



ETSI
TECHNICAL
REPORT

ETR 311

September 1996

Source: ETSI TC-NA

Reference: DTR/NA-005001

ICS: 33.020

Key words: IN, TMN, UPT

**Universal Personal Telecommunication (UPT);
Requirements, services and information for UPT management**

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 1996. All rights reserved.

Contents

Foreword	5
1 Scope	7
2 References	7
3 Definitions and abbreviations	8
3.1 Definitions	8
3.2 Abbreviations	9
4 Introduction.....	10
4.1 Approach.....	10
4.2 Assumptions	11
5 UPT management requirements.....	13
5.1 Subscriber Administration - service provisioning.....	14
5.1.1 Requirements from the subscriber to the PNO	14
5.1.2 Requirements from the user to the PNO.....	15
5.1.3 Requirements from other PNOs.....	15
5.1.4 Internal PNO requirements.....	15
5.2 Subscriber administration - service profile management.....	15
5.2.1 Requirements from the subscriber to the PNO	15
5.2.2 Requirements from the user to the PNO.....	16
5.2.3 Requirements from other PNOs.....	16
5.2.4 Internal PNO requirements.....	16
5.3 Network provisioning management	16
5.3.1 Requirements from the subscriber to the PNO	17
5.3.2 Requirements from the user to the PNO.....	17
5.3.3 Requirements from other PNOs.....	17
5.3.4 Internal PNO requirements.....	17
5.4 Charging, billing and accounting management.....	19
5.4.1 Requirements from the subscriber to the PNO	19
5.4.2 Requirements from the user to the PNO.....	20
5.4.3 Requirements from other PNOs.....	21
5.4.4 Internal PNO requirements.....	21
5.5 Quality of service and network performance administration.....	22
5.5.1 Requirements from the subscriber to the PNO	22
5.5.2 Requirements from the user to the PNO.....	22
5.5.3 Requirements from other PNOs.....	23
5.5.4 Internal PNO requirements.....	23
5.6 Maintenance management	24
5.6.1 Requirements from the subscriber to the PNO	24
5.6.2 Requirements from the user to the PNO.....	24
5.6.3 Requirements from other PNOs.....	24
5.6.4 Internal PNO requirements.....	25
5.7 Security administration.....	26
5.7.1 Requirements from the subscriber to the PNO	26
5.7.2 Requirements from the user to the PNO.....	27
5.7.3 Requirements from other PNOs.....	28
5.7.4 Internal PNO requirements.....	28
6 Analysis of UPT scenarios	29
6.1 Service profile management by UPT user in home domain	31
6.2 Service Profile management by UPT user in visiting domain	32
6.3 Service Profile management by UPT subscriber in home domain	32
6.4 Service provisioning for UPT subscriber in home domain.....	33
6.5 Registration of the UPT user in home domain.....	34

6.6	Registration of the UPT user in visiting domain	35
6.7	Make outgoing call by UPT user in home domain.....	35
6.8	Make outgoing call by UPT user in visiting domain.....	36
6.9	Request bill by UPT subscriber in home domain	36
6.10	Authentication of UPT user in home domain.....	37
6.11	Authentication of UPT user in visiting domain.....	37
6.12	Authentication of UPT subscriber in home domain.....	38
6.13	Complaint by UPT subscriber in home domain.....	39
6.14	Deployment of UPT by PNO in home domain.....	39
6.15	Security event in home domain	43
6.16	Security event in visiting domain	44
6.17	Performance management by PNO in home domain	44
6.18	Performance management by PNO in visiting domain	45
6.19	UPT service modification in home domain.....	46
6.20	Request statistics by subscriber in home domain.....	48
6.21	Request statistics by PNO in home domain.....	48
6.22	UPT subscription procedure in home domain.....	49
7	UPT management information	49
7.1	The UPT SA management service	51
7.2	The UPT NPM management service	51
7.3	The UPT CBAM management service.....	51
7.4	The UPT QNPM management service	52
7.5	The UPT MM management service	52
7.6	The UPT SCA management service.....	52
8	UPT management services	53
8.1	UPT Subscriber administration	53
8.2	UPT network provisioning management	54
8.3	UPT Charging, billing and accounting management.....	54
8.4	UPT QoS and network performance management.....	55
8.5	UPT maintenance management	55
8.6	UPT security administration	55
Annex A:	Authentication mechanisms provided by the SDF.....	56
Annex B:	The X.500 UPT information model.....	57
Annex C:	Bibliography.....	58
History	59

Foreword

This ETSI Technical Report (ETR) has been produced by a joint working group of NA4 and NA6 experts of Technical Committee NA (Network Aspects) 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

The purpose of this ETSI Technical Report (ETR) is to provide guidance to network operators and/or service providers for providing and managing a Universal Personal Telecommunication (UPT) service. It also takes into account the co-operation of UPT service providers, i.e., by interconnection of the respective network functionality. The functional network architecture assumed as the basis for this study, and the assumptions taken here, are further outlined in clause 4 below.

This ETR provides high level requirements, functions, services, and information to be supported or exchanged between the management organizations of the co-operating parties, and between the management organizations and the respective networks. The information provided is of a general and high level nature. This report should therefore only be seen as providing an initial framework for actual management specifications for Q3 and X interfaces.

This ETR is based on the general UPT specifications. Where necessary, the more detailed UPT documents of the phase 1 descriptions and phase 2 descriptions were considered. The "assumptions" in subclause 4.2 explain the UPT environment and specify the selected options with respect to the UPT service features.

In this ETR, extensive use of scenarios is made. These scenarios are analysed to identify the information flows on q3 and x reference points of the selected functional architecture, and to identify the corresponding management functions. Subclause 4.1 provides further discussion on the approach taken here. The scenarios are focused at addressing the following management areas:

- subscriber administration;
- network provisioning management;
- charging, billing and accounting management;
- QoS and network performance management;
- maintenance management; and
- security administration.

NOTE 1: The term "management area" used in this document should not be seen as referring to the "telecommunication managed area" as identified in ITU-T Recommendation M.3200 [1].

NOTE 2: The term "subscriber administration" is used in this document as identical to the term "customer administration" as defined in ITU-T Recommendation M.3200 [1]. To comply with Intelligent Network (IN) terminology, the term subscriber administration is preferred here.

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] ITU-T Recommendation M.3200: "TMN management services: overview".
- [2] TCR-TR 007: "UPT Vocabulary".
- [3] ETS 300 779: "Network Aspects (NA); Universal Personal Telecommunication (UPT); Phase 1 - Service description".
- [4] ETR 083: "Universal Personal Telecommunication (UPT); General UPT security architecture".
- [5] ETR 055-08: "Universal Personal Telecommunication (UPT); The service concept; Part 8: Man-machine interface aspects".

- [6] ETR 065: "Universal Personal Telecommunication (UPT); Requirements on charging, billing and accounting".
- [7] ETR 055-06: "Universal Personal Telecommunication (UPT); The service concept; Part 6: Subscriptions and service profiles".
- [8] ETS 300 670: "Universal Personal Telecommunication (UPT) phase 1; Intelligent Network (IN) Capability Set 1 (CS1); Application of core Intelligent Network Application Protocol (INAP)".
- [9] ETS 300 391-1 (1995): "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 1: Specification".
- [10] ETS 300 790: "Universal Personal Telecommunication (UPT); Security architecture for UPT phase 2; Specification".

3 Definitions and abbreviations

3.1 Definitions

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

Management Service (MS): A (TMN) management service is seen as an area of management activities which provide for the support of an aspect of Telecommunications Management, described in the user requirements.

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

Management Information Model (MIM): The management information model presents an abstraction of the management aspects of network resources and the related support management activities. The model determines the scope of the information that can be exchanged on a standardized manner.

Managed Objects (MOs): The OSI management view of a resource within the OSI environment that may be managed through the use of OSI management protocol(s).

managed object class: A named set of managed objects sharing the same (named) sets of attributes, notifications, management operations (packages), and which share the same conditions for presence of those packages.

UPT user: The (UPT) user is a person who has been authorized to use UPT facilities by a UPT subscriber. The UPT user will be associated with a unique UPT number.

NOTE 1: For simplicity sake, in this document the term "user" is used as a synonym to "UPT user".

UPT subscriber: The (UPT) subscriber is a person or legal entity with a contractual relationship with a UPT service provider, on behalf of one or more UPT users, and is responsible for the payment of charges due to that service provider.

NOTE 2: For simplicity sake, in this document the term "subscriber" is used as a synonym to "UPT subscriber".

UPT service provider: The UPT service provider has overall responsibility on service operation and on database management. The UPT service provider will commercially manage the UPT service. Specifically, the UPT service provider will distribute to UPT subscribers UPT numbers and make arrangements for provision of the UPT service to the UPT user. The UPT service provider also manages the billing arrangements.

UPT network operator: The UPT network operator is a network operator who provides the network capabilities required for the UPT service. UPT network operators will acquire revenue from the UPT service providers and other network operators for the service they offer.

UPT access provider: The UPT access provider is an organization or individual (...) who provides an access point or terminal to a network, to enable interaction with the UPT service.

UPT PNO: The (UPT) Public Network Operator (PNO) encompasses all aspects of UPT network operator, UPT service provider and UPT access provider. The concept of PNO is introduced in this ETR mainly for simplicity sake but also because of the lack of clear separation between network operator and service provider domains.

3.2 Abbreviations

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

AE	Authenticating Entity
ARA	Access Registration Address
CCAF	Call Control Agent Function
CCF	Call Control Function
DAP	Directory Access Protocol
DO	Directory Object
DUA	Directory User Agent
DSA	Directory System Agent
FE	Functional Entity
IN	Intelligent Network
INAP	Intelligent Network Application Part
IP	Intelligent Peripheral
MF	Management Function
MO	Managed Object
MS	management service
OCPIN	Outgoing Call PIN
OSI	Open Systems Interconnection
PIN	Personal Identification Number
PNO	Public Network Operator
PNOh	PNO of the home domain
PNOo	PNO of the originating domain
PUI	Personal User Identity
RAA	Remaining Authentication Attempts
SAPIN	Secure Answer PIN
SCF	Service Control Function
SCFh	SCF of the home domain
SCFo	SCF of the originating domain
SCP	Service Control Point
SDF	Service Data Function
SDFh	SDF of the home domain
SDFo	SDF of the originating domain
SDP	Service Data Point
SLA	Service Level Agreement
SPIN	Special PIN
SRF	Specialized Resource Function
SSF	Service Switching Function
SSP	Service Switching Point
QoS	Quality of Service
TMN	Telecommunication Management Network
TMNh	TMN of the home domain
TMNo	TMN of the originating domain
UPT	Universal Personal Telecommunication

4 Introduction

This clause deals with the approach for the specification of requirements, functions, services, and information for UPT management. It also describes the assumptions that were made to outline the management environment. These assumptions were made to be able to cover all objectives, as stated in clause 1, with reasonable effort.

4.1 Approach

The approach comprises the following five steps:

- 1) Identification of roles and specification of a UPT management functional architecture (see subclause 4.2).
- 2) Capture of UPT management requirements. These requirements are then structured according to the categorization of management services as identified in ITU-T Recommendation M.3200 [1] (see clause 5).
- 3) Analysis of UPT scenarios in terms of information flows over q3 and x reference points and identification of required Management functions (see clause 6).
- 4) Identification of global UPT information required for supporting the management requirements and scenarios (see clause 7).
- 5) Specification of UPT management services; identification of the roles that are relevant for each management service and listing the required Management functions for each role (see clause 8); cross-checking with the management requirements.

NOTE: The cross checking between management services and management requirements is not explicitly described in this document; in fact, the management scenarios, functions, information flows and services only meet a sub-set of the management requirements as identified in clause 5.

This can be visualized as follows:

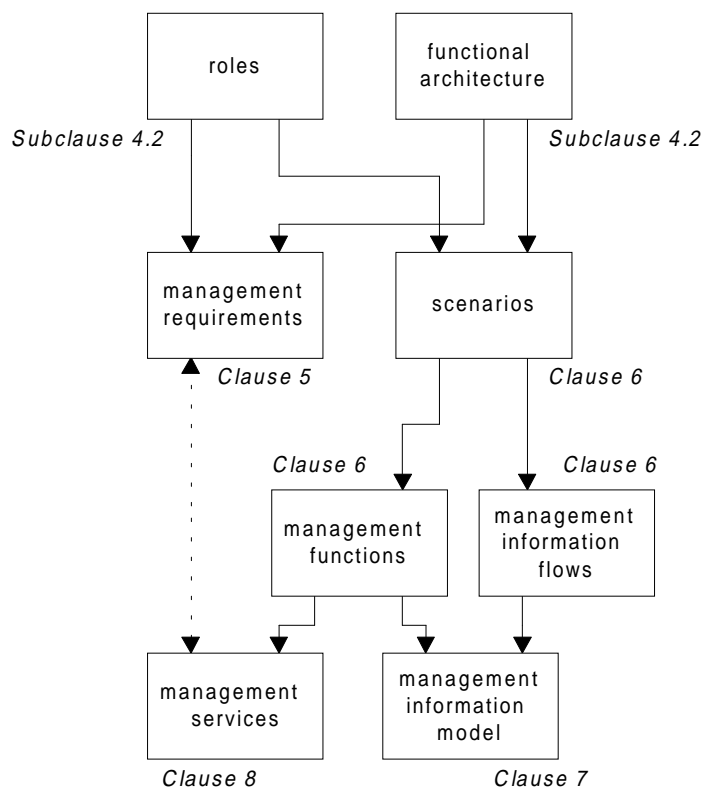


Figure 1: The technical approach taken in this study

4.2 Assumptions

The following figure provides a visualization of a functional architecture that was chosen as the basis for this ETR.

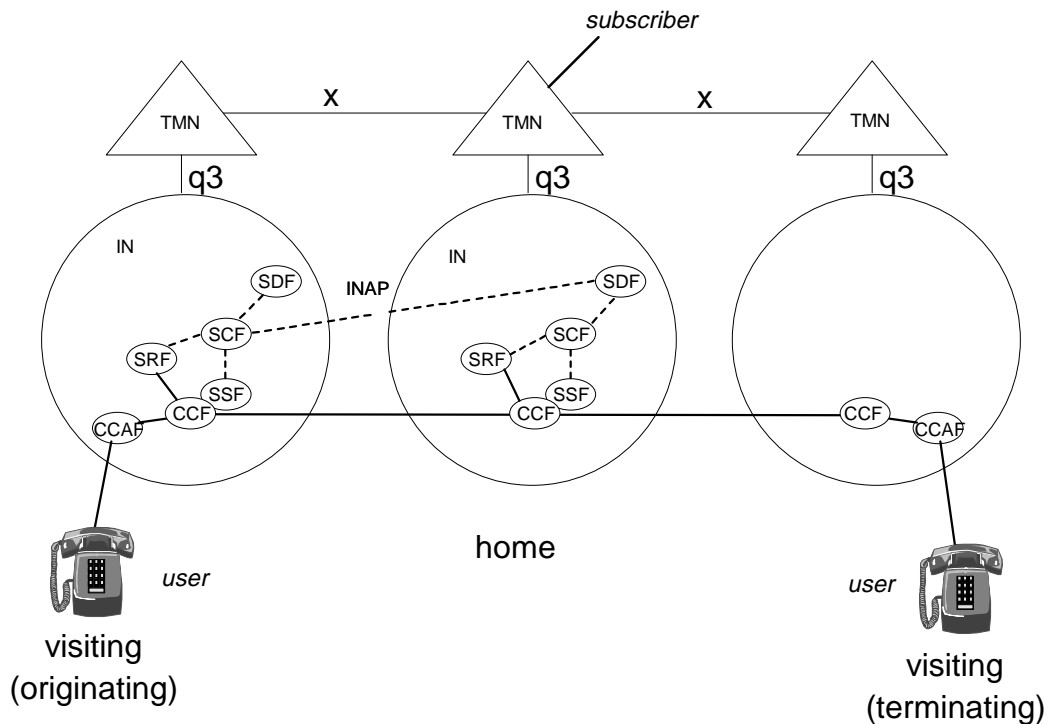


Figure 2: Example of a UPT management functional architecture

This figure visualizes three network domains (large circles) with corresponding management organizations (triangles). In the network domains some typical IN functional entities that are used in the discussion below are presented. Some connections between networks and management organizations are indicated. In the remainder of this subclause, this will be further explained.

In this ETR, the following assumptions are taken (see figure 2):

- Ass.1: The architecture consists of 1 home domain and 2 visiting domains. The visiting domains may play the role of originating and terminating domain. Note that a domain encompasses a network and a TMN for management purposes.
- Ass.2: The home domain is IN-structured and provides UPT.
 If a call is originated in a visiting domain, then that domain has to be IN structured and has to support UPT, i.e. by enabling registration/deregistration and understanding UPT numbers.
 If a call is terminated in a visiting domain, then that domain may or may not be IN-structured. It may or may not support UPT.
- Ass.3: UPT should provide all service features as described in the UPT service descriptions for phase 1 and phase 2 (refer to [8] for a description of the UPT phase 1 service features).
- Ass.4: According to UPT phase 1, only an IN signalling relation between the SCF of a visiting domain and a SDF of a home domain is assumed for service interworking. In the texts below, this relationship is indicated as a SCFo-SDFh relationship.

According to the UPT philosophy, a UPT user should invoke the UPT service of that PNO he is directly connected to. This means that a UPT user in visiting location should invoke the UPT service of the visited PNO, simply to save costs. However, the UPT services of two PNOs may be different e.g. regarding the service features. In this case, a UPT user should either accept the "restricted" service facilities of the visited PNO, or make an international UPT call via his home SCP. The latter might be an expensive option. Therefore, a PNO may decide to make its UPT service more widely available to its subscribers via special arrangements with other PNOs,

namely by having these PNOs to support his specific service features. This can be achieved in two ways:

- a) the service logic is provided to these other PNOs. These other PNOs can then integrate the relevant parts of this service logic to their SCPs;
- b) the stage 1 descriptions and the UPT service feature descriptions of the "home PNO service" are provided to these PNOs. These other PNOs can then modify their UPT service logics accordingly (where appropriate).

In both ways, a common view to the user (same look and feel) and to the data can be obtained.

Ass.5: In this ETR, the parties involved can play several roles. For this study, the following roles are identified:

- UPT user;
- UPT subscriber;
- PNO.

The PNO encompasses all aspects of network operator, service provider and access provider. The PNO role is introduced in this ETR mainly for simplicity sake but also because of the lack of clear separation between network operator and service provider domains. These roles are further defined in clause 3.

Ass.6: All PNOs use TMNs to manage their networks and services (via Q3 interfaces) and to exchange information between the respective management organizations (via X interfaces).

Ass.7: The subscriber has two possibilities to access data for management purposes:

- a) access via IN to SCF/SDF (for interrogation and modification of his user profiles); and
- b) direct access to the TMN (e.g. for interrogation and modification of his subscriber profile).

NOTE 1: For clarity, in this document the term "user profile" is used instead of the term "UPT service profile", as defined in ETR 065 [6].

NOTE 2: This "direct access to the TMN" could be supported by an X-interface, an F-interface, other machine-machine interfaces (X.25) or simply by post, Email, fax, telephone etc. In fact, even the relationship between the UPT user and the PNO could be supported in a similar "direct" way. It is however not in the scope of this ETR to make any statements on what would be the best or architecturally most correct option here.

NOTE 3: Direct access of a subscriber to the TMN should not be implemented before a threat analysis has been done and the necessary security mechanisms have been implemented.

Ass.8: Subscriber profiles may be stored in the TMN, SDF or in other locations. However, for the sake of this ETR it is assumed that the subscriber profile is only stored in the home TMN, i.e., no communication of subscriber profile to SDF is described. The user (service) profiles are assumed to be located in the SDF.

Ass.9: It is assumed that sufficient security mechanisms exist for the communication between the identified parties. In particular, the following assumptions are made:

- a) security mechanisms for end-user - network communication:

The main security features and measures taken into account in this ETR are:

- weak authentication;
- strong authentication; and
- black list.

Weak authentication is based on a personal identification number and is foreseen for the UPT user.

Strong authentication is based on cryptographic techniques. It requires a UPT authentication device.

In the scope of this ETR it is assumed, that the authentication of a UPT user in the visiting domain is processed by means of the INAP protocol between SCFo and SDFh. The used protocols, procedures and mechanisms are not subject of this ETR.

Detailed information can be obtained in ETR 083 [4], ETS 300 391-1 [9] and ETS 300 790 [10].

- b) security mechanisms for subscriber- TMN communication: Here sufficient security mechanisms are assumed to exist. For this area, reference is made to developing activities in the ETSI NA technical committee.
- c) security mechanisms on the Q3 and X interfaces: also for these mechanisms reference is made to developing activities in the ETSI technical committee.

Ass.10: Charging records may be stored in a number of different locations. However, for the sake of this ETR it is assumed that the charging records are not stored in the SDFh. If a user is in visiting location, a charging record is created by the visiting network, transferred to the TMN of the visiting network and finally via the X interface sent to the TMN of the home network.

5 UPT management requirements

This clause captures general UPT management requirements. These requirements should not be seen as exhaustive; also, some may be overlapping. Purpose of this clause is merely to identify a check list of requirements for the identification and cross-checking of the functions, information and services identified in the succeeding clauses. Individual service/network operator implementations may deviate from the requirements and functionality described below. Although the requirements identified below are identified specifically for the purpose of this ETR, a lot of the identified requirements can be seen as more generally applicable to management of IN based services and networks.

The requirements are structured according to the list of management services as identified in ITU-T Recommendation M.3200 [1]. The following table list these management services and indicates in which subclause the UPT management requirements are listed. When no subclause is indicated, the corresponding management service is not analysed for UPT or not used to categorize the requirements listed below.

Table 1: The management services of M.3200

no.	name of the management service	subclause
A	Subscriber Administration	5.1 and 5.2
B	Network Provisioning Management	5.3
C	Work Force Management	
D	Charging, Billing and Accounting Management	5.4
E	QoS and Network Performance Management	5.5
F	Traffic Measurements and Analysis Administration	
G	Traffic Management	
H	Routing and Digit Analysis	
I	Maintenance Management	5.6
J	Security Administration	5.7
K	Logistics Management	

The subclauses in this clause list the management requirements per "management service area", as indicated in table 1. The requirements between the roles as identified earlier (PNO, user, subscriber) are described, and the required PNO functionality (both on the TMN and the IN network) is then deduced.

Also "internal PNO requirements" are identified; these should be seen as requirements that do not (necessarily) originate directly from the requirements of other roles. At the beginning of each subclause, a short description of the management service area is provided, in line with ITU-T Recommendation 3200 [1].

5.1 Subscriber Administration - service provisioning

Subscriber Administration supports the processes of exchanging data with the subscriber or user for the purpose of offering the UPT service and to configure the network with the required subscriber data and functions required in order to produce the service (service provisioning). It also supports the process of exchanging data with the network for the purpose of service profile management. This subclause deals with the service provisioning part; service profile management is described in subclause 5.2.

5.1.1 Requirements from the subscriber to the PNO

- The subscriber should be able to request a (customized) subscription.
- The subscriber should be able to specify the moment (time and date) of activation of the subscription.
- The subscriber should be able to end his subscription.
- The subscriber should be able to complain.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- the TMN should be able to assign resources to the subscription;
- the TMN should be able to create a subscription (including the subscriber profiles);
- the TMN should be able to activate and deactivate a subscription at a specified time and date;
- the TMN should be able to support subscriber complaint handling (e.g. it should be able to log subscriber complaints);
- the TMN should be able to request the SDF to create user profiles;
- the TMN should be able to install, remove or modify (customized) announcements in the SRF;
- the TMN should be able to request the SSF to add subscriber specific options for triggering, call gapping, service filtering, charging, etc.

b) Required functionality of the SCF:

(no requirements identified)

c) Required functionality of the SDF:

- The SDF should be able to support creation, deletion or modification of subscription data (user profiles, authentication information, etc.).

d) Required functionality of the SRF:

- The SRF should be able to have announcements installed, removed or modified (customized).

e) Required functionality of the SSF:

- The SSF should be able to add subscriber specific options for triggering, call gapping, service filtering, charging etc.

5.1.2 Requirements from the user to the PNO

(not applicable)

5.1.3 Requirements from other PNOs

(no requirements identified)

5.1.4 Internal PNO requirements

(no requirements identified)

5.2 Subscriber administration - service profile management

Subscriber administration supports the processes of exchanging data with the subscriber or user for the purpose of offering the UPT service and to configure the network with the required subscriber data and functions required in order to produce the service (service provisioning). It also supports the process of exchanging data with the network for the purpose of service profile management. This subclause deals with the service profile management part.

5.2.1 Requirements from the subscriber to the PNO

- The subscriber should be able to interrogate and modify his subscriber profile and his user profile according to the access rules agreed with the PNO.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should be able to (de)activate subscriber and user profiles.
- The TMN should support recovery of a subscriber/user profile (e.g. after an unintentional/malicious deletion of a profile).
- The TMN should be able to request the SDF to modify, (de)activate and interrogate user profiles.

b) Required functionality of the SCF:

(no requirements identified)

c) Required functionality of the SDF:

- The SDF should be able to support modification, (de)activation and interrogation of user profiles.
- The SDF should be able to notify the TMN of modifications and interrogations of user profiles.

d) Required functionality of the SRF:

(no requirements identified)

e) Required functionality of the SSF:

(no requirements identified)

5.2.2 Requirements from the user to the PNO

- The user should be able to interrogate or modify his user profile (via the IN).

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should support recovery of a user profile (e.g. after an unintentional/malicious deletion of a profile).

b) Required functionality of the SCF:

- The SCF should be able to (de)activate a user profiles.

c) Required functionality of the SDF:

- The SDF should be able to allow modifications of user profiles.
- The SDF should be able to notify the TMN of modifications or interrogations of user profiles.

d) Required functionality of the SRF:

(no requirements identified)

e) Required functionality of the SSF:

(no requirements identified)

5.2.3 Requirements from other PNOs

(no requirements identified)

5.2.4 Internal PNO requirements

- The PNO should be able to change and interrogate subscriber and user profiles.

5.3 Network provisioning management

Network provisioning management supports the processes from network planning to installation of resources (both hardware and software) ITU-T Recommendation M.3200 [1]. This ETR is mainly concerned with software installation i.e. UPT service deployment (logic and data). Service deployment covers initial deployment as well as installation of new releases of UPT software. Also, maintenance and enhancements of existing versions of UPT software are considered as service deployment activities.

Service deployment may be originated from the PNO itself (e.g. after analysis has shown that a market is expected for a new service (feature)) or from an individual subscriber (tailor made services).

5.3.1 Requirements from the subscriber to the PNO

- The subscriber should be able to request a (tailor made) service (see also subclause 5.1.1).

For a description of the required functionality of the TMN and the IN FEs, see subclause 5.1.1 and subclause 5.3.4.

5.3.2 Requirements from the user to the PNO

(not relevant)

5.3.3 Requirements from other PNOs

- The PNO should be able to co-ordinate and synchronize the process of service deployment with co-operating PNOs.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs (see also assumption 4):

a) Required functionality of the TMN:

- The TMN should be able to communicate with other TMNs to provide information on the availability of the UPT service.
- The TMN should be able to negotiate with other TMNs the exchange of information concerning UPT management, i.e., planning, configuration, performance, security and trouble ticketing.
- The TMN should be able to communicate with other TMNs so as to receive service specific resources (service logic, data and announcements) and instructions for installation.
- The TMN should be able to interact with other TMNs, in order to establish links, connections and signalling between resources in the different networks.

b) Required functionality of the SCF:

- The SCF should be able to establish a relationship with an SDF in another PNO's network (e.g. to request service data). Therefore, a list of SDF data addresses should be kept in the SCF. Upon request of the TMN, items of the list should be added, modified or deleted.

c) Required functionality of the SDF:

- The SDF should keep a list which indicates the addresses of all entities (e.g. SCPs) that may access the SDF data and the access rights of those entities. Upon request of the TMN, the SDF should be able to create, modify or delete the items in this list.

d) Required functionality of the SRF:

- The SRF should be able to have UPT announcements and service data installed (e.g. data needed for the translation of dialling tones received from the user into messages for the SCF).

e) Required functionality of the SSF:

(no requirements identified)

5.3.4 Internal PNO requirements

- The PNO should be able to co-ordinate and synchronize the process of service deployment.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

General requirements:

- The TMN should be able to co-ordinate and synchronize the process of service deployment (e.g. where multiple NEFs like SCFs, SRFs, SDFs are needed to support the service to be deployed).
- The TMN should be able to direct the NEFs to test specific service resources (e.g. to direct the SSF to test a trigger table or to direct the SCF to test service logic).
- The TMN should be able to set a newly deployed service free for use at a specified date and time.

Requirements related to the installation of software in the SCFs:

- The TMN should be able to interrogate the SCFs so as to retrieve information on service logic.
- The TMN should be able to validate software held on an SCF in order to check its integrity and to terminate validation.
- The TMN should be able to back-up a software item.
- The TMN should be able to order an SCF to revert back to a previous version of the service logic software.
- The TMN should be able to control the installation of UPT service logic on the SCFs, including the installation of patches (e.g. upgrades).
- The TMN should be able to initiate the execution of software in the SCF.
- The TMN should be able to remove service logic software from an SCF.
- The TMN should be able to restrict use of software resources on a managed system for administrative purposes.

Requirements related to service specific announcements:

- The TMN should be able to install announcements in the SRFs.

Requirements related to preparation of SSFs:

- The TMN should be able to provide the SSFs with instructions to amend the trigger table, call gapping, service filtering, charging etc.

Requirements related to preparation of SDFs:

- The TMN should be able to instruct the SDFs to install, modify and delete service data (e.g. an initial user black list).

b) Required functionality of the SCF:

- The SCF should be able to install UPT service logic (or patches) upon request of the TMN and send confirmation messages.
- The SCF should be able to initiate the execution of software upon request of the TMN.
- The SCF should be able to discard service logic upon request of the TMN.
- The SCF should be able to revert back to a previous version of the service logic software upon request of the TMN.

- The SCF should be able to provide information on service logic upon request of the TMN (e.g. what service logic software is present, what software is available for use, relationships between software etc.)
- The SCF should be able to restrict software resources from being used upon request of the TMN.
- The SCF should be able to activate service logic software at a date and time specified by the TMN.

c) Required functionality of the SDF:

- The SDF should be able to install, modify and delete service data (e.g. an initial user black list).

d) Required functionality of the SRF:

- The SRF should be able to have UPT announcements and service data installed (e.g. data needed for the translation of dialling tones received from the user into messages for the SCF).

e) Required functionality of the SSF:

- The SSF should be able to amend the trigger table, call gapping, service filtering, charging etc.

5.4 Charging, billing and accounting management

Clarification of terms:

- Charging is the process whereby information is generated, collected and transferred in order to make it possible to process usage information and to calculate the charges for which the subscriber may be billed. This is also sometimes referred to as "usage metering" and "tariffing".
- Billing is the process of transformation of the collected charging information into bills requiring payment.
- Accounting is an administrative procedure between operators aiming at sharing the costs due to inter-operator traffic. This is also sometimes referred to as "inter-PNO billing".

5.4.1 Requirements from the subscriber to the PNO

- The subscriber should receive bills according to parameters specified in his subscriber profile. Bills may be received periodically or upon the subscriber's request.
- The subscriber should be able to set individual options for charging and billing at the time of subscription (as a part of the subscriber profile).
- The subscriber should be able to activate and de-activate charging options according to his subscriber profile.
- The subscriber should be able to modify individual options for charging and billing during the life-time of the subscription according to his subscriber profile; e.g., the subscriber should be able to set and modify a maximum credit allowed to a specific user.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should be able to install and retrieve charging information to/from the network.
- The TMN should be able to process charging information and to generate bills according to the parameters specified in the subscriber profile.
- The TMN should be able to install, activate, replace and delete specific charging algorithms and procedures.

- The TMN should be able to set tariff structures.
- The TMN should be able to install, replace and delete charging and billing related announcements in the SRF (e.g. special announcements informing users of the charges to be expected for a call may be installed in the SRF. These announcements should be modified if new tariff structures are applied).
- The TMN should be able to instruct the CCF/SSF to install charging mechanisms (e.g. to select chargeable items to be included in the usage records).

b) Required functionality of the SCF:

- Charging records and options may be located in the SCF. If so, the SCF should be able to transfer this information to the TMN.

c) Required functionality of the SDF:

- Charging relevant information may be located in the SDF, e.g. as part of the user profile. If so, the SDF should be able to transfer this information to the TMN.

d) Required functionality of the SRF:

- The SRF should be able to have charging and billing related announcements installed, replaced and deleted (e.g. either the calling or the called party, or both, may be played a special announcement informing them of the charges to be expected for that call).

e) Required functionality of the CCF/SSF:

- Usage data should be produced by the CCF/SSF in the originating network (under certain circumstances also in the terminating network, i.e. in case of ISDN call forwarding).
- The CCF/SSF should be able to transfer the usage information to the TMN.

5.4.2 Requirements from the user to the PNO

- The UPT user may be able to retrieve cost information in three different situations:
 - a) before use (an indication of service usage costs per time unit are given);
 - b) during use (an indication of the costs up until that moment is given);
 - c) after use (the total costs of the service usage are given).
- The UPT user should be informed if his credit limit is exceeded.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should be able to install and retrieve charging information to/from the network.
- The TMN should be able to check a user's credit against his limits (off-line credit checking).
- The TMN should be able to exclude a UPT user from further use of resources in case of a credit limit violation.

b) Required functionality of the SCF:

- In case of credit limit violation, the SCF should notify the TMN.
- Charging records and options may be located in the SCF. If so, the SCF should be able to transfer this information to the TMN.

c) Required functionality of the SDF:

(no requirements identified)

d) Required functionality of the SRF:

(no requirements identified)

e) Required functionality of the CCF/SSF:

- Usage data should be produced by the CCF/SSF in the originating network (under certain circumstances also in the terminating network, i.e. in case of ISDN call forwarding).
- The CCF/SSF should be able to transfer the usage information to the TMN.

5.4.3 Requirements from other PNOs

- The PNO should be able to balance the costs with co-operating PNOs according to the agreed inter-PNO accounting arrangements.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN (acting as a visiting TMN) should be able to forward charging information to the home TMN of the associated subscriber.
- The TMN should support functionality needed to participate in clearing mechanisms with other UPT providers.
- The TMN should be able to set charging mechanisms in the IN network.
- The TMN should be able to retrieve charging information from the IN network.

b) Required functionality of the SCF:

- The originating SCF should be able to retrieve charging information from the SDF in the home network (needed for on-line credit checking) and to make this information available to the originating TMN.

c) Required functionality of the SDF:

- The SDF should be able to check a user's credit against his limits (on-line credit checking; only for users of home PNO subscribers); in case of credit limit violation, the SDF should notify the home TMN.

d) Required functionality of the SRF:

- The SRF should be able to have charging and billing related announcements for the users of the home PNO subscribers be installed, replaced and deleted.

e) Required functionality of the CCF/SSF:

- The CCF/SSF should be able to produce usage data for the users of the home PNO subscribers.

5.4.4 Internal PNO requirements

(no requirements identified)

5.5 Quality of service and network performance administration

Quality of service and network performance administration is concerned with the detection of QoS degradation. This "quality of service" can concern both the UPT service (features) itself (calls, authentication, registration procedures and service profile management activities), and the customer care activities (billing, service provisioning, etc.). QoS degradation can be detected by specific tests, by network performance monitoring, or by subscriber complaints.

5.5.1 Requirements from the subscriber to the PNO

- The subscriber should be able to contact its PNO in case of a QoS degradation;
- The subscriber should be notified of a UPT service malfunctioning.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should be able to detect QoS degradations and provide indications of the cause of the degradation;
- The TMN should be able to notify the subscriber of QoS degradations under the conditions agreed in the SLA.

b) Required functionality of the SCF:

- The SCF should be able to detect resource performance degradations and to notify its TMN of these situations.

c) Required functionality of the SDF:

- The SDF should be able to detect resource performance degradations and to notify its TMN of these situations.

d) Required functionality of the SRF:

- The SRF should be able to detect resource performance degradations and to notify its TMN of these situations.

e) Required functionality of the CCF/SSF:

- The CCF/SSF should be able to detect resource performance degradations and to notify its TMN of these situations.

5.5.2 Requirements from the user to the PNO

- The user should be notified of a UPT service malfunctioning (e.g. via SRF announcements).

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should be able to detect QoS degradations as perceived by its service users and provide indications of the cause of the degradation;
- The TMN should be able to install in the SRF an announcement for indication of the QoS degradation to the user;
- The TMN should be able to re-set the triggering in the SSF for the degraded services, so that the error announcements by the SRF will be played. It is also possible that the SCF contains some specific service logic to handle such a situation.

b) Required functionality of the SCF:

- The SCF should be able to detect resource performance degradations and to notify its TMN of these situations.

c) Required functionality of the SDF:

- The SDF should be able to detect resource performance degradations and to notify its TMN of these situations.

d) Required functionality of the SRF:

- The SRF should be able to detect resource performance degradations and to notify its TMN of these situations.

e) Required functionality of the CCF/SSF:

- The CCF/SSF should be able to detect resource performance degradations and to notify its TMN of these situations.

5.5.3 Requirements from other PNOs

- The PNO should be able to keep other PNOs informed about network or service performance degradations.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should be able to keep other TMNs informed of exceptional situations in its own UPT network that may influence the QoS (e.g. maintenance activities or fault situations which temporarily influence service offering).

b) Required functionality of the SCF:

- The SCF should be able to detect resource performance degradations and to notify its TMN of these situations.

c) Required functionality of the SDF:

- The SDF should be able to detect resource performance degradations and to notify its TMN of these situations.

d) Required functionality of the SRF:

- The SRF should be able to detect resource performance degradations and to notify its TMN of these situations.

e) Required functionality of the CCF/SSF:

- The CCF/SSF should be able to detect resource performance degradations and to notify its TMN of these situations.

5.5.4 Internal PNO requirements

- The PNO should receive detailed information of all QoS degradations.
- The PNO should be provided with means to react to all sorts of QoS and network performance degradations.

See subclause 5.5.2 for a description of the functionality required in the TMN and the IN FEs.

5.6 Maintenance management

Maintenance management supports the processes of fault detection, fault reporting, fault localization and protection of resources (both hardware and software) used to provide UPT.

5.6.1 Requirements from the subscriber to the PNO

The QoS management activities as described in the subclause 5.5 will inform the subscriber of fault situations that impact the services as provided to the subscriber. Therefore, here just reference is made to subclause 5.5.1.

5.6.2 Requirements from the user to the PNO

The QoS management activities as described in the subclause 5.5 will inform the user of fault situations that impact the services as provided to the user. Therefore, here just reference is made to subclause 5.5.2.

5.6.3 Requirements from other PNOs

- The PNO should be able to inform other PNOs about fault situations.
- The PNO should be able to receive reports of fault situations of other PNOs.
- The PNO should be able to react to reports of fault situations of other PNOs according to pre-defined inter-PNO arrangements.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should be able to keep other TMNs informed of exceptional situations in its own UPT network (e.g. maintenance activities or fault situations which temporarily influence service offering).
- The TMN should be able to interact with other TMNs to request (or view) information on the status and condition of resources from other PNOs.
- The TMN should be able to request other TMNs to execute (or participate in) tests and to provide the test results.
- The TMN should be able to execute (or participate in) tests upon the request of another TMN and to provide the test results.
- The TMN should be able to receive indications of exceptional situations from other TMNs (e.g. when a particular SCF in the other PNOs network is temporarily unavailable for interaction).

b) Required functionality of the SCF:

See subclause 5.6.4.

c) Required functionality of the SDF:

See subclause 5.6.4.

d) Required functionality of the SRF:

See subclause 5.6.4.

e) Required functionality of the CCF/SSF:

See subclause 5.6.4.

5.6.4 Internal PNO requirements

- The PNO should receive detailed information of all fault situations;
- The PNO should be provided with means to react to all fault situations.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

Requirements related to alarm handling:

- The TMN should be able to set alarm and event thresholds in SCF, SDF, SRF and SSF;
- The TMN should support fault diagnosis and fault correlation;
- The TMN should be able to support the recovery of subscriber profiles, user profiles or any other UPT service related data.

Requirements related to change-over:

- The TMN should be able to designate backup resources for SCF, SDF, SRF and SSF;
- The TMN should be able to log the relationships between resources and their backup resources;
- The TMN should be able to define criteria (thresholds) according to which a change-over to backup resources (or change-back to primary resources) will be carried out;
- The TMN should be able to monitor change over threshold parameters and initiate a change-over (change-back) if threshold values are reached.

Requirements related to testing:

- The TMN should support diagnostic testing (to find the cause of a fault) as well as confidence testing (preventive tests so as to verify correct functionality of a resource);
- The TMN should be able to initiate, suspend, resume and terminate tests in SCF, SDF, SRF and SSF;
- The TMN should be able to specify tests that may be initiated, suspended, resumed or terminated when pre-defined conditions are encountered;
- The TMN should support the scheduling and sequencing of tests;
- The TMN should support the logging of test results.

b) Required functionality of the SCF:

- Alarms and events should be logged;
- The SCF should create, modify and delete alarm and event thresholds as requested by the TMN;
- The SCF should initiate, suspend, resume and terminate tests as requested by the TMN (e.g. tests of service logic);
- The SCF should be able to report test results to the TMN.

c) Required functionality of the SDF:

- Alarms and events should be logged;
- The SDF should create, modify and delete alarm and event thresholds as requested by the TMN;
- The SDF should initiate, suspend, resume and terminate tests as requested by the TMN;
- The SDF should be able to report test results to the TMN.

d) Required functionality of the SRF:

- The SRF should be able to log events and to send alarms to the TMN;
- The SRF should be able to create, modify and delete alarm and event thresholds as requested by the TMN;
- The SRF should be able to initiate, suspend, resume and terminate tests as requested by the TMN (e.g. tests of announcements);
- The SRF should be able to report test results to the TMN;
- The SRF should be able to install, replace or delete announcements related to fault management. Examples are: announcements telling the user that a service feature is temporarily unavailable due to abnormal conditions.

e) Required functionality of the CCF/SSF:

- Alarms and events should be logged;
- The SSF should create, modify and delete alarm and event thresholds as requested by the TMN;
- The SSF should initiate, suspend, resume and terminate tests as requested by the TMN (e.g. tests of trigger table);
- The SSF should be able to report test results to the TMN.

5.7 Security administration

The purpose of security administration is to protect the TMN and the network elements against unauthorized access, and to guard against abuse of the UPT service.

5.7.1 Requirements from the subscriber to the PNO

Requirements related to security of the UPT service (execution)

- The subscriber should be able to prove his identity by means of the authentication procedure requested by the PNO;
- The subscriber should be able to change the authentication mechanisms for its users;
- The subscriber should be able to negotiate with the PNO the access rights to subscriber profile data and user profile data.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should provide adequate authentication mechanisms to prove the identity of subscribers;
- The TMN should provide adequate means to store confidential subscriber authentication information;
- The TMN should provide adequate means to change the access rights to subscriber profile data.

b) Required functionality of the SCF:

(no requirements identified)

c) Required functionality of the SDF:

- The SDF should provide adequate authentication mechanisms to prove the identity of subscribers;
- The SDF should provide adequate means to store confidential subscriber authentication information;
- The SDF should support the modification of authentication mechanisms for UPT users;
- The SDF should provide adequate means to change the access rights to user profile data;

Annex A provides additional information on authentication mechanisms provided by the SDF.

d) Required functionality of the SRF:

(no requirements identified)

e) Required functionality of the CCF/SSF:

(no requirements identified)

5.7.2 Requirements from the user to the PNO

Requirements related to security of the UPT service (execution)

- The UPT user should be able to prove his identity by means of the authentication procedure requested by the UPT network.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

(no requirements identified)

b) Required functionality of the SCF:

(no requirements identified)

c) Required functionality of the SDF:

- The SDF should provide adequate authentication mechanisms to prove the identity of users.
- The SDF should provide adequate means to store confidential user authentication information.

d) Required functionality of the SRF:

- The SRF should be able to have security related announcements installed, replaced or deleted. These are announcements to guide the user through the authentication process. Example are: announcements to request the user to type his PIN or announcements telling that the PIN was incorrect, asking the user to retry.

e) Required functionality of the CCF/SSF:

(no requirements identified)

5.7.3 Requirements from other PNOs

- The PNO should be able to prove the identity of another PNO by authentication procedures.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

- The TMN should provide adequate authentication mechanisms to prove the identity of other PNOs;
- The TMN should provide adequate means to store confidential PNO authentication information.

b) Required functionality of the SCF:

(no requirements identified)

c) Required functionality of the SDF:

(no requirements identified)

d) Required functionality of the SRF:

(no requirements identified)

e) Required functionality of the CCF/SSF:

(no requirements identified)

5.7.4 Internal PNO requirements

- The PNO should be able to prove the identity of his staff by means of authentication procedures;
- The PNO should be able to secure the access to its network and its TMN from third parties;
- The PNO should be able to modify security mechanisms for subscribers and users.

To be able to satisfy these requirements, the following functionality is to be included in the TMN and the IN FEs:

a) Required functionality of the TMN:

Requirements related to management of security

- For each service feature, the TMN should be able to define the level of security (e.g. type of authentication to access a particular feature);
- The TMN should be able to modify the black list stored in the AE;

- The TMN should process and log security related information (e.g. creation and logging of statistics on security critical events);
- The TMN should be able to modify security mechanisms for subscribers.

b) Required functionality of the SCF:

(no requirements identified)

c) Required functionality of the SDF/AE:

Requirements related to management of security

- In case of security alarm (e.g. security critical event), the SDF should notify the TMN. The following information items should be collected by the SDF and should be sent to the TMN: security critical event identification, PUI, the terminal access number, time and date and authentication type (weak, one pass strong, two pass strong);
- The SDF should support the creation, modification and deletion of black lists;
- The SDF should be able to modify security mechanisms for users.

d) Required functionality of the SRF:

(no requirements identified)

e) Required functionality of the CCF/SSF:

(no requirements identified)

6 Analysis of UPT scenarios

In this clause, a number of UPT scenarios is analysed to identify the information flows on q3 and x reference points. Also the corresponding management functions are identified. This analysis serves to identify the information and the management services in the succeeding clauses (clauses 7 and 8). Based on figure 2, figure 3 illustrates the functional architecture indicating the various reference points.

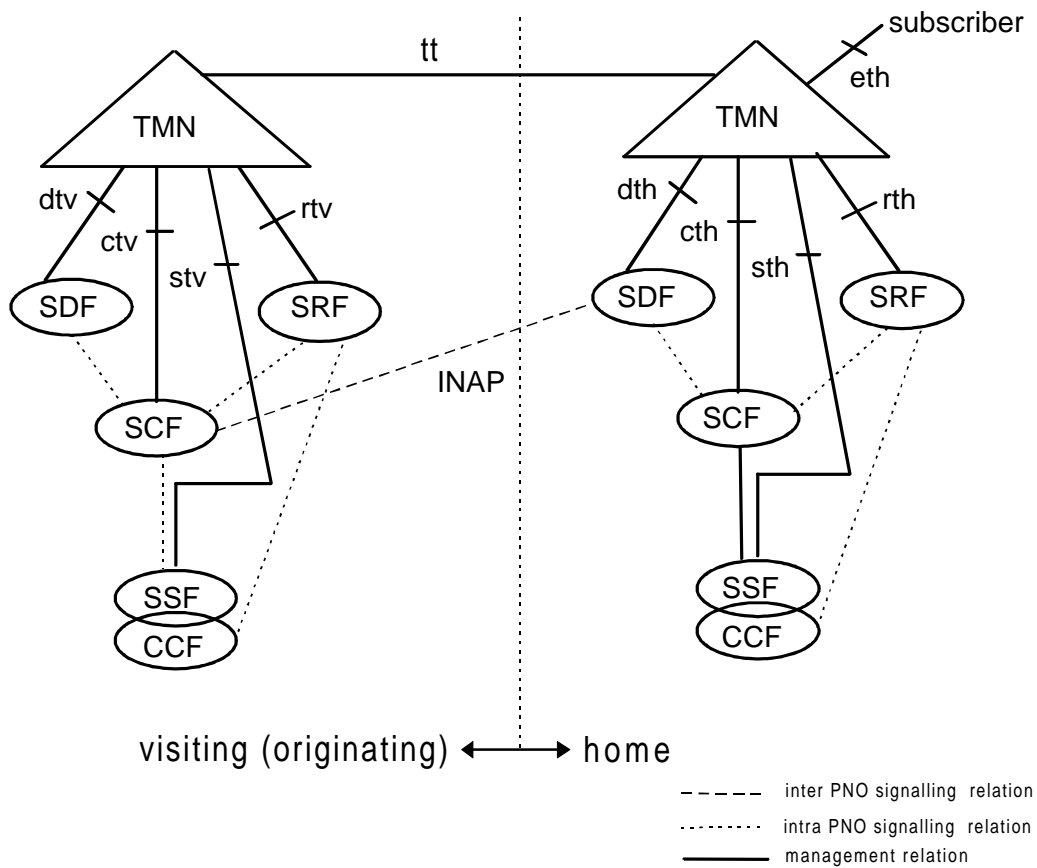


Figure 3: The reference points for information flows

The figure depicts the relationship between two TMNs in separate domains and their associated IN functional entities. The separate TMNs communicate with each other over a TMN x reference point. As this figure is used as a basis for the following UPT scenarios and in order to aid clarification a unique acronym was assigned to each reference point. These acronyms are adopted in the scenario tables below giving the reader a clear mapping between these tables and figure 3. Each reference point is denoted as a three letter acronym ABC, where A and B have possible values c, d, e, r, s, t; and C has possible values h or v. Hereby, the values (letters) c, d, e, r, s, t, h and v have the following meaning:

letter	relates to
c	SCF
d	SDF
r	SRF
s	SSF
e	external (subscriber)
t	TMN
h	home domain
v	visiting domain

As an example, reference point dtv is the reference point between SDF and TMN in the visiting domain. The x reference points between the TMNs is denoted as tt. With the exception of this reference point and reference point eth (subscriber to TMN, see also assumption 7 in subclause 4.2), all reference points are q3 compliant.

Table 2 lists the UPT scenarios which are analysed below. The scenarios have been chosen to identify the most essential information for the identified reference points. The scenarios should however not be seen as exhaustive.

Table 2: Overview of UPT scenarios

number	activity	role	domain	comment
1	service profile management	UPT user	home	
2	service profile management	UPT user	visiting	
3	service profile management	UPT subscriber	home	via TMN and via IN
4	service provisioning	subscriber	home	new subscriber via TMN
5	registration	UPT user	home	
6	registration	UPT user	visiting	
7	make outgoing call	UPT user	home	
8	make outgoing call	UPT user	visiting	
9	request bill	UPT subscriber	home	via TMN
10	authentication	UPT user	home	
11	authentication	UPT user	visiting	
12	authentication	UPT subscriber	home	via TMN and via IN
13	complaint	UPT subscriber	home	e.g. bad QoS, too high bill, etc.; via TMN
14	deployment of UPT	PNO	home	via Q3 and X
15	security event	UPT user	home	e.g. fraud, violation
16	security event	UPT user	visiting	
17	performance management	PNO	home	
18	performance management	PNO	visiting	
19	service modification	PNO	home	via Q3 and X
20	request statistics	UPT subscriber	home	via TMN
21	request statistics	PNO	home	
22	UPT subscription procedure	UPT subscriber	home	add UPT user (via TMN)

In all scenarios it is assumed that authentication of the actor is required beforehand, unless explicitly stated otherwise. The authentication procedures are described in subclauses 6.10 to 6.12.

The analysis of each scenario is performed in 3 steps:

- 1 Short description of the scenario.
- 2 For each of the scenario, an analysis of the information flow(s) for the reference points as indicated in figure 3. To this aim, for each scenario a table is created, wherein for each information flow its parameters (information elements) and the management purpose for having the visibility of these parameters is indicated. These "purposes" are structured according to the same categorization as used for the management requirements (see table 1 in clause 5). Note however that these purpose areas should only be seen as suggestion and clarification why the information elements were identified. The reason for this information to be available on the respective reference points may in practice be PNO specific.
- 3 Determination of Management functions (MFs) at both ends of the reference point.

6.1 Service profile management by UPT user in home domain

Description:

The service profile management enables the UPT user to access and modify his user profile data which are contained in his user profile, in order to provide, tailor and withdraw UPT service features and options. The information elements in the user profile that can be selected by the user are defined e.g. in subclause 2.4 of ETR 055-08 [5].

Information flow:

IF	ref. point	from	to	information elements	purpose
IF 1.1	dth	SDFh	TMNh	procedure ID PUI date time attribute ID duration terminal number old value new value	DJE DJ DJ DJ DJ E J J J
NOTE: The letters in the purpose columns refer to the letters in table 1, clause 5.					

Management functions:

- MF1.1: Collect and log the information elements.
 This MF is located in the SDF.
- MF1.2: Retrieve and process the information elements from the network.
 This MF is located in the TMN.

6.2 Service Profile management by UPT user in visiting domain

Description:

The service profile management enables the UPT user to access and modify his user profile data which are contained in his user profile, in order to provide, tailor and withdraw UPT service features and options. The information elements in the user profile that can be selected by the user are defined e.g. in subclause 2.4 of ETR 055-08 [5].

Information flow:

IF	ref. point	from	to	information elements	purpose
IF 2.1	dth	SDFh	TMNh	same as IF1.1 plus PNOo ID	same as IF1.1 DJ
IF 2.2	ctv	SCFo	TMNo	same as IF1.1 plus PNOh ID	same as IF1.1 DJ

Management functions:

- MF2.1: Collect and log the information elements.
 This MF is located in the SDFh and the SCFo.
- MF2.2: Retrieve and process the information elements from both originating (visiting) and home networks.
 This MF is located in TMNo and TMNh.

6.3 Service Profile management by UPT subscriber in home domain

- Case 1: Management of user profiles (of his UPT users)

Description:

Service profile management enables the UPT subscriber to access and modify the user profile data which are contained in the user profiles of his UPT users, in order to provide, tailor and withdraw UPT service features and options.

NOTE: According to assumption 7 (see subclause 4.2), the UPT subscriber performs this management procedure with UPT service logic via the IN. In general, he will have different access rights (to user profile data) than the UPT user.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF3.1	dth	SDFh	TMNh	same as IF1.1 plus subscriberID	same as IF1.1 plus A ADJ

Management functions:

MF3.1: Collect and log the information elements.
 This MF is located in the SDFh.

MF3.2: Retrieve and process the information elements from the home network.
 This MF is located in TMNh.

- Case 2: Management of his subscriber profile

Description:

Service profile management enables the UPT subscriber also to access and modify the subscriber profile data which are contained in his subscriber profile, in order to provide, tailor and withdraw UPT service features and options.

NOTE: According to assumption 7, the UPT subscriber performs this management procedure via the TMN (reference point eth). According to assumption 8, the subscriber profile is only stored in the TMNh.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF3.2	eth	subscr.	TMNh	procedure ID subscriberID attributeID new value	ADEJ ADJ AJ AJ
IF3.3	eth	TMNh	subscr.	confirmation error	A A

Management functions:

MF3.3: Retrieve, log and process the information elements from the subscriber.
 This MF is located in the TMNh.

MF3.4: Send confirmation message to UPT subscriber.
 This MF is located in the TMNh.

MF3.5: Send error message to UPT subscriber.
 This MF is located in the TMNh.

6.4 Service provisioning for UPT subscriber in home domain

Description:

An individual contacts a PNO and requests the UPT service. After the negotiation of the contract the individual is a UPT subscriber. The PNO which is playing the role of single point of contact will be the home PNO for the UPT subscriber.

NOTE: see subclause 6.22 for adding new UPT users.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF4.1	eth	subscriber	TMNh	name address billing information requested authentication procedures requested security options requested charging options requested basic services	A A A A A A A
IF4.2	eth	TMNh	subscriber	subscriber ID subscribed authentication procedures subscribed security options subscribed charging options subscribed basic services	A A A A A

Management functions:

- MF4.1: Retrieve the subscriber data (the information elements).
 This MF is located in the TMNh.
- MF4.2: Create the subscriber profile.
 This MF is located in the TMNh.
- MF4.3: Activate the subscriber profile.
 This MF is located in the TMNh.
- MF4.4: Send subscription result to the subscriber.
 This MF is located in the TMNh.

6.5 Registration of the UPT user in home domain

Description:

In order to make use of the UPT subscription, the UPT user needs to register with the UPT service provider (i.e. PNO). With this, the user indicates that calls directed to his personal number should be routed to a certain terminal (specified by the ARA given) or that he wants to perform outgoing UPT calls from the specified ARA. A general description of UPT InCall, OutCall and AllCall registration can be found in ETS 300 779 [3].

In case of a remote registration the specified ARA will be different from the address of the terminal where the user carries out the registration. Therefore, the terminal number has also to be collected by the network.

The registration is validated by the SCF according to the settings in the user profile stored in the SDF. The user is informed if the registration was successful or not. The procedure to notify the user of the registration result is not part of any management function.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF 5.1	dth	SDFh	TMNh	proc. ID PUI ARA terminal number date time registration result duration	DEJ DJ J J DJ DJ J E

Management functions:

- MF5.1: Collect and log the registration information (the information elements).
 This MF is located in the SDFh.
- MF5.2: Retrieve and process the registration information from the network.
 This MF is located in the TMNh.

6.6 Registration of the UPT user in visiting domain

Description:

From the point of view of the user, there is no difference between a registration in the visiting domain and a registration in the home domain as described in subclause 6.5.

As the registration in the visiting domain involves two PNOs, management information will have to be collected in both networks.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF6.1	dth	SDFh	TMNh	same as IF5.1 plus PNOo ID	same as IF5.1 DJ
IF6.2	ctv	SCFo	TMNo	same as IF5.1 plus PNOh ID	same as IF5.1 DJ

Management functions:

- MF6.1: Collect and log registration information (the information elements).
 This MF is located in the SDFh and the SCFo.
- MF6.2: Retrieve and process registration information from the network.
 This MF is located in TMNo and TMNh.

6.7 Make outgoing call by UPT user in home domain

Description:

The UPT user makes a call from the home network. The called party may or may not be a UPT user. The network recognizes the UPT access code and inhibits the normal charging procedure. The charging rate applicable depends on if the called party is UPT in roamed position or not.

It is assumed that the call records are not stored in the SDFh (see assumption 10). The information elements of the call records are described in ETR 065 [6].

Information flow:

IF	ref. point	from	to	information elements	purpose
IF7.1	cth	SCFh	TMNh	callRecord	D
IF7.2	sth	CCF/SSFh	TMNh	callRecord	D

Management functions:

- MF7.1: Collect and log usage information.
 This MF is located in the CCFh/SSFh and/or in the SCFh.
- MF7.2: Retrieve and process usage information from the network.
 This MF is located in the TMNh.

6.8 Make outgoing call by UPT user in visiting domain

Description:

The UPT user makes a call from the visiting network. The called party may or may not be a UPT user. The network recognizes the UPT access code and inhibits the normal charging procedure. The charging rate applicable depends on if the called party is a UPT user in roamed position or not. The originating network collects the charging data and stores it in the visiting TMN.

It is assumed that the charging records are not stored in the SDF (see assumption 10).

Information flow:

IF	ref. point	from	to	information elements	purpose
IF8.1	ctv	SCFo	TMNo	same as IF7.1 plus PNOh ID	D D
IF8.2	stv	CCF/ SSFo	TMNo	same as IF7.1 plus PNOh ID	D D
IF8.3	tt	TMNo	TMNh	same as IF7.1 plus PNOo ID	D D

Management functions:

- MF8.1: Collect and log usage information (the information elements).
This MF is located in the CCFo/SSFo and/or in the SCFo.
- MF8.2: Retrieve and process usage information from the network.
This MF is located in the TMNo.
- MF8.3: Send charging information to home PNO of calling party.
This MF is located in the TMNo.
- MF8.4: Retrieve and log charging information from visiting PNO.
This MF is located in the TMNh.

6.9 Request bill by UPT subscriber in home domain

Description:

The request bill feature enables the UPT subscriber to get a bill showing the costs associated with the use of the UPT service by its UPT users. In the scenario it is not considered how detailed this bill should be and how it should be presented to the UPT subscriber. The method by which the bill is presented to the UPT subscriber does not have any influence on the network functionality.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF9.1	eth	subscriber	TMNh	subscriber ID procedure ID billing period UPT number	D D D D
IF9.2	eth	TMNh	subscr.	(itemized) bill	D

Management functions:

- MF9.1: Retrieve the bill request (the information elements) from the subscriber.
 This MF is located in the TMNh.
- MF9.2: Calculate bill and send to subscriber.
 This MF is located in the TMNh.

6.10 Authentication of UPT user in home domain

Description:

The UPT user provides authentication information to the IN network in order to prove his claimed identity.

Authentication will mostly be required to be successfully performed as a prerequisite to several other UPT service features including registration, service profile modification, direct outgoing call, etc. For this reason it is considered here, that the service feature authentication will not be charged separately. Instead we assume, that the proper charging will be applied as part of the invoked service feature.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF10.1	dth	SDFh	TMNh	Procedure ID PUI Time Date Terminal Number Auth. status (+cause) # unsuccessful attempts	J J J J J J J

Management functions:

- MF10.1: Collect and log the information elements.
 This MF is located in the SDFh.
- MF10.2: Retrieve and process the information elements from the network.
 This MF is located in the TMNh.

6.11 Authentication of UPT user in visiting domain

Description:

From the point of view of the user, there is no difference between an authentication in the visiting domain and an authentication in the home domain as described in subclause 6.10. However, the visiting domain may not support the same authentication mechanisms as the home domain. See assumption 4 in subclause 4.2 for a discussion on this.

As the authentication in the visiting domain involves two PNOs, management information will have to be collected in both networks.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF11.1	dth	SDFh	TMNh	same as IF10.1 plus PNOo ID	J J
IF11.2	cto	SCFo	TMNo	same as IF10.1 plus PNOh ID duration	D JD D

Management functions:

- MF11.1: Collect and log the information elements.
 This MF is located in SCFo and SDFh.
- MF11.2: Retrieve and process the information elements from the network.
 This MF is located in the TMNo and the TMNh.

6.12 Authentication of UPT subscriber in home domain

Authentication by the TMNh

Description:

The subscriber provides authentication information to the TMN in order to prove his claimed identity.

Subscriber authentication is a prerequisite to several TMN management activities, such as modification of the subscriber profile, request billing information, etc.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF12.1	eth	subscr.	TMNh	subscriber ID authentic. information	J J
IF12.2	eth	TMNh	subscriber	successful error	J J

Management functions:

- MF12.1: Retrieve and process subscriber input for the authentication procedure.
 This MF is located in the TMNh.
- MF12.2: Verify the identity of the subscriber.
 This MF is located in the TMNh.
- MF12.3: Notify the subscriber about the authentication result.
 This MF is located in the TMNh.

Authentication by the IN network

Description:

The subscriber provides authentication information to the IN in order to prove his claimed identity.

Subscriber authentication is a prerequisite to the UPT service feature "Service Profile Management by UPT Subscriber" which allows him to modify the user profiles of his subscription. Due to the higher security requirements of the UPT subscriber only a strong authentication should be performed.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF12.3	dth	SDFh	TMNh	Procedure ID Subscriber ID Time Date Terminal Number Auth.status (+cause) # unsuccessful attempts	J J J J J J J

Management functions:

MF12.4: Collect and log information elements.
 This MF is located in the SDFh.

MF12.5: Retrieve and process information elements from the network.
 This MF is located in the TMNh.

6.13 Complaint by UPT subscriber in home domain

Description:

A subscriber issues a complaint to the home PNO. This complaint can concern all UPT service and customer care related issues like the quality of the UPT service, the bill, security issues, service provisioning etc.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF13.1	eth	subscriber	TMNh	procedureID subscriber ID complaint description	BDEJ BDEJ BDEJ
IF13.2	eth	TMNh	subscr.	complaint confirmation	BDEJ
IF13.3	eth	TMNh	subscr.	complaint handling result	BDEJ

Management functions:

MF13.1: Retrieve the complaint information (the information elements) from the subscriber.
 This MF is located in the TMNh.

MF13.2: Send a complaint confirmation to the subscriber.
 This MF is located in the TMNh.

MF13.3: Investigate and solve the complaint.
 This MF is located in the TMNh.

MF13.4: Send complaint handling result (with possible payment return) to the subscriber.
 This MF is located in the TMNh.

6.14 Deployment of UPT by PNO in home domain

Description:

The software to run the UPT service is installed in the equipment of the home PNO. After the installation and activation procedure, the PNO is capable of offering and operating UPT subscriptions.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF14.1	cth	TMNh	SCFh	UPT service logic test instructions installation instructions activate instructions	B B B B
IF14.2	dth	TMNh	SDFh	generic UPT data initial black list test instructions installation instructions activate instructions	B B B B B
IF14.3	rth	TMNh	SRFh	UPT announcements test instructions installation instructions activate instructions	B B B B
IF14.4	sth	TMNh	SSFh	trigger criteria feature interaction settings call gap parameters service filter parameters service key settings charging options test instructions installation instructions activate instructions	B B B B B B B B B
IF14.5	cth	SCFh	TMNh	test results installation results	B B
IF14.6	dth	SDFh	TMNh	test results installation results	B B
IF14.7	rth	SRFh	TMNh	test results installation results	B B
IF14.8	sth	SSFh	TMNh	test results installation results	B B
IF14.9	tt	TMNh	TMNx	deployment information	B

Remark to IF14.9: TMNx belongs to any other co-operating PNO (see subclause 4.2, assumption 4).

Management functions:

- Management functions related to the UPT service logic:

- MF14.1: Send UPT service logic: TMN sends UPT service logic to SCF; the SCF could temporarily store the UPT service logic in a buffer e.g. for testing purposes.
This MF is located in the TMN.
- MF14.2: UPT service logic received: SCF notifies the TMN that the UPT service logic was received.
This MF is located in the SCF.
- MF14.3: Test UPT service logic: TMN directs SCF to test the UPT service logic.
This MF is located in the TMN.
- MF14.4: Results of service logic test: SCF notifies TMN that the test of the UPT service logic was successful.
This MF is located in the SCF.
- MF14.5: Install UPT service logic: TMN directs SCF to install the UPT service logic in a specific part of the memory.
This MF is located in the TMN.
- MF14.6: UPT service logic installed: SCF notifies TMN that the UPT service logic is installed.
This MF is located in the SCF.

- Management functions related to the generic UPT data:

- MF14.7: Create generic UPT data: TMN creates and configures the generic UPT data.
This MF is located in the TMN.
- MF14.8: Send generic UPT data: TMN sends the generic UPT data to SCF/SDF.
This MF is located in the TMN.
- MF14.9: Generic UPT data received: SCF/SDF notifies TMN that the Generic UPT data were received.
This MF is located in the SCF/SDF.
- MF14.10: Test generic UPT data: TMN directs SCF/SDF to test the generic UPT data.
This MF is located in the TMN.
- MF14.11: Results of the generic UPT data test: SCF/SDF notifies TMN that the test of the generic UPT data was successful.
This MF is located in the SCF/SDF.
- MF14.12: Install generic UPT data: TMN directs SCF/SDF to install the generic UPT data in a specific part of memory.
This MF is located in the TMN.
- MF14.13: Generic UPT data installed: SCF/SDF notifies TMN that the generic UPT data are installed.
This MF is located in the SCF/SDF.

- Management functions related to the black list:

- MF14.14: Create black list: TMN creates and configure black list.
This MF is located in the TMN.
- MF14.15: Send black list: TMN sends the black list to SCF/SDF.
This MF is located in the TMN.
- MF14.16: Black list received: SCF/SDF notifies TMN that the black list was received.
This MF is located in the SCF/SDF.
- MF14.17: Test black list: TMN directs SCF/SDF to test the black list.
This MF is located in the TMN.
- MF14.18: Results of the service logic test: SCF/SDF notifies TMN that the test of the black list was successful.
This MF is located in the SCF/SDF.
- MF14.19: Install black list: TMN directs SCF/SDF to install the black list in a specific part of the memory.
This MF is located in the TMN.
- MF14.20: Black list installed: SCF/SDF notifies TMN that the black list is installed.
This MF is located in the SCF/SDF.

- Management functions related to the UPT announcements:

- MF14.21: Prepare UPT announcements: TMN prepares the UPT announcements.
This MF is located in the TMN.
- MF14.22: Send UPT announcements: TMN sends the UPT announcements to SRF.
This MF is located in the TMN.

- MF14.23: UPT announcements received: SRF notifies TMN that the UPT announcements were received.
This MF is located in the SRF.
- MF14.24: Test UPT announcements: TMN directs SRF to test the UPT announcements.
This MF is located in the TMN.
- MF14.25: Results of the service logic test: SRF notifies TMN that the test of the UPT announcements was successful.
This MF is located in the SRF.
- MF14.26: Install UPT announcements: TMN installs the UPT announcements in the SRF.
This MF is located in the TMN.
- MF14.27: UPT announcements installed: SRF notifies the TMN that the UPT announcements are installed.
This MF is located in the SRF.

- Management functions related to SSF settings:

- MF14.28: Update SSF settings: TMN directs the SSF to update the parameters related to the information elements of IF14.4 (trigger criteria etc.).
This MF is located in the TMN.
- MF14.29: SSF settings updated: SSF notifies TMN that the parameters are updated.
This MF is located in the SSF.
- MF14.30: Test SSF settings: TMN directs SSF to test the new parameter settings.
This MF is located in the TMN.
- MF14.31: Results of the SSF settings test: SSF notifies TMN that the test of the new parameter settings was successful.
This MF is located in the SSF.

- Other Management functions:

- MF14.32: Test UPT: The UPT service as a whole is tested (e.g. in a pilot).
This MF is located in the TMN and the IN network.
- MF14.33: Activate UPT: The UPT service is released for usage (i.e. activated).
This MF is located in the TMN and in the IN network.

- Information flows and Management functions related to inter-PNO aspects:

- MF14.34: Send deployment information to other TMN: PNO notifies co-operating PNOs about new deployments as far as relevant for the other TMN (see also subclause 4.2, assumption 4 and subclause 5.3.3 A)).
This MF is located in the TMN.
- MF14.35: Receive deployment information from other TMN: PNO is notified by an other co-operating PNO about new deployments.
This MF is located in the TMN.

6.15 Security event in home domain

Description:

The UPT user fails to provide the correct information while performing a procedure in the home network. An announcement is issued by the network. The following events are modelled:

- The UPT user fails to provide the correct PIN during authentication;
- The UPT user fails to repeat the correct new PIN during change of PIN;
- The UPT user attempts InCall registration from invalid terminal access;
- The UPT user violates the allowed number of outgoing call using follow-on;
- The UPT user attempts Remote InCall Registration to invalid address (ARA). For example dedicated number or wrong address;
- The UPT user performs an unauthorized or non-existent service feature attempt;
- The UPT user attempts the authentication procedure while his/her PUI is blocked;
- The UPT user tries to change an attribute to invalid value.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF15.1	cth	SCFh	TMNh	Procedure ID PUI Terminal Number Date Time Cause ARA Service feature ID Attribute ID Attribute value	J J J J J J J J J J
IF15.2	dth	SDFh	TMNh	Procedure ID PUI Terminal Number Date Time Cause	J J J J J J

Management functions:

- MF15.1: Collect and log security event information (the information elements). This MF is located in SDFh and SCFh.
- MF15.2: Inform the TMN of possible breaches of security. This MF is located in SDFh and/or SCFh.
- MF15.2: Retrieve and process the security events from the network. This MF is located in TMNh.
- MF15.3: Determine if security violations have occurred. This MF is located in TMNh.

6.16 Security event in visiting domain

Description:

The UPT user fails to provide the correct information while performing a procedure in visited network. An announcement is issued by the network. The same events as in subclause 6.15 are modelled.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF16.1	ctv	SCFo	TMNo	IF15.1 plus PNOh ID	J J
IF16.2	dth	SDFh	TMNh	IF15.1 plus PNOo ID	J J

Management functions:

MF16.1: Collect and log security event information (the information elements).
This MF is located in SDFh and SCFo.

MF16.2: Retrieve and process the security events from the network.
This MF is located in TMNh and TMNo.

6.17 Performance management by PNO in home domain

Description:

The role of performance management is to gather statistical data for the purpose of monitoring and correcting the behaviour and effectiveness of the network, network element or equipment and to aid in planning and analysis.

The TMN in home domain (TMNh) collects network performance data from the Network Element Functions (NEFs) to derive the Quality of Service (QoS) as perceived by the users. The TMN may request performance data to be sent from the NE, or performance reports may be sent automatically on a scheduled or threshold basis.

In a long term configuration, UPT should be supported by all networks (e.g. PSTN, ISDN, B-ISDN, mobile and private networks) in service. The performance of the networks may therefore influence the performance of UPT.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF17.1	cth	TMNh	SCFh	performance ID perf. parameter ID	E E
IF17.2	dth	TMNh	SDFh	performance ID perf. parameter ID	E E
IF17.3	sth	TMNh	CCFh/ SSFh	performance ID perf. parameter ID	E E
IF17.4	rth	TMNh	SRFh	performance ID perf. parameter ID	E E
IF17.5	cth	SCFh	TMNh	performance ID perf. parameter ID value	E E E
IF17.6	dth	SDFh	TMNh	performance ID perf. parameter ID value	E E E
IF17.7	sth	CCFh/ SSFh	TMNh	performance ID perf. parameter ID value	E E E
IF17.8	rth	SRFh	TMNh	performance ID perf. parameter ID value	E E E

Management functions:

- MF17.1: Collect and log performance information.
 This MF is located in the IN FEs (CCF/SSF, SCF, SDF and SRF).
- MF17.2: Request performance information from the IN FEs.
 This MF is located in the TMNh.
- MF17.3: Send performance information to the TMN.
 This MF is located in the IN FEs.
- MF17.4: Retrieve and process performance information from the network.
 This MF is located in the TMNh.
- MF17.5: Calculate the quality of service as perceived by the users. This should cover both the quality of the UPT service (features) invocation and the quality of the administrative (customer care) operations (billing, service provisioning etc.).

6.18 Performance management by PNO in visiting domain

Description:

See subclause 6.17.

Information flow:

All information described in subclause 6.17 is also relevant for performance management by the PNO of a visiting domain. As the home PNO is responsible for the service offered to the subscriber, it may want to request the performance information as retrieved by the visited PNO(s) for its own purpose (e.g. calculation of QoS). This additional inter-PNO communication is described below.

IF	ref. point	from	to	information elements	purpose
IF18.1	tt	TMNh	TMNx	performance ID perf. parameter ID	E E
IF18.2	tt	TMNx	TMNh	performance ID perf. parameter ID value	E E E

Remark: TMNx belongs to any other co-operating PNO (see clause 4, assumption 4).

Management functions:

- MF18.1: Request performance information.
This MF is located in the TMNh.
- MF18.2: Send performance information to other PNO.
This MF is located in the TMNx.
- MF18.3: Retrieve, process and log performance information from other PNOs
This MF is located in the TMNh.

6.19 UPT service modification in home domain

Description:

This event occurs when:

- a new release of the UPT software is being installed;
- the existing UPT software is being amended (e.g. a new supplementary service is introduced); or
- the existing software is being maintained (e.g. correction of a software flaw).

UPT service modification may require a reconfiguration of the database (e.g. when a new service feature is added).

Information flow:

IF	ref. point	from	to	information elements	purpose
IF19.1	cth	TMNh	SCFh	same as IF14.1 plus swapping instructions	B B
IF19.2	dth	TMNh	SDFh	same as IF14.2 plus database configuration ~ instructions	B B
IF19.3	rth	TMNh	SRFh	same as IF14.3	B
IF19.4	sth	TMNh	SSFh	same as IF14.4	B
IF19.5	cth	SCFh	TMNh	same as IF14.5 plus swapping instructions	B B
IF19.6	dth	SDFh	TMNh	same as IF14.6 plus: database consistency status	B B B
IF19.7	rth	SRFh	TMNh	same as IF14.7	B
IF19.8	sth	SSFh	TMNh	same as IF14.8	B
IF19.9	tt	TMNh	TMNx	modification information	B

Remark to IF19.9: TMNx belongs to any other co-operating PNO (see subclause 4.2, assumption 4).

Management functions:

Same as in subclause 6.14 plus:

- MF19.1: Send UPT service logic module: TMN sends a UPT service logic module (e.g. new service feature) to SCF.
This MF is located in the TMN.
- MF19.2: UPT service logic module received: SCF notifies TMN that the UPT service logic module was received.
This MF is located in the SCF.
- MF19.3: Test UPT service logic module: TMN directs SCF to test the UPT service logic module.
This MF is located in the TMN.
- MF19.4: Results of the service logic test: SCF notifies TMN that the test of UPT service logic module was successful.
This MF is located in the SCF.
- MF19.5: Install UPT service logic module: TMN directs SCF to install the UPT service logic module in a specific part of the memory.
This MF is located in the TMN.
- MF19.6: UPT service logic module installed: SCF notifies TMN that the UPT service logic module is installed.
This MF is located in the SCF.
- MF19.7: Swap to other UPT release: TMN directs SCF to swap new/old version of UPT service program.
This MF is located in the TMN.
- MF19.8: Result of UPT swapping: SCF notifies TMN about the swapping result (successful or unsuccessful).
This MF is located in the SCF.
- MF19.9: Test UPT database consistency: TMN directs SCF/SDF to test the consistency of the UPT database.
This MF is located in the TMN.
- MF19.10: UPT database consistent: SCF/SDF notifies TMN that the UPT database is consistent.
This MF is located in the SCF/SDF.
- MF19.11: UPT database not consistent: SCF/SDF notifies TMN that the UPT database is not consistent.
This MF is located in the SCF/SDF.
- MF19.12: Reconfigure UPT database: TMN directs SCF/SDF to reconfigure the UPT database.
This MF is located in the TMN.
- MF19.13: Send modification information to other TMN: PNO notifies other co-operating PNOs about modifications of the UPT service software (see also subclause 4.2, assumption 4).
This MF is located in the TMN.
- MF19.14: Receive modification information from other TMN: PNO is notified by an other co-operating PNO about modifications of the UPT service software (see also subclause 4.2, assumption 4).
This MF is located in the TMN.

6.20 Request statistics by subscriber in home domain

Description:

The UPT subscriber request statistics (e.g. a report of usage data or billing information) via his home PNO. In this scenario it is assumed that the requested information is already available from the TMN. It may be possible that for the statistics request default parameters have been stored. In that case (if the UPT subscriber did not set parameters in the statistics request message) the statistics provided to the UPT subscriber will be based upon the default settings. In any case, parameters indicated by the UPT subscriber will override the default.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF20.1	eth	subscriber	TMNh	procedure ID statistics ID subscriber ID parameter ID UPT number	DE DE DE DE DE
IF20.2	eth	TMNh	subscriber	statistics report	DE

Management functions:

- MF20.1: Retrieve the subscriber statistics request (the information elements).
This MF is located in the TMNh.
- MF20.2: Create and log the statistics report.
This MF is located in the TMNh.
- MF20.3: Send the statistics report to the subscriber.
This MF is located in the TMNh.

6.21 Request statistics by PNO in home domain

Description:

The PNO (i.e. an operator) requests statistics (e.g. usage data or billing information in form of a report) via his work station function. In this scenario it is assumed that the requested information is already available from the TMN. It may be possible that for the statistics request feature, default parameters have been stored. In that case (if the PNO did not set parameters in the statistics request message) the statistics provided to the PNO will be based upon the default settings. In any case, parameters indicated by the PNO will override the default.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF21.1	f	PNO	TMNh	statistics ID parameter ID operator ID	DE DE DE
IF21.2	f	TMNh	PNO	statistics report	DE
NOTE: "f" represents the reference point between PNO (operator) and the TMN.					

Management functions:

- MF21.1: Retrieve the statistics request (the information elements).
This MF is located in the TMNh.
- MF21.2: Create and log the statistics report.
This MF is located in the TMNh.
- MF21.3: Send the statistics report to the PNO.
This MF is located in the TMNh.

6.22 UPT subscription procedure in home domain

Description:

A UPT subscriber adds a new UPT user to his subscription via a TMN subscription procedure.

Information flow:

IF	ref. point	from	to	information elements	purpose
IF22.1	eth	subscriber	TMNh	procedure ID subscriber ID user profile data	A A A
IF22.2	eth	TMNh	subscriber	UPT number PUI PIN (in a secure way) subscription confirmation	A A A A
IF22.3	dth	TMNh	SDFh	user profile	A
NOTE: The user profile information elements are listed in ETR 055-06 [7].					

Management functions:

- MF22.1: Retrieve the subscriber data (the information elements).
This MF is located in the TMNh.
- MF22.2: Create relevant data for new user (e.g. UPT number, PUI, etc.).
This MF is located in the TMNh.
- MF22.3: Create the user profile.
This MF is located in the TMNh.
- MF22.4: Send the user profile to the SDFh.
This MF is located in the TMNh.
- MF22.5: Receive and store user profile.
This MF is located in the SDFh.
- MF22.6: Activate the user profile.
This MF is located in the TMNh.
- MF22.7: Inform subscriber about relevant data for new user.
This MF is located in the TMNh.

7 UPT management information

This clause provides an overview of the main management information required for supporting the scenarios and requirements as previously described in this ETR. It does not provide a complete and detailed description of all UPT management information. Instead, the results of this clause should be seen as a first step towards a complete specification for UPT management interfaces.

For all reference points as identified in figure 3 (clause 6), as well as for the TMN internal reference points, a management interface specification could be produced, based on the analysis of the preceding clauses. The scenario tables in clause 6 can be used to summarize the information elements that are visible for the reference point under study. The relation between these information elements can then be modelled via E-R diagrams. In connection with the identified operations on these data as described in the Management functions, this can then serve as the basis for the management information model of the corresponding interface. In this process, existing specifications should be re-used where possible. In this context, the relation to the X.500 UPT information model as defined in ETS 300 670 [8] deserves some extra clarification. Annex B discusses this relation.

The remainder of this clause is restricted to providing an overview of the UPT management services and information that were identified in the preceding clauses. The Object Management Tool notation has been used to visualize this overview.

As identified in table 1 of clause 5, the following 6 management areas were identified to categorize the requirements (clause 5):

- Subscriber Administration (A);
- Network Provisioning Management (B);
- Charging, Billing and Accounting Management (D);
- QoS and Network Performance Management (E);
- Maintenance Management (I);
- Security Administration (J).

The following figure categorizes the information, as identified in the previous clauses, in 6 "UPT management services", analogous to the 6 management areas listed above:

- UPT Subscriber Administration (UPT SA);
- UPT Network Provisioning Management (UPT NPM);
- UPT Charging, Billing and Accounting Management (UPT CBAM);
- UPT QoS and Network Performance Management (UPT QNPM);
- UPT Maintenance Management (UPT MM);
- UPT Security Administration (UPT SCA).

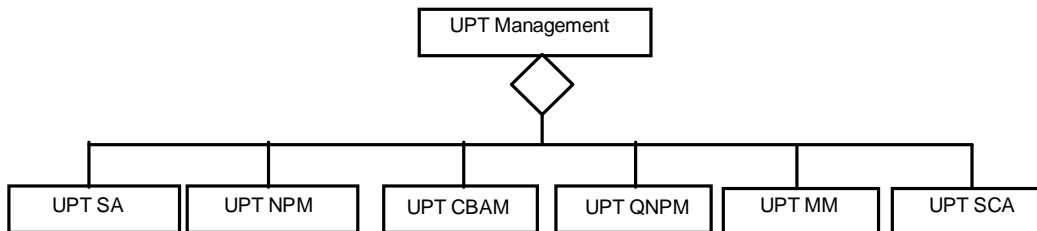


Figure 4: The 6 UPT management services

NOTE: Although in this and the following figures in this clause, use has been made of OMT-like diagrams, it is not intended that these figures describe relations between object classes. Instead, these figures merely visualize the relation between the UPT management services, its sub activities, and the data that is used herein. The symbols used in these figures are explained via the following textual description on how to read figure 5 (see below): "The UPT SA management service" contains (diamond symbol) the (sub-) activities UPT Profile Management and UPT Provisioning. Each of these activities uses data (solid ball indicating more data than one). In the UPT Profile Management activity, the data that is most relevant here is "user profile" and "subscriber profile" (the triangle indicate a specialization relation).

The UPT management services indicated in figure 4 are further detailed below.

7.1 The UPT SA management service

As described in subclause 5.1, UPT Subscriber Administration (SA) supports the processes of exchanging data for the purpose of offering the UPT service and to configure the network with subscriber and user data. This includes functionality for service provisioning and profile management, see figure 5. The service provisioning includes both the subscription procedures for the subscriber himself (scenario 6.4) and the addition of new users (scenario 6.22) initiated by the subscriber (normally executed by the PNO).

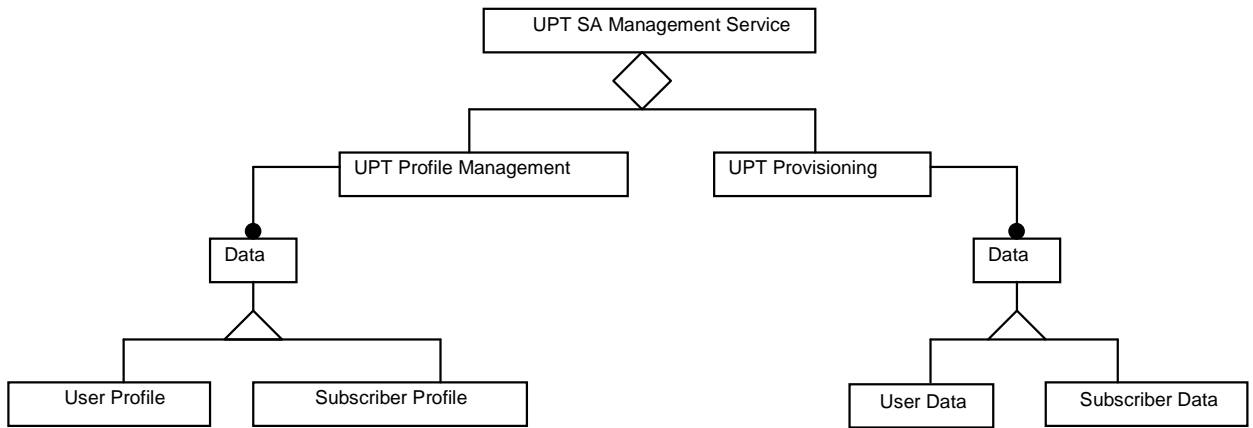


Figure 5: The UPT SA management service

7.2 The UPT NPM management service

Network Provisioning Management (NPM) supports the processes from network planning to installation of resources. For this management service, mainly UPT service deployment (logic and data) is considered, see figure 6.

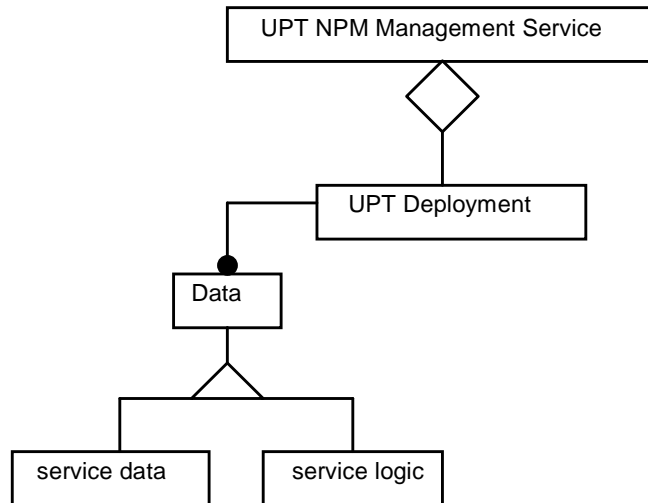


Figure 6: The UPT NMP management service

7.3 The UPT CBAM management service

Charging, Billing and Accounting Management (CBAM) includes charging for usage of the UPT service features (calls, registration procedures and service profile management activities) and for UPT service provisioning and subscriber profile management, see figure 7. It is assumed that authentication is not charged.

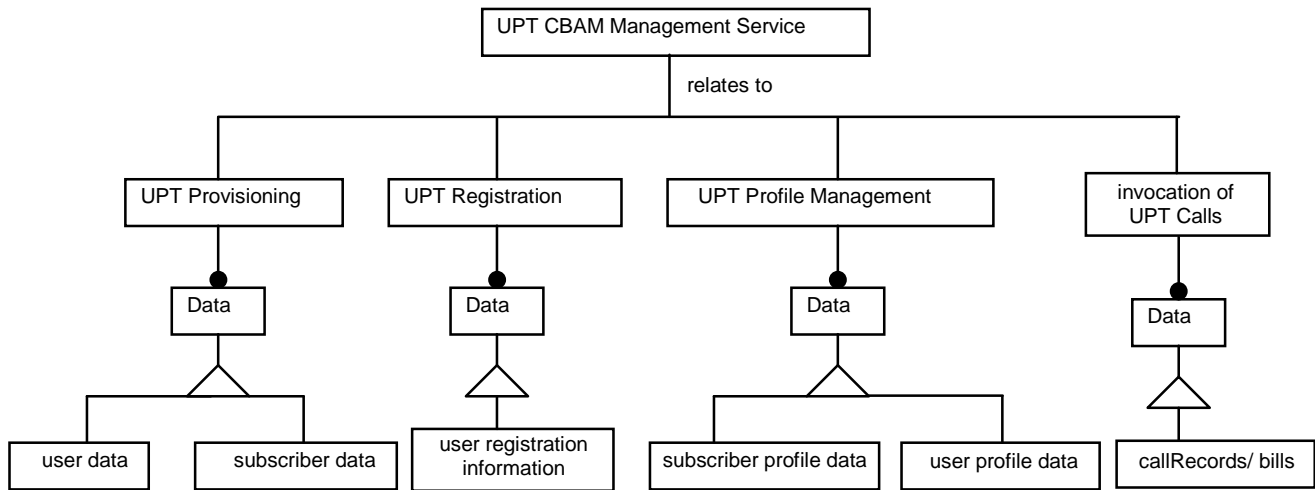


Figure 7: The UPT CBAM management service

7.4 The UPT QNPM management service

Quality of service and Network Performance Administration (QNPM) is concerned with the detection of QoS degradations. This "quality of service" can concern both the UPT service (features) itself (calls, authentication, registration procedures and service profile management activities), and the customer care activities (billing, service provisioning, etc.). Complaints may be issued by the subscriber if the QoS is below the agreed level. See figure 8.

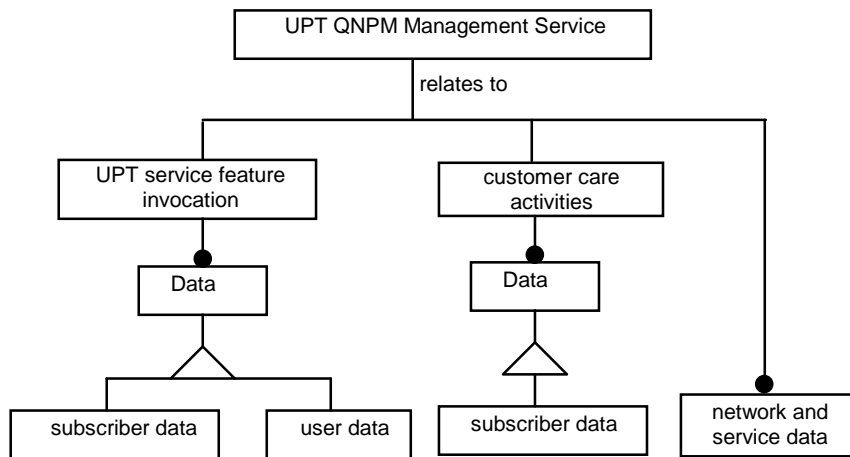


Figure 8: The UPT QNPM management Service

7.5 The UPT MM management service

Maintenance Management (MM) is concerned with the detection, localization and reporting of faults. The information for this UPT management service is very similar to the UPT QNPM management service as outlined in the previous subclause, as for UPT, only the direct impact of faults on the UPT service (i.e. the UPT service quality) is relevant as far as the user/subscriber is concerned. Therefore, this UPT MM management service is not treated here any further.

7.6 The UPT SCA management service

The purpose of Security Administration (SCA) is to protect the TMN and the network elements against unauthorized access, and to guard against abuse of the UPT service. Security issues are relevant both for the invocation of UPT service (features) (calls, authentication, registration procedures and service profile management activities), and the customer care activities (billing, service provisioning, etc.), see figure 9.

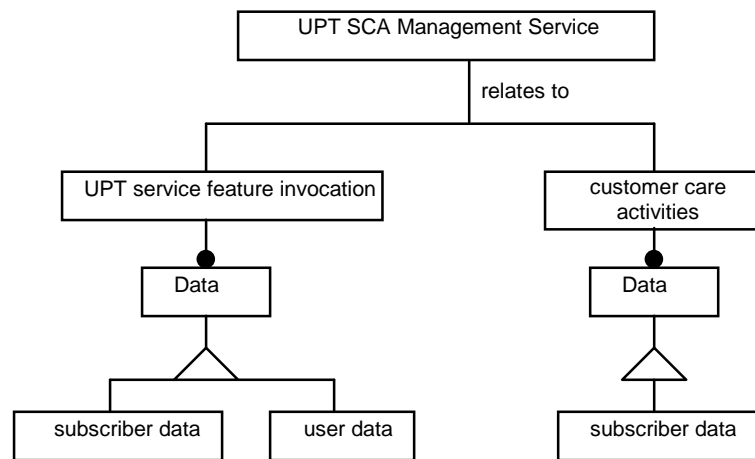


Figure 9: The UPT SCA management service

8 UPT management services

This clause provides a description of the UPT management services which support the necessary functionality identified in the previous clauses. This clause is based on the preceding clause 7, where for each UPT management service a global identification of information was provided, based on the requirements and scenario analysis. This clause further elaborates on clause 7, by identifying the roles that are relevant for each management service and by listing the required management operations for each role. This information is extracted from the scenarios (clause 6). Each management service is described by using the following template.

Table 3: UPT management services template

1.	Name
2.	Short description.
3.	Users
4.	Detailed description
5.	management operations

8.1 UPT Subscriber administration

1.	UPT Subscriber Administration.
2.	This MS supports the processes of exchanging data for the purpose of offering the UPT service and to configure the network with subscription information.
3.	Potential users of this MS are PNO and subscriber.
4.	This MS can be divided into two areas. - UPT Profile Management: provides the functionality which enables user- and subscription profile management. - UPT Provisioning Management: provides the functionality which enables to add/remove users from the subscription and to add/remove subscriptions.
5.	The different roles require different functionality for this MS. The available operations related to the different roles are listed below: - PNO: - change/add/remove users and subscriptions. - change/add/remove user- and subscription profiles. - UPT Subscriber: - change/add/remove user and subscriber profiles. - change/add/remove subscriber data and options (e.g. billing options).

8.2 UPT network provisioning management

1.	UPT Network Provisioning Management.
2.	This MS supports UPT service deployment (logic and data), including updates.
3.	Only the PNO is user of this management service.
4.	This MS can be divided into two areas: - intra-PNO service provisioning: all activities needed to co-ordinate and synchronize the process of service deployment. - inter-PNO service provisioning: all activities needed to co-ordinate and synchronize the process of service deployment with co-operating PNOs.
5.	The available operations for the PNO are listed below: - PNO: - test service logic - update, install and delete service logic - install announcements - configure SSF settings (see IF14.4) - exchange deployment information with other PNOs - test UPT service invocations (e.g. in a pilot) - activate UPT service - de-activate UPT service

8.3 UPT Charging, billing and accounting management

1.	UPT Charging, Billing and Accounting Management.
2.	This MS supports the processes whereby information is generated, collected and transferred in order to make it possible to process usage information and to calculate the charges for which the user/subscriber may be billed. Also the bill production and invoicing of subscribers and other PNOs is seen as part of this management service.
3.	Potential users of this MS are PNO and subscriber.
4.	This MS can be divided into three areas: - Charging for usage of the UPT service features (calls, registration procedures and service profile management activities). - Charging for UPT service provisioning. - Charging for subscriber profile management activities.
5.	The different roles require different functionality for this MS. The available operations related to the different roles are listed below: - PNO: - retrieve charging information for all UPT subscriptions related to registration, provisioning, profile management and calls. - UPT Subscriber: - retrieve charging information for own UPT subscription related to registration, provisioning, profile management and calls.

8.4 UPT QoS and network performance management

1.	UPT QoS and Network Performance Management.
2.	This MS supports the processes for exchanging data for the purpose of detecting QoS degradations.
3.	Potential users are PNO and UPT Subscriber.
4.	This MS can be divided into two areas: - UPT service (feature) performance: this area deals with the performance of calls, authentication, registration procedures and service profile management activities. - Customer care performance: this area deals with performance of customer care activities (billing, service provisioning, etc.).
5.	The different roles require different functionality for this MS. The available operations related to the different roles are listed below: - PNO: - collect network performance parameters and calculate the quality of service as perceived by the users. - UPT Subscriber: - retrieve QoS data for own UPT subscription and inform users if appropriate. - contact the PNO in case of a QoS degradation (complaint).

8.5 UPT maintenance management

This UPT MM management service is not treated here any further (see subclause 7.5).

8.6 UPT security administration

1.	UPT Security Administration.
2.	The purpose of Security Administration (SCA) is to protect the TMN and the network elements against unauthorized access, and to guard against abuse of the UPT service.
3.	Potential users are PNO and UPT Subscriber.
4.	This MS can be divided into two areas: - Security of the invocation of UPT service (features) (calls, authentication, registration procedures and service profile management activities). - Security for the customer care activities (billing, service provisioning, etc.).
5.	The different roles require different functionality for this MS. The available operations related to the different roles are listed below: - PNO: - retrieve security information from the network and/or from the subscriber access to the TMN. - determine security violations. - UPT Subscriber: - retrieve security information related to own UPT subscription and inform users if appropriate.

Annex A: Authentication mechanisms provided by the SDF

The AE (Authenticating Entity) is a physical entity which is protected against analysing or changing its contents. It is part of, or associated with the SDF.

- the authentication of a UPT user is performed in the SDF/AE in the home network;
- keys, PINs and black lists are stored in the AE;
- black lists are stored in the SDF which specify those PUIs that should not be accepted to get access to the UPT service (e.g. because the UPT user has exceeded a credit limit). The SDF should be able to add and delete users from the black list;
- if strong authentication is supported by PNO, key management procedures have to be applied. The following information items are required in the AE: PUIs and keys of all UPT users which have a subscription with the PNO (1 PUI and 1 key per user). For the one-pass strong authentication mechanism, also one sequence number per UPT user is required. For the two-pass authentication mechanism, the AE contains a random number generator. If one- and two-pass strong authentication are permitted for one subscription, there should be a different key for each authentication method;
- if weak authentication (based on PINs) is supported by the PNO, the AE should contain PUI, PIN, SPIN (optional), RAA (counter of trials), SPIN counter (optional). For weak authentication, there are no key management procedures invoked. The PIN and the PUI are required for each UPT user. A PUI may be blocked e.g. after a number of unsuccessful authentication attempts (only with weak authentication). If weak secure answer and/or special PIN for outgoing calls are provided, the AE should also contain SAPIN and/or OCPIN.

Annex B: The X.500 UPT information model

ETSI SPS technical committee has already provided a X.500 information model for UPT (ETS 300 670 [8]). This X.500 information model describes the operations to the UPT SDP data for service invocation purposes. It is acknowledged that the PNO will have, to a large extent, the need to access this SDP data in a similar way via his TMN. For example the operator might want to access a user profile for specific purposes, such as to make statistics of the changes made in the user profile on request of a UPT subscriber. For the specification of this management access to SDP data re-use of, or reference to the X.500, specifications can be made. This leaves open the possibility to, in fact, satisfy part of the management access to the SDP by the X.500 protocol (the Directory Access Protocol, DAP). The architecture for this situation is visualized in figure B1.

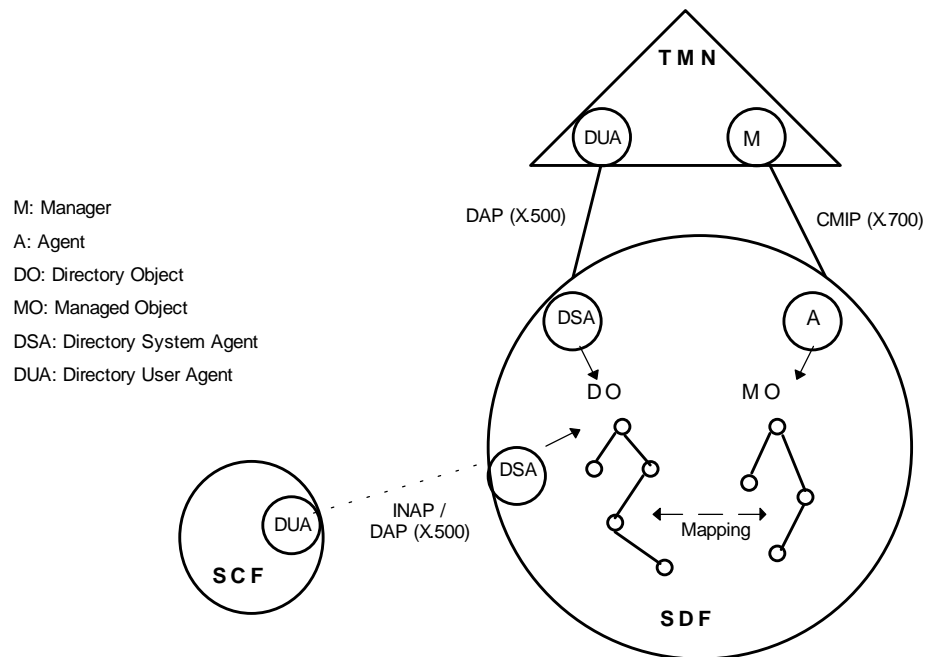


Figure B1: X.500 and X.700 relation for the SDF

In this situation, the TMN access to the SDP is satisfied by two protocols, X.500 (DAP) and X.700 (CMIP). The data operations to the SDP, like update/delete user profile, are described in the X.500 UPT information model. The management operations are modelled by the X.700 model. In this X.700 model, the following aspects are modelled:

- the management view of the SDF data (e.g., notifications of fraud detections, or counters of changes made to a specific user profile in a specific time frame);
- other aspects of the SDP as required by management (e.g. hardware fault alarms);
- the relation between the X.500 and X.700 models. For example, a reference to the respective X.500 data entity (object or attribute ID) in the X.700 construct (attributes, objects) can be provided to model the mapping to the X.500 model.

It should be noted that the architecture as visualized in figure B1 presupposes the OS to support the DAP (X.500) protocol for accessing the SDP data (i.e. a DUA needs to be included in the OS). In practice this might however not provide an additional requirement, as most OSs would be already provided with that functionality. A platform application (API) might be available in the OS to abstract from the underlying protocols (X.500 or X.700) for the user (or management application).

Annex C: Bibliography

- ITU-T Recommendation M.3020: "TMN interface specification methodology".
- ITU-T Recommendation M.3010: "Principles for a telecommunications management network".
- ISO/IEC 7498-4: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework".
- ITU-T Recommendation X.701: "Information technology - Open Systems Interconnection - Systems Management Overview".
- ETR 208: "Human Factors (HF); HF aspects of Universal Personal Telecommunications (UPT); User requirements.
- ETS 300 374-1: "Intelligent Network (IN); Intelligent Network Capability Set 1 (CS1) Core Intelligent Network Application Protocol (INAP) Part 1: Protocol specification".
- "Object-Oriented Modelling and Design", James Rumbaugh.
- ETR 224: "Intelligent Network (IN); Capability Set 2 (CS2); IN intra domain management requirements for CS2".

History

Document history	
September 1996	First Edition