# ETSI TECHNICAL REPORT

**ETR 340**

**December 1996**

Source: ETSI TC-NA/STAG

Reference: DTR/NA-002609

ICS: 33.020

**Key words:** Security, management

# Telecommunications Security; Guidelines for security management techniques

**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

Blank page

## Foreword

This ETSI Technical Report (ETR) has been produced by the Network Aspects Security Techniques Advisory Group (NA/STAG) 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.

Blank page

# 1 Scope

This ETSI Technical Report (ETR) is an introduction and guide on how to identify security management functions that are necessary to monitor and control security functions in a system. It also recommends where to allocate standardization tasks in order to develop specifications for those functions. Objectives for and targets of security management are presented at three different levels of a telecommunications system, corresponding to systems security, security services and security mechanisms.

A comprehensive treatment of detail specifications is beyond the scope of this document, but some examples of managed attributes and associated management operations are included for authentication and key management. Further information on this topic can be found in RACE Common Functional Specification H407 [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] ISO 10040 (1991): "Open Systems Interconnection, Systems Management Overview".

[2] ISO 10164 (1991): "Open Systems Interconnection, Systems Management".

[3] ISO 10165-4 (1991): "Open Systems Interconnection, Part 4: Guideline for the Definition of Managed Objects".

[4] ISO 7498-4: "Management Framework for OSI".

[5] ISO 7498-2: "Information Processing Systems-Open Systems Interconnection-Basic Reference Model-Part 2: Security Architecture".

[6] RACE Common Functional Specification H407: "Management of Security".

[7] ISO DIS 10181-2: "Open Systems Interconnection-Security Frameworks for Open Systems: Authentication Framework".

[8] ISO 11770-1: "Key Management-Part 1: Key Management Framework".

[9] ISO 10736: "Transport Layer Security Protocol".

[10] IEEE 802.10D: "LAN Security: Key Management Protocol".

[11] ETR 237: "Security Technical Advisory Group (STAG); Baseline security standards; Features and mechanisms".

[12] ISO 10164-8: "Security Audit Trail Function".

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

[14] ETR 336: "Telecommunication Management Network (TMN); Standardization of security for the TMN".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of this document, the security-related definitions given in ETR 232 [13] apply.

## 3.2 Abbreviations

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

| | |
|---|---|
| API | Application Programming Interface |
| CMIP | Common Management Information Protocol |
| CMIS | Common Management Information Service |
| GSM | Global System for Mobile communication |
| IF | Interface |
| MO | Managed Object |
| OSI | Open System Interconnection |
| PIN | Personal Identification Number |
| TLSP | Transport Layer Security Protocol |
| TMN | Telecommunication Management Network |
| UPT | Universal Personal Telecommunications |

# 4 Introduction

There is an increasing demand for the availability of telecommunication services on a European and global scale. Local and national, public and private networks and systems from different vendors are being integrated in order to meet the requirements. One crucial aspect of this process is the integration and interworking of network management.

Standards are necessary at different levels and in different parts of telecommunications systems. Normative work is in progress in the management area, both within ETSI, ISO and the ITU. A common management architecture and information model is defined for all classes of management by ISO (ISO 10040 [1], ISO 10164 [2], ISO 10165-4 [3]). The common infrastructure has been applied and further developed for the networking environment by ETSI and ITU in the standards for Telecommunication Management Network (TMN) (see ETR 336 [14]).

Security management is one functional area within telecommunication management. As stated in ISO 7498-4 [4] the purpose of security management is to support the application of security policies by means of functions which include the creation, deletion and control of security services and mechanisms; the distribution of security-relevant information and the reporting of security-relevant events. Security management functionality provides the means for the security manager to monitor and control information, functions and events that are relevant for security.

In addition to OSI management and TMN specifications, which cover all generic parts of management, standardization has to address also specific aspects of security management.

At the system level the main objectives are to select and specify the security management information and operations necessary to implement the overall security policy, to monitor and control the security state of the system and to react to emergency situations in the security context. Security management operations are covered in clause 5 of this document.

At the service/mechanism level there are a number of attributes and parameters which need to be accessible by management for the sake of monitoring, maintenance and control. These attributes and parameters are specified in managed objects. Managed security objects are further discussed in clause 6.

Security management information and operations are specified in system level standards, like GSM and UPT, while managed security objects are included in standards which define security services and mechanisms, such as authentication, access control and key management. These security specific components, together with the management infrastructure, provide the capability of security management. The corresponding allocation of standardization tasks will be discussed in clause 8 in more detail.

Clause 7 presents an overview of common tools and procedures that help the security administrator to initialize security functions, assess the security state of the system and handle security incidents.

Figure 1 shows the relation between different management and security components. It is important to make the distinction between security management and the protection of management operations, i.e. the security of management. The selection and integration of security measures to protect management belongs to the system specification and design process. Examples are the authentication of operators and controlled access to network assets. The protection of security management requires special attention. As an example, consider the handling of secret information (e.g. keys) for authentication and for encryption services. If the protection of this part of security management is lost, the security of all management information may become compromised.

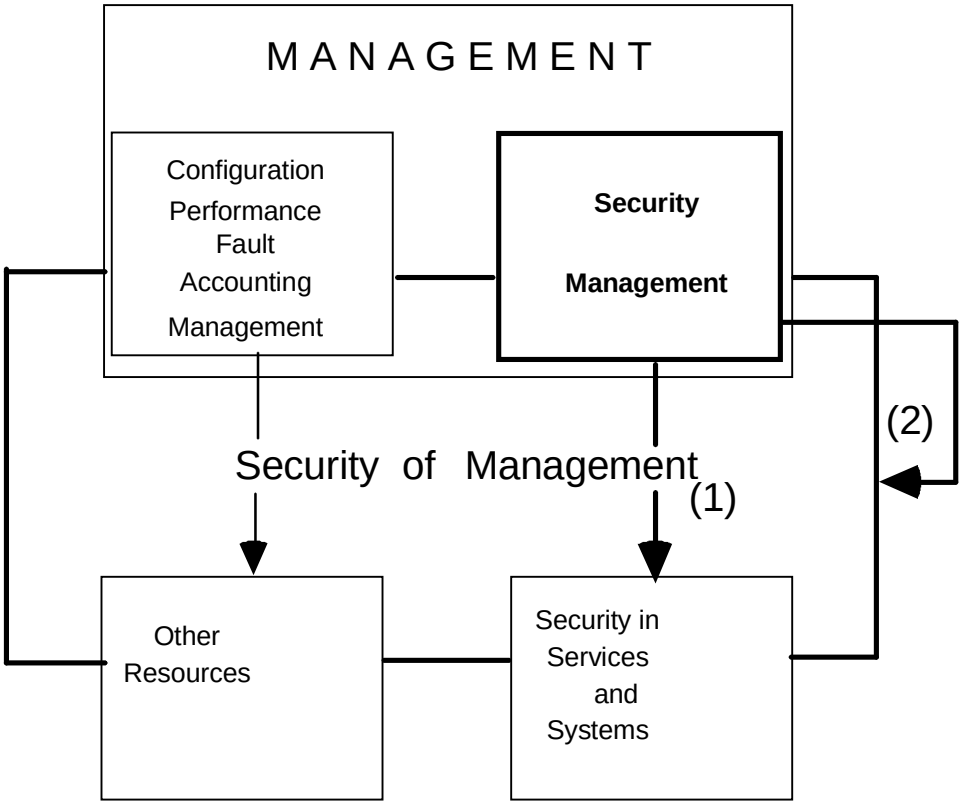


**Figure 1**

NOTE: The security services and mechanisms, which protect security management, also need to be managed. In figure 1, arrow (2) indicates management of management-related security services, while arrow (1) shows management of security protecting end user services.

Further details about the security of management may be found in the reference given in annex A.

# 5 Security management operations

In this section the management aspects of already installed and initialized security services and mechanisms will be discussed on the basis of authentication and key management as examples, chosen among the security services of the ISO Security Architecture in ISO 7498-2 [5].

Security management operations are initiated by the security manager and transported over the network through the management and communication infrastructure to the target system. The counterpart of the manager in the target system is the "agent", having the task to perform the wanted actions on the managed security objects and send security relevant reports on status and events back to the manager.

Further aspects of architecture and functional specifications for security management are discussed in the RACE Common Functional Specification H407 [6].

Management activities include operations on security functions (services, mechanisms) and on security information (user data, context information). Management activities related to security services can be divided in three categories:

- creation and installation of a security function;

- removing a security function;

- updating or modifying the parameters of a security function.

**Authentication service**

The type of information and the corresponding parameters to be managed will depend on the authentication method in use (see ISO DIS 10181-2 [7]. In commonly used methods the user is in possession of some secret knowledge and the system which has to verify the user has access to a registry of identities and associated knowledge related to the secret information. The term user may refer both to human users and to entities or processes of the system.

The management of authentication involves the maintenance of the above information and the corresponding parameters. There are generic management operations, common for different authentication methods, and operations, that are specific for a certain method.

Generic management of authentication services include:

- install and remove users;

- enable and disable user state;

- enter and change users authentication information;

- monitor successful and unsuccessful authentications.

Specific management of passwords (or PINs) used for simple authentication includes installation, removal, change of authentication information and monitoring of format (e.g. length, syntax, semantics) of passwords.

In the case of strong (cryptographic) authentication, e.g. those based on asymmetric algorithms, specific management operations involve the management of public key certificates.

**Key management (ISO 11770-1 [8]**

Virtually all security services need key material for their functions. The term key management is generally used to cover all aspects associated with the creation, distribution and maintenance of both short-term and long-term keys. Examples are the provision of short-term keys for confidentiality and integrity services and of long-term keys for authentication. Where keys are provided or maintained within a security service using them, key management will be part of the management of that service.

On the other hand, session keys can also be provided to security protocols, such as the Transport Layer Security Protocol (see ISO 10736 [9]), by a specific key service application, performing functions frequently referred to as key management. This generic key service application and the associated parameters has to be managed like any other security service, leading to the somewhat peculiar, but correct expression "management of key management".

Generic management operations associated with key management include:

- setting of variables, relevant for keys used by security protocols;
- monitoring of key service entities;
- distribution of short term keys;
- replacement of long term keys;
- control of use of keys;
- archiving and backup of keys;
- revocation of secret keys or certificates.

# 6 Managed objects

In clause 5 security specific management operations were introduced and discussed. In order for the agent to be able to perform those operations on systems from different vendors, the targets of management have to be described in a generic and well-defined form, independent of the actual implementation. In terms of standardization this means that standards for security services and mechanisms have to include uniform descriptions of attributes to be managed. According to ISO the appropriate form for such description is the managed object.

Managed objects are representations of real resources, in our case of security services and mechanisms, specified in accordance with agreed, common models, rules and templates. Definitions of managed objects by ISO can be found in ISO 10165-4 [3]. In this way, different implementations of the same standard will appear identical, seen by the manager and the agent of the management system. The mapping between the Managed Object (MO) representing a real resource and the resource itself is then a local, implementation dependent issue.

Some of the existing or emerging standards for security services and mechanisms already features managed object specifications, either as an integral part or as an addendum. Examples are the ISO Transport Layer Security Protocol (see ISO 10736 [9]) and the evolving Key Management standard, IEEE 802.10D [10], the latter having been submitted as a contribution to ISO SC21/WG8.

The present ambition of ETSI and other international standardization bodies is to supply a comprehensive library of managed objects with all relevant standards. In the ETR 237 [11] reference is made to available managed object specifications.

# 7 Common tools and procedures

**Initialization and off-line management actions**

There are a number of management actions related to security that have to be handled manually or by off-line procedures. Typical for this category of actions is the installation of high level cryptographic (master) keys at the time of the installation of a service or when such keys expire.

Similar actions are called for during security recovery, described at the end of this section. Set-up and initialization procedures are also needed at the installation, updating and replacement of trusted hardware and software.

**Audit trail and its management (ISO 10164-8 [12])**

Security relevant events are recorded and analysed in security audit trails in order to assess the effectiveness of a given security policy, to monitor whether resources are misused and to assist in the analysis of the security state of the system. Auditing is the analysis of security relevant events, e.g. attacks, either real-time or by using the recorded logs of audit trails.

The management of security audit covers the set-up and the administration of audit services and facilities. Generic management operations in the security audit context are:

- create, modify and delete objects and attributes which specify the selection criteria for security relevant events;

- initiate and terminate the generation of security audit messages, records and security alarms;

- initiate the transmission of security audit trail for archiving or backup purposes.

The following list is an example of specific audit requirements showing the events relevant to key management operations.

- generation, loading and deletion of keys;

- wrong usage of keys;

- expiration of crypto-periods;

- backup and archiving of keys;

- creation, deletion and updating of variables, relevant for keys used by security protocols.

**Security recovery**

If security audit and alarm functions indicate that the security of the system or a subsystem became compromised, recovery actions shall be triggered in order to:

- isolate the compromised subsystem;

- restore the system resources in a safe state;

- re-enforce the security policy;

- analyse the incident and propose adequate modifications.

Further efforts are necessary to define functions and procedures for security recovery and to integrate them into the overall management architecture.

# 8 Requirements for standardization

On-line remote management in a distributed environment involves a number of entities and requires support at different levels of the system. Figure 2 below is an attempt to give an overview and a rough classification of the different areas of standardization concerned in one or another way with security management. It is clear from the above discussions and from the figure at hand that security management in an open multi-vendor telecommunications environment is only possible if all three basic components, i.e. management applications, infrastructure and managed objects are specified and implemented according to harmonized standards.

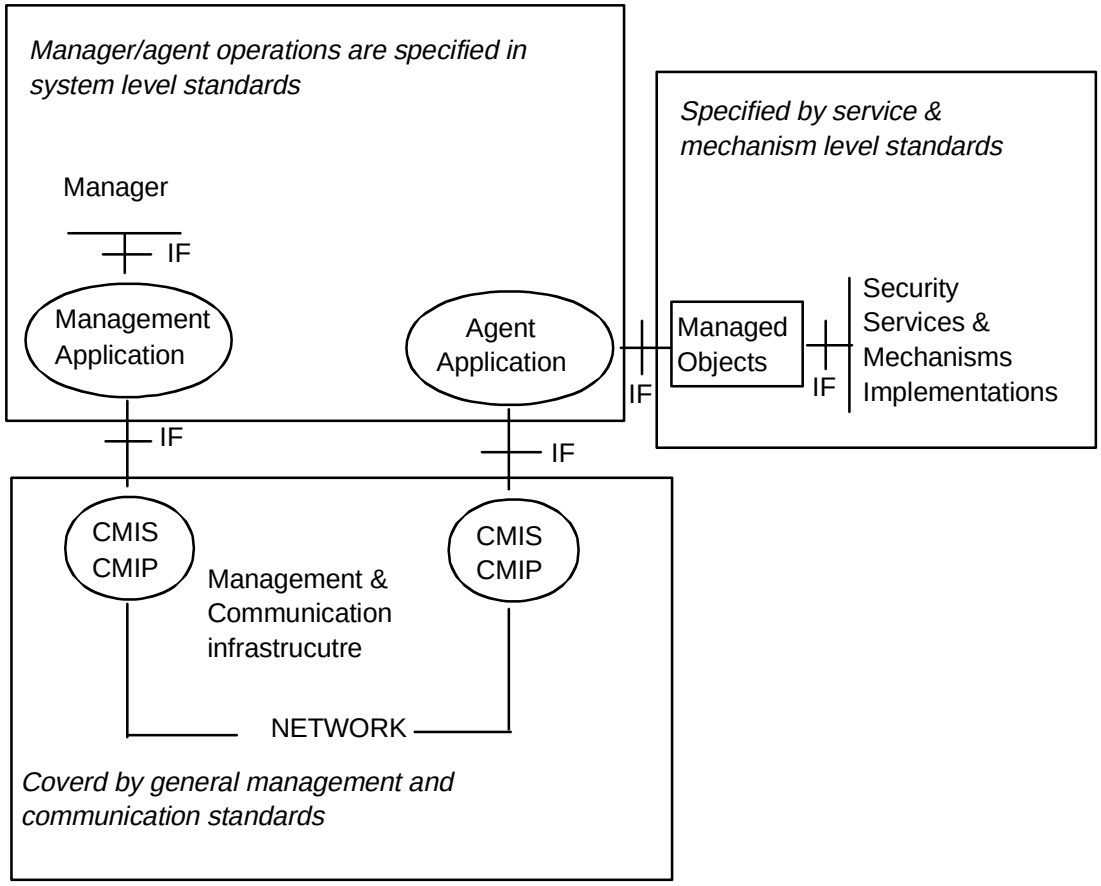


**Figure 2**

The specification of standards for the security of a system involves both the necessary security services/mechanisms and their management. Figure 2 gives some guidance to locate the work to be done concerning security management. The security services in the upper-right box are presented as managed objects to the manager in the upper-left box. The infrastructure provides for the information exchange between the remote systems. The interfaces (IF) indicated may be either internal or open programmable interfaces (APIs), and may, or may not be standardized.

Management operations have been discussed in clause 5. System standards, such as GSM or TMN, have to specify:

- parameters, events, alarms, etc., to be handled by security management for each security service;

- operations and actions related to all the above information.

The common tools and procedures, as described in clause 7, provide the means for the security administrator to monitor and handle security-related events from an overall system perspective. At least generic requirements for initialization of security services, for audit trail and for security recovery are to be included in the standard for a telecommunications system. Details may depend on the prevailing security policy.

In order to achieve compatibility between the manager and agent sides of secure management it is required that, whenever applicable, the above specifications are based on:

- OSI management standards, specifically the CMIP/CMIS protocol and service ISO 10040 [1], ISO 10164 [2]; and

- the managed objects as defined in ISO 10165-4 [3] and specified for the security service to be managed.

Hence, the prerequisite for interoperable solutions is that the standards for the chosen security services/mechanisms include managed object definitions according to ISO 10165-4 [3]. Consequently, there are potentially two possible tasks when security services are to be specified in the ETSI standardization process. In the first case there is a standard for the service from e.g. ISO available. Than, the task is to check that adequate managed objects are included. If not, there is the task to initiate such action or do the work in ETSI and contribute it to the relevant body. The second case is when the service or mechanism is being standardized by ETSI. In that case the working group should include the definition of managed objects into its program.

ISO and ITU-T infrastructure standards for management are rather stable at the CMIP-level. In special cases, as for the development of security standard profiles for TMN it may become necessary to propose to ITU some modifications in TMN.

## History

| Document history | |
|---|---|
| December 1996 | First Edition |
| | |
| | |
| | |
| | |

ISBN 2-7437-1193-0
Dépôt légal : Décembre 1996