



**ETSI
TECHNICAL
REPORT**

ETR 179

April 1995

Source: ETSI TC-NA

Reference: DTR/NA-070306

ICS: 33.080

Key words: Management, UPT

**Universal Personal Telecommunication (UPT);
UPT management aspects**

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

Copyright Notification: No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1995. All rights reserved.

6.2.2.6	UPT MOs related to performance management.....	23
6.2.2.7	UPT MOs related to fault management	23
Annex A:	Security management aspects	25
History	27

Foreword

This ETSI Technical Report (ETR) was 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.

Introduction

Universal Personal Telecommunication (UPT) is a service based on the Intelligent Network (IN) concept. UPT management aspects will, therefore, be based on IN Service Management (SM) aspects. The IN Service Management Functions (SMFs) are modelled according to the Telecommunications Management Network (TMN) functional architecture and described in the IN management model.

Meanwhile, there are some UPT-specific management functions and Managed Objects (MOs) which have not been taken into account in the documents related to the IN management aspects. This ETR describes the UPT-specific management functions and identifies UPT-specific MOs. The emphasis is placed on the delta between IN and UPT management.

The UPT management model is described in clause 5. The descriptions of UPT-specific Management Functions (MFs) and the identifications of UPT-specific MOs for each Management Functional Area (MFA) are given in clause 6.

Blank page

1 Scope

This ETSI Technical Report (ETR) describes UPT management aspects in terms of UPT Management Functional Areas (MFAs), UPT Management Functional Components (MFCs), UPT Management Function Sets (MFSs) and UPT-specific Management Functions (MFs) based on Open Systems Interconnection (OSI) MFAs.

A description of UPT management model and an identification of UPT-specific Managed Objects (MOs) are also included.

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] CCITT Recommendation F.851: "UPT Service description".
- [2] ITU-T Recommendation M.20: "Maintenance philosophy for telecommunications networks".
- [3] ITU-T Recommendation M.60 (1994): "Maintenance terminology and definitions".
- [4] ITU-T Recommendation M.3010 (1993): "Principles for a telecommunications management network".
- [5] ITU-T Recommendation M.3100 (1993): "Generic network information model".
- [6] ITU-T Recommendation M.3200 (1993): "TMN management services: overview".
- [7] ITU-T Recommendation M.3400 (1993): "TMN management functions".
- [8] CCITT Recommendation Q.121 (1989): "Signal code".
- [9] ITU-T Recommendation Q.1204: "Intelligent network distributed functional plane architecture".
- [10] CCITT Recommendation X.701 (1992): "Information technology - Open Systems Interconnection - Systems management overview".
- [11] ITU-T Recommendation X.720 (1993): "Information technology - Open Systems Interconnection - Structure of management information: Management information model".
- [12] CCITT Recommendation X.721 (1992): "Information technology - Open Systems Interconnection - Structure of management information: Definition of management information".
- [13] ITU-T Recommendation X.722 (1993): "Information technology - Open Systems Interconnection - Structure of management information: Guidelines for the definition of managed objects".
- [14] CCITT Recommendation X.800 (1991): "Security architecture for Open Systems Interconnection for CCITT applications".
- [15] ETR 055-6: "Universal Personal Telecommunication (UPT); The service concept; Part 6: Subscription and service profiles".

- [16] ETR 055-7: "Universal Personal Telecommunication (UPT); The service concept; Part 7: User procedures and user states".
- [17] ETR 062: "Network Aspects (NA); Baseline document on the integration of Intelligent Network (IN) and Telecommunication Management Network (TMN)".
- [18] ETR 083: "Universal Personal Telecommunication (UPT); General UPT security architecture".
- [19] ISO 7498-4: "Information processing systems - Open systems Interconnection - Basic Reference Mode - Part 4: Management framework".
- [20] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".
- [21] ISO/IEC DIS 10165-1: "Information technology - Open Systems Interconnection - Management information services - Structure of management information: Management Information Model".
- [22] ISO/IEC 10165-4: "Information technology - Open Systems Interconnection - Structure of management information - Part 4: Guidelines for the definition of managed objects".

3 Definitions

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

UPT Management Model (MM): The UPT MM addresses the UPT specific management aspects of the Intelligent Network Conceptual Model (INCM).

UPT Management Functional Area (MFA): The UPT MFA is a group of UPT Management Functional Components (MFC), and is used for facilitating further referencing of UPT MFCs.

UPT MFC: The UPT MFC is a group of UPT MFSs, and is used for facilitating further referencing of UPT MFSs.

UPT MFS: UPT MFS is a grouping of UPT Management Functions (MFs) that logically belong together. The UPT MFS is the smallest reusable item of functional specification. The UPT MFS must be considered as a whole and corresponds to the requirements part of the OSI Service Management Functions (SMFs).

UPT Management Function (MF): A UPT MF is the smallest part of the UPT management service as perceived by the user of the service and is an integral part of a UPT MFS. In reality it will generally consist of a sequence of actions on a defined managed object or objects.

Managed Object (MO): The (OSI) Management of a resource within the OSI environment that may be managed through the use of OSI management protocol(s).

4 Abbreviations

For the purposes of this ETR the following abbreviations apply:

B-ISDN	Broadband Integrated Services Digital Network
B-OSF	Business Operation Systems Function
CCF	Call Control Function
DTMF	Dual Tone Multi Frequency
FE	Functional Entity
GSM	Global System for Mobile Communication
IN	Intelligent Network
INCM	IN Conceptual Model
ISDN	Integrated Services Digital Network
MF	Management Function
MFA	Management Functional Area
MFC	Management Functional Component
MFS	Management Function Set
MM	Management Model
MO	Managed Object
NEF	Network Element Function
NO	Network Operator
OSI	Open Systems Interconnection
OSF	Operation Systems Function
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
PUI	Personal User Identity
SCEF	Service Control Element Function
SCF	Service Control Function
SDF	Service Data Function
SM	Service Management
SMAF	Service Management Agent/Access Function
SMF	Service Management Function
SP	Service Provider
SRF	Specialized Resource Function
SSF	Service Switching Function
TMN	Telecommunications Management Network
UMTS	Universal Mobile Telecommunications Systems
UPT	Universal Personal Telecommunication
VAC	Variable Authentication Code
VASP	Value Added Service Profile
WSF	Work Station Function

5 UPT management model

The UPT MM is based on the Intelligent Network (IN) MM and addresses the UPT specific management aspects of the INCM. The Functional Entities (FEs) identified in ITU-T Recommendation Q.1204 [9] related to the IN service creation and Service Management (SM), can be mapped to the proper function blocks in the Telecommunications Management Network (TMN) functional architecture. Since the TMN layered model addresses the distributed aspect of the network to be managed, and the TMN model is of a generic nature, a more detailed definition of IN management functions is required.

It is certainly accepted by both CCITT and ETSI that the management of IN and consequently the management of UPT will be based on TMN. That means the UPT management will be based on O-O techniques.

The specification of TMN Q interfaces is based on the MO techniques described in CCITT Recommendations X.700 series and M.3000 series.

In addition, it is recommended in the baseline document on the integration of IN and TMN (ETR 062 [17]) that the TMN functions of Operation Systems Function (OSF) and Work Station Function (WSF) be used in place of SMF and Service Management Agent/Access Function (SMAF) respectively.

Until now, there are no UPT requirements on the use of the Service Control Element Function (SCEF). Therefore, the use of the SCEF is not considered here.

Considering the above information, a possible integrated UPT management model based on the TMN OS functional hierarchy¹⁾ is shown in figure 1.

1) The detailed information concerning TMN OS functional hierarchy are given in ITU-T Recommendation M.3010 [4] and ETR 062 [17].

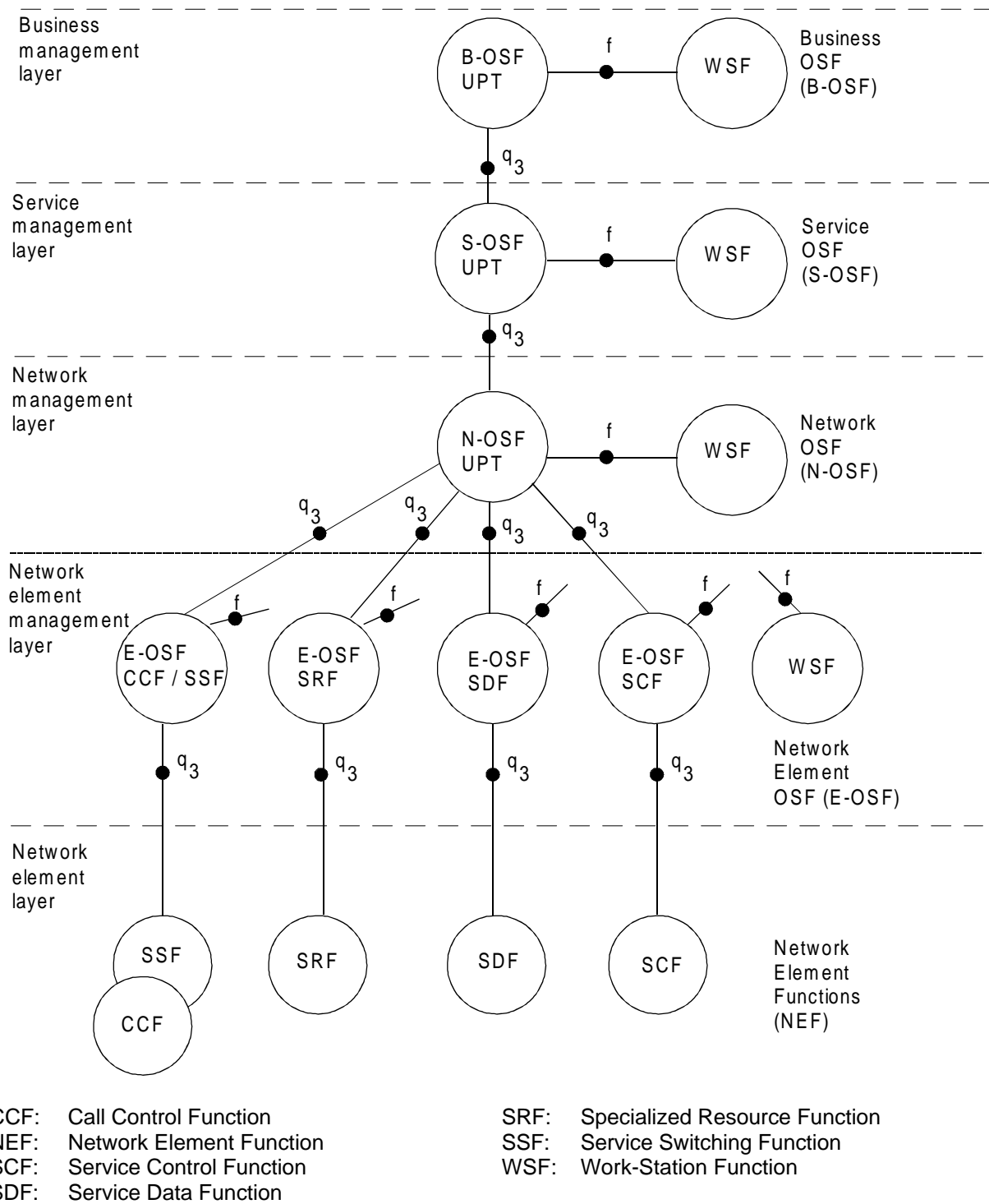


Figure 1: TMN layered architecture mapped on the UPT functional entities

6 UPT MFs and MOs

This clause describes the UPT Management Functional Areas (MFAs) based on OSI's MFAs, UPT Management Functional Components (MFCs), UPT Management Function Sets (MFSs) and UPT-specific Management Functions (MFs).

The identifications of UPT-specific Managed Objects (MOs) for each MFA are also included.

6.1 UPT MFAs

The UPT MFs are classified in accordance with the field of use into seven Management Functional Areas (MFAs):

- a) service profile management;
- b) service provisioning management;
- c) charging, billing and accounting management;
- d) security management;
- e) inter-network management;
- f) performance management;
- g) fault management.

The above MFAs are based on the five OSI's MFAs (performance management, fault management, configuration management, accounting management and security management) which have been specified in ITU-T Recommendation M.3400 [7] and ISO/IEC 7498-4 [19]. In order to make the complex UPT configuration management easier understandable it is here splitted into three MFAs (service profile management, service provisioning management and inter-network management).

The UPT MFA is a group of UPT MFCs and is used for facilitating further referencing of UPT MFCs.

The UPT MFC is a group of UPT MFSs, and is used for facilitating further referencing of UPT MFSs.

The UPT MFS is a group of UPT MFs that logically belong together. The UPT MFS is the smallest reusable item of functional specification. The UPT MFS should be considered as a whole and corresponds to the requirements part of the OSI SMF.

A UPT MF is a smallest element in support of the UPT management requirements; it is an integral part of a UPT MFS. It represents an interaction between two co-operating systems in order to achieve a management goal. In reality it will generally consist of a sequence of actions on a defined managed object or objects.

UPT MFSs, and their corresponding MFs are supported by MOs.

UPT MFs can be compiled into UPT management services that refer to managed objects.

The relationships between the UPT management terms (MFA, MFC, MFS, MF and MO) are shown in figure 2.

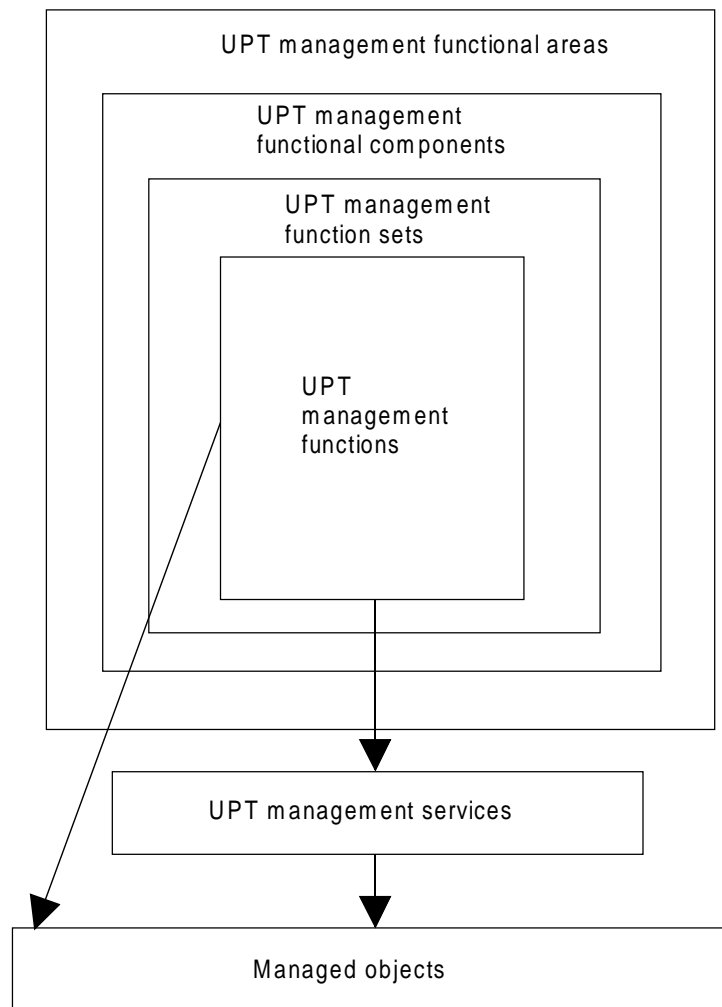


Figure 2: Relationship between UPT management terms

6.1.1 Service profile management

UPT service profile management is the ability to update, maintain and control the UPT service profile data, which are contained in UPT user service profiles and UPT subscriber service profiles, to provide, tailor and withdraw UPT service features. The UPT user, UPT customer (UPT subscriber) or UPT service provider can modify a service profile according to his access rights.

UPT service profile interactions by UPT users are considered to be part of the service itself, as they are intrinsic to UPT, and, therefore, they are not considered to be part of UPT management.

The information which is stored in service profiles can be divided in fixed and variable information. This information is classified and identified in ETR 055-6 [15].

The following MFCs related to UPT service profile management are described:

- a) **profile interrogation management:** provides information on the current status of a service profile. A subscriber may obtain information only about users which are allocated to him;
- b) **profile modification management:** provides the ability to change appropriate parameters of the service profile;
- c) **service profile status:** provides the ability to activate or deactivate a service profile.

6.1.1.1 UPT MFSs and functions related to profile interrogation management

- a) Profile interrogation management.

Only one MFS has been identified for this MFC.

Functions:

- **retrieve service profile:** function to retrieve a UPT service profile;
- **select service profile:** function to select the appropriate information of a UPT service profile (according to the access rights).

6.1.1.2 UPT MFSs and functions related to profile modification management

- a) Profile modification management.

Only one MFS has been identified for this MFC.

Functions:

- **retrieve service profile:** function to retrieve a UPT service profile;
- **select service profile:** function to select the appropriate information of a UPT service profile (according to the access rights);
- **validate request:** function for validating a request to edit a data entry in a service profile. This function is required i.e. to validate if an access point is semantically correct, authorised for UPT registration, in service and routable from the UPT support network;
- **edit service profile:** function for editing a UPT service profile;
- **store service profile:** function to store a UPT service profile.

6.1.1.3 UPT MFSs and functions related to service profile status

- a) Service profile status.

Only one MFS has been identified for this MFC.

Functions:

- **activate service profile:** function to activate a UPT service profile (i.e. UPT service profiles can be created without immediate activation);
- **deactivate service profile:** function to deactivate a UPT service profile.

An example of UPT MFs related to service profile management is shown in figure 3.

6.1.2 Service provisioning management

In order to have available the UPT service, the UPT subscriber has to subscribe to the service with the Service Provider (SP). Service provisioning management is that part of subscriber management covering the provisioning of UPT services at the time of subscription and during the subscription time. The SP has access to all the information required by this functionality without any restrictions. At the subscription time the UPT subscriber has to agree with the SP which information can be accessed by him and by associated UPT users.

The following MFCs related to service provisioning management are described:

- a) subscription management.

Covers handling of UPT subscription requests and administration of subscriber services after the time of subscription;

- b) resource management.

Covers the management of network and service resources and the assignment of subscriber resources for the purpose of provisioning.

6.1.2.1 UPT MFSs and functions related to subscription management

- a) Subscription request handling.

It supports the reception and processing of subscriber requests for UPT services at the time of subscription.

The following functions are performed at the time of subscription:

Functions:

- **analyse subscriber request:** function to analyse the subscriber request and to present information to the subscriber about details of the service being requested;
- **customer contract support:** function to support the set up of customer contracts;
- **check credit status:** function to check the subscriber credibility;
- **co-ordinate subscription delivery:** function to co-ordinate the delivery of a UPT service subscription (i.e. to create UPT service profiles or to create subscriber accounts).

- b) Subscriber service administration.

Subscriber service administration handles the functionality that is required to manage services of the existing subscribers and information related to the subscribers themselves.

Functions:

The following functions related to the subscriber service administration are described:

- **create service profile:** function to create a UPT user service profile;
- **delete service profile:** function to delete a UPT service profile;
- **attach service profile:** function to create an association between a UPT service profile and UPT user;
- **detach service profile:** function to remove the relationship between a UPT service profile and a UPT user;
- **handle usage data:** function to maintain UPT service usage data;
- **manage subscriber account:** function to maintain subscriber account records.

6.1.2.2 UPT MFSs and functions related to resource management

- a) Resource management.

The resource management supports the interrogation, reservation and assignment of network or service resources.

Functions:

- **retrieve resource data:** function to retrieve data on resources;
- **reserve resource:** function to reserve a resource for a subscription;
- **assign resource:** function to assign a resource to a subscription i.e. a subscriber account;
- **check resource availability:** function to check the availability of a resource.

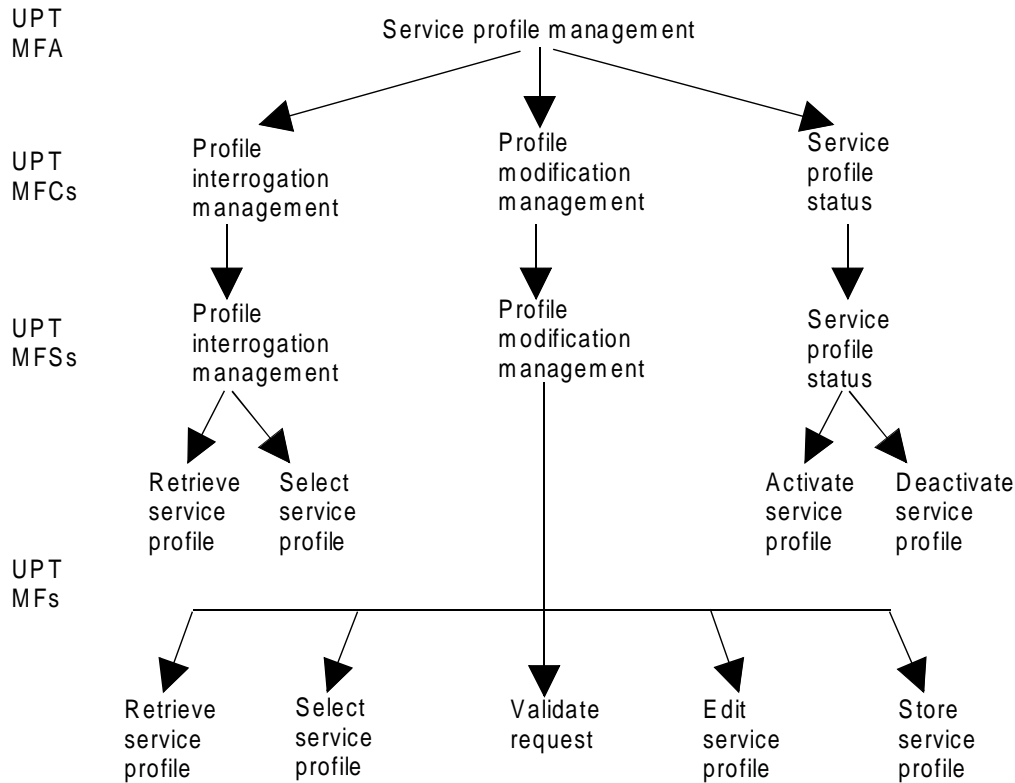


Figure 3: UPT management functions related to service profile management

6.1.3 Charging, billing and accounting management

Charging, billing and accounting management covers a set of functions which enables the activation and use of telecommunications resources and services to be measured and the cost to the subscriber for usage to be determined.

The following MFCs related to charging, billing and accounting management are described:

- a) charging and billing management.

The charging and billing management enables the usage of resources and services per subscription to be measured, and enables the processing of charging data for billing and cost advice. It also deals with setting up tariffs for services or resources;

- b) cost accounting management.

The description is further study;

- c) inter-administration accounting management.

The Inter-administration accounting management enables revenues to be shared between the involved service providers.

This subclause only deals with the decomposition of charging management.

6.1.3.1 UPT MFSs and functions related to charging management

a) Collection and exchange of charging data.

This MFS is involved with charging data collection process. The functions included here may be invoked by (and involve co-operation of) different domains and roles e.g. Service Provider (SP), home Network Operator (NO) and visited NO.

Functions:

- **initiate charging data collection:** this function involves a request to initiate charging data collection;
- **terminate charging data collection:** this function involves a request to terminate of charging data collection.

b) Creation and deletion of charging record.

This MFS is involved with setting up and deleting charging records. The functions included here may be used by (and involve the co-operation of) different domains and roles e.g. SP, home NO and visited NO.

Functions:

- **create charging record:** this function involves a request to create a charging record for invoicing to a subscriber, or on the contrary, for refunding to a subscriber;
- **delete charging record:** this function involves a request to delete a charging record.

6.1.4 Security management

The following MFC related to UPT security management is described:

a) authentication management.

Establishes and maintains the procedures and information necessary for the operation of authentication in the UPT service.

For more information on security management aspects, see annex A.

6.1.4.1 UPT MFSs and functions related to authentication management

a) Authentication policy.

Authentication policy provides the UPT SP with the functions required to establish and maintain the rules enforcing the authentication policy.

Functions:

- **create authentication policy;**
- **create policy rule** (e.g. Personal Identification Number (PIN) format description);
- **modify policy rule.**

NOTE: An authentication policy is a record (MO). It contains the specification of the set of rules to be enforced by the functions included in this MFS. The authentication policy is defined by the UPT SP.

b) Authentication SM

Covers functions to manage the authentication security service.

Functions:

- **create user identity;**
- **delete user identity;**
- **suspend user entry after a number of unsuccessful attempts;**
- **reactivate user entry;**
- **select authentication mechanism.**

c) Variable Authentication Code (VAC) management.

Covers the management of the mechanisms used for authentication based on VAC.

Functions:

- **initialise VAC mechanism;**
- **resynchronise VAC mechanism.**

d) PIN mechanism management.

Covers the management of the mechanism used for authentication based on PIN or SPIN.

Functions:

- **create PIN;**
- **request to change PIN;**
- **change PIN;**
- **request policy rule.**

6.1.5 Inter-network management

In a long term configuration, UPT should be supported by all the networks (e.g. Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), Broadband Integrated Services Digital Network (B-ISDN), the Global System for Mobile Communication (GSM) and Universal Mobile Telecommunications Systems (UMTS)) in service. In addition, any user of any network should be able to set-up or receive a communication with a UPT user. To reach these objectives, the interworking aspects and their management between these networks and UPT should be performed.

The inter-network management is that part of configuration management required to provided UPT between networks including UPT support networks and non-UPT networks.

The following network types may be considered:

- UPT support networks, which have the capabilities to control and manage UPT service;
- non-UPT networks, which have only capability needed to connect UPT calls to UPT support networks.

There are two interface points between these two network types:

- type A is an interface point between UPT support network and non-UPT network;
- type B is an interface point between two UPT support networks.

The following MFCs related to inter-network management are described:

- a) end-to-end UPT service configuration management.

It includes the functions required to configure a network in order to provide end-to-end UPT services between co-operating networks;

- b) UPT service network configuration management.

It includes the functions required to configure a network in order to provide the UPT service;

- c) UPT service access network configuration management.

It includes the functions required to configure a non-UPT network in order to provide access to the UPT services provided in a different network.

6.1.5.1 UPT MFSs and functions related to end-to-end UPT service configuration management

Functions:

- **deployment:** function to deploy UPT related service logic and data into the network;
- **test:** function to test UPT related service logic and data;
- **activate:** function to activate UPT related service logic and data.

6.1.5.2 UPT MFSs and functions related to UPT service network configuration management

Functions:

- **deployment:** function to deploy UPT related service logic and data into the network;
- **test:** function to test UPT related service logic and data;
- **activate:** function to activate UPT related service logic and data.

6.1.5.3 UPT MFSs and functions related to UPT service access network configuration management

Functions:

- **deployment:** function to deploy UPT related service logic and data into the network;
- **test:** function to test UPT related service logic and data;
- **activate:** function to activate UPT related service logic and data.

6.1.6 Performance management

Performance management provides functions to evaluate and report upon the behaviour of telecommunication equipment and on the effectiveness of the network. Its role is to gather statistical data for the purpose of monitoring and correcting the behaviour and effectiveness of the network or equipment and to aid in planning and analysis.

In general, performance management must provide tools to perform the following tasks:

- performance monitoring;
- performance control;
- performance analysis.

The detailed information are given in ITU-T Recommendation M.3400 [7].

The description of the UPT MFCs related to performance management is for further study.

6.1.7 Fault management

Fault management is a set of functions enabling the detection, isolation and correction of abnormal operation of the telecommunication network and its environment. It provides facilities for the performance of the maintenance phases from ITU-T Recommendation M.20 [2].

The following UPT MFCs related to fault management are described:

- a) alarm monitoring and reporting management.

Covers functions to monitor equipment alarm events and conditions coming from the networks that support the UPT service;

- b) fault notification management.

Covers the functions enabling the detection, isolation, correction and reporting of abnormal operations of the networks that support the UPT service. It only considers the notification of faults that are relevant to the UPT service.

6.1.7.1 UPT MFSs and functions related to alarm monitoring and reporting management

- a) UPT alarm detection.

This MFS allows to collect all UPT related alarms from underlying networks dropping those that are not relevant.

Functions:

- **detect alarm:** function to collect alarms from the involved networks, including their reception and acknowledgement;
- **select UPT-related alarm:** function to select the network alarms that are relevant to the UPT service;
- **forward UPT alarm:** function to allow the forwarding of alarm indications.

- b) UPT alarm filtering.

This MFS deals with the selection of those alarms that have to be logged and those that have to produce an alarm report.

Functions:

- **configure alarm filter:** function to allow the configuration of the criteria used to filter alarms before being logged or reported;
- **alarm sieve:** function to provide the mechanisms to analyse alarms and, depending on the selected criteria, to drop them or let them being logged or reported.

c) UPT alarm logging.

This MFS allows to store alarms and its corresponding reports.

Functions:

- **configure log:** function to allow the configuration of the criteria used to log alarms;
- **manage log:** function to perform creation, deletion, updating and query of alarm records within an alarm event log.

d) UPT alarm reporting.

This MFS deals with the generation of the report associated to an alarm event, and the sending to the user of the MFA.

Functions:

- **create UPT alarm report:** function to create a UPT alarm report;
- **send UPT alarm report:** function to send an alarm report to a given selected party;
- **acknowledge UPT alarm report:** function to assure that the alarm report sent to a given party has been successfully received.

This is specially important when the alarm report should initiate some kind of restoration procedures by the receiver.

6.1.7.2 UPT MFSs and functions related to fault notification management

a) UPT fault notification preparation.

This MFS deals with the collection and forwarding of fault indications and the creation of the corresponding notification messages.

Functions:

- **create fault notification:** function to create a fault message;
- **forward fault indication:** function to forward fault indications to a specified recipient;
- **select recipient:** function to select receivers of a given fault notification.

6.2 Managed objects

6.2.1 TMN managed objects

A Managed Object (MO) is the OSI management view of a resource that is subject to management, such as a layer entity, a connection or an item of physical communication equipment. Therefore, a MO is the abstraction of such a resource that represents its properties as seen by (and for the purpose of) management. An essential part of the definition of a MO is the relationship between these properties and the operational behaviour of the resource. This relationship is not modelled in a general way.

MOs can be specific to an individual layer, in which case they are known as (N) - layer managed objects. Those MOs that are relevant to more than one layer, to a specific management function (management support object) or to the system as a whole are known as system managed objects (CCITT Recommendation X.701 [10]).

6.2.1.1 Managed objects knowledge

For the information contained in the MOs of a system to meet the requirements for extensibility it is necessary to provide tools to explore the MOs in a system.

The detailed information are given in ITU-T Recommendation X.720 [11] and ISO/IEC DIS 10165-1 [21].

6.2.1.2 Managed object creation

Creation of managed object instances may occur in the following ways:

- MOs may be created and deleted as a result of the operation;
- MOs may be created and deleted by management;
- MOs may be created and deleted by means outside the scope of OSI.

The detailed information are given in ITU-T Recommendation X.722 [13] and ISO/IEC 10165-4 [22].

In addition, the general principles for MO definitions are described in ITU-T Recommendations X.720 [11] and X.721 [12].

6.2.2 The identification of UPT-specific MOs

This subclause identifies the UPT- specific MOs for each UPT MFA.

A development path for UPT MOs is shown in figure 4.

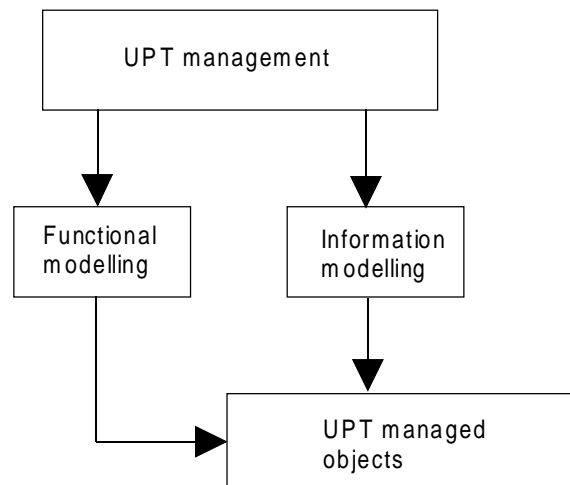


Figure 4: Development of the UPT managed objects

6.2.2.1 UPT MOs related to service profile management

a) MOs in service profile management:

- UPT service profile;
- authorisation data;
- user identity;
- service access point;
- network access point;
- subscriber account record;
- UPT user service profile;
- UPT service usage record.

6.2.2.2 UPT MOs related to service provisioning management

- a) MOs in subscriber service provisioning management:
- UPT subscriber service profile;
 - subscriber/user order record;
 - subscriber/user account record;
 - subscriber/user contract record;
 - UPT service class specification;
 - UPT service profile;
 - UPT service usage record.

6.2.2.3 UPT MOs related to charging, billing and accounting management

- a) MOs in charging management:
- charging record;
 - call record;
 - split charging record;
 - UPT user service profile;
 - UPT subscriber service profile;
 - UPT subscriber account;
 - UPT service usage record.

6.2.2.4 UPT MOs related to security management

- a) MOs in authentication management:
- authentication policy;
 - authentication policy rule;
 - user registry;
 - user registry entry;
 - authentication mechanism;
 - master key registry;
 - verification authentication information.

6.2.2.5 UPT MOs related to inter-network management

The identification of UPT MOs related to inter-network management is for further study.

6.2.2.6 UPT MOs related to performance management

The identification of UPT MOs related to performance management is for further study.

6.2.2.7 UPT MOs related to fault management

- a) MOs in alarm monitoring and reporting management:
- UPT service profile;
 - alarm filter;
 - alarm record;
 - alarm level;
 - Value Added Service Profile (VASP);
 - UPT service class specification;
 - alarm forwarding discriminator:
 - event log;
 - event record;
 - alarm data alarm report;
 - event log.

b) MOs in fault notification management:

- fault log;
- fault forwarding discriminator;
- UPT service profile;
- fault record;
- event log.

Annex A: Security management aspects

The detailed information related to the OSI security management and security architecture are given in ISO 7498-2 [20] and CCITT Recommendation X.800 [14]. The ETSI UPT security architecture is described in ETR 083 [18].

The following items related to UPT security management aspects are for further consideration:

a) key management.

A key management is necessary for the use of enhanced authentication mechanisms, integrity mechanisms, and encipherment mechanisms.

Key management deals with key generation, key distribution, and key storage. An important aspect is the life time of keys.

b) personalisation of security devices.

It has to be considered how to personalise UPT access devices. There might be differences between the personalisation procedures for different devices (e.g. Dual Tone Multi Frequency (DTMF) devices, smart cards). There should be an on-line procedure to change PINs. It has to be distinguished between PINs stored and verified in the device, and PINs stored and verified by the UPT operator. In the latter case there might be an additional "Special PIN" (used e.g. for unblocking of user access) that needs special considerations.

c) security audit trail.

The task of security audit trail is to detect actual threats against the UPT system like unauthorized access to system or user data and unauthorized change of access rights.

The system should contain an audit component which is able to log the following events with the following data:

- use of the identification and authentication mechanisms (date, time, user identity supplied (Personal User Identity (PUI) or operator identity), network address, success or failure of the attempt);
- attempted access to an object subject to the administration of rights (date, time, user identity, name of the object, type of access attempt, success or failure of the attempt);
- actions by UPT service operators (date, time, user identity type of action, name of the object to which the action relates, (e.g. introduction, deletion or suspension of users, introduction or removal of storage media, start up or shut down of the system)).

It should be possible to restrict the audit to one or more selected users.

Access to audit data shall only be permitted to authorized users. They are responsible for the observance of privacy laws. The use of audit data should be strictly controlled.

Tools to examine and to maintain the audit files shall exist and be documented. The structure of audit records shall be described completely. The mechanisms to obtain, maintain and evaluate audit trail are out of the scope of UPT. They are system specific. They might be supported by methods of artificial intelligence.

d) event handling.

Dependent on the evaluation of real time data (e.g. call record), adequate actions have to be carried through, in order to enforce the security policy. These actions might be alarms to the security administrator or blocking of user access to the system.

The mechanisms for event handling are out of the scope of UPT. They are system specific. They might be supported by methods of Artificial Intelligence (security control board for risk management).

e) inter domain security.

The security level offered to a UPT user may depend on various parameters:

- the security policy of the UPT service provider;
- the choice of optional security mechanisms;
- the choice of authentication procedures;
- the choice of UPT access devices;
- the actual use of the UPT procedures.

As a consequence of the types of security mechanisms applicable for UPT and depending on the security policy of the UPT service provider, a UPT user may be offered a set of possible optional security levels to decide upon subscription time. These levels are to be decided by the UPT service provider and may include the following options:

- choice of user action authentication;
- choice of user event control mechanisms;
- required user identity and/or location confidentiality.

If UPT service providers with different security policies are involved (e.g. home location and visited location providers), special procedures for inter-domain security are required. Inter-domain security will be necessary in all UPT phases when e.g. the UPT service providers of home location and visited location have to distribute access data.

f) interaction with third parties.

The UPT user will use the terminal access of an ordinary line subscriber and thus interact with his subscription.

In order to protect the UPT user and the line subscriber from each other, some security measures are required.

History

Document history	
April 1995	First Edition
February 1996	Converted into Adobe Acrobat Portable Document Format (PDF)