1 TMN system description (clause 7)

The logical and physical architecture of a TMN is described, focusing on the following properties:

- functional description of each TMN component and its interfaces;
- provide insight in the physical implementation of each TMN component and the Data Communication Network (DCN), above all describe the assumptions and principles;
- identify the kind of co-operation with non-TMN components, above all describe the assumptions, principles and the possibilities of integration concerning security;
- identify the kind of information which is processed and stored, either permanently or temporarily, and its importance to the correct functioning (integrity) of the TMN component, to the privacy of the subscribers and TMN component users, and to the bearing of an operating company business;

- identify the information flows between the TMN components;

- identify the assets/resources inside a TMN domain in need of protection;

- identify all actors, parties and their roles.

6.2 Security objectives for TMN (clause 8)

The security objectives for TMN describe what should be achieved by applying security to TMN.

6.3 Legislation issues (clause 9)

Legislation issues in form of laws and regulations will have several effects on the security solution for a TMN. In most countries it is for instance required to protect the privacy of system users. The use of cryptographic methods may not be restricted in some countries, while in others they are prohibited or severely restricted.

6.4 Threat analysis and risk assessment for TMN (clause 10)

A potential threat to a TMN is doing no harm unless there is a corresponding weakness in the TMN architecture and until the point in time when the weakness is exploited by an intruder. Thus, a careful analysis of all threats that can be identified should be performed.

Based on the known threats, it is necessary to perform a risk assessment for ranging the threats in order of importance. In evaluating each potential threat, one should attempt to characterise it according to:

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

6.5 Security requirements for TMN (clause 11)

Based on the ordered list of threats as result of the risk assessment, the security requirements for TMN can be specified, i.e. the threats should be converted into security requirements. In addition, the security objectives, the legislation and the procedural issues should be taken into account for specifying security requirements.

6.6 Security services and mechanisms for TMN (clause 12)

For each security requirement a security service will be selected and located into the TMN architecture to fulfil the requirement and counter the threat. For realising a security service a number of security mechanisms can be selected. For selecting security services and mechanisms existing security standards will be taken into account. The selection of a security service and its mechanisms will also be affected by legislation and procedural issues.

6.7 Methodology for TMN security standardization (clause 13)

For the description of the future work on TMN security in ETSI a methodology for the standardization process has been defined.

6.8 Identification of existing security standards (annex A and B)

Currently, a number of ITU-T Recommendations and ETSI standards for security exist. These standards should be evaluated and taken into account for a TMN security solution. Therefore, each of the following steps will be based on general results concerning security as described in existing ITU-T standards. This is part of the methodology as mentioned in the previous subclause.

The steps are:

- which parts of these standards can be reused for TMN;
- how it is possible, to integrate these reusable parts into the TMN architecture; and
- what are new subjects for standardization (in addition to the reusable parts).

6.9 Subjects for TMN security standardization (annex C)

The result of this step-wise approach will be a set of subjects which is going to be standardized. For the description of the future work on TMN security in ETSI it is necessary to prioritise the given subjects for TMN security standardization. Prioritisation will be based on the result of the risk assessment.

7 System description

The purpose of this clause is to provide a TMN system description which can be used as a common ground for specifying security in TMN. Because TMN is a framework, it is not possible to produce a system description in the traditional sense. Still the need of a model to refer to in the process of introducing security is obvious.

The target is an abstraction which makes it possible to avoid the many details of reality 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 Recommendation M.3010 [3]).

7.1 TMN functional architecture

Figure 2 shows the TMN functional architecture in terms of TMN function blocks and TMN reference points. A description of each block and reference point can be found in ITU-T Recommendation M.3010 [3]. The function blocks exchange information using transport mechanisms provided by a Data Communication Function (DCF). The DCF provides functionality equivalent to layers 1 to 3 of the OSI reference model. A Message Communication Function (MCF) is used to connect each functional component to the DCF providing functionality equivalent to layers 4 to 7 of the OSI reference model.

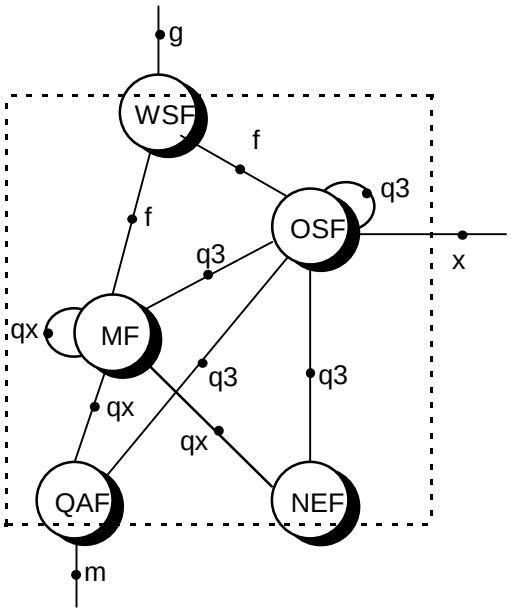

Figure 2: TMN functional architecture

Each function block will be combined from a set of functional components. For security, it is important to note that ITU-T Recommendation M.3010 [3] has defined a functional component called the Security Function (SF) which is optional within each function block.

7.2 TMN information architecture

The TMN information architecture describes the TMN in terms of:

- **the management information model**, which defines the structure of management information and actions that may be performed upon them. Managed Objects (MOs) are used to present an abstract view of resources to be managed. The TMN function blocks provide necessary functionality to perform management operations upon MOs. Each function block, apart from the Work Station Function (WSF), can support a local Management Information Base (MIB);

- **the management information exchange,** which describes mechanisms for communicating management information. All management exchanges support the manager/agent concept realised through the use of Common Management Information Service Element (CMISE) and Common Management Information Protocol (CMIP). Information exchange through the use other Application Service Elements (ASEs), such as File Transfer Access and Management (FTAM), is also possible. At the moment, two application layer contexts are considered for use within the TMN environment:

    - Association Control Service Element (ACSE), Remote Operation Service Element (ROSE), CMISE, Service Management Application Service Element (SMASE); and

    - ACSE, FTAM, SMASE.

7.3 TMN physical architecture

The TMN physical architecture describes the TMN in terms of physical elements (TMN building blocks) and interfaces between them. It is related to the TMN functional architecture as follows:

- **relationship between reference points and physical interfaces:**

    - physical interface will always have a corresponding reference point. A reference point, on the other hand, will not necessarily be implemented as a physical interface;

- **relationship between TMN function blocks and TMN building blocks:**

    - table 1, taken from ITU-T Recommendation M.3010 [3], shows which mappings of TMN function blocks to TMN building blocks that are allowed.

Table 1: Mapping of TMN function blocks to TMN building blocks

	Network Element Function	**Mediation Function**	**Q-interface Adapter Function**	**Operations System Function**	**Work Station Function**
Network Element	M	O	O	O	O
Mediation Device		M	O	O	O
Q-interface Adapter			M		
Operations System		O	O	M	O
Work Station					M
M Mandatory; O Optional.					

7.4 How to apply the TMN architecture models

The important question is which of the three TMN architecture models (functional, information or physical) that, from a security viewpoint, is best suited as a TMN system description.

When selecting security measures for a TMN system, it is obvious that one has to consider its physical realisation. This implies that the TMN physical architecture is relevant. The physical architecture is not

sufficient by itself though, since it only describes the physical distribution of TMN building blocks. It does not describe the TMN assets (i) that has to be protected and how they are distributed (ii) within the physical TMN. This is where the TMN information architecture and the TMN functional architecture come in.

1) For standardization one can identify two types of TMN assets that require security protection:

   - *information*, which includes MOs and management information that is exchanged between TMN building blocks;

   - *Management Application Functions* which result in operations on MOs.

The TMN information architecture provides a framework for defining the information part, while the TMN functional architecture provides a framework for describing management functionality within the TMN.

2) The physical distribution of the TMN assets identified above will depend on:

   - how the TMN assets are related to the TMN functional architecture;

   - how the TMN functional architecture is mapped onto the TMN physical architecture. As can be seen from table 1 in ITU-T Recommendation M.3010 [3] allows numerous possibilities for mapping TMN function blocks onto TMN building blocks. The result is that one specific physical architecture instance may support several different ways of distributing the same TMN assets.

From the considerations above it seems obvious that one has to consider all three TMN architecture models at the same time.

For standardization of security of TMN the following use of the architecture models is recommended:

1) the functional architecture should be used as a reference when relating security to the TMN. The reason is that the functional architecture is a stable reference for locating TMN assets in the sense that it is independent of physical realisation. More specifically, security requirements should be related to the various reference points;

2) different TMN scenarios need to be considered, which will involve different instances of the functional architecture. For each instance, various sets of TMN assets (functions and related information models) will be applicable at a particular reference point. Based on such scenarios it should be possible to derive a set of different security requirements that each TMN reference point should be able to support;

3) if a reference point is not realised as a physical interface, then security measures need not be standardized. **Standardized** security measures will only be used at physical interfaces between TMN building blocks. Security measures for protecting the internal structure of building blocks is out of scope of standardization.

7.5 Architectural scoping

Related to the TMN functional architecture in figure 2 the following simplifications has been chosen:

- to leave the g- and m-reference point out of scope for standardization since it lies outside the TMN;

- to leave the QAF for further study. The QAF is used to connect to the TMN a non-TMN equivalent of an OSF or a NEF. From a security point of view a QAF should be nothing more than a special type of MF. Results achieved from discussing security in connection with MFs might be directly applicable to the QAF.

These simplifications result in the following simplified functional architecture:

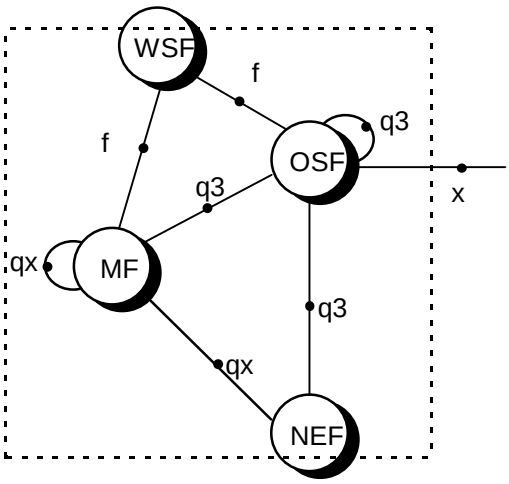

Figure 3: Simplified functional architecture

It is recognised in ITU-T Recommendation M.3010 [3] that TMN building blocks may support other interfaces in addition to the 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 of the TMN and therefore outside the scope of TMN standardization.

7.6 Actors and roles

For the purpose of TMN security standardization, only technical security will be considered, which means that relevant actors to consider are *TMN users*. A TMN user is defined in RACE CFS H210 [4] as a person or process applying TMN management services for the purpose of fulfilling management operations. TMN users can further be categorised dependent on whether they belong to the organisation running the TMN (internal users) or whether they access the TMN as external users.

Each time a TMN user access 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 the most 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.

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

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

7.7 Security domains

ITU-T Recommendation M.3010 [3] introduces the concept of LLA (Logical Layered Architecture) 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 OSF, called an OSF-domain. MFs and 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 is 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 be dangerous 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. It therefore seems more appropriate to define 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:

- q3 (OSF-NEF, OSF-MF, OSF-OSF);
- qx (MF-MF, MF-NEF).

Possible inter-security domain relationships:

- x (OSF-OSF);
- f (WSF-OSF, WSF-MF);
- q3 (OSF-OSF).

Note that the above mentioned relationships refer to security domains and not management domains. An important thing to note is that a q3 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 exist between the involved entities.

8 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. Focus is on what security will achieve rather than how it is done. These generic security objectives form, together with the system description, a basis for threat analysis and risk assessment of the TMN architecture.

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

According to STAG, the Security Technical Advisory Group of ETSI, the description of basic security objectives is one of several steps in requirements capture. STAG states in their document "Security requirements capture":

"Depending on the internal structure and the intended tasks of the system a list of basic security objectives of a very general and generic nature should be defined before any detailed security investigation takes place. Knowing that an absolute secure system is illusory and prohibitively expensive the security objectives definition should give a clear orientation for the succeeding investigations."

Examples of security objectives are anonymity of users or legal acceptability of all orders and invoices.

8.1 Security objectives derived from ITU-T Recommendation M.3010

When looking at security aspects of TMN, one has to consider the purpose of TMN itself which may be expressed as:

- the possibility to achieve interoperability between products of different technology and from different vendors both within the TMN and between the TMNs;

- multi-operator applicability of management solutions and compatibility between operators;
- cost reductions for operation of networks;

- cost reduction for development of management solutions, including the reuse and portability of management applications;

- the basis for efficient customer services including the possibility to allow for customer access to customer related management information (Customer Query and Control).

Of course security should not counteract these objectives but contribute to them.

In ITU-T Recommendation M.3010 [3] the basic objectives for TMN state:

"Security and distributed data integrity are recognised as fundamental requirements for the definition of a generic architecture. A TMN may allow access and control from sources considered outside the TMN (e.g. inter-TMN co-operation and network user access). Security mechanisms may be needed at various levels (managing systems, communications functions, etc.)."

In the TMN architectural requirements ITU-T Recommendation M.3010 [3], the need of security is mentioned explicitly:

"The TMN architecture should provide a certain degree of reliability and security in the support of management functions".

Also some architectural requirements of ITU-T Recommendation M.3010 [3] strongly imply the use of security solutions:

"The TMN architectures should:

- make it possible for customers, value added service providers and other Administrations to access management functions;

- make interworking between separately managed networks possible, so that inter-network services can be provided between Administrations."

8.2 Formulation of security objectives for TMN

A legitimate TMN user is a TMN user who is allowed to perform operation(s) on assets in the TMN.

The security measures taken in a TMN aims to insure that within the TMN and between co-operating TMNs, assets are treated according to rules in force, stating:

- who is authorized to do what to what (subject and object);
- when and where actions are allowed (context);
- what the correct assurance level should be (effectiveness and correctness);
- how actions are monitored; and
- how much it should cost.

Rules may be laws, regulations, business agreements, business practices, company policies, etc.

Thus the *security objectives for 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;
- legitimate actors should only 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, this should be handled in a controlled way, thus minimising the damaged 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.

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

The generic objectives are phrased according the view and language of enterprise management. In the following clauses the 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 security objects for TMN of this subclause will be met:

- confidentiality;
- data Integrity;
- accountability;
- availability.

Threat analysis and risk assessment in clause 10 and functional requirements in clause 11 will be based on these, more formal terms. For definitions see clause 10.

The rest of the objectives deals with the monitoring and control of the security state of the system. They will be dealt with in relevant subclauses of clause 11 on recovery, architecture and security management.

9 Legislation issues

9.1 Introduction

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

9.2 Applicable legislation areas

The following areas of legislation possibly influencing standardization of TMN security have been identified:

- privacy, comprising:
    - "privacy of letter": keeping information exchanged between customers away from 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 third parties;
    - "inspection and correction": the right of the customer to inspect and correct information about himself stored 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 communication between entities in case of a dispute in a court of law.

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

National and international security and 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 co-operate and provide information in case of (criminal) investigations (legal interception).

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.

9.3 Sources of legislation

In the previous subclause legislation was categorised into subjects. In the document "Security Techniques Advisory Group (STAG); A guide to legislation, recommendations and guidelines governing the provisioning of security features" legislation has been categorised into sources for laws and regulations concerning telecommunications security. These sources and their possible influence on TMN security are:

- 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 co-operation 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 for TMN security could be the following: *Specific provisions are needed for confidentiality, integrity and auditing in the interception process;*

- ITU,
  seems to be less relevant for TMN security;

- other international conventions,
  many of these conventions deal with human rights, for telecommunications privacy and secrecy are the most relevant ones. Copyright laws are considered to be not relevant for TMN security;

- national laws,
  applicable laws again deal with privacy, secrecy and legal interception;

- rules issued by the regulator,
  the regulator is the national body (appointed by national law) which is given the authority to issue rules and regulations on the telecommunication area. These rules may include security issues;

- codes of practice,
  agreed policies between telecommunication companies and organisations to deal with security issues. For TMN security these codes of practice might become an important issue when TMNs are connected together.

9.4 Possible consequences for TMN security standardization

Basically for TMN 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 subclauses gave some indication concerning these requirements:

  - necessity to provide a certain level of integrity of the TMN;
  - possibility to support legal interception and access to management data for Justice and Police departments;

- 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.

10 Threat analysis and risk assessment

The purpose of this clause is to provide a threat analysis and risk assessment of TMN. More particularly, a description of main threats and parameters is given, in order to evaluate risks and to choose among some proposed security profiles.

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).

RACE CFS H210 [4] contains a thorough discussion on threats which distinguish between three kinds of threats: An accidental threats is a threat whose origin does not involve any malicious intent. An administrative threat arises from a lack of administration of security. Intentional threats involve a malicious entity which may attack either the communication itself or network resources. The following board presents a general list of security threats according to those definitions. Such a list may be used for describing general security profiles for management networks. For more detail, please refer to RACE CFS H210 [4] (physical and accidental threats which are out of the scope of TMN standardization are printed in italic, administrative threats are left out):

Table 2: Accidental and intentional threats

Accidental threats	Intentional threats
- operational errors; - *transmission errors;* - *network resources failures;* - *network resources overload;* - *natural calamity.*	- masquerade; - eavesdropping; - unauthorised access; - loss or corruption of information; - repudiation; - forgery; *- computer security (viruses, trapdoors, Trojan horses,...);* *- physical attacks;* *- denial of service attacks;* *- corruption of TMN entities;* *- covert channels.*

Accidental threats such as operational errors may be taken into account by TMN standardization work as long as their consequence are the same as intentional threats. In order to give a more accurate analysis of threats, taking into account TMN architecture, we focus on intentional threats involving communication between different actors of TMN. The aim of this approach is to give a shorter list of threats that may be used directly in a standardization work of TMN. A threat analysis of TMN should thus address the following items:

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

- **eavesdropping**: a breach of confidentiality by monitoring communication;

- **unauthorised access**: an entity attempts to access data in violation to the security policy in force;

- **loss or corruption of information**: the integrity of data transferred is compromised by unauthorised deletion, insertion, modification, reordering, 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.

Table 3 gives a map of threats and objectives.

Table 3: Mapping of threats and objectives

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

A potential threat to a system is doing no harm unless there is a corresponding weakness in the system and until the point in time when a weakness is exploited by an intruder. Thus, an analysis of threats do not give an overall view of attacks on a system: some generic weaknesses/vulnerabilities need to be identified. Besides, threat analysis should be part of an iterative process: new threats may emerge when countermeasures are established.

The specification of security requirements will then be based upon an analysis of each threats according to risk assessment. It will depend on the different reference points defined in TMN. The following statements give a first framework for this analysis:

- repudiation is less relevant to Q interface, since all actors in intra-domain activities belong to the same authority;

- threats directed at interface Q and F are quite similar, even if the end user entering the TMN system from a workstation through F interface may be seen as external to the TMN;

- data confidentiality requirements at an interface will depend on the type of data transmitted. A particular emphasis may be set on transmission of accounting data.

In evaluating each threat, one should attempt to characterise it according to cost/effort involved and according to potential benefit/damage that can be done. According to technical reports of STAG ("Security Techniques Advisory Group (STAG): Security requirements capture"), this study may be split into an evaluation of the likelihood of each threat and an evaluation of the impact of such threats against each main TMN objectives. Security requirements and services will then have to be fitted to a given system according to those different parameters: several security-related question cannot be answered for a general TMN framework.

11 Requirements

This clause comprises generic requirements for security, architectural requirements which are relevant for security and requirements for the management of security.

11.1 Introduction

How to approach the requirement issue? There is at least one document ("Security Techniques Advisory Group (STAG); Security requirements capture"), that describes the process of capturing security requirements in addition to the clause concerning methodology in this ETR.

Security requirements are derived by applying the security objectives and a threat analysis and risks assessment to the actual system under development. Security requirements are expressed in technical terms and closely related to the actual system in general and to the configuration of its components in particular. Another significant input to requirements capture is the security policy in force, which accommodates also external conditions, such as legislation and national security issues (e.g. legal interception). The security policy may be in some respects "open ended", i.e. allowing for different options under different circumstances. One example is the strength of cryptographic algorithms to be used depending upon the demand to align with policies of communicating partners/countries.

Security requirements are met by the integration of security services/mechanisms into the system. Although the same word is often used to state security requirements and to identify security services which implement those requirements, one should keep in mind that we deal here with two distinct steps of the design process and a requirement may be met by different combinations of services/mechanisms. As an example, consider the requirement of authorized access to management information. The information being stored in the MIB the services "authentication" and "access control" will satisfy the requirement. When transmitted the information has to be encrypted, hence, the service "confidentiality" will apply to meet the same requirement.

It is important to differ between analysis of a specific system combined with a security policy in force and a general study of a concept or framework like TMN. In the latter case there is no explicitly stated security policy to base the study on, only the generic security objectives. One has to look upon the broad spectra of what might be part of a security policy in order to find components that telecommunication providers may choose from to meet their specific needs in the area. On the other hand, in a co-operative, future scenario, a telecommunication provider cannot choose security level independently. Co-operation imply a basic trust level which may be expressed as a set of baseline security requirements.

Another fact to take into consideration is the existing results available in this area. A lot of resources has been put into requirement capture and these results are still valid. One way to use them is to begin to survey and evaluate existing requirement analyses and to conclude where the focus of TMN security lies. Following the overall objectives stated in clause 5 of this ETR, it is not a purpose at this time to derive new requirements by analysing system or network specific circumstances.

Last it is important to remember that requirements have to be assigned some sort of priorities in order to be useful in the continuing process. However, future work and its scoping is left to the adequate clauses towards the end of this ETR.

The following subclauses 11.2 to 11.5 define and discuss different classes of requirements, subclause 11.6 deals with priorities and subclause 11.7 is an overview of existing results taken into account by this clause.

11.2 Classification of requirements

When discussing security in TMN, requirements do not only mean security requirements. Security solutions also have to take into consideration requirements imposed by the TMN architecture.

In this clause requirements are divided into security requirements, architectural requirements and requirements on management of security.

Security requirements state which security measures should be taken. The following subclause is divided into a functional and an implementation-related part.

The architectural requirements state how security measures should be designed in order to comply with the TMN framework.

The requirements on security management state what management applications should be introduces and how they should be designed in order to provide the security administrator with the proper tools to monitor and to control security services in an effective and correct way.

Administrative and life-cycle requirements, however important, but will not affect the architecture are left outside this subclause.

11.3 Security requirements

Functional and implementation-related security requirements are presented in this subclause. As stated earlier, the requirements are still rather generic. They become more specific when the placement of security functions within the TMN, their strength and granularity , etc. have been specified. This will be done for typical, real world configurations and with regard taken to actual threats, risks and cost considerations.

11.3.1 Functional security requirements

This subclause will allocate functional requirements security functions in order to cover the threats listed in clause 10. This has been done in table 4. From this the security requirements have been mapped to the security objectives stated in clause 8 (table 5). The list is limited to requirements which are generic in nature and have substantial impact on components and architecture.

Table 4: Mapping of functional requirements and threats

Functional requirement	Masquerade	Eaves-dropping	Unauthorised access	Loss or corruption of information	Repudiation	Forgery
Verification of identities	x		x			
Controlled access and authorization			x			
Protection of confidentiality		x	x			
Protection of data integrity				x		
Strong accountability					x	x
Activity logging	x		x		x	x
Alarm reporting	x		x	x		
Audit	x		x		x	x

The objectives used are the four formal ones defined in clause 8, each with a column in the table below, indicating the set of functional requirements to meet the objective in question.

Table 5: 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		
Strong accountability			x	
Activity logging			x	
Alarm reporting	x	x	x	x
Audit			x	x

The functional requirements of tables 5 and 4 are further discussed in the text which follows. One might observe that the requirement for any of these functions does not automatically invoke a security service as defined by ISO. In practice, however, there is a coincidence in some of the cases. These issues will be discussed in more detail in the security profile standards.

Verification of identities

The TMN shall provide capabilities to establish and verify the claimed identity of any actor in the TMN.

The reason for this is to support the other security services and to provide accountability for actions taken. No distinction should be made between persons and inanimate objects.

This is the most important security requirement to a TMN environment. Without a reliable authentication service throughout the TMN, every other effort to secure the system is in vain.

As a base line, strong authentication should be used for O&M staff. Specific attention is needed to the way the work is usually organised, which leads to common passwords and logged on sessions left unattended during breaks and after hours. Single sign on and procedures for take over of sessions will be favoured.

Techniques involving certification authorities and Trusted Third Parties (TTPs) may be used for external access to the TMN like in the case of vendors, VPNs and service providers.

Peer-entity authentication will be made at association-establishment time between entities within the TMN. For example an OSS have to trust the identity of an NE sending a critical alarm.

Note that care should be taken to preserve the confidentiality and integrity of communicated and stored authentication information.

Note also that communications across domains and jurisdictional boundaries should not affect accountability or the possibility to perform effective audits.

Controlled access and authorization

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

There are many reasons for providing access control. Some are obvious to all TMNs like operators with insufficient training should not be able to perform critical actions that may affect the availability to a substantial part of the telecommunication network. Other reasons may be less obvious outside the context of a specific organisation and its policy. The access control policy of any TMN should be part of the security policy of that domain and is outside the scope of this subclause.

In a general study like this, access control is merely a question about what an access control may be based on and what granularity is reasonable.

A security architecture for TMN should not impose any limitations regarding what an access control decision may be based on. At the same time, the architecture should not assume anything about the quality of the information which is available for access control decisions.

The proposed level of granularity is access control on object instances.

Though there is much to say about access control, the rest is left outside this subclause because it is implicitly covered by ITU-T Recommendation X.741 | ISO/IEC 10164-9 [8], Objects and attributes for access control.

Protection of confidentiality

A TMN shall support the capability to keep stored and communicated data confidential.

Beside a service to the other security services, mainly because of the need to handle cryptographic keys, confidentiality is needed to protect the customers and their information. A telecommunication operator holds quite a lot of information about its customers like billing data and statistics.

In the future there may also be a need in Business Layer of TMN interoperability, but today the area is not mature enough to be analysed.

For a TMN the need for confidentiality is relatively low compared to integrity and access control. Large impact on capacity and complexity of key generation and distribution calls for limited use.

Confidentiality is not only a question about cryptographic techniques but also reuse of objects (data objects and media like magnetic tape).

Protection of data integrity

The TMN shall be able to grant the integrity of stored and communicated data.

If this is not met, if it is possible to disturb the management network by damaging or altering its data or management operations, there is a major risk that this will effect the availability of the telecommunication network and cause denial of service to its customers.

The requirement is as important as access control to decrease management network's vulnerability to a deliberate attack.

For example, an attacker may choose to fake a critical but false alarm from a major network element in order to withdraw attention from the real breach.

Since management network also deals with accounting data, integrity techniques may also be the direct means to protect the economical interests of the telecommunication operator and its customers.

Strong accountability

The TMN shall provide the capability that an entity can not deny the responsibility for any of its performed actions as well as their effects.

Any individual (user) in a TMN shall hold the responsibility for any of his/her actions. The individual shall also be aware that he/she can be called to account for possible his/her actions have caused.

Activity logging

The TMN shall 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 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 objects. In implementations of open systems various resources may allocated to store such information. In OSI management these resources are modelled by logs and log records contained in the logs.

The management needs for the type of information that is to be logged may change from time to time. Furthermore, when such information is retrieved from a log the manager, the log manager shall 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.

Alarm reporting

The TMN shall provide the capability to generate alarm notifications on certain adjustable and selective events.

The security alarm reporting function is a systems management functions which may be used by an application process in a centralised or decentralised management environment to exchange information for the purpose of systems management. The security alarm notification defined by this systems management function provides information regarding operational condition and quality of service, pertaining to security.

Audit

The TMN shall provide the capability to analyse and exploit logged data on security relevant events in order to check them on violations of the system security policy.

An audit is to 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, to detect breaches in security and to recommend any indicated changes in control, policy and procedures (ITU-T Recommendation X.800 | ISO 7498-2 [9]).

11.3.2 Computer security and implementation aspects

In addition to security functionality, it is essential that the software and hardware environment of the implemented security functions maintains the requested level of security. Some of the more important components in this respect are the correct configuration of operating systems and the elimination of system defects. Recommendations considering hardware versus software implementations of vital parts of the security system, such as cryptographic facilities and key storage, are another important area.

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.

11.3.3 Security recovery

The TMN shall be able to recover from attempted breaches on security.

Whenever a attempt to breach 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.

11.3.4 Architectural requirements

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

RACE CFS H210 [4] lists some requirements that has to be satisfied by the security measures taken to fit in to the TMN framework. The most important are:

- measures should be based on the principles of the functional model;
- measures should conform to the object oriented data and information model of TMN;
- measures should be applicable to all kinds of TMN domains in the public and private sector;
- solutions should be scaleable to fit small and large TMNs;
- solutions should include 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.

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

11.3.5 Requirements on management of security

A TMN shall contain information models and management capabilities for the services applied to secure the TMN.

STAG presents in "Security Techniques Advisory Group (STAG); Guidelines for Security Management Techniques" an introduction and guide for standards development on how to identify security management components and operations that are necessary to monitor and control security features in a system. Objectives for targets of security management are presented at three different levels of a telecommunications system, corresponding to the management of systems security, security services and security mechanisms, respectively.

11.4 Priority of requirements

The set of requirements will not be useful unless requirements are given priority. There is a need to differentiate between possible requirements and baseline requirements. For inter working between TMNs there is a need to standardize a minimum level of security in order to build trust between the domains. One way of doing that is to classify how important a requirement on a service is.

Priority issues are treated in clause 13 of this ETR.

11.5 Existing results

Starting with a survey of existing results in the area, there are four important sources of requirements, originating from RACE and ANSI. With some difficulty RACE CFS H210 may be pointed out as the main source due to its broader scope.

11.5.1 ANSI T1.233-1993 OAM&P - security framework for TMN interfaces [5]

This approved American National Standard states top level requirements on security in TMN and how a TMN should meet these requirements by conforming to certain ISO security standards.

ISO standards are pointed out for peer-entity authentication, access control, security alarm and security audit trail.

Data integrity, data confidentiality and non-repudiation are left for further study. In other words the document is not complete in its present version.

11.5.2 ANSI T1.XXX-199X OAM&P - baseline security requirements for TMN [6]

This standard **proposal** contains a breakdown of the high level requirements stated in the above mentioned "Security Framework".

The detailed requirements are not approved yet and are subject to change.

This document introduces the idea of a set of standardized baseline requirements in order to build trust over the X-interface.

Baseline Security Requirements for TMN is a detailed and straight forward set of requirements on secure management of telecommunications.

11.5.3 RACE IBC CFS H210 TMN security architecture [4]

The specification describes threats and security aspects from several TMN viewpoints.

RACE CFS H210 is an ambitious, overall study of security in TMN. Not only security requirements are described but also architectural requirements that have to be satisfied by a TMN security architecture.

The underlying threat analysis leads to both an analysis of security in the different functional areas and one analysis of requirements related to the functional architecture.

RACE CFS H210 is not a source that one "complies" with because it does not choose any solutions. It merely points out the possibilities and alternatives. For example, it does not state the difference in priority between significant requirements for authentication and the more redundant need for non-repudiation. RACE CFS H210 is a useful checklist to follow when it comes to completion or validation of a security architecture for TMN.

11.5.4 RACE IBC CFS H211, security of service management [7]

Even though the scope of the CFS is limited to the service management level of TMN and concentrates mainly on interfaces external to the TMN results may be reused for other parts as well.

H211 lists security requirements stated by different functional areas on different sides of the interfaces. The list of requirements are not complete but useful.

H211 also identifies the concepts of functional profiles.

12 Security services, functional classes and security management

12.1 Introduction

This clause describes the security services which are likely be used to counteract threats to TMN services and data. Its goal is to identify which questions exist with regard to security services which have to be answered to be able to do standardization of security in TMN. The following approach has been chosen:

In the first subclause the basic set of services is described related to the security requirements of the clause 11. The basic set of security services has been derived from the RACE CFS H.210 [4] and H.211 [7], the services themselves are those defined in ITU-T Recommendation X.800 | ISO 7498-2 [9].

In the next subclause for each of the security services is described their applicability for use in the different layers of the OSI model for the TMN case.

The subsequent subclause on functional classes and security sub-profiles describes sets of security services. The goal of defining and using this classes and profiles is to limit the possible choices of combinations of security services. A number of sets is defined to be able to deal with different levels of functionality of security.

12.2 Security requirements and security services

This subclause lists, using the requirements defined in clause 11, the security services which are used to fulfil these security requirements. Table 6 gives an overview of the relationship between requirements as listed in clause 11 and security services. This subclause only defines the security services which are covered by standard solutions, possible other services (e.g. detection of denial of service) are left out. The security alarm, audit trail and recovery service is in the next subclauses only mentioned at the accountability service.

Table 6: Mapping of security requirements and security services

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
Protection of confidentiality - transferred data	confidentiality
Protection of data integrity - stored data	access control
Protection of data integrity - transferred data	integrity
Strong Accountability	non repudiation
Activity logging	security alarm, audit trail and recovery
Alarm reporting	security alarm, audit trail and recovery
Audit	security alarm, audit trail and recovery
(All)	security alarm, audit trail and recovery

12.2.1 Requirement: verification of identities

The TMN shall provide capabilities to establish and verify the claimed identity of any actor in the TMN.

To deal with identification and authentication the following security services should be made available:

- **user authentication**

  User authentication delivers corroboration of the identity of the (human) user.

- **authentication**

  The authentication service delivers proof that the identity of an object or subject is indeed the identity it claims to have. This service is used to counter masquerade or replay attacks. It can be divided into two kinds:

  - peer entity authentication, establishing proof of the identity of the peer entity at one particular moment in time during a communication relationship;

  - data origin authentication, establishing proof of identity of the peer entity responsible for a specific data unit.

Usage of an authentication services establishes the proof for that particular instant of time. To ensure continued proof of authentication the authentication has to be repeated or it has to be linked to an integrity service.

12.2.2 Requirement: controlled access and authorization

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

Security services to meet this requirement:

- **access control**

  The access control service provides means to ensure that (stored) objects are accessed by subjects only in an authorized manner. Objects concerned may be the physical system, the system software, applications and data. The limitations of access to these objects are laid out in access control information, which specify:

  - the means to determine which entities are authorized to have access to an object;
  - what kind of access is allowed (reading, writing, modifying, creating, deleting).

  More specific for TMN access control can be divided in 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. No distinction is possible between objects the association applies to.

  - 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 managed objects themselves.

Granting access to objects needs checking of the identity of the entity trying to gain access. This means that usage of access control is always linked to the usage of an authentication service.

12.2.3 Requirement: protection of confidentiality

A TMN shall support the capability to keep stored and communicated data confidential.

The security services to support this requirement are:

- **Stored data: access control**

  See subclause 12.2.2.

- **Communicated data: Data confidentiality**

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

  - selective field confidentiality;
  - connection confidentiality.

12.2.4 Requirement: protection of integrity

The TMN need to be able to grant the integrity of stored and communicated data.

Security services can be divided in services for the integrity of stored data and services for the integrity of communicated data:

- **Stored data: access control**

  See subclause 12.2.2.

- **Communicated data: data integrity**

  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.

12.2.5 Requirement: strong accountability

The TMN shall provide the capability that an entity can not deny the responsibility for any of its performed actions as well as their effects.

Supported by the following services:

- **non repudiation**

  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.

12.2.6 Requirements: activity logging, alarm reporting and audit

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

The TMN shall provide the capability to generate alarm notifications on certain adjustable and selective events.

The TMN shall provide the capability to analyse and exploit logged data on security relevant events in order to check them on violations of the system security policy.

The TMN shall be able to recover from attempted breaches on security.

These requirements are supported by the security service:

- **security alarm, audit trail and recovery**

12.2.7 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 increase 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 an implementation point of view). Deliberate attacks on availability are not considered.

12.2.8 Security services and OSI layers

This subclause describes by which layer (to a higher layer) the services as described in the previous subclause can be provided in a meaningful way for TMN purposes. It is assumed that if a layer provides a security service this service is provided to the layer above the considered layer. The provision of services by layers laid out in ITU-T Recommendation X.800 | ISO 7498-2 [9] is used as a basis to limit the possibilities.

user authentication

This service is depending on interaction with the user. It is therefore outside the OSI model.

authentication (peer entity and data origin)

Layers by which this service normally can be provided (according to ITU-T Recommendation X.800 | ISO 7498-2 [9]) are:

- 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 model: in the application process itself.

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

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.

- 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.

security alarm, audit trail and recovery

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

integrity

- selective field integrity.

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

- connection integrity 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.

confidentiality

- selective field confidentiality.

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

- connection 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.

non repudiation

- non repudiation - proof of sending;
- non repudiation - proof of delivery.

  This services can be used in the application layer or in the application process itself.

This is summarised in table 7:

Table 7: Linking security services and OSI reference model

	Layers						
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 confidentiality	-	-	+	+	-	+	+
non repudiation - proof of sending	-	-	-	-	-	-	+
non repudiation - proof of delivery	-	-	-	-	-	-	+

12.3 Functional classes and security sub-profiles

12.3.1 Grouping of security measures

Security measures can be grouped into "Functional Classes" (FC). This has also been proposed in RACE CFS H211 [7], but 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.

The use of FCs in the interdomain case

It is a requirement that security of a particular TMN is not negatively influenced as a result of interdomain activities. The rules for domain interaction should be defined in an interdomain 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.

The use of FCs in the intradomain case

In the intradomain case functional classes can facilitate the definition of security. According to RACE CFS H211 [7], FCs also can 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 Information Technology Security Evaluation Criteria (ITSEC).

It is for discussion if for the purpose of interdomain interaction one operator can require the application of a particular FC for the intradomain 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. Requiring a minimum internal security level 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 FCs.

12.3.2 Functional classes

Functional classes are used to define a concise group of security services aimed at meeting a certain security level. This subclause works out a set of functional classes which serves as an example how functional classes can be defined. It is not meant to be the final set to be used in any forthcoming specification.

In RACE CFS H211 [7] functional classes *for the X-interface* are proposed at three distinct security levels:

1) minimal functional class;
2) basic functional class;
3) advanced functional class.

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 defined are built on the classes from RACE CFS H211 [7], but they are changed in the following ways:

- RACE CFS H211 [7] defines functional classes only for the X-interface, the classes should also include the Q interfaces;
- data origin authentication without integrity is not very useful;
- confidentiality is supposed to be a 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.

The following table (derived from RACE CFS H211 [7]) provides an overview of the FCs.

Table 8: FCs 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 strong 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; - Sslective 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 interdomain case and FCs for the intradomain case. The requirements will be different in both cases and for that reason also the security measures might be different.

To find out which FCs are needed and relevant the next part gives an overview of the different cases.

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 (intradomain);

2) FCs defined by a domain authority and applicable to the domain interactions (interdomain). This 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 a FC is for further study.

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

Also can be thought of a trade off between the different cases, e.g., when the interdomain 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 a FC represents a minimum set of security measures that can be extended with additional measures as is appropriate.

12.3.3 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.

12.4 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.

13 Methodology for security standard elaboration

The process of TMN security standardization shall be made as efficient as possible. It shall therefore follow the methodology as described below. This methodology will guide one through the standardization process step by step.

The figure illustrates the main steps in this standardization process. In the following each step will be described:

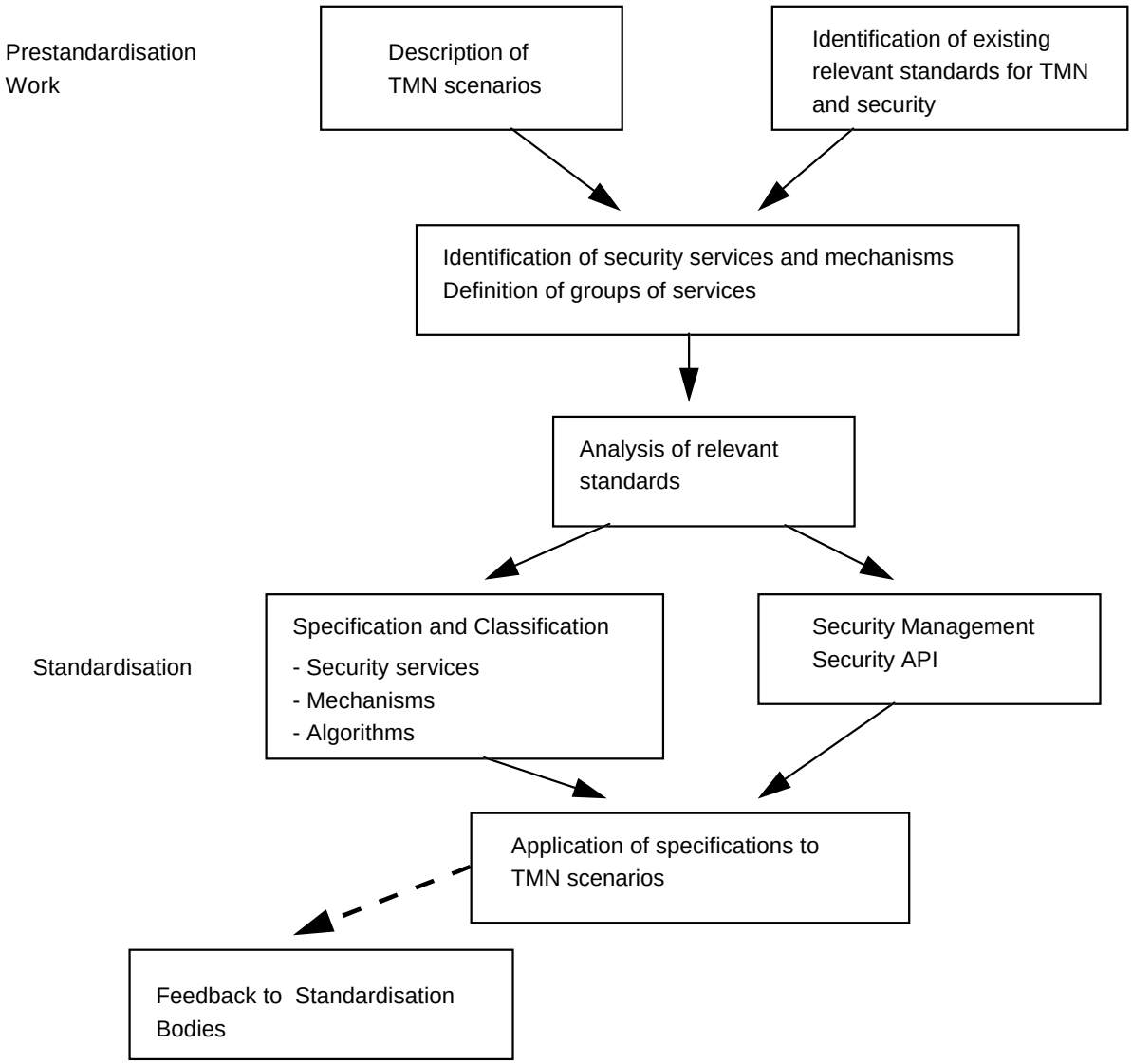

Figure 4: Methodology for EN elaboration

The EN elaboration is based on the scope of the future standardization work as described in the previous clause. The EN elaboration will be divided into two major steps:

- the pre-standardization work; and
- the standardization work.

The **pre-standardization work** includes:

- the description of TMN scenarios;
- the identification of existing relevant standards for TMN and security;
- the identification of security services and mechanisms; and
- the analysis of relevant standards.

13.1 Description of TMN Scenarios

As proposed in subclause 7.4, different TMN scenarios shall be described as a basis for security services needed. These scenarios shall include intra-security and inter-security domains (as described in subclause 7.1).

For each scenario, trusted relationships between TMN function blocks will be identified.

13.2 Identification of existing relevant standards for TMN and security

For each security service existing standards concerning the service and its related security mechanisms will be identified.

13.3 Identification of security services and mechanisms

Based on the TMN scenarios, the security services and mechanisms needed for TMN security will be identified. Security services that will use the same mechanism shall be arranged in a service group. For each service group the existing standards concerning services and mechanisms are identified (relevant standards). If possible, security mechanisms of different strength will be determined for each service group.

13.4 Analysis of relevant standards

It shall be verified, that the various existing standards identified to be relevant for TMN security are described in a complete, correct and uniform way. If not, the respective existing standard shall be revised.

An analysis will be made of the standards and how they apply to TMN security.

The **standardization work** includes:

- specification and classification of security services, mechanisms and algorithms;
- security management and security API;
- application of specifications to TMN scenarios; and
- feedback to standardization bodies.

13.5 Specification and classification of security services, mechanisms and algorithms

For each service group the relevant security services (including association context management), mechanisms and algorithms are specified by profiling the (revised) existing standards, if possible. To facilitate the selection of equivalent mechanisms for the various service groups, security classes may be used. Each security class contains mechanisms of the same strength for the various service groups.

Security mechanisms, which will protect the communication links or which will provide end-to-end connections, will be integrated into the existing TMN protocols. Therefore, existing security features of the protocols and/or existing standardized security protocols (for example GULS) will be profiled, if possible.

13.6 Security management and security API

The management of the security services, mechanisms and algorithms is described by profiling the (revised) existing standards, if possible.

If system internal APIs shall be included in TMN security standardization, these APIs should be specified by profiling (revised) existing standards, if possible.

13.7 Application of specifications to TMN scenarios

The specifications will be applied to the TMN scenarios by assigning the services and mechanisms to the function blocks and / or TMN reference points. As mentioned in subclause 7.5 the reference points g and m will be left out of the scope of standardization since they are lying outside the TMN.

To simplify the security administration and to minimize the performance impairment caused by the security mechanisms, each security measurement shall be executed in a TMN only once (for example: single login). If trusted relationships between TMN function blocks are existing (see subclause 14.1), a function split between equivalent security mechanisms will be defined.

13.8 Feedback to standardization bodies

If an existing standard needs to be revised, the respective standardization body should be informed.

Annex A: Relevant standards

This list gives possibly applicable standards and recommendations. The list is not considered exhaustive.

- IEEE Std 802.10-1992, IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS). (Currently only contains: IEEE Std802.10b-1992, Secure Data Exchange (SDE) (Clause 2)).

- ITU-T Recommendation X.800 | ISO 7498-2 (1989): "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

- ISO 8649 (1988): "Information processing systems - Open Systems Interconnection - Service definition for the Association Control Service Element".

- ISO 8649 (1988): "Information processing systems - Open Systems Interconnection - Service definition for the Association Control Service Element Amendment 1:1990 Authentication during association establishment".

- ISO 8649 (1988): "Information processing systems - Open Systems Interconnection - Service definition for the Association Control Service Element Amendment 2:1991 Connectionless-mode ACSE Service".

- ISO 8650 (1988): "Information processing systems - Open Systems Interconnection - Protocol specification for the Association Control Service Element".

- ISO 8650 (1988): "Information processing systems - Open Systems Interconnection - Protocol specification for the Association Control Service Element Amendment 1:1990 Authentication during association establishment".

- ITU-T Recommendation X.217 | ISO 8649 (1996): "Information processing systems - Open Systems Interconnection - Service definition for the Association Control Service Element".

- ITU-T Recommendation X.227 | ISO/IEC 8650-1 (1996): "Information technology - Open Systems Interconnection - Connection-oriented protocol for the Association Control Service Element: Protocol specification".

- ITU-T Recommendation X.237 | ISO/IEC 10035-1 (1995): "Information technology - Open Systems Interconnection- Connectionless protocol for the Association Control Service Element: Protocol specification".

- ISO 8731-1 (1987): "Banking - Approved algorithms for message authentication - Part 1: DEA".

- ISO 8731-2 (1992): "Banking - Approved algorithms for message authentication - Part 2: Message authenticator algorithm".

- ITU-T Recommendation X.501 | ISO/IEC 9594-2: "Information technology - Open systems interconnection - The directory: Models".

- ITU-T Recommendation X.509 | ISO/IEC 9594-8: "Information technology - Open systems interconnection - The directory: Authentication framework".

- ISO/IEC 9796 (1991): "Information technology - Security techniques - Digital signature scheme giving message recovery".

- ISO/IEC 9797 (1994): "Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm".

- ISO/IEC 9798-1 (1991): "Information technology - Security techniques - Entity authentication mechanisms - Part 1: General model".

- ISO/IEC 9798-2 (1994): "Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms".

- ISO/IEC 9798-3 (1993): "Information technology - Security techniques - Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm".

- ISO/IEC 9798-4 (1995): "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".

- ISO/IEC 9979 (1991): "Data cryptographic techniques - Procedures for the registration of cryptographic algorithms".

- ISO/IEC 10118-1 (1994): "Information technology - Security techniques - Hash-functions - Part 1: General".

- ISO/IEC 10118-2 (1994): "Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher algorithm".

- ITU-T Recommendation X.736 | ISO/IEC 10164-7 (1992): "Information technology - Open Systems Interconnection - Systems Management - Part 7: Security alarm reporting function".

- ITU-T Recommendation X.740 | ISO/IEC 10164-8 (1993): "Information technology - Open Systems Interconnection - Systems Management - Part 8: Security audit trail function".

- ITU-T Recommendation X.741 | ISO/IEC DIS 10164-9 (1993): "Information technology - Open Systems Interconnection - Systems Management - Part 9: Objects and Attributes for Access control".

- ITU-T Recommendation X.810 | ISO/IEC DIS 10181-1: "Information technology - Open Systems Interconnection - Security Frameworks for Open Systems: Overview".

- ITU-T Recommendation X.811 | ISO/IEC DIS 10181-2: "Information technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 2: Authentication Framework".

- ITU-T Recommendation X.812 | ISO/IEC DIS 10181-3: "Information technology - Open Systems Interconnection - Security frameworks in open systems - Part 3: Access control".

- ITU-T Recommendation X.813 | ISO/IEC DIS 10181-4: "Information technology - Open Systems Interconnection - Security frameworks in Open Systems - Part 4: Non-repudiation".

- ITU-T Recommendation X.814 | ISO/IEC DIS 10181-5: "Information technology - Security frameworks in open systems - Part 5: Confidentiality".

- ITU-T Recommendation X.815 | ISO/IEC DIS 10181-6: "Information technology - Security frameworks in open systems - Part 6: Integrity"

- ITU-T Recommendation X.816 | ISO/IEC DIS 10181-7: "Information technology - Open Systems Interconnection - Security Frameworks for Open Systems: Security Audit Framework".

- ISO/IEC ISP 11183-1 (1992): "Information technology - International Standardized Profiles AOM1n OSI Management - Management Communications - Part 1: Specification of ACSE, presentation and session protocols for the use by ROSE and CMISE".

- ISO/IEC ISP 11183-2 (1992): "Information technology - International Standardized Profiles AOM1n OSI Management - Management Communications - Part 2: CMISE/ROSE for AOM12 - Enhanced Management Communications".

- ISO/IEC ISP 11183-3 (1992): "Information technology - International Standardized Profiles AOM1n OSI Management - Management Communications - Part 3: CMISE/ROSE for AOM11 - Basic Management Communications".

- ITU-T Recommendation X.273 | ISO/IEC 11577: "Information technology - Open Systems Interconnection - Network layer security protocol".

- ITU-T Recommendation X.274 | ISO/IEC 10736: "Information technology - Telecommunication and information exchange between systems - Transport layer security protocol".

- ITU-T Recommendation X.830 | ISO/IEC DIS 11586-1: "Information technology - Open Systems Interconnection - Generic Upper Layers Security - Part 1: Overview, Models and Notation".

- ITU-T Recommendation X.831 | ISO/IEC DIS 11586-2: "Information technology - Open Systems Interconnection - Generic Upper Layers Security - Part 2: Security Exchange Service Element (SESE) Service Definition".

- ITU-T Recommendation X.832 | ISO/IEC DIS 11586-3: "Information technology - Open Systems Interconnection - Generic upper layers security: Security Exchange Service Element (SESE) protocol specification".

- ITU-T Recommendation X.833 | ISO/IEC DIS 11586-4: "Information technology - Open Systems Interconnection - Generic upper layers security: Protecting transfer syntax specification".

- ISO/IEC DISP 12059-8: "Information technology - International Standardized Profiles - OSI Management - Common information for management functions - Part 8: Security audit trail".

- ISO/IEC DISP 12060-6: "Information technology - International Standardized Profiles - OSI Management - Management functions - Part 6: Security management capabilities (including profiles AOM2421, AOM2422 and AOM2423)".

- ITU-T Recommendation X.802 | ISO/IEC 13594: "Information technology - Lower layers security model".

- ITU-T Recommendation X.803 | ISO/IEC 10745: "Information technology - Open Systems Interconnection - Upper layers security model".

- ECMA TR/46: "Security in Open Systems: Security Framework for the Application Layer of Open Systems".

- ECMA 138: "Security in Open Systems: Data Elements and Service Definitions".

- ECMA 206: "Association Context Management including Security Context Management".

- ECMA 219: "Authentication and Privilege Attribute Security Application with related key distributed functions".

- ECMA 235 "The ECMA Generic Security Service Application Programming Interface".

- RFC1508: "Generic Security Service Application Programming Interface".

- RFC1421: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. February 1993".

- RFC1422: "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management. February 1993".

- RFC1423: "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers. February 1993".

- RFC1424: "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services. February 1993".

- RFC1446: "Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)".

- X/Open CAE Specification C441: "Generic Security Service API (GSS-API) Base (formerly P308 GSS-API, 1/94)".

- X/Open Snapshot S307: "GSS-API Security Attribute and Delegation Extensions".

- "OIW Stable Implementation Agreements for Open Systems Interconnection Protocols: Part 12 - OS Security".

Annex B: Bibliography

- Department of Defence Trusted Computer System Evaluation Criteria, DoD 5200, 28-ST, (Orange Book), 1985.

- Information Technology Security Evaluation Criteria (ITSEC), version 1.2, June 1991.

- ANSI: "OAM&P - Security Requirements for Electronic Bonding Between Two TMNs".

- Race CFS H407: "Management of Security".

- Race CFS H411: "Security Aspects of Information exchanges".

- TCRTR 038: "Security Techniques Advisory Group (STAG): A Guide to the ETSI Security Standards Policy".

- TCRTR 049: "Security Techniques Advisory Group (STAG): Security Requirements Capture".

- TCRTR 028: "Security Techniques Advisory Group (STAG): A glossary of security terminology".

- TCRTR 037: "Security Techniques Advisory Group (STAG): Requirement specification for an Encryption Algorithm for Operators of European Public Telecommunication Networks".

- ETG (EWOS Technical Guide) 48 Rev1: "Application of Security Specifications in Functional Profiling", EWOS, February 1996.

- ETG 54: "Specification of Security Aspects in Functional Profiles", EWOS, September 1995.

Annex C: Scope of the first phase of standardization work in ETSI and EWOS

C.1 Introduction

This annex is intended to give a scope for the work for the first phase of standardization of the security of TMN. It means that the security functions described below are considered to be the most important to be available in a standardized way as soon as possible. There are four areas in which a decision is taken:

1) the set of security services which is going to be standardized;
2) the interfaces of a TMN system for which security is to be standardized;
3) the application part of the protocols in which security will be integrated;
4) the set of security mechanisms which is going to be standardized.

C.2 Security services

In clause 12 a number of security functional classes have been defined for application in the TMN environment. From these classes one should be chosen for the first phase of TMN security standardization. The following criteria have been applied in the selection:

1) the class should be balanced in functions: not too ambitious but also not too weak and therefore unusable; translated into standardization it means that a specification should be delivered within a reasonable time and it should have sufficient functionality;

2) it should match reasonable/most applicable requirements and counter appropriate threats;

3) it should be able to handle the services which are going to be the first ones offered to network operators and/or customers.

With regard to security services as a criteria for scoping, some security services are considered to be less important than others. According to clause 11 on requirements this is the case for confidentiality and non-repudiation. Table 9 lists the priorities of the different security services. Please note that the priority assigned is for the **first phase of standardization work** and not a priority for requirements. For the non-repudiation of sending service the work in the first phase will not include the distribution and management of certificates. If the time schedule and available manpower allows the lower priority items will be covered also in this first phase.

Table 9: Standardization priority for security services

security service	priority
user authentication	high
peer authentication	high
data origin authentication	high
access control	high
integrity	high
security alarm, audit trail and recovery	high
confidentiality	medium
non-repudiation of origin	high
non repudiation of delivery	low

The FC (clause 12) which actually fits this table best is class number 2. To limit the amount of work the selective field integrity services will be left out.

C.3 Mapping of security services on TMN architecture

This clause describes interfaces for which security is going to be standardized. Interfaces inside a TMN and to the outside world have been described in clause 7. They can be divided into two categories:

1) interface to external world (i.e. X interfaces):

- other network operators;
- customer networks;

2) interfaces to internal world (Q3, Qx, F interfaces).

Clause 11 identifies a difference with respect to the security requirements on the two categories of TMN interfaces for the requirement of accountability: the X-interface may more often require a non-repudiation service. This means that there is only a small difference between the interfaces, which could influence the prioritization of the first phase of standardization; this difference is considered to be too small to decide for one of the two interfaces. Any differences in security functionality between interfaces will result from the sensitivity of the data accessible through a particular interface and the actions possible on this interface. These differences are not especially present between different types of interfaces but can also be present between two interfaces of the same type; one Q3 interface may therefore require a different set of security services than an other Q3 interface.

In general it is the security policy which decides which measures are to be taken on a certain interface - a security policy which can result in a different set of services/mechanisms for each interface. The services and mechanisms available on the different interfaces can be the same, but to accommodate different sets for each service mechanisms of different strength will be specified. From this pool of different mechanisms a certain set can then be chosen to accommodate the applicable security policy.

Conclusion is that no priority with respect to interfaces will be set: the specified security services will be applicable to both the Q3 and X interface.

C.4 Application protocols

The TMN security standardization will consider as a first priority the usage of certain application level protocols in the TMN. These protocols are:

1) CMIP;
2) FTAM.

C.5 Security mechanisms

One of the general conclusions of this ETR is that no statements can be made on the sensitivity of data and actions available on a particular instance of a TMN interface. This means that the mechanisms which are to be specified should be able to support different levels of strength of security.

When specifying mechanisms of different strength, care should be taken that the levels of mechanisms supplying different services should match. The mechanisms should therefore be standardized in such a way that they can easily be combined in a coherent set which supplies a certain level of security.

Such a set combined with the functional class is defined as a *security profile*.

C.6 Conclusions

The conclusions with respect to scoping of the standardization work are:

- priority for standardization will be given to the following security services:

    - user authentication;
    - peer authentication;
    - data origin authentication;
    - access control;
    - integrity;
    - security alarm, audit trail and recovery;
    - non repudiation of origin;

- no priority is given with respect to interfaces;
- application protocols given priority are CMIP and FTAM;
- security mechanisms will be specified in different levels of strength.

History

Document history	
January 1997	First Edition

ISBN 2-7437-1159-0
Dépôt légal : Janvier 1997