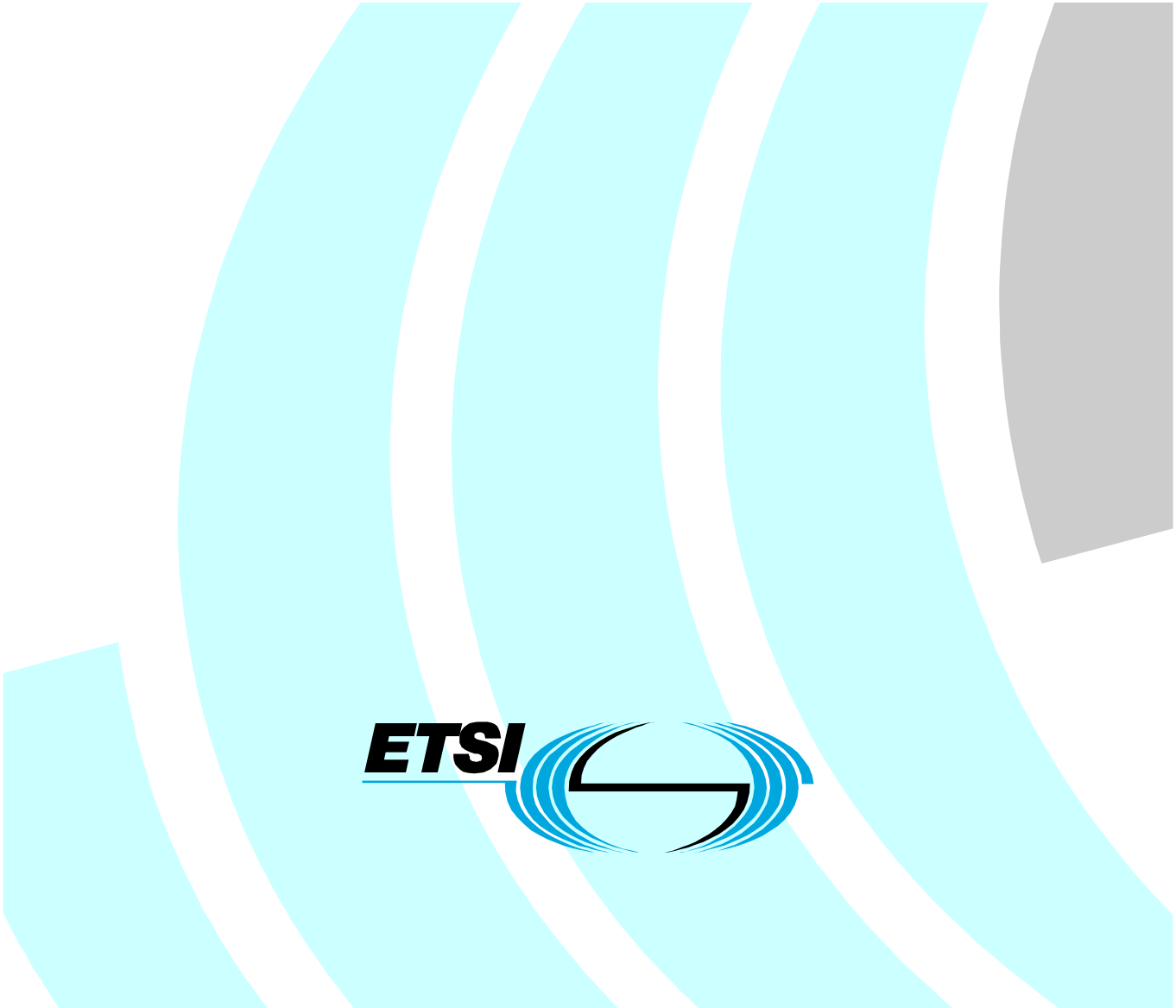
ETSI TS 101 303 V4.1.1 (2003-11)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Service Independent Requirements Definition; Service and Network Management Framework; Overview and Introduction



Reference
RTS/TIPHON-01004R4

Keywords
internet, IP, management, network, service,
telephony, VoIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

Introduction

The present document forms part of TIPHON Release 4 and provides an overview and introduction to service and network management

The Definition for Release 4 including all associated deliverables is contained in TR 101 301 [18] where the relationship of the present document with other TIPHON release 4 deliverables is shown.

1 Scope

The present document establishes and defines the management principles and high-level requirements for the management of TIPHON services and networks.

In particular, the present document identifies:

- an overview of the management architecture, including the interactions between the management plane and the TIPHON application plane and TIPHON transport plane.
- the end to end processes required to support the management (e.g. provision, maintenance and billing) of TIPHON service capabilities. Including the management model required to support the interactions necessary to ensure inter-operability between customers, service providers (including Value Add service providers), network providers and Trusted Third Parties etc.
- high-level management requirements
- managed resource model(s) (i.e. candidate manageable entities, in other words, resources that can be controlled and/or monitored, within the TIPHON architectural model).

The present document is intended to provide a framework for the further development of TIPHON management specifications as well as management products based on those requirements. The present document can be seen as a framework for the development of all other Technical Specification addressing the management of TIPHON.

TR 101 835 [10] provides details of the steps involved in a TIPHON release.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ITU-T Recommendation M.3010: "Principles for a Telecommunications management network".

[2] ITU-T Recommendation M.3200: "TMN management services and telecommunications managed areas: overview".

[3] ITU-T Recommendation M.3400: "TMN Management Functions".

[4] TeleManagement Forum GB910: "Telecom Operations Map (TOM)".

[5] TeleManagement Forum GB921: "enhanced Telecom Operations Map (eTOM)".

[6] Void.

[7] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by and ISDN and network capabilities of an ISDN".

[8] ITU-T Recommendation I.140: "Attribute technique for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[9] ITU-T Recommendation I.210: "Principles of telecommunication services supported by an ISDN and the means to describe them".

[10] ETSI TR 101 835: "Telecommunications and Internet Protocol Harmonization over Networks (TIPHON); Project method definition".

[11] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Abstract Architecture and Reference Points Definition; Network Architecture and Reference Points".

[12] ITU-T Recommendation M.3020: "TMN Interface Specification Methodology".

[13] ITU-T Recommendation M.3013: "Considerations for a telecommunications management network".

[14] ETSI TR 101 329-7: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON systems; Part 7: Design guide for elements of a TIPHON connection from an end-to-end speech transmission performance point of view".

[15] ITU-T Recommendation Q.821: "Stage 2 and Stage 3 description for the Q3 interface - Alarm surveillance".

[16] ETSI TR 101 303: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Requirements definition study; Introduction to service and network management".

[17] ETSI TS 102 024-4: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; End-to-end Quality of Service in TIPHON Systems; Part 4: Quality of Service Management".

[18] ETSI TR 101 301: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Release Definition; TIPHON Release 3 Definition".

[19] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Capability Definition; Service Capabilities for a simple call".

[20] ITU-T Recommendation X731: "Information technology - Open Systems Interconnection - Systems Management: State management function".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

actor: organization playing one or more roles

administrative domain: network controlled by a single operator

NOTE: It encompasses both network and management domains.

management domain: collection of one or more management systems, and zero or more managed systems and management sub domains that is administered by a single operator

role: activity performed by an actor (e.g. organization)

NOTE: Each actor can play many roles. A role is defined by a set of properties or attributes that describe the capabilities of an entity that can be performed on behalf of other role(s).

Service Level Agreement (SLA): formal negotiated agreement between two parties

NOTE: It is a contract, or part of one, that exists between the service provider and the service customer, designed to create a common understanding of services, priorities, responsibilities, etc.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ALC	Automatic Level Control
ATM	Asynchronous Transfer Mode
B2B	Business to Business
BC	Bearer Control
BPM	Business Process Model
CC	Call Control
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
eTOM	enhanced Telecommunications Operations Map
ETS	Emergency Telecommunication Service
FCAPS	Fault, Configuration, Accounting, Performance, Security
IP	Internet Protocol
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
MC	Media Control
MD	Mediation Device
MIB	Management Information Bases
NE	Network Element
NEF	Network Element Function
NO	Network Operator
OAM&P	Operations, Administration, Maintenance and Provision
OMG	Object Management Group
OS	Operations System
OSF	Operations System Function
QA	Q Adaptor
QoS	Quality of Service
RAD	Requirements, Analysis and Design
SC	Service Control
SC	Service Customer
SCN	Switched Circuit Networks
SLA	Service Level Agreement
SLS	Service Level Specification
SNMP	Simple Network Management Protocol
SP	Service Provider
SPOA	Service Point of Attachment
TMF	TeleManagement Forum
TMN	Telecommunications Management Network
TNM	TIPHON Network Management
TOM	Telecommunications Operations Map
UML	Unified Modelling Language
UTRAD	United TMN Requirements
VASP	Value added Service Provider
WS	Work Station
WSF	Function

4 Network and service management overview

4.1 Management principles

telecommunications management comprises such activities as the Planning, Installation, Sales, Provision, Maintenance, Charging/Billing and Customer Query/Control of telecommunication services and networks. These are often encapsulated in the term FCAPS (Fault, Configuration, Accounting, Performance and Security).

The general principles of telecommunications management are contained in ITU-T Recommendation M.3010 [1] (Principles for a telecommunications management network).

A telecommunications management network provides a set of capabilities that allow for the exchange and processing of management information to assist service providers and network operators in conducting their business efficiently.

A telecommunications management network is conceptually a separate network that interfaces a telecommunications network at several different points to send/receive information to/from it and to control its operations. However, a telecommunication management network may use parts of the telecommunications network to provide its communications.

4.2 Network and service management architecture

The architecture(s) for telecommunications management are contained in ITU-T Recommendation M.3010 [1] (Principles for a telecommunications management network).

Three basic aspects are included in the management architecture. These are:

- the functional architecture;
- the information architecture; and
- the physical architecture.

The functional architecture describes the appropriate distribution of functionality within the management network, appropriate in the sense of allowing for the creation of function blocks from which a management network of any complexity can be implemented. The definition of function blocks and reference points between them leads to the requirements for the interface specifications. Figure 1 illustrates the functions and reference points in the functional architecture.

The information architecture is based on standardized open management paradigms that support the standardized modelling of the information to be communicated. telecoms management standardization activities will not develop a specific management paradigm but build upon industry-recognized solutions, focusing primarily on object-oriented techniques. Specific management paradigms may be used in standards when judged to be adequate.

The physical architecture describes interfaces that can actually be implemented and examples of physical components that make up the management network.

4.2.1 Functional architecture

The management functional architecture, at its simplest, comprises functions connected by reference points. Functions include Network Element Function (NEF), Operations System Function (OSF) and Work Station Function (WSF). The NEF can be viewed as the management aspects of the TIPHON functions. Reference points include the q reference point, between function blocks within an administrative domain, the x reference point, between function blocks in different administrative domains and an f reference point between OSFs and WSFs.

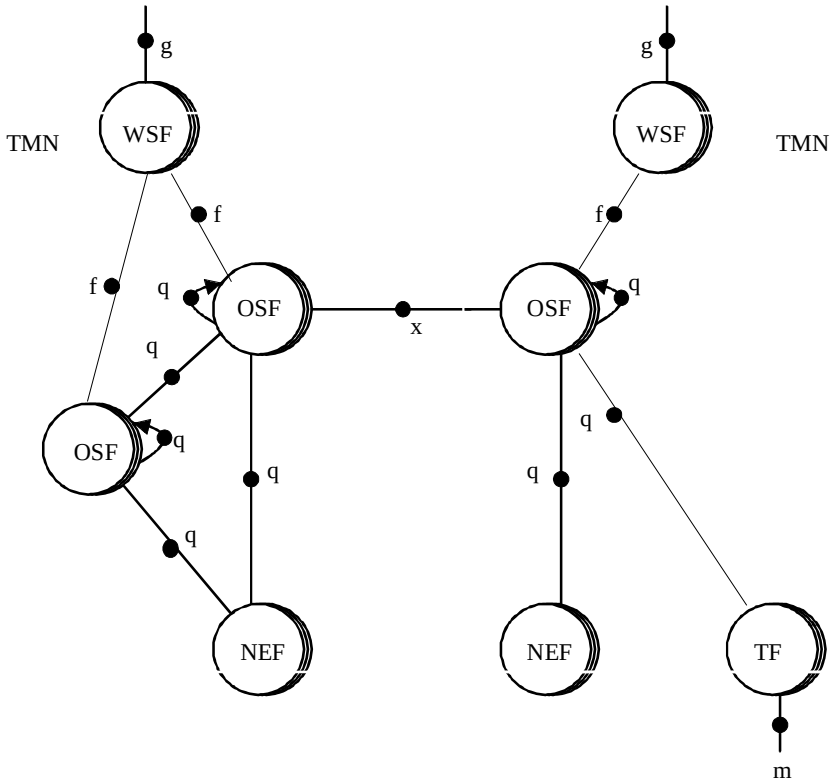


Figure 1: The functional architecture

Within the functional (logical) architecture telecommunications management can be divided into a number of layers of management, these are element management, network management, service management and business management (figure 2).

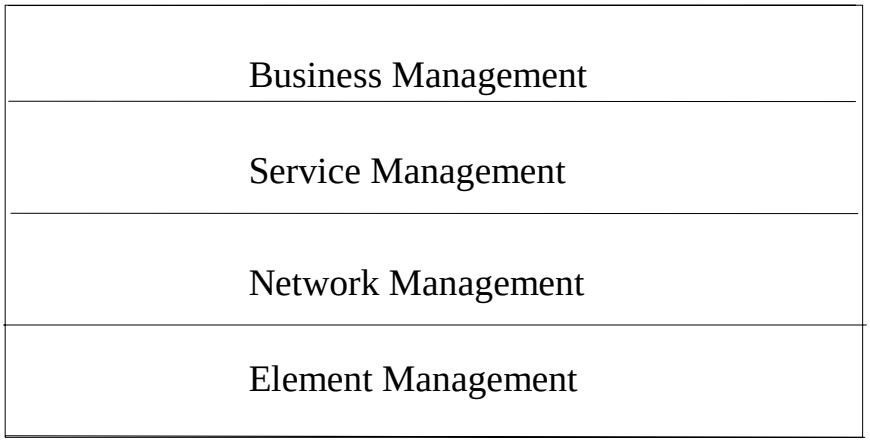


Figure 2: Management layers

The present document addresses the network and service management layers.

The network management layer provides the functionality to manage a network by co-ordinating activity across the network and supports the "network" demands made by the service management layer. It knows what resources are available in the network, how these are interrelated and geographically allocated and how the resources can be controlled. It has an overview of the network. Furthermore, this layer is responsible for the technical performance of the actual network and will control the available network capabilities and capacity to give the appropriate accessibility and quality of service.

The network management layer provides, as an objective, a technology independent view to the service management layer.

The network management layer has the following five principal roles:

- the control and co-ordination of the network view of all network elements within its scope or domain;
- the provision, cessation or modification of network capabilities for the support of service to customers;
- the maintenance of network capabilities;
- maintenance of statistical, log and other data relating to the network and interact with the service manager layer on performance, usage and availability.

The service management layer is responsible for, the contractual aspects of services that are being provided to customers or available to potential new customers. Some of the main functions of this layer are service order handling, complaint handling and invoicing.

The service management layer has the following four principal roles:

- providing the basic point of contact with customers for all service transactions including provision/cessation of service, accounts, QoS, fault reporting;
- interfacing with network operators;
- interaction with service providers;
- maintaining statistical data (e.g. QoS);
- interaction between services.

4.2.2 Information architecture

To effectively manage complex networks and support telecoms provider's business processes, it is necessary to exchange management information between management applications implemented in multiple managing and managed systems. Thus the telecommunication management environment is a distributed information processing application.

In order to promote interoperability, the information architecture is based on standardized open management paradigms that support the standardized modelling of the information to be communicated.

ITU-T telecoms management standardization activities have not developed specific management paradigms but build upon industry-recognized solutions, focusing primarily on object-oriented techniques. Specific management paradigms can be used in management standards when judged to be adequate.

This approach encourages the reuse of standardized information definitions to reduce the overall standardization effort. Object-oriented techniques such as encapsulation, inheritance, and specialization are preferred. Where information is expected to be utilized in conjunction with more than one management paradigm, the information should first be defined in a paradigm-neutral manner utilizing industry-recognized techniques after which it would be then be mapped onto paradigm-specific formats.

As management information and actions play crucial roles for administrations, security techniques have to be applied in the telecoms management environment in order to assure the safety of the information exchanged over the interfaces and residing in the management application. Security principles and mechanism are also related to the control of access rights of the users to information associated with management applications.

4.2.3 Physical architecture

At its simplest, the physical architecture can be said to comprise systems interconnected by interfaces. The key systems are the Operations System (OS), the Network Element (NE), the Q Adaptor (QA), Mediation Device (MD) and the Work Station (WS). One or more reference points, from the functional architecture, map to an interface. Intra domain interfaces (e.g. within a management domain) are Q interfaces (between OSs and NE and OS) and F interfaces between OSs and WSs. Inter domain interfaces (e.g. between management domains) are X interfaces.

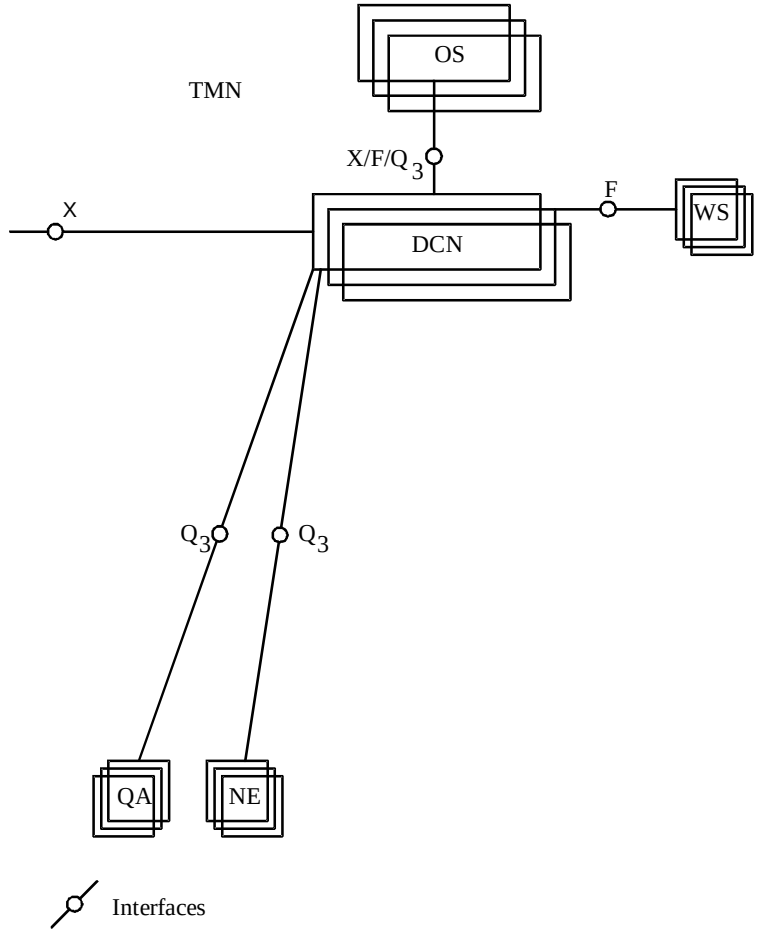


Figure 3: Example of a simplified physical architecture

A management network can be implemented in a variety of physical configurations, thus enabling each to be both unique and based on standards. It is recognized that physical systems may contain more than one function block in which case the name of the system should reflect its primary function (e.g. Operations System).

4.2.4 Relationship between the management architectures and an implementation

Two of the above architectures (functional and information) provide a framework that allows requirements to be documented about *what* an implementation should do.

The functional architecture framework permits the specification of what functions have to be achieved in the implementation. The information architecture permits the specification of what information (i.e. data) has to be stored so that the functions defined in the functional architecture can be achieved in the implementation. The functional specification based on the functional architecture framework, and the information specification based on the information architecture framework should be developed to express business needs to be met by the implementation. The implementation, that meets the requirements of the functional and information specifications, may vary greatly from one solution to another. telecoms management implementations are not currently a subject for standardization.

A physical architecture (implementation) blends and balances a number of divergent constraints such as cost, performance, and legacy deployments, as well as new functionality being delivered. Since every implementation will have different sets of these constraints to cope with, reality dictates that there will be many physical architecture implementations. These implementation architectures are the result of different distributions of the fundamental elements.

The fundamental elements are expressed in the functional and information architectures, their distribution being architected into an implementation. There are many possible and different distributions. Each implementation has to satisfy the needs identified and expressed in both the functional architecture and the information architecture specifications.

This is illustrated in figure 4.

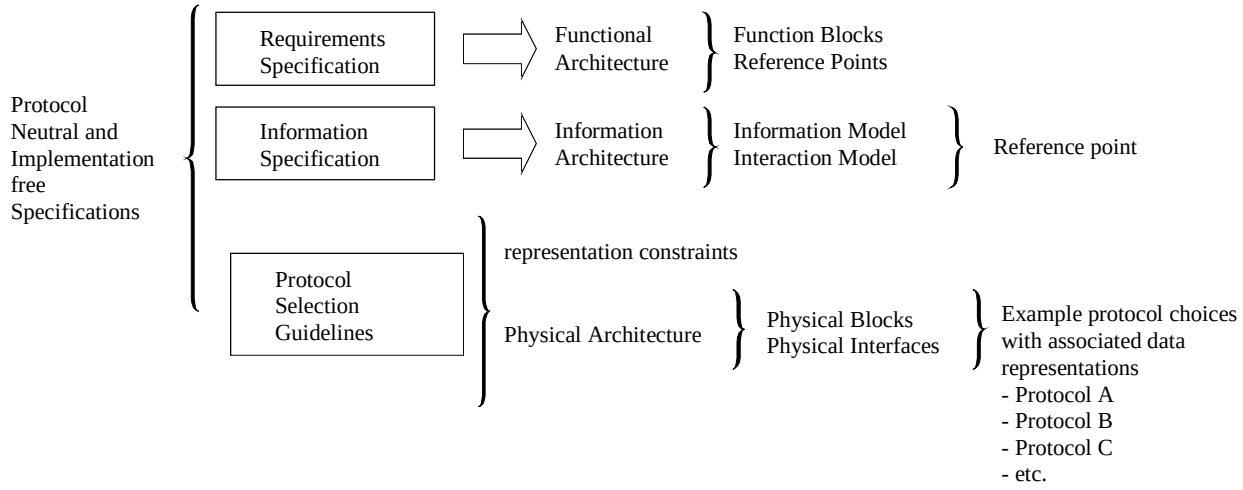


Figure 4: Relationship between the management architectures

4.3 Network and service management processes

Within the ITU-T Recommendations, management activities are grouped into management services . These management services are described from the user's viewpoint. Each management service addresses an area of management activity that provides for the support of an aspect of OAM&P of a telecommunication network.

The management services are used as a mechanism to capture the management requirements and document them in a uniform way. The management services are described in the ITU-T Recommendation M.3200 [2] series of recommendations.

Management functions are used by the management service to implement their functionality. management functions are the collection of the functional requirements for the interface specifications. These functions are also described from the user's perspective and are protocol independent. The management functions are collected together in ITU-T Recommendation M.3400 [3].

The TeleManagement Forum built upon the work of the ITU and produced the telecommunications Operations Map (TOM) [4]. This has now been extended to produce the eTOM, the enhanced TOM [5].

The Telecom Operations Map is the common framework for telecommunications operations process and the guide for all other work within TM Forum. It builds upon the management services and management functions developed by the ITU and provides the common language and framework for supporting implementation of end-to-end telecommunications operations automation.

The TM Forum has developed a business reference model that shows the relevant business relationships:

- between service customers and service providers;
- between and among service providers; and
- between service providers and equipment, providing the network infrastructure.

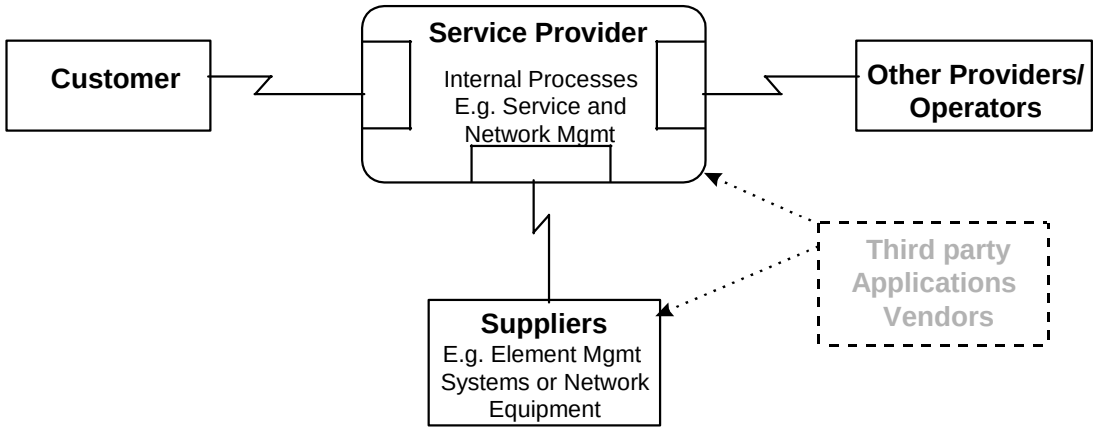


Figure 5: Business reference model

The business reference model (see figure 5) illustrates the principal points of contact between service providers and their customers/suppliers.

4.3.1 Business process model

Building upon the above reference model, the TM Forum has defined a Business Process Model (BPM). This provides some level of agreement between the parties identified above in terms of their views of the business process they support and the information they consume and generate as a result of the operation of these business processes. The BPM developed by the TM Forum covers both services management and network management business processes - as shown in figure 6.

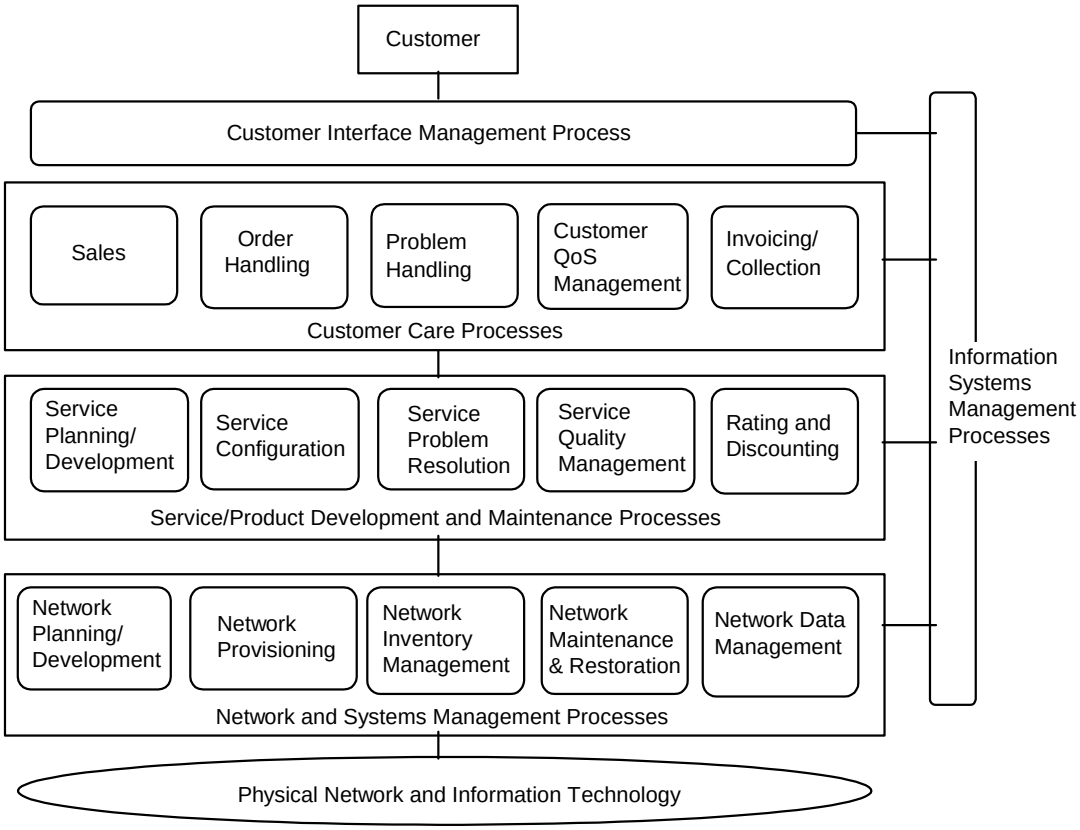


Figure 6: Business process model

4.3.2 Flow-through processes

The BPM described above provides an extremely good framework for agreement upon business process interactions and associated information flows between the players identified earlier in the business reference model. However, in today's communications market place there is increased need to support the end-to-end automation of business processes within the service provider environment. In addition a greater awareness of the way in which individual business processes interact (or flow-through) can assist in the plug and play of system components (which may be supplied by third party provides). In order to support this industry need, TM Forum has further refined the BPM into three fundamental flow-through business Processes. These support the telecom services of:

- service fulfilment;
- service assurance; and
- billing.

A representation of these flow-through business processes and the relationships to the processes in the TM Forum's BPM is shown in figure 7.

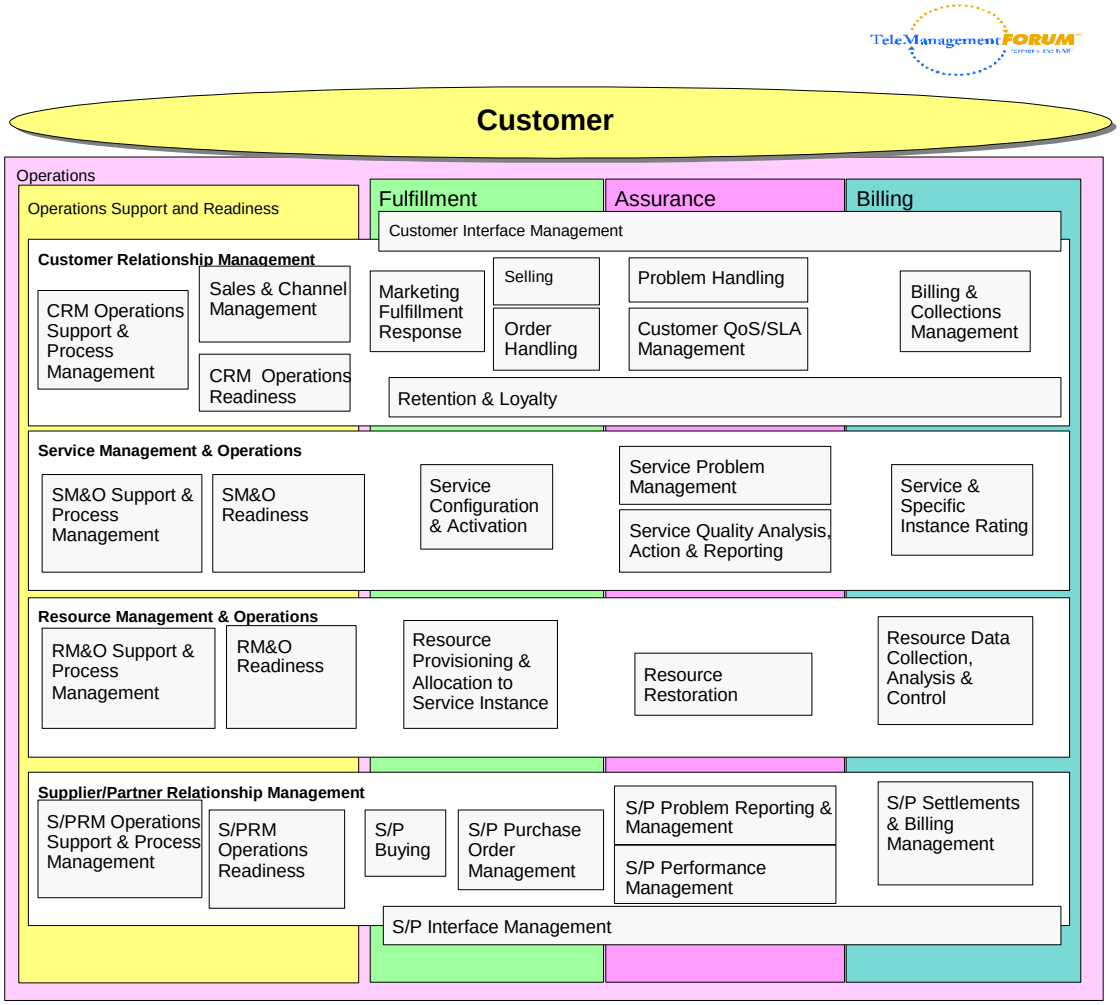


Figure 7: Flow-through business processes

5 Relationship between service and network management and the TIPHON architecture

5.1 General

As has been stated in clause 4.1, telecommunications management is conceptually a separate network that interfaces a telecommunications network at several different points to send/receive information to/from it and to control its operations. Thus, in order to provide management support to a TIPHON environment, it will be necessary to identify the manageable aspects of the TIPHON architecture [11]. This clause identifies the relationship between the management and TIPHON architectures and further identifies the business roles needed to support TIPHON.

5.2 Relationship to TIPHON application and transport plane

The TIPHON network architecture and reference configurations specification [11] identifies 4 functional planes. The management plane contains the service and network management functionality as defined in ITU-T Recommendation M.3000 series of recommendations.

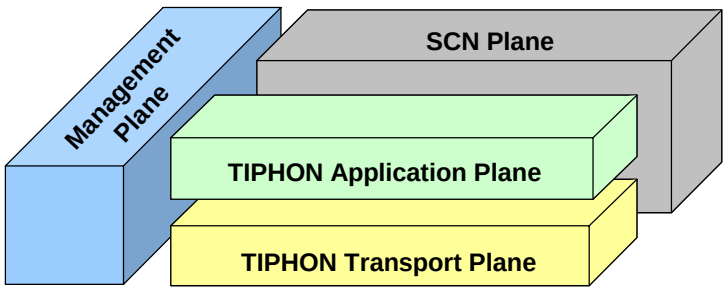


Figure 8: TIPHON planes

5.3 Relationship to TIPHON functional layers

The information flows between the TIPHON functional layers and the management plane are represented by the reference points in figure 9. The content of the information flows exchanged at each reference point depends on the managed resources within the functional layers and the management activity.

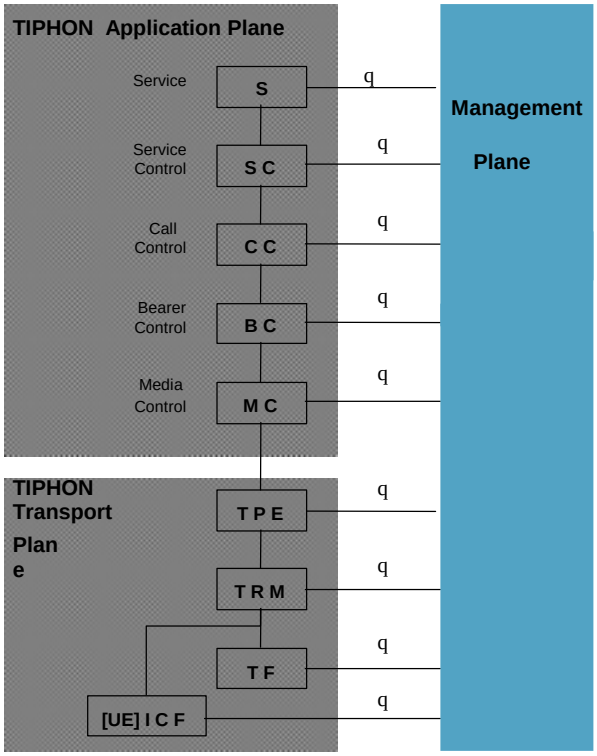


Figure 9: TNM Reference points

5.4 Interconnection between management plane and TIPHON planes

The management plane functional architecture connects to the TIPHON IP Telephony application plane and IP transport plane via management reference point q.

Each TIPHON function will have an associated network element function (NEF) which will interface with the management plane via a q reference point (figure 10).

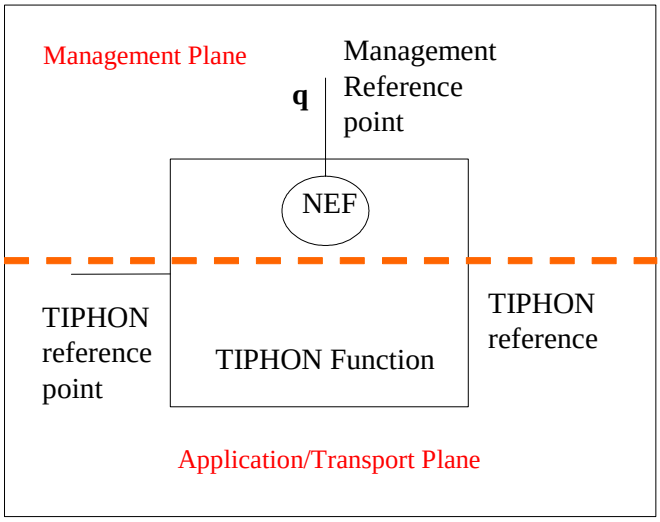


Figure 10: TIPHON function management reference point

5.5 Management layers, ownership domains and management interfaces

In the telecoms management model, the design of management domains allows the partitioning of systems or element management into manageable subsets. A collection of similar managed objects is named a management domain. In the present document two additional types of domain are used. TIPHON defines 3 network domains, which correspond to: SCN plane, TIPHON application plane and the TIPHON transport plane. TIPHON also defines ownership domains, which separate the operations of one service provider from the operations of another.

Figure 11 shows the management information flows between the management domains and their interfaces. These flows require mapping with the TIPHON network architecture to add the network management requirements to the existing reference points as defined in the TS 101 314 [11].

For TIPHON release 4, the network management framework shall support the service capabilities and higher order of service application as defined in TS 101 314 [11].

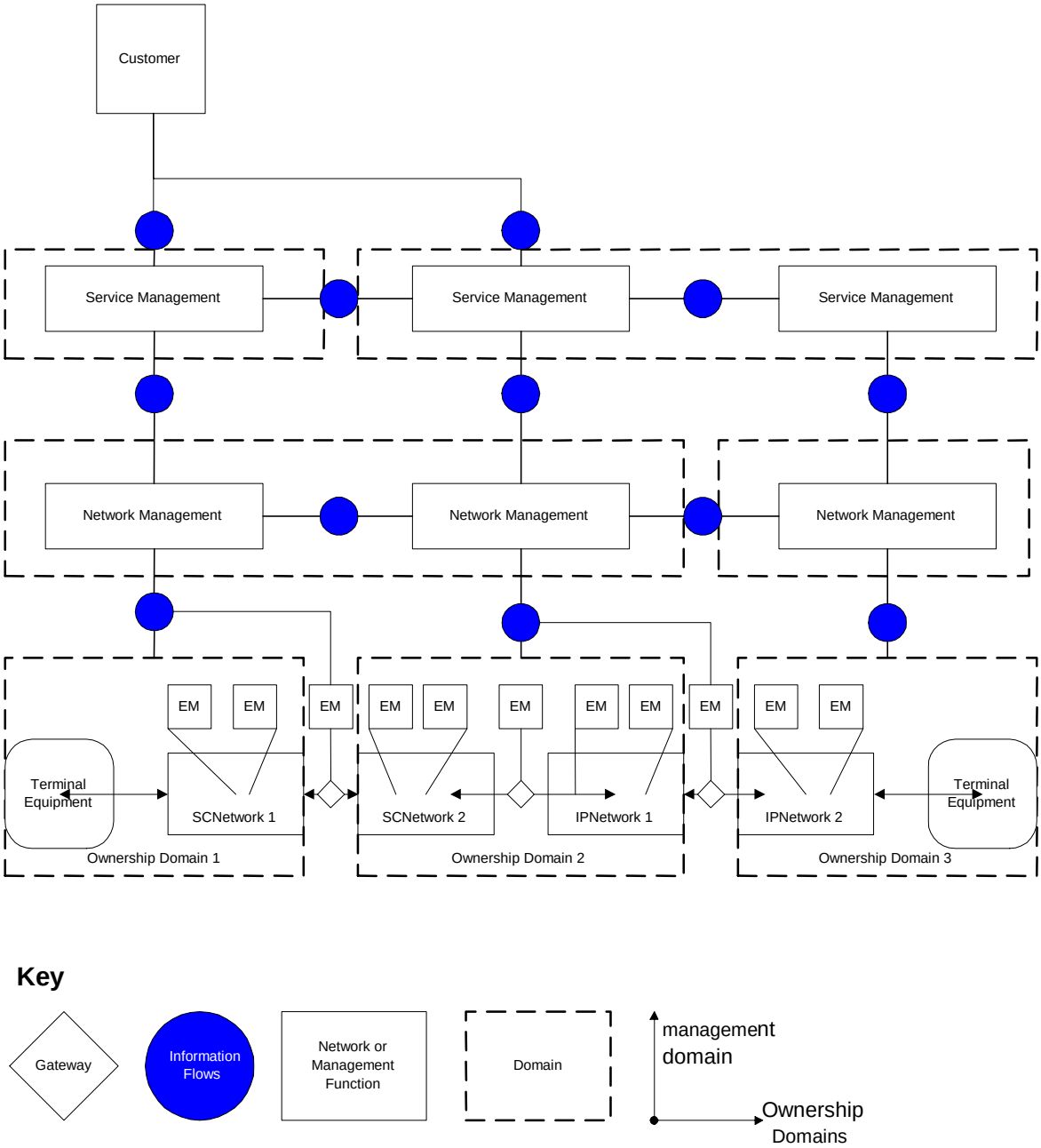


Figure 11: Management domains and interfaces

The management requirements and functions defined in the present document are applicable to the TIPHON planes (TIPHON application plane, TIPHON transport plane). Information flows are defined to exist between management domains (layers) and between ownership domains.

NOTE: The information flows between the network element manager and the network element is out of scope of TIPHON release 4.

5.6 Relationship to TIPHON reference configuration

Functions within the management plane will have interactions with the functions within the TIPHON application and transport planes.

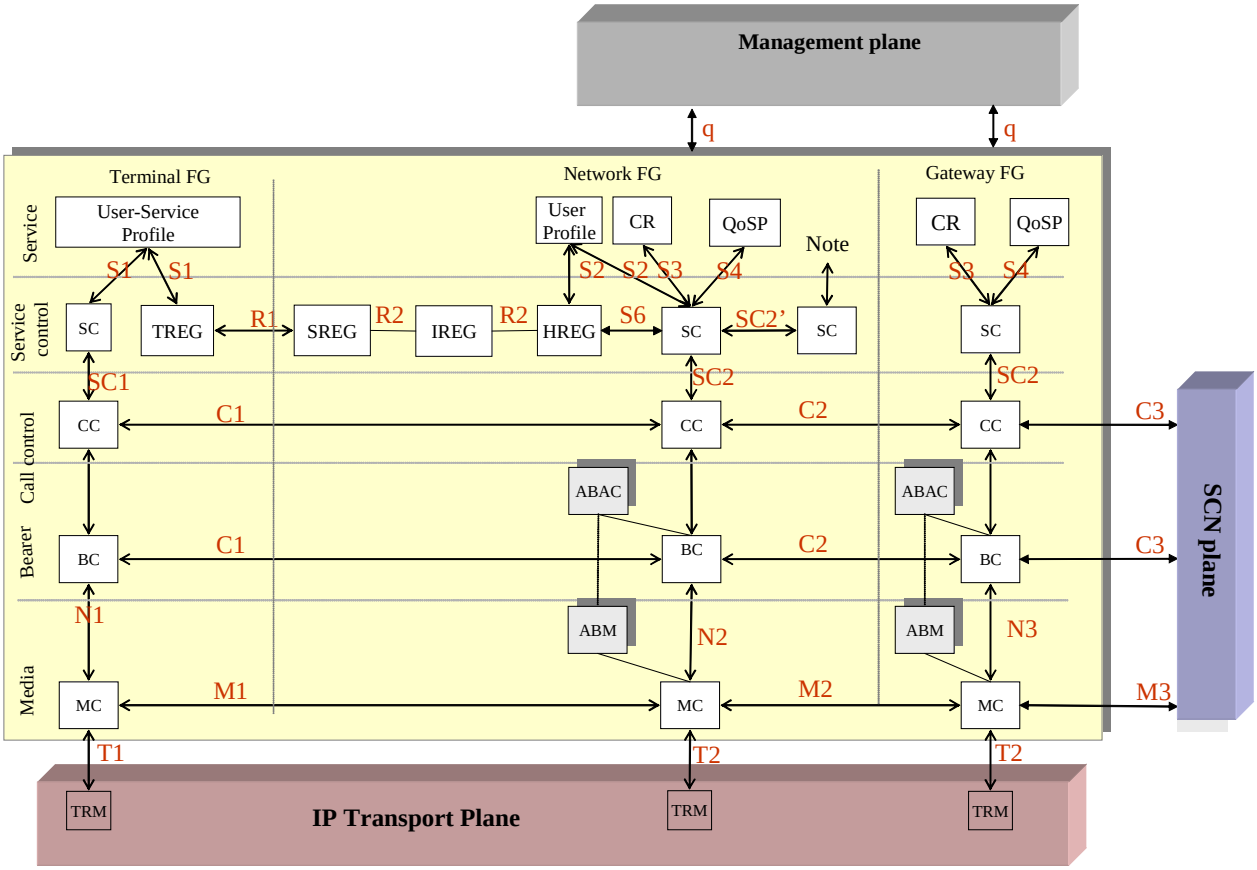


Figure 12: General reference configuration

The present document addresses specifically the service and network management layers of the management plane. In addition to interactions with the TIPHON planes, these layers will interact with management layers in other administrative domains.

The key management relationships for TIPHON release 4 will be those between the network management layer and the element management layer, and those between management domains.

Figure 13 illustrates these relationships.

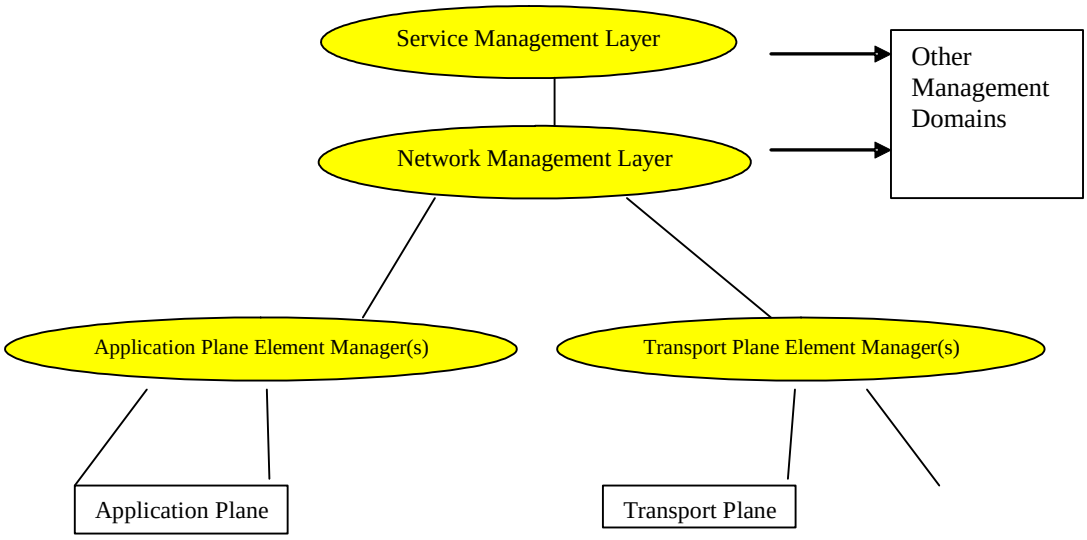


Figure 13: Relationship between management layers and TIPHON planes

5.7 Relationship with TIPHON business role model

In TS 101 314 [11] the following network based business roles are identified. This model is based on the TINA-C business model and has been extended to reflect current commercial developments.

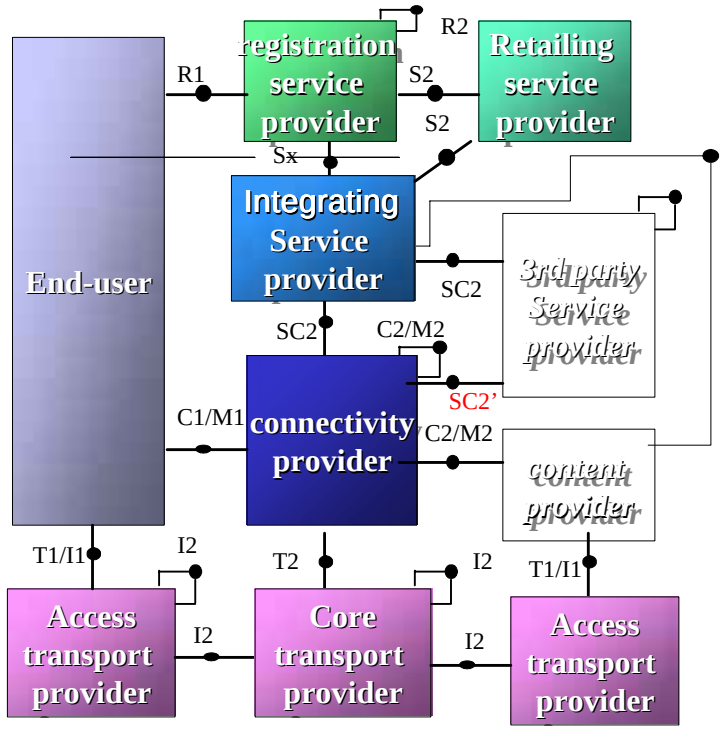


Figure 14: TIPHON business roles

The management role model described in clause 9 is an extension to this model, containing a number of additional "management" roles.

5.8 Relationship between TIPHON reference configuration and business roles

Figure 15 shows the mapping between these roles and the TIPHON architecture. This figure identifies which TIPHON functions fall within the domain of the TIPHON roles. management interactions between the roles will address the management of these functions.

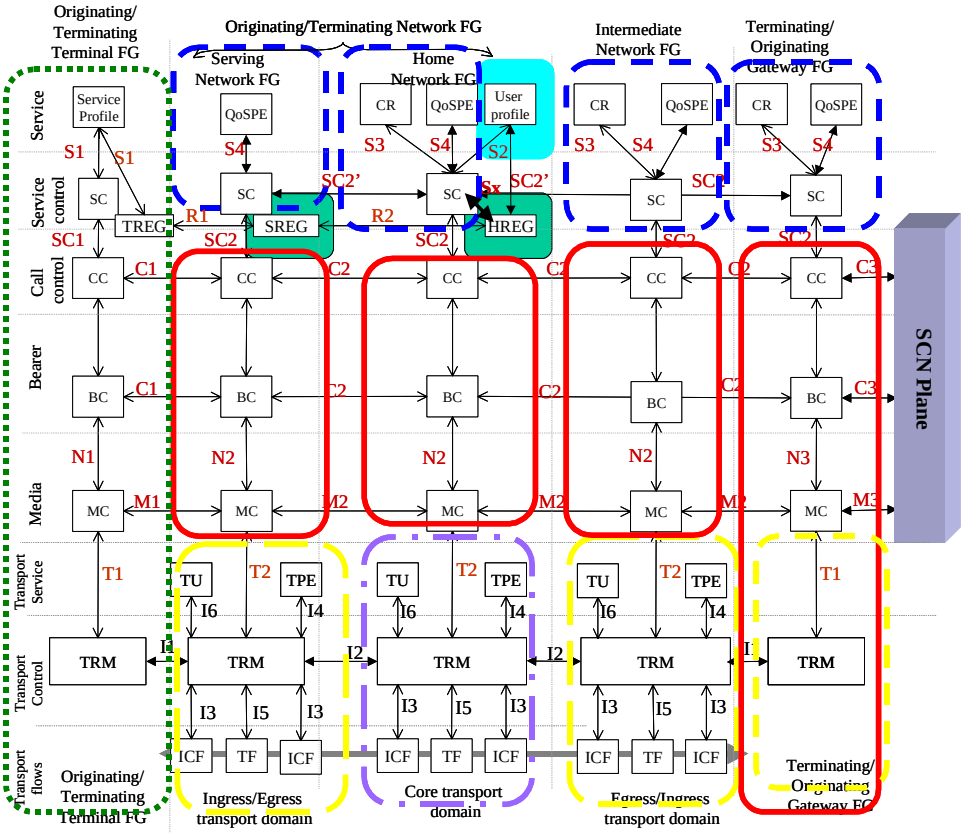


Figure 15: Mapping of business roles to the architecture

Legend: The line coding is as follows.

Line/shading	Role	Line/shading	Role
Green	End-user	red	Connectivity provider
Yellow	Access Transport provider	blue	Integrating service provider
Purple	Core transport provider	Green filled	Registration service provider
		Light blue filled	Retailing service provider

6 Comparison of management methodology and TIPHON project method

6.1 Management methodology

The management methodology is described in ITU-T Recommendation M.3020. [12] (TMN interface specification methodology). The TMN interface specification methodology UTRAD (Unified TMN Requirements, Analysis and Design) describes the process to derive interface specifications based on user Requirements, Analysis and Design (RAD). These 3 steps are generally equivalent to the 3-Stage method used by the ITU-T for ISDN Recommendations I.130 [7], I.140 [8], I.210 [9].

The ITU-T Recommendation M.3020 [12] requirements phase is intended to be understandable to subject matter experts and protocol neutral. Using UML use cases aspects such as security policy, scope of the problem domain in terms of the applications, resources, and roles assumed by the resources are captured. The requirements specify roles, responsibilities and the relationships between the constituent entities for the problem space.

In the analysis phase the requirements are used to identify the interacting entities, their properties and the relationships among them. This allows the interfaces offered by the entities to be defined. These entities, in the UML notation, become classes. The class descriptions along with the interfaces exposed should be traceable to the requirements. The relationship between the classes, defined in the analysis phase, and the classes in the design phase is not necessarily one to one.

The analysis phase is independent of design constraints. The information specified in the analysis phase includes class descriptions, data definitions, class relationships, interaction diagrams, message sequence diagrams, state transition diagrams and activity diagrams. The class definitions include specification of operations, signal (asynchronous stimulus such as receipt of operations, events and exceptions), attributes and behaviour captured as notes or textual description.

In the design phase an implementable interoperable interface specification is produced. This will involve the selection of a target specification language. The design phase specifications are dependent on the specific network management paradigm chosen.

6.2 Comparison with TIPHON project method

The TIPHON project method (TR 101 835 [10]) extends the scope of the ITU-T 3-Stage approach to include explicit testing (Step E), mapping (Step D) and pre-requirements studies (Step A). The steps and their deliverables are:

- step A release definition- deliverables are the release definition and plan
- step B capabilities and requirements - deliverables are the service capability and service independent requirements definitions
- step C reference architecture - deliverables are the functional architecture and information flow/reference point definitions
- step D Implementation framework - deliverables are the protocol framework, interface protocol requirements, management framework management process requirements definitions
- step E Technology mapping and vVerification - deliverables are the technology mappings, compliance specifications (protocol implementation, technology and security)

The TIPHON method's steps map closely to the stages in the ITU-T management methodology (Requirements to Step B, Analysis to Step C and D, and Design to Step E).

TIPHON Step	Output	Management Stage	Output
Step A	Release definition and plan		
Step B	Service Capability Service Independent Requirements	Requirements	Business level requirements Specification level requirements (Requirements Roles, and Resources)
Step C	Functional Architecture Information Flow Reference Points	Analysis	Information Flows Class Diagrams
Step D	Protocol Framework, Interface Protocol requirements, Management Framework Management Process requirements		
Step E	Technology mappings, Compliance Specifications (Protocol Implementation, Technology and Security	Design	Protocol specific information models Conformance statements

7 High level requirements and assumptions

7.1 General requirements and assumptions

7.1.1 Network and service management framework

These requirements and assumptions are extracted from TR 101 303 [16]:

- the architecture and functional decomposition of TIPHON service and network management shall be based on ITU-T Recommendation M.3010 [1] and M.3013 [13];
- the interface definition methodology for TIPHON management systems shall be based upon ITU-T Recommendations M.3020 [12];
- the TNM framework shall include:
  - the TMN layers;
  - FCAPS processes (Fault, Configuration, Accounting, Performance, Security);
  - the definition of information flows between layers, functions and domains;
  - the use of a formal methodology for modelling of the management information based upon the OMGs Unified Modelling Language (UML).
- the TNM framework shall also include:
  - the definition of information interfaces between TIPHON systems and management systems;
  - the definition of management Information Bases (MIB) based on the UML models.
- the TNM will exploit wherever possible:
  - the business and service processes as defined by the TeleManagement Forum (TMF);
  - the management communication protocols and information bases already defined by IETF and ITU-T.

7.1.2 General assumptions

Communication between different organizations (i.e. roles performed different organizations) will follow standard business (e.g. e-business) process. TIPHON will not specify contractual aspects, it will only identify the key information to be transferred to support TIPHON networks and services.

Not all the reference points (relationships) identified in clause 5.3 will be standardized.

The key relationships that need to be studied capture the relationships between the following roles:

- retailingSP to Integrating SP;
- integrating SP - Connectivity provider;
- connectivity provider to transport provider;
- management system to TIPHON network element Manager(s).

Interfaces between element managers and network elements will not be the subject of standardization within TIPHON. TIPHON may however identify requirements for these interfaces. These interfaces may be proprietary or standardized in other bodies (e.g. IETF, ATM Forum, ITU, etc.). In all cases it is expected that these interfaces will be open (i.e. publicly available).

7.2 QoS requirements and assumptions

These requirements and assumptions are extracted from TR 101 329-7 [14].

7.2.1 Assumptions

In order to guarantee end to end speech quality:

- service provider equipment must meet specified performance requirements and be correctly configured by service providers (network Planning and Design and Configuration);
- underlying transport networks, involved in the call end-to-end (IP as well as SCN), must be designed to deliver specific performance criteria at all times. It is implicit that guarantees can only be achieved over managed IP networks, engineered to deliver a given level of performance, and where traffic levels are controlled. (network Planning and Design and Configuration);
- the realization of end to end speech quality in a TIPHON system is affected by network transmission planning. (network Planning and Design);
- the following management steps are likely to be involved in implementing a TIPHON system:
  - planning and configuration;
  - maintenance;
  - monitoring and Verification.

7.2.2 Transmission planning

In order to deliver the intended end-to-end speech transmission quality in TIPHON systems, transmission planning should be performed during the design phase of TIPHON related equipment. It is not sufficient to design equipment or networks just along the requirement limits of the respective TIPHON class.

Any variation of transmission parameters should only be judged on the basis of E-model calculations for critical end-to end connections. Any assumption whether or whether not a specific parameter variation will be perceived by the user should always be based on E-model calculations.

Special care should be taken with devices which dynamically vary one or more transmission parameters, e.g. Automatic Level Control (ALC) devices; experiences with such devices have shown that they have the potential to impact end-to-end speech transmission quality, severely.

7.2.3 Maintenance

After TIPHON equipment and networks have been designed, planned and rendered operative in compliance with one the TIPHON QoS classes it might - nevertheless - occur that users complain about too low speech quality.

In such cases, it is very important to be able to carry through a diagnosis of end-to-end speech transmission performance. For that it will be needed to keep track of all parameter changes (e.g. of send and receive loudness rating) carried out either automatically or by user interaction.

This should be considered already during the design phase of TIPHON equipment and networks, e.g. by providing tools to set parameters back to default values or by providing a log file function.

7.2.4 Monitoring and verification

Even if a specific TIPHON system has been operated for some time at the desired level of customer satisfaction it will be required to continuously monitor and check the end-to-end speech transmission quality.

Verification will require access to the actual settings of all major transmission parameters - including those which were accessible to the user.

7.3 Subscription management requirements and assumptions

7.3.1 Subscription management assumptions

The following assumptions are made in developing the Subscription management requirements:

Business model assumptions:

- the provider of the service package to the subscriber may be different from either the service provider or the network operator;
- the model shall allow for retailers, service integrators and third parties that are independent of the service provider and the network operator.

Network and control assumptions:

- the invocation of a service capability in real time shall be the responsibility of the network and any associated control.

User equipment assumptions:

- this issue is not addressed in this TIPHON release.

7.3.2 High level requirements

7.3.2.1 General

Subscription management shall provide:

- the management of the subscription related aspects of the user profile (subscription profile);
- support for the replication and distribution of subscriber profile components (fragments of the user profile) across administrative, network and systems domains;
- control of the synchronization and distribution of user profilecomponents across administrative, network and systems domains;
- the capabilities required by the customer care operations for the control and modification of user profile information;

- the capabilities that need to be offered to Business to Business (B2B) tradingpartners, such as value add service providers.

7.3.2.2 Business model requirements

Subscription management features shall support the distribution of Subscription management components across several organizations and administrative domains to support industry business model comprising, VASP, SP , NO, Retailers, Reseller, service Integrator, etc.

Subscription management shall allow for the optional use of third parties to facilitate trading relationship between organizations. This requirement is needed for trusted third parties but not limited to trusted third parties.

7.3.2.3 Subscription management requirements

Requirements on home network operator:

- the primary area where subscription profile components are stored is in the home network in the home network registration function. This function will be used by the network for distribution and replication of this data in other entities;
- subscription management shall allow for the creating, reading, updating and deleting of subscription profile data in the home network registration function;
- subscription management shall support the data structures and organization described in UMTS user profiles/service profiles.

Requirements for support of the user profile:

- the interaction between thesubscription management processes and other process acting on common components of the user profile and the subscription profile shall be defined;
- subscription management shall support user profile requirements, including user profile constraints on the common components. E.g. a single logical user profile per user;
- subscription management shall not place restrictions on the allocation of ownership /stewardship of components of the user profile that are not common with the subscription profile;
- subscription management shall be able to control the ownership of components common to the user profile and the subscription profile.

Requirements on terminal equipment:

- Tthis issue is not addressed in this TIPHON release requirements on home network;
- subscription management shall manage subscription profile components within the home network.
- subscription profile components will be needed for:
  - data related to subscription identification and numbering. E.g. private identity, public identity, registration status;
  - data related to roaming;
  - data related to authentication and ciphering;
  - data related to SPOA selection information;
  - data related to applications and service triggers.

Requirements on Authentication:

- subscription management shall be able to create, read, modify and delete data about a user in an authentication system.

7.3.2.4 Process requirements

Modifications by the subscription management to subscription profile components shall be recorded in an historical log.

Subscription management shall provide a process to support a subscriber wishing to check their subscription configuration.

Authentication of a subscriber shall be provided to prevent anyone other than the subscriber or an authorized person from gaining access to their subscription profile.

It shall be possible to replicate and distribute the subscription profile components following rules established and defined by subscription management feature.

7.3.2.5 Interfaces

Interfaces supporting relationships between organizations shall use mainstream e-commerce technology methods.

7.3.2.6 Business aspects and integration

Interfaces between trading partners shall meet the commercial and legal standards required for the business to business transactions.

To claim to be TIPHON compliant management interfaces between Subscription management components within an organization shall be open and use industry standard solutions (e.g. CORBA, CMIP, OSSJ, and SNMP).

7.3.2.7 Security

Secure mechanisms shall be available for the transfer of subscription profile components to, from or between authorized entities.

Access to subscription profile component shall only be permitted in an authorized and secure manner.

The secure mechanisms to be applied shall be appropriate to the level of confidentiality of the data, the endpoints of the transfer and the routes that are available for the transfer of the data. The owner of the data, normally the body storing the master copy of the data, shall be responsible for applying the appropriate level of security to the transfer of the data.

The secure mechanisms available to subscription management shall include the following:

- A Before any transfer takes place, it shall be possible for the sender of the data to verify the identity of the recipient.
- B It shall be possible for the recipient of data to identify the sender.
- C It is permissible for either the sender or recipient of data to employ the services of a third party, known to, and trusted by, both in order to provide authentication of identity.
- D The validity of an authentication of identity shall, if required, be subject to a maximum time limit.
- E It shall be possible for the sender of data to render the data to be unreadable by any party not authorized to receive it.
- F It shall be possible for the recipient of data to detect whether the sender has made any change to the data subsequent to its transmission.
- G The security mechanisms shall provide verification that the data has been sent by the sender and received by the recipient (non-repudiation).
- H It shall be possible for the sender and/or the recipient to create an audit log of all data transfer transactions of a specified type, provided that this requirement is made known before any transfer takes place.
- I Transaction security for the change of data should be available in order to ensure the consistent change of data at different locations.

Subscription management feature will need to bridge between the TIPHON network security functions and the security used in mainstream e-commerce solutions such as those in ebXML.

7.3.2.8 Privacy

Subscription management shall fulfil local privacy regulations.

7.4 Performance management requirements and assumptions

7.4.1 Policy and capability

To be able to discover from the E164 number the network endpoint and access segment that currently services the customer.

To be able to discover the current policy decision and policy enforcement points for a given access segment/given customer.

To be able to validate the current policy enforced within the network domain.

To be able to discover the policy being enforced in an adjacent service domain.

To be able to validate that the two are compatible.

To be able to discover policy being enforced in the customer owned network

To be able to discover limitations imposed by the terminal that the user has connected. (Analogue phone, IP Phone, PC).

To be able to validate that this and own network policy are compatible.

NOTE: It seems to be necessary to define what is in a "policy" for the purposes of performance/quality management.

7.4.2 Routing, admission and egress

NOTE: Physical transport routes and connectivity are not covered (e.g. SDH rings) since it is assumed that management of these is essentially unchanged by IP telephony.

7.4.2.1 Admission

To be able to discover which ingress node applies for a particular endpoint or access segment and where admission control is applied. And how it is configured for that endpoint or access segment.

To be able to discover the information source used to configure the above and discover the data it contains.

To be able to compare the two.

To be able to discover the current loading of ingress/admission elements and of queues.

Where appropriate, to be able to discover alternate/fallback entities and equipment.

7.4.2.2 Transport And routing

To be able to discover the two way routing of signalling between an endpoint and its call control entity, and identify any intermediate Gateways and Interworking Functions, including which network nodes they are hosted on.

To be able to discover the current configuration of "Virtual circuits" e.g. MPLS.

To be able to discover the current transport network route topology.

To be able to use this information to infer the routing of media streams (both directions) for given endpoints, customers, service types.

7.4.2.3 Egress

To be able to discover which egress node applies for specific called and calling party pairs. Note that where alternate routings apply there can be more than one possible egress node.

To be able to discover the type and configuration of these egress nodes, especially any policy enforcement rules and related measurements.

To be able to discover the current loading of egress elements and of their queues.

NOTE: Egress means here egress from the service provider/network operators Administrative Domain.

7.4.2.4 Service control

To be able to discover which instances of

- call controller;
- intermediate gateways/IWF;
- service quality management entities.

currently apply for a particular endpoint or access segment, and which physical equipment they are currently hosted on.

To be able to discover configuration data from them related to that endpoint or access segment. More work is needed to list out the key configuration information needed. However, it includes:

- records of improper call terminations and reason codes;
- call usage records;
- quality criteria currently applicable for endpoint, customer, service type. Both measurements and rules;
- in mobile IP, identification of past and present Foreign Agents and their transport addresses;
- see also addressing clause.

7.4.2.5 Addressing

From the unique identifier (E164, ENUM etc.), to be able to trace, where applicable, current:

- log on name and password;
- network endpoint IP address and hardware address;
- terminal IP address and hardware address.

And the reverse.

To be able to identify the functional entities (e.g. DNS, DHCP, and LDAP Server) responsible for:

- network log on;
- issue of IP address;
- configuration of terminal/soft client e.g. from user profile, for network capability;
- resolution of called party unique identifier e.g. E164, ENUM to transport address(es).

And the physical equipment they are hosted on.

To be able to discover current configuration data from those entities.

Where appropriate, to be able to discover alternate/fallback equipments and entities.

Where a "chain of responsibility" exists, to be able to discover the next in line.

7.4.2.6 Testing and analysis

This issue is not addressed in this TIPHON release.

7.4.2.7 Usage

This issue is not addressed in this TIPHON release.

7.4.2.8 Security

This issue is not addressed in this TIPHON release.

7.5 Fault management requirements and assumptions

The following requirements shall be met by the TIPHON service and network management framework:

- Fault management functions and associated managed objects shall be applicable to all TIPHON network entities (gateways with various PSTN interfaces, call control entities - gatekeepers, media gateway controllers or call agents, MCU, terminals - IP telephones, residential gateways, etc.). In order to meet this requirement, the work should primarily be based on the functional entities of the IP telephony plane described in [4].

- Management functions shall be independent of VoIP signalling protocols (IETF SIP/MGCP/MEGACO, ITU-T Recommendation H.323/H.248, etc.). This implies a common terminology to reference class members and potential some mapping work (for e.g., when logging events on a particular call, the call identifier parameter should be mapped to its equivalent parameters in all sig protocol: SIP Call-ID general-header field, H.225 CallIdentifier, MGCP CallId, etc.).

- In its first release, information models and TIPHON network management specifications shall be implementable with currently available management protocols.

- For each management function, the level of requirement must be clearly stated for each TIPHON release; we will define a set of mandatory/optional alarm events and even log attributes for each TIPHON network entities and for each TIPHON releases (alarm perceived severity, alarm status, probable cause, alarm thresholds, etc.). Alarm Severity Assignment profiles should be included.

- The states of managed objects shall follow the general definitions of X.731 [20] (operational state: disabled | enabled; administrative state: locked | shutting down | unlocked; usage state: idle | active | busy).

7.5.1 Alarm surveillance requirements for TIPHON

Alarm surveillance includes alarm reporting, alarm summary, alarm severity assignment profiles, alarm indication management and log control. The definition of alarm surveillance used in this TD is based on ITU-T Recommendation Q.821 [15].

From TR 101 303 [16]: alarm surveillance functions are used to monitor NEs about events or conditions:

- the event data is generated by a NE upon the detection of an abnormal condition. Examples of such events are detection of transmission data errors, the violation of a performance threshold, and the detection of faulty equipment;

- event data can be reported at the time of occurrence, logged for future access, or both.

The purpose of this clause is to identify the requirements for TIPHON entities in TIPHON release 3, in particular:

- The level of requirement for each alarm surveillance functions: alarm reporting, alarm summary, alarm event criteria (severity assign.), alarm indication management, log control;

- Categories of alarm event types for TIPHON systems: communications alarm type, quality of service alarm type, Processing error alarm type, Equipment alarm type, Environmental alarm type;

- Event information: Probable causes (define specific list of causes for TIPHON NE, perceived severity (define severity assignment profile guidelines for each type of VoIP NE), etc.;

- Log control: event logging including remote logging requirements.

7.6 Emergency telecommunications service requirements and assumptions

7.6.1 Requirements

To support service management interactions between the Emergency Telecommunication Service (ETS) customer and provider. For the purpose of this clause, the terms service customer and service provider refers to the customer and provider of emergency services.

To interchange of critical telecommunications service management information - During emergency operations, interaction between the SCs and SPs through sharing of critical information related to availability and status of telecommunication resources would be beneficial. SCs could maintain knowledge of service availability and could provide reports to SPs of service problems and failures. SCs could also have a view of resource configurations supporting the operational needs at hand. SPs would be able to provide reports of status and availability of resources, failure points, recovery notices, and alerts of lost capabilities. When the ETS is only activated during a declared emergency, the SC can directly notify the SP on-line to activate the ETS service for the area impacted. An effective service management interface and a simple data interchange mechanism are needed to provide this important capability.

7.7 Service Level Agreements (SLAs) requirements

7.7.1 Requirements

Service Level Interconnection:

The agreement for service level interconnection will need to specify (TS 101 878 [19]):

- a common base service application or applications that will be inter-worked;
- common standardized service capabilities at the service level together with the values of any particular parameters (e.g. a form of profile);
- any additional common but non-standardized functionality at the service level;
- a common naming scheme with a co-ordinated system for allocating names to users;
- a service provider identity that the roaming user will use at registration time;
- an agreed naming scheme for identifying each network (for routing, it is necessary to determine the home network name from the called user name);
- the technology (protocols) for implementing the interconnection.
- together with the relevant quality of service values and the commercial arrangements.

Roaming level interconnection:

The agreement for roaming level interconnection will need to specify:

- service capabilities needed for the roaming users along with parameters that may be prescribed or signalled during service usage;
- a service provider identity that the roaming user will use at registration time;
- service applications that are to be resolved locally (such as emergency calls);
- the technology (protocols) for implementing the interconnection.

together with the relevant quality of service values and the commercial arrangements.

Transport level interconnection:

The agreement for transport level interconnection will need to specify:

- any non-standardized functionality at the transport level that is the subject of innovation;
- technology (Protocols) e.g. IP or ATM used to implement the inter-domain transport and signalling.

together with the relevant quality of service values and the commercial arrangements.

7.8 General security policy

A general security policy needs to be implemented to counter the identified threats. The following security requirements should be included within this policy.

7.8.1 Bill limitations

It can be necessary to protect users from bills of unexpected amounts. Further it may be necessary to protect users from misuse of their accounts, and to protect operators from misuse of services.

Different methods, or combinations of methods, are possible to realize this requirement:

- absolute bill limitation:
  - when a subscriber opens an account, there can be an option to set a credit limit on the account. The total amount of the current bill of the subscriber may be checked at call set-up. A policy can be implemented about the acceptance or not of the call in case of exceeding bill limit. This can limit damage if abuse takes place.
- bill limitation with respect to time:
  - another possible measure would be to limit the bill with respect to time. Thus, the credit limit may be on a day-by-day basis, on a weekly basis, or provide an overall limit. That means, if e.g. a limit per week is agreed and this limit is exceeded (at call set-up or during a call), the user access would be blocked for the rest of the week.
- origin and destination limits:
  - another security measure may be for certain accounts (for new or less trustworthy subscribers) to limit the destinations of calls. The limit may be within a given area, within the country, or even only to a specified destination address. Likewise, a limit may be put on the caller's location for outgoing calls.

7.8.2 Secure billing administration

The billing administration may have to consider security very carefully. Billing data and related personal data can be stored, processed, and transmitted in such a way that user privacy and data integrity are guaranteed. Itemized bills may be a means for the TIPHON subscriber to check the correctness of the billing. Thus, the billing administration can send to the user an explained bill with the called numbers and split in different part like regional calls, national calls, and international calls. However, to avoid conflicts with privacy requirements, the subscriber can also have the possibility to get only summarized bills.

7.8.3 Subscriber and terminal management

Limiting the access to services by means of subscription restriction or equipment restriction can reduce otherwise unacceptable risks. This can be achieved in a number of ways such as by the use of black lists to identify rogue subscribers or rogue equipment. Service may be denied to subscribers or equipment that appears on such a black list.

A white list gives unrestricted access to subscribers and equipment (within any limits set by their service profile). Intermediate variants of these lists may be maintained to track potential bad debt or potential fraud.

7.8.4 Customer hotline

A customer hotline can be provided by the operator in order to answer users' questions like "My service does not work", "I have received too high a bill". This service may be useful for security reasons in case of theft or loss of terminal or in case of unexpected behaviour of the service of a subscriber where specific procedures should be implemented. In case of theft or loss of terminal, this procedure can be:

- location of the stolen or lost terminal in order to find it;
- block incoming and outgoing calls;
- put the TIPHON number on a black list;
- no charging for the subscriber of calls performed after the report of the theft; and
- de-registration of the terminal after location.

7.8.5 Security related reports to the user

Recording and presentation of information about actions performed by users in the system (event reporting) may often function as a supporting security service. (Users' knowledge of this fact may in turn work as a deterrent factor). Announcements must be carefully designed to enlighten users and third parties of the different states of their connection or relation with the operator/service provider. There can be a facility to inform TIPHON users about actions that affect their privacy and security or the charging. This information can be given on-line by announcements, special dial tones, or short messages.

For example, the following information can be given to the users:

"BILL LIMITATION EXCEEDED".

7.8.6 Secure dialogue between operators

Secure dialogues can consist of a mutual authentication procedure, a confidentiality service and a data integrity service on the communication link. It can be provided by:

- mutual authentication;
- link encryption;
- link data integrity;
- non-repudiation; and
- key management to support this.

7.8.7 Contractual agreements between operators

Contractual agreements relating to security issues can be included in the roaming agreement between two operators.

When agreeing upon a roaming agreement two operators may define some security conditions. Those conditions can be:

- frequency of exchange of blacklists;
- liability of a visited network if it does not take the appropriate measures to stop a fraud;
- level of security audit guaranteed;
- follow the rules concerning the use of data an other network can get access to;
- co-operation in case of fraud;
- integrity of file transfer;

- minimum frequency of authentication to be performed for visiting TIPHON users; and,
- in case of dispute, one network operator should be able to provide the other network with every information related to billing.

7.8.8 Contractual agreements between service providers and subscribers

Contractual agreements relating to security issues shall be included in the conditions for the subscription. Security conditions to be agreed and signed by the subscriber could be:

- to follow the rules (as declared by the TIPHON service provider and adjoined to the subscription contract) regarding secure handling of his PIN if used to protect terminal;
- to report to the service provider immediately loss of terminal which might lead to fraud or misuse;
- to accept limitations of service with regard to agreed levels of credit control/bill limitation; and
- to accept limitations of service which the service provider later on may find necessary to introduce to protect the service as such against misuse or fraud.

7.8.9 Security related reports to the service provider

Recording and reporting the use of security services will allow the service provider to conduct security audits in order to detect actual threats against the TIPHON system. Such audits may be used to investigate unauthorized use of a TIPHON terminal or unauthorized change of profile or abnormal patterns or misbehaviour or abuses.

The following data may be audited:

- use of the authentication mechanism (date, time, TIPHON-id, location, number dialled, success or failure of the attempt);
- attempted access to the service profile (date, time, TIPHON-id, name of the object, type of access attempt, success or failure of the attempt); and
- actions by TIPHON service providers staff (date, time, TIPHON-id, type of action).

In practice the audit will be restricted to specific sets of users.

Access to audit data should only be permitted to authorized persons (see also C2, C4 and C5).

Dependent on the evaluation of audit data (on-line or off-line) some actions have to be carried out in order to enforce the security policy. These actions may include: alarms to the security administrator, or blocking of the subscription.

7.8.10 Secure subscription process

A secure subscription process can restrict subscription fraud. A security policy may be applied to new subscribers in order to be to be confident in the ability and motivation of a subscriber to pay any bills. This may be achieved by authenticated or verified delivery of proofs of identity.

It may be possible for subscriptions to be made available on a pre-paid (contract less) basis. It can be possible to inhibit service when the pre-payment is exceeded.

The operator may restrict the number of subscriptions per subscriber.

8. Managed resource models

8.1 Service resource model

The following TIPHON Functions, documented in TS 101 314 [11] have been identified as candidate managed resources:

- user service profile function;
- user profile function;
- Call Routing function (CR);
- accounting function;
- Quality of Service Policy (QoSP) function;
- terminal registration functional group;
- home network functional group;
- network functional group;

The following TIPHON Functions have been identified as candidate managed resources:

- service capabilities (e.g. carrier pre-selection);
- calling party;
- called party;
- call (temporary logical association);
- consumer;
- retailer;
- service provider;
- connectivity provider.

The following TIPHON Functions, identified in TS 101 314 [11] have been identified as candidate managed resources:

- Name (e.g. E.164, ICANN).

8.2 Service control model

The following TIPHON Functions, identified in TS 101 314 [11] have been identified as candidate managed resources:

- Service Control function (SC);
- terminal registration function (TREG);
- network registration function (SREG);
- network registration function (IREG);
- network registration function (HREG);
- network functional group;
- terminal registration functional group;

- serving network functional group;
- intermediate network functional group;
- home network functional group.

The following additional TIPHON Functions have been identified as candidate managed resources:

- call detail record.

8.3 Call control model

Candidate Manageable Entities:

The following TIPHON Functions, identified in TS 101 314 [11] have been identified as candidate managed resources:

- Call Control Function (CC);
- network functional group.

8.4 Bearer control model

The following TIPHON Functions, identified in TS 101 314 [11] have been identified as candidate managed resources:

- Bearer Control function (BC);
- Aggregate Bearer Access Control Function (ABAC);
- bearer;
- network functional group.

8.5 Media control model

The following TIPHON Functions, identified in TS 101 314 [11] have been identified as candidate managed resources:

- Media Control Function (MC);
- Aggregate Bearer Management Function (ABM);
- Gateway functional group;
- Network functional group.

8.6 General manageable entities

The following general TIPHON functions have been identified as candidate managed resources:

- Domain(s);
- Admin Domain;
- Plane (e.g. Application plane);
- Functional Group;
- Gateway;
- Network;
- Terminal.

9 Management role model

In order to better understand the relationships between management activities, while not standardizing a physical organizational structure, a number of management roles have been identified. A role is an activity performed by an actor (e.g. organization). Each actor can play many roles.

Many combinations of these roles into organizations are possible. Historically one monolithic service provider combined all service provider and transport provider roles, however, it is possible for each role to be played by a separate organization.

This model is an expansion of the TIPHON business role model identified in clause 5.6 and identifies those roles which play a major role in the management of TIPHON services .

9.1 Candidate roles

Role: An activity performed by an Actor (e.g. organization). Each Actor can play many Roles. A Role is defined by a set of properties or attributes that describe the capabilities of an entity that can be performed on behalf of other Role(s).

Customer/User Roles

Customer: a customer role enters into a contract (service level agreement) with a service provider for the provision of one or more services. It is the customer role that has the authority to enter into a contract, change some (usually but not exclusively cost based) service features and receive bills for services supplied.

End User: The role that makes use of the service. (An end user is in the domain of the customer. An end user is interested in using communications and data services, e.g., telecom, internet/intranet, mobile/wireless, etc. The user may be allowed to change some service features, subject to the terms of the customers SLA.

Service Provider Roles

Retailing service provider: supplies retail services (i.e. services for sale to an end customer), is responsible for the relationship with the end-user. The retailing service provider maintains the user database.

Integrating Service Provider: Creates unique service offerings from the wholesale parts offered by multiple service providers (connectivity provider, third party service providers, transport providers). Integrating SPs roles will be required for the access network, the Home network, Intermediate networks and gateways

Registration SP: implements the registration service that enables all the other services to work.

Registration service provider: Provides the standardized service of registration and hence implements the (home) Registration functional entity. Note that a (registration) service provider may proxy for another implementing the ServingRegistration (SREG) functional element.

Third Party SP: provides added value on top of a service offered by a service / connectivity provider, it does not provide a whole service on its own.

Connectivity Provider: sells services wholesale to a retailing service providers for use by end-users (e.g. telephony).

Content Provider: is a service provider who provides content to end-users over a telecommunications network.

Transport Provider Role

transport provider provides generic transport services (up to ISO layer 3) to end-users and service providers. The transport provider roles may be split between:

- **access transport provider,** (e.g. implemented using 3G cellular, xDSL, FTTx, Cable etc.) connects an end user with the core network, and a
- **core transport provider**, specializing in long distances (usually using fiber or microwave links).

Management Roles

Retailing: The role of selling TIPHON services to retail customers

Terminal Configuration: A role that sets the initial configuration of a terminal or modifies it in a controlled and audited manner.

Validation Authority: The role that takes a service Customer mandate for an order and communicates (using a transaction that cannot be repudiated) that the customer did in fact originate a request for a specific Option, or set of options.

9.1.1 Typical actors/organizations

Although not the subject of standardization, some typical Actors and scenarios are identified in this clause.

User/Customer : an individual or organization that subscribes to a TIPHON service.

Service Provider (SP): a company or organization that provides telecommunication services as a business. SPs may operate networks, or they may simply integrate the services of other providers (who operate networks) in order to deliver a total service to their customers. Providing telecommunication service to any one end customer may involve multiple SPs, where one provider may "sub-contract" with other providers to fulfil the customer's needs (TMF 701).

Note that the term service provider is now being used generically and may include Telecom Service Providers (TSPs), Internet Service Providers (ISPs) and Application Service Providers (ASPs) and another organization that provides services, e.g. internal IT organizations that need or have SLA capabilities or requirements.

Service Integrator (Actor): An organization that takes a set of services from other providers and derives an end-to-end set of services. It has responsibility for the QoS to the customer.

Trusted Third Party (Actor): An organization that performs an agreed role on behalf of two or more other roles (e.g. authentication, trust, market place services, etc.)

User Equipment Supplier (Actor): An organization that supplies User equipment to service customers.

Clearing House (Actor): An organization that collects and processes roaming and billing information from a number of carriers. It then transfers the compiled data to the proper carrier for credits and billing.

9.2 Examples of possible relationships between organizations (actors)

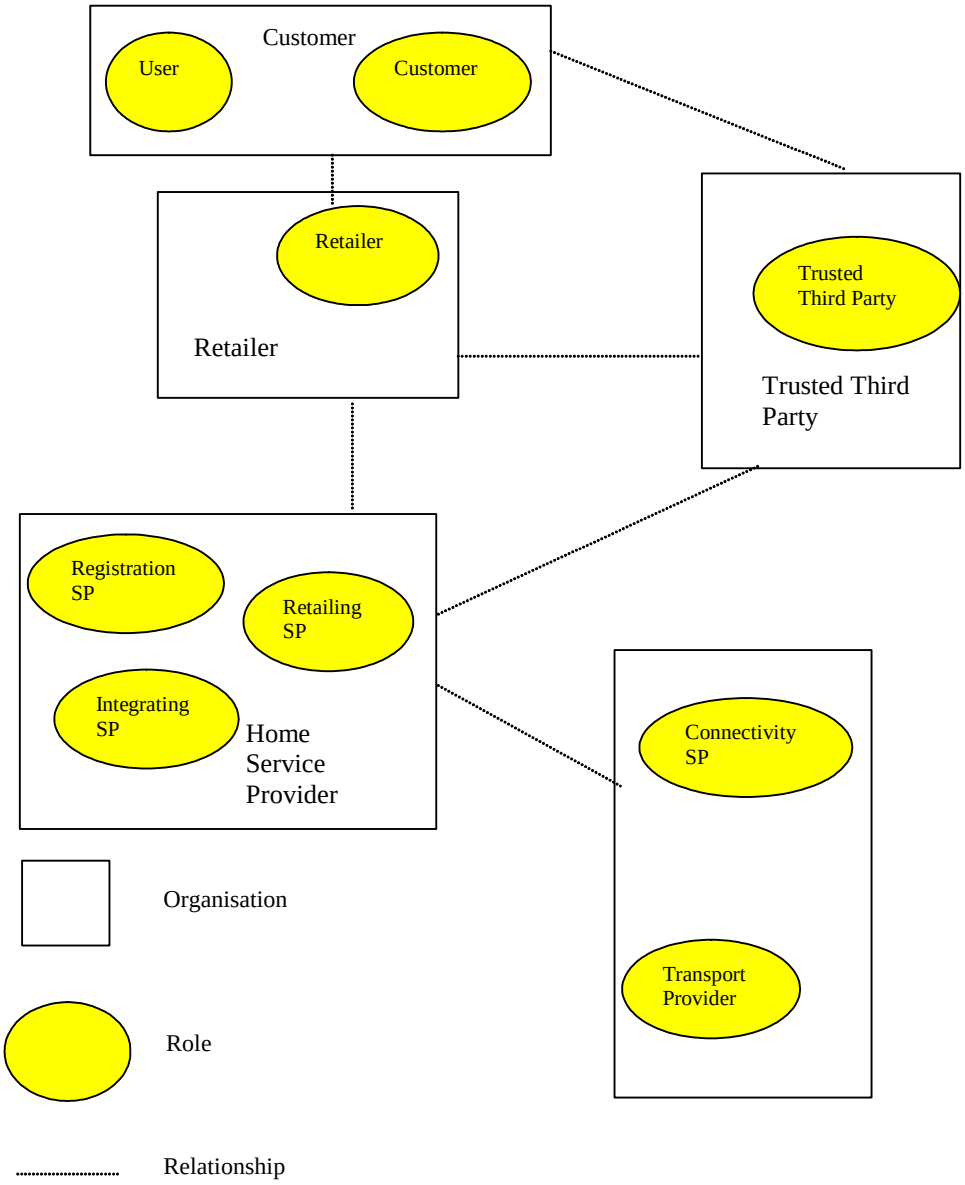


**Figure 16: Example business role model -
domestic customer subscribes to a "TIPHON" simple call service**

A high-street retailer sells the customer a simple call service, provided by the home Service Provider (SP). This may be part of a larger package of services. The service is established using the network capabilities of the access network operator. This transaction is supported by a trusted third party.

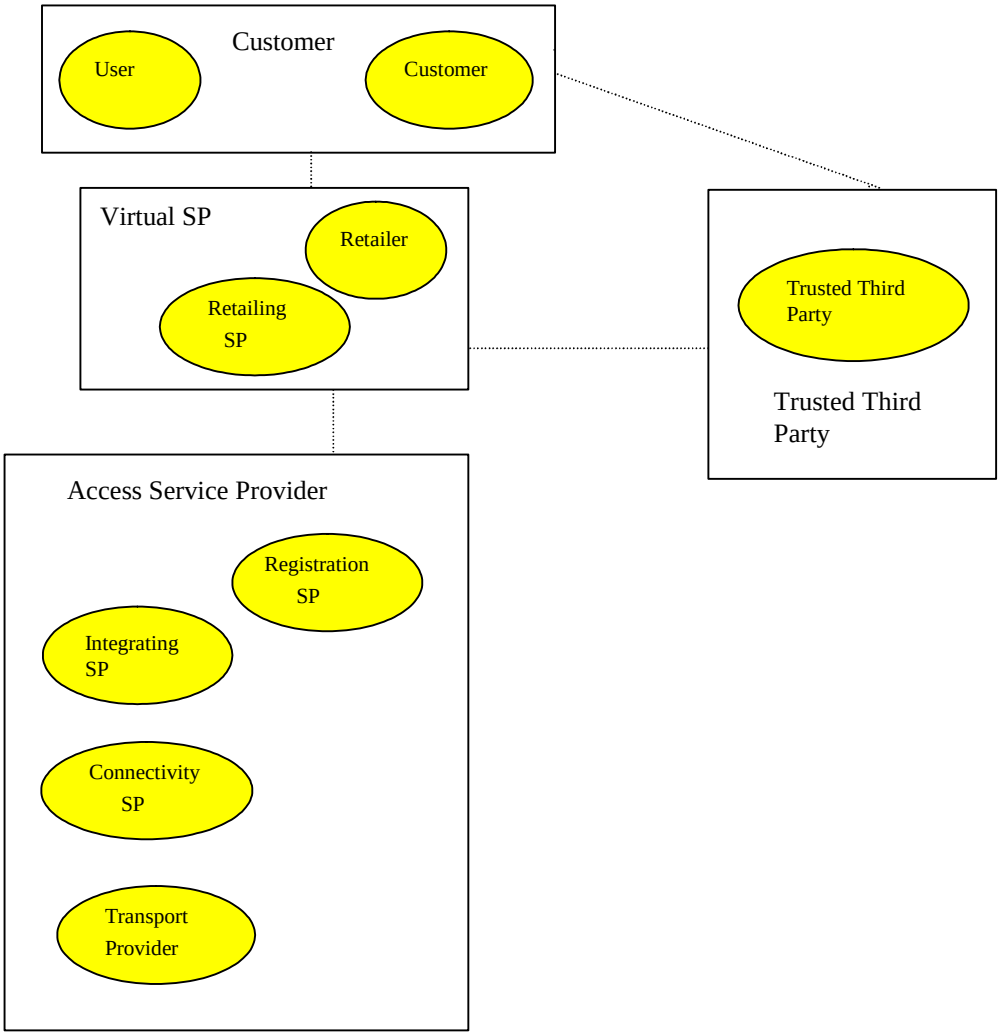


Figure 17: Example business role model
domestic customer subscribes to a "TIPHON" simple call service version 2

In this example, the retailer and retailing SP roles are performed by a single actor (virtual service provider). The service is established using the capabilities of the access service provider and network operator. This transaction is supported by a trusted third party (e.g. credit card company).

Figure 18: Example business role model -
two SPs make routing/QoS agreement

A home service provider makes an agreement (SLA) with a transit SP to carry calls towards one, or more, addresses at an agreed QoS, cost and call volume/time of day profile.

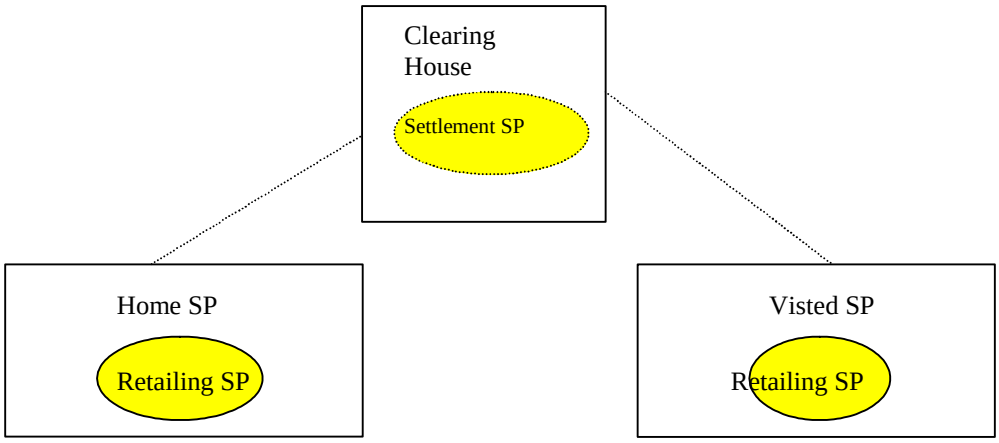


Figure 19: Example business role model - settlement via a clearing house

Settlements between two service providers who have no settlements agreement (SLA) are transmitted via a settlement SP who has SLAs with both parties.

10 Key TIPHON management processes

This clause identifies the key management Processes required in order to ensure the operation of TIPHON services within and across multiple domains. These processes have been identified using the eTOM [5] level 3 process decomposition.

10.1 Processes

10.1.1 Fulfilment

Resource management and operations:

- resource provisioning and allocation to service instances:
  - Resource provisioning and allocation to service instances processes encompass the configuration of resources, and logical resource provisioning for individual customer instances. This involves updating of the Resource Inventory Database to reflect the resource being used for a specific customer;
- network provisioning and allocation to service instances;
- application provisioning and allocation to service instances;

Service management and operations:

- service configuration and activation.

Customer relationship management:

- order handling.

10.1.2 Assurance

Customer Relationship management

- problem handling;
- customer QoS/SLA management.

Service management and operations:

- service problem management;
- service quality analysis, action and reporting.

Resource management and operations:

- resource problem management.

Resource problem management processes are responsible for the day-to-day management of problems with groups of resources (resource classes), and ensuring that the resources are working effectively and efficiently. The objective of these processes is to proactively deal with resource problems, before complaints are received about affected services.

Resource Restoration:

Resource Restoration processes deal with resolving problems with groups of resources, so that the resource capability is restored.

- resource quality analysis, action and reporting;
- resource data collection, analysis and control;
- network data collection, analysis and control.

10.1.3 Billing

Customer relationship management:

- billing and collections management.

Service management and operations:

- service specific instance rating.

Resource management and operations:

- resource data collection analysis and control.

Resource data collection, analysis and control processes encompass the collection of usage, network and information technology events, including resource information, for customer usage reporting and billing. This also includes analysis of the collected information to understand the impact on resource performance, and based on analysis of this, installs controls to optimize this performance.

These processes collect and format data for use by many other processes within the enterprise:

- network data collection analysis and control;
- application data collection analysis and control.

10.2 Key interactions

It should be noted that inter-domain and intra-domain interactions could be between actors (organizations) or within a single actor (organization) depending on the business model in use.

10.2.1 Inter-domain

Pre Service:

SP - SP:

- Service level agreements.

Service provision:

Customer - retailing SP:

- SLA.

Service assurance:

Customer - retailing SP:

- billing;
- trouble teporting;
- customer care.

SP -SP

- SLA reporting (e.g. trouble reporting, QoS reporting);
- accounting.

10.2.2 Intra-domain

Pre Service:

- service level agreements;
- service plan and build;
- network plan and build.

Annex A (informative): Example scenarios

A.0 Subscription management

Part of this profile will be provided by the service provider and the Customer, other info will come from the network.

The following list provides an initial proposal of the information, in a TIPHON Subscription profile (e.g. management view of a User Profile):

- General subscription information;
  - unique customer ID;
  - customer name;
  - contact address (e.g. terminal location for fixed terminal);
  - User Network Interface ID;
  - billing address;
  - priority;
  - public/private Ids;
- Capability description;
  - registration;
  - simple call;
  - number portability;
  - roaming capabilities (Yes/No, where allowed);
  - addressing (including address allocation and translation);
  - billing/accounting data;
- Terminal capabilities;
- Network capabilities;
- User preferences
  - subscribed services;
  - authorized services;
  - service availability;
  - QoS profile;
  - service class (QoS profile);
  - alerting preferences (ring tone type - part of R4);
- Parameters
  - domain/network ID;
  - routing Information;

- forwarding number;
- new address/destination number (for number portability);
- authentication info (provided in e.g. Register message; service request to SpoA);
- security information (Keys etc);
- duration of Registration;
- duration of Service availability;
- home service provider/Domain ID;
- serving service provider/Domain ID;
- home Registrar ID;
- serving Registrar ID;
- home SpoA ID;
- serving SpoA ID;
- media and service proxy IdsCapabilities;

- Service profiles;
- CLI conveyance Y/N;
- COLP Y/N;
- Call FWD Y/N;
  - type:
    - unconditional: all calls;
    - no reply: all calls;
    - not available: all calls;
    - busy: all calls;
    - selective: certain numbers - list;
    - call deflection: on user rejected calls;
  - diversion numbers;
- ICB Y/N;
  - types:
    - selective: list of numbers;
    - anonymous: calls with ID held - CLI restriction indicator;
    - unconditional: all calls - do not disturb;
    - over-ride: do not bar these numbers - list of numbers;
- AoC Y/N;
  - types:
    - start of vall Y/N;
    - during call Y/N;

  - end of call Y/N;
  - user initiated Y/N;
- Call waiting indication Y/N;
- Call queuing Y/N;
  - queue size Y/N;
- Call hold Y/N;
- Terminal portability Y/N;
- Message waiting Y/N;
- Call transfer Y/N;
- 3 party conference calls Y/N;
- Reminder/alarm call Y/N;
  - set timers Y/N;
- SMS Y/N;
- Call completion services Y/N;
  - types:
    - CCBS Y/N;
    - CCNR Y/N;
    - CCNA Y/N;
- Network call-back Y/N;
- Network redial Y/N;
- Etc.

In the following table, which is structured as the recommended 3GPP user profile, is a first attempt at identifying ownership, Data users and data storage location.

Owners and Users can be - User, Customer, NO, SP, VASP

Data Locations (Location of master copy of the data) - Terminal, network (home), management system (e.g. NO or SP), VASP.

Table A.1

Service Profile Components	Owner	Users	Location
General information	SP/Customer	SP, NO, VASP	SP
Capability Description	SP/Customer	SP, NO, VASP	??
User Preferences	User	User, NO,SP, VASP	Network
Parameters	SP	SP,NO, Network, VASP	Network
Service Profiles	SP	SP,NO, Network, VASP	Network

A.1 TIPHON subscription management use case

Table A.2

Name	TIPHON Subscription management Profile Creation
Summary	A customer requests a simple call service
Actor(s)	Customer, Retailer, Trusted Third Party, Integrating SP, Home SP
Pre-Conditions	*A list of all system and environment conditions that must be true before the use case can be triggered.* SLAs must exist between: Retailer and integrating SP Integrating SP and home SP Home SP and Access NO *(issue SLAs with Trusted Third Party?)*
Begins When	Subscription request received by retailer
Description	*The various tasks that make up the use case, not necessarily in sequence* *Customer and retailer negotiate service package* *Retailer applies for service from integrating service provider* *Integrating SP*
Ends When	Subscription to service
Exceptions	*A summary list of all exception conditions and faults detected by the use case during its operation*
Post-Conditions	*A list of all system and environmental; conditions that must be true if the use case has terminated without internal error* Customer Has service Service provider has customer
Traceability	*A itemized list of all requirements exposed by this use case*.

A.2 Example business role model

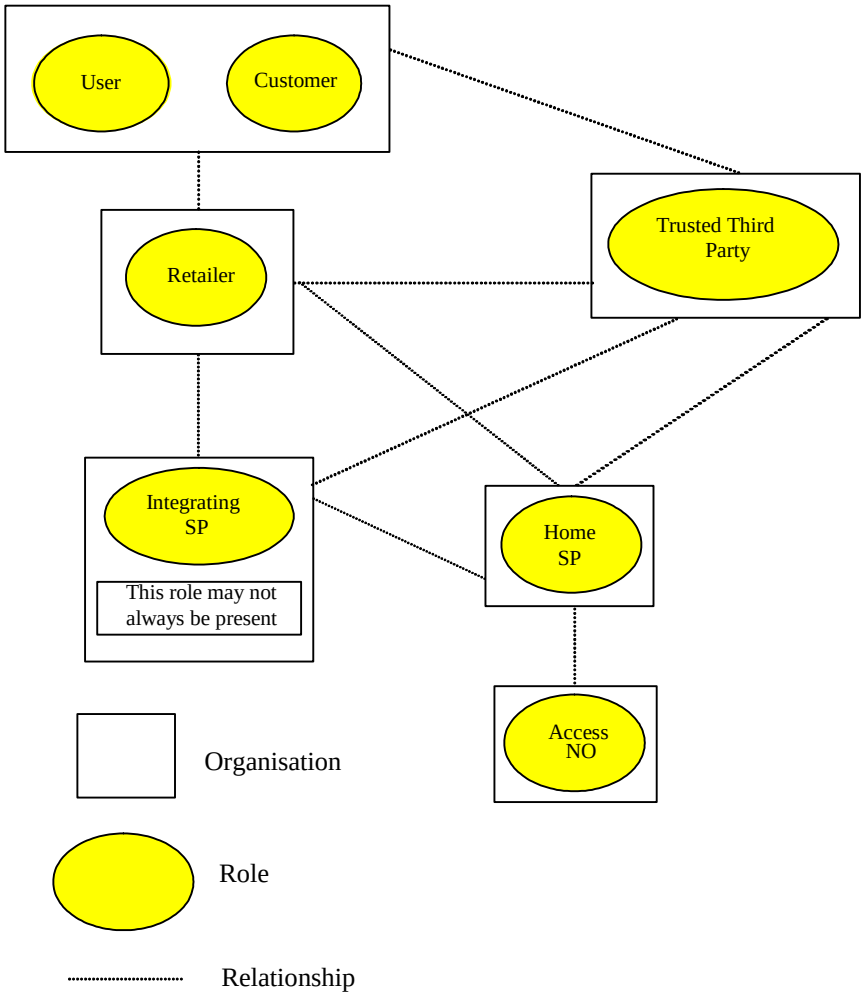


**Figure A.1: Example business role model -
domestic customer subscribes to a "TIPHON" simple call service**

A high-street retailer sells the customer a simple call service, provided by the Service Provider (SP). This may be part of a larger package of services supplied by the integrating service provider or directly from the home SP. The service is established by the network capabilities of the access network operator. This transaction is supported by a trusted third party (e.g. credit card company).

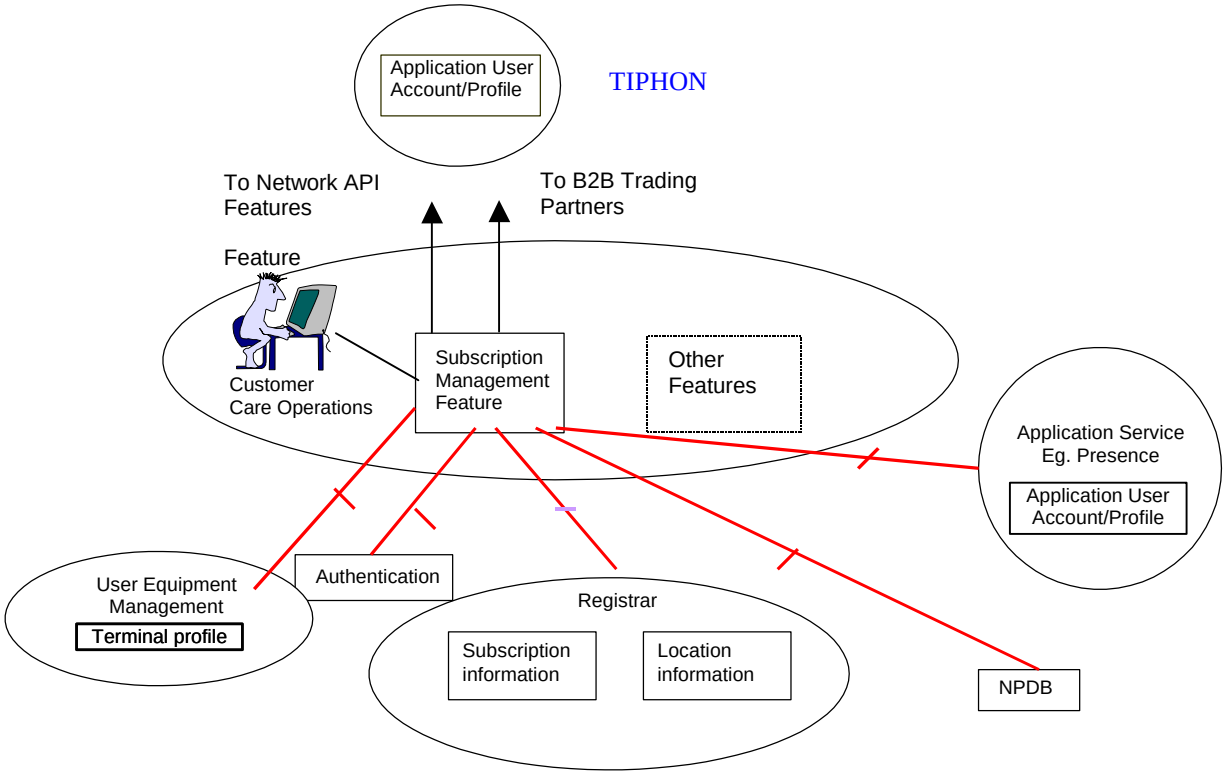


Figure A.2: Subscription management relationships

History

Document history		
V1.1.1	June 2001	Publication as TR 101 303
V1.1.2	December 2001	Publication as TR 101 303
V4.1.1	November 2003	Publication