INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Y.140.1

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2004)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT GENERATION NETWORKS

Global information infrastructure – General

Guideline for attributes and requirements for interconnection between public telecommunication network operators and service providers involved in provision of telecommunication services

ITU-T Recommendation Y.140.1

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	**Y.100–Y.199**
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Y.140.1

Guideline for attributes and requirements for interconnection between public telecommunication network operators and service providers involved in provision of telecommunication service

Summary

Based on the framework set forth in ITU-T Rec. Y.140, this Recommendation concentrates on one of the interconnection scenarios relevant to GII, the interconnection between operators of public telecommunication networks (PTNOs) and service providers (SPs). After looking at the situation before and during transition to a full implementation of the so-called enterprise model, attributes of reference points for interconnection between PTNOs and SPs are dealt with in some detail. Separate clauses treat the various aspects of these attributes, in particular, security, service interaction, charging/billing, service availability, access to a network address and management. The content of this Recommendation should be seen as a guideline for consideration by involved parties when implementing the GII concept within a Next Generation Network.

Source

ITU-T Recommendation Y.140.1 was approved on 29 March 2004 by ITU-T Study Group 13 (2001-2004) under the ITU-T Recommendation A.8 procedure.

Keywords

Essential requirements for service provision, Global Information Infrastructure, interconnection, interconnection interfaces, public policy, reference points for interconnection.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Introduction

The objective of this Recommendation is to elaborate on one aspect of ITU-T Rec. Y.140 and is intended to supplement it. The reader should be aware of the content and considerations of ITU-T Rec. Y.140.

ITU-T Rec. Y.140 describes the reference points for technical interconnection between various entities involved in the provision of telecommunication services. One of the areas identified by ITU-T Rec. Y.140 as to where technical interconnection is required, is "for the access and/or interconnection of a service provider to products of a public network operator" (item b of clause 8/Y.140).

This Recommendation (ITU-T Rec. Y.140.1) looks in more detail at this relationship between the service provider and the network operator, and at the elements of the interconnection interface that results as a consequence of this relationship.

It needs to be recognized at the outset that the elements of the technical interconnection between these two entities, the network operator and the service provider, arise not only from the needs of these two entities. External forces also play a role in determining the elements of interconnection that will exist between these two entities. For example, service subscribers' needs will also influence the nature of the interconnection between the network operator and the service provider. Also, government regulators may impose certain requirements on the nature of the interconnection between the two parties. (It is to be noted in passing that there may be an inverse relationship between the extent to which the network operator and the service provider take the needs of the service subscriber into account voluntarily, and the need for government regulation, as a matter of public policy, to require the two entities to do so. If the network operator and service provider act voluntarily in a way that satisfies public policy, the need for government regulation may be reduced. This relationship is also known as co-regulation.)

Also, the nature of the technical interconnection that is agreed upon between the two parties will need to be captured in a contractual agreement between them.

Figure 1 portrays these relationships in diagram form. The focus of this Recommendation is on the technical aspects of the interconnection between the network operator and the service area (the shaded area). However, it is recognized that the interests of other parties (identified in the diagram outside the shaded area) may impact this relationship. Therefore, although the Recommendation only addresses the shaded area, references in the Recommendation are made, where appropriate, to identify places where these external forces may impact these reference points. Contractual agreements are also outside the scope of this Recommendation. Also, in some places, the Recommendation identifies reference points that may be impacted by external contractual agreements.

More background information about how the influence of the changing regulatory environment may impact the technical aspects of these reference points may be found in the attached bibliography.

ITU-T Recommendation Y.140.1

Guideline for attributes and requirements for interconnection between public telecommunication network operators and service providers involved in provision of telecommunication services

1 Scope and purpose

This Recommendation deals with the interconnection of service providers and (public) networks (in short, this type of interconnection will be called service provider access). The Recommendation should not be seen as an obligation for the parties involved, but should be considered as a Guideline assisting in recognizing and implementing the adequate essential attributes and/or requirements in a voluntary manner facilitating the public policy objectives.

Therefore, two aspects/perspectives have to be considered:

a) service providers' requirements on network operators in delivering telecommunication services; and

b) network operators' requirements for the provision of service provider access.

As illustrated in Figure 1/Y.140, a set of possible reference points for interconnection (RPIs) is introduced. In clause 8/Y.140, it is pointed out that there might be a couple of essential attributes and/or requirements relating to different classes of interconnection interfaces. Class b of these relates to the interconnection of service providers to (products of) public network operators. This Recommendation proposes a description of attributes/requirements for the class b interconnection interfaces.

Indirect SPA, i.e., accesses where intermediate networks are involved, will not be considered in this Recommendation.

An example of a possible scenario is given in Figure 1. It shows an environment of involved parties where many different roles and relationships exist. In this Recommendation, only the grey shadowed area is dealt with.

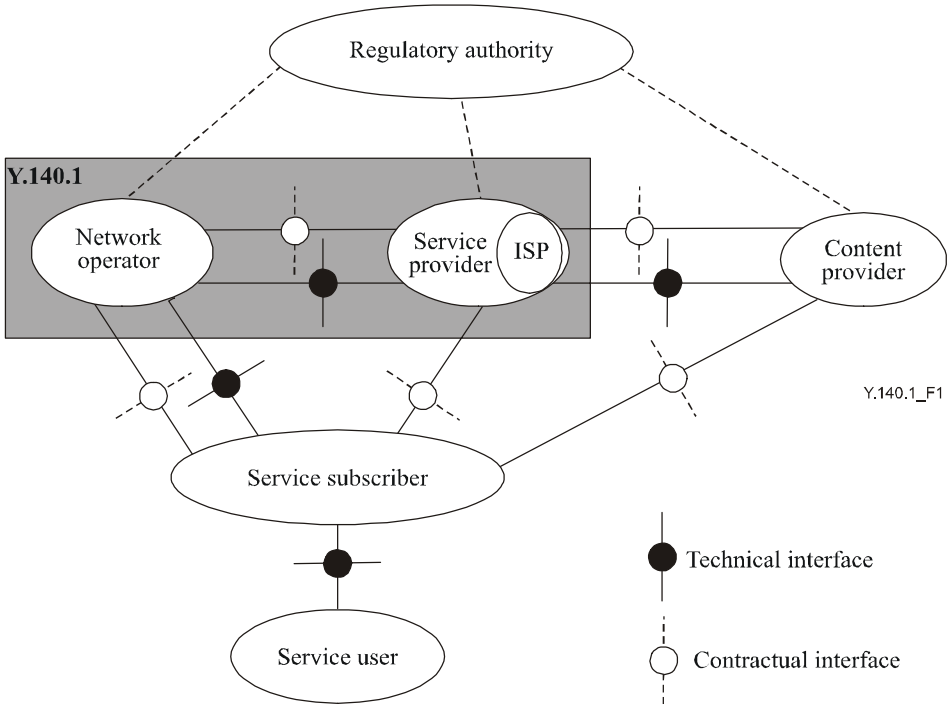

Figure 1/Y.140.1 – Example of relationships between involved parties

The scope of this Recommendation is to describe generic functional requirements regarding the service provider access. The priority of each requirement is based on the need perceived from the viewpoint of either the service provider, a, or the (public) network operator, b. To fulfil these requirements, appropriate protocols may have to be enhanced or developed, particularly taking into account network integrity considerations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T Recommendation F.115 (1995), *Service objectives and principles for future public land mobile telecommunication systems*.

[2] ITU-T Recommendation H.235 (2003), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.

[3] ITU-T Recommendation J.93 (1998), *Requirements for conditional access in the secondary distribution of digital television on cable television systems*.

[4] ITU-T Recommendation J.95 (1999), *Copy protection of intellectual property for content delivered on cable television systems*.

[5] ITU-T Recommendation Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks*.

[6] ITU-T Recommendation X.800 (1991) | ISO/IEC 7498-2:1989, *Security architecture for Open Systems Interconnection for CCITT applications*.

[7] ITU-T Recommendation Y.140 (2000), *Global Information Infrastructure (GII): Reference points for interconnection framework*.

[8] ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

[9] ETSI ES 201671 V2.1.1 (2001), *Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic*.

[10] ETSI TS 101 331 V1.1.1 (2001), *Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies*.

[11] ETSI ETR 232 ed.1 (1995), *Glossary of security terminology*.

[12] ETSI EG 201 722 V1.2.1 (2000), *Intelligent Network (IN); Service provider access requirements; Enhanced telephony services*.

[13] ETSI EG 201 781 V1.1.1 (2000), *Intelligent Network (IN); Lawful interception*.

[14] ETSI EG 201 807 V1.1.1 (2000), *Network operators' requirements for the delivery of service provider access*.

[15] ETSI EG 201 897 V1.2.1 (2002), *Service Provider Access Requirements in a Fixed and Mobile Environment*.

[16] ETSI EG 201 899 V1.1.1 (2001), *Modelling Service Provider Access Requirements using an API Approach*.

[17] ETSI EG 201 916 V1.1.1 (2001), *Development of standards to support Open Inter-Network Interfaces and Service Provider Access*.

[18] ETSI EG 201 965 V1.1.1 (2001), *Service Provider Access Management Requirements for Open Network Access*.

3 Terms and definitions

For the purpose of this Recommendation, the term "Service" or "service" is used in a broader sense and should not be understood in the limited sense of the defined term of ITU-T SG 2 as fully specified "Telecommunication Service".

For the purpose of this Recommendation, the following definitions apply:

3.1 authentication: A process which allows for checking with certainty the identity of a party involved in a communication. Authentication generally follows identification, establishing the validity of the claimed identity, providing against fraudulent actions.

3.2 availability[1]: The property of being accessible and usable upon demand by an authorized entity [8], [6].

3.3 confidentiality[1]: The property that information is not made available or disclosed to unauthorized individuals, entities or processes [8], [5].

3.4 Fraud (protection)

3.4.1 fraud: The act of acquiring pecuniary advantage by misrepresentation or unauthorized action.

3.4.2 fraudster: A party who commits fraud.

---

[1] The definitions of the terms "security", "availability", "integrity" and "confidentiality" are closely linked together and should be used in the context of the others.

3.4.3 equipment fraud: Fraudulent use of the telecommunication network involving the abuse of terminal equipment, such as a payphone.

3.4.4 network fraud: Fraudulent use of the telecommunication network infrastructure involving the abuse of network technical facilities, sometimes using a terminal equipment.

3.4.5 service fraud: Fraudulent use of telecommunication services, sometimes involving the expected or unexpected interaction of two or more services.

3.4.6 subscription fraud: Fraudulent use of the telecommunication network by a party who has no intention of paying their due bill.

3.4.7 telecommunication fraud: Fraud which is committed directly against the telecommunication network or its subscribers.

3.5 Integrity[1]

a) The property that data has not been altered or destroyed in an unauthorized manner [8], [6], [5].

b) The ability of a function to withstand being usurped for unauthorized use, or modified to yield unauthorized results [3], [4].

3.6 lawful interception: Action (based on the law), performed by a network operator/access provider/service provider, of making available certain information and providing that information to a law enforcement monitoring facility [13].

3.7 privacy:

– A mode of communication in which only the explicitly enabled parties can interpret the communication. This may be achieved, e.g., by encryption and shared key(s) for the cipher [2].

– The right of individuals to control or influence what information related to them may be collected and stored, and by whom and to whom that information may be disclosed.

NOTE – Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security [6], [1].

3.8 public policy: In the context of telecommunications, public policy is policy that is made by regulators in their determination of public good and which they may implement by regulations that are imposed on telecommunication entities.

3.9 security[1]: The protection of information availability, integrity and confidentiality [11].

4 Abbreviations

This Recommendation uses the following abbreviations:

NNI Network-Network Interface

PTN Public Telecommunication Network

PTNO Public Telecommunication Network Operator

SLA Service Level Agreement

SP Service Provider

---

1 The definitions of the terms "security", "availability", "integrity" and "confidentiality" are closely linked together and should be used in the context of the others.

SPA Service Provider Access

SPAI Service Provider Access Interface

SPAR Service Provider Access Requirement(s)

NOTE – The term "Service" (with capital S) is avoided as it is "owned" by SG 2.

5 Security

In this Recommendation security-related issues are addressed in clause 7 "Attributes of Reference Points for Interconnection between PTNOs and SPs", particularly in 7.1 "Security aspects". In that clause, security aspects are addressed in relation to the viewpoints of end users on the one hand, and SPs and PTNOs on the other hand. Furthermore, aspects of integrity (7.1.1), authentication (7.1.2) and confidentiality (7.1.3) are dealt with, terms which are closely linked to security. As the Recommendation is to be used basically as a guide, primarily security aspects of general nature are considered. This is also reflected in clause 2 "References (informative)" where, e.g., most of the ETSI documents listed are Guides.

6 Situation before and during transition to a full implementation of the enterprise model

Currently, the enterprise model as described in ITU-T Rec. Y.110 is not fully implemented. In the past, networks were basically designed for those services which network operators themselves wanted to offer to their customers. In that situation, in most cases, it was sufficient to design networks in such a way that they were able to generate and deliver the networks operator's "own" services. Hence, it was sufficient to provide technical support for in-house purposes only with respect to access, billing, signalling, integrity, management, and so on. Even if such services were delivered across more than one network (e.g., across countries or competing network operators), there was no real requirement to support access of third parties to network internal functions. With the policy decisions to trust (rely on) market forces and to open up the market, fundamental changes of the telecommunications' regulatory environment took place.

Firstly, to stimulate competition, the incumbent network operators were obligated by regulators to grant access to their networks, and parts thereof, to third parties.

With the growing liberalization and evolving new technologies, the design of telecommunication networks has changed. Those important changes with regard to philosophy and architecture are outlined, e.g., in ITU-T Recs Y.110 and Y.140.

As a consequence of this "new approach", the telecommunications industry is being reshaped by fundamental changes in ownership, market structure and technological advancement resulting in many new challenges. To cope with this new situation, accommodation of the different, and sometimes divergent, interests of at least three parties (end users, network operators and third party service providers) has to be ensured.

One of the most important requirements is to ensure integrity of the network, the service and the data. While in the past the whole management, including service generation, was done by one party (the network operator), now there is a requirement to open at least parts of the network management to assist service provision e.g., for signalling, reservation of bandwidth, billing and charging, etc. One interest of a service provider may be to get more or less direct access to the network. Without additional measures, this may affect the original (transport) network in such a way that other services and/or data of other users lose their integrity and/or privacy. Furthermore, the original network operator may be affected by a third party in such a way that he is unable to ensure a priority scheme for emergency communications.

Another example may be that a service provider wants to have access to information on terminal capabilities to offer a customized service, or to "modify" the capabilities, behaviour, functionalities

and conditions of a terminal. These requests would disturb the rights of at least the user if they take place without an explicit and individual endorsement by the user. Therefore, it is necessary to have mechanisms in the terminal, the transport network and the service provision which permit the support and respect of the interests and rights of the parties involved.

These scenarios may be taken as an example for the requirements/attributes which could be needed to implement the enterprise model as described in ITU-T Rec. Y.110, and to respond to the requirements of a fully competitive telecommunication market.

This Recommendation considers several (not exhaustive) properties/attributes of RPIs and should assist in developing interfaces which respect the interests of the involved parties as far as possible.

7 Attributes of reference points for interconnection between PTNOs and SPs

NOTE – The content of this clause is based on ETSI Guides [12] to [18].

The mutual relationships between PTNOs and SPs are generally laid down in Service Level Agreements (SLAs). They contain details on the information to be exchanged between the SP and the PTNO and what mechanisms shall be used for this purpose.

7.1 Security aspects

NOTE – Actual and regularly updated information on security-related matters is provided on the ITU Website [B-7].

End users, SPs and PTNOs have a range of different business objectives and requirements regarding the provision of telecommunication services over PTNs. A number of those objectives have been identified. In order to meet them, security aspects need to be carefully considered in a new environment with a multitude of interconnections and access configurations for SPs.

Requirements of end users and other parties involved in the service provision may compete with each other. For example, a user may want to visit websites anonymously, whereas prosecution authorities are interested in tracing the surfer's activities.

Among the general security risks are: anti-user spoofing (illicit masquerading; replay identity attacks; diverting and theft of service, etc.); data integrity (data is exactly what was sent: nothing added, nothing changed, nothing removed), protection against eavesdropping (listening, copying of data), data/service privacy (the parties in the communication can be secure that their communication is, and remains, private), trust of parties used when accessing data/transiting data, non-repudiation (irrefutable evidence that one got the data that was sent, held and generated by a trusted source) and protection against denial of service attacks.

Whilst checksums, authentication and encryption solve some of these issues, non-repudiation and protection against denial of service attacks do not have straightforward service-based solutions. Network and protocols need to be designed to circumvent these problems partially. Other areas of fraud are for the attention of the police (such as refusal to pay, stealing, etc.). Networks will require secure and reliable accounting and traceability to protect against service theft and diversion of the use of resources.

From the viewpoint of the end users, the key requirements are:

– availability of the services;
– correct billing;
– fraud protection;
– confidentiality;
– [sometimes] anonymity; and
– privacy.

From the viewpoint of the SPs and PTNOs, the key requirements are:

– availability of the network, services, and maintenance;
– correct charging;
– capability of tracing individual calls;
– protection of subscriber-related data against intruders; and
– elimination of fraudulent use of the equipment of the PTNOs and SPs.

Security violations may have a significantly negative business impact for both SPs and NOs, e.g., loss of income, reputation and market share.

In particular, network integrity is a key issue when inter-network relationships are established between PTNOs and SPs.

In connection with the SPA, a basic set of facilities may be needed to secure the interfaces between the PTNOs and SPs. A threat analysis of intelligent network-based interconnections is presented in ETSI TR 101 365, and some guidelines on the relevant security measures are given in ETSI TR 101 664.

Screening and mapping functions are used to control and secure bilateral agreements on the interfaces between the PTNs. Today, the PTNOs have screening and mapping facilities on some of the interconnecting NNIs, such as the ISDN user part connections of Signalling System No. 7. These facilities and functions need to be gradually extended to cover all of the interfaces between the PTNOs and SPs.

Further security aspects associated with mobile, Internet and broadband networks include transfer of terminal/personal identity information (e.g., International Mobile Subscriber Identity (IMSI), Electronic Signature, etc.) between the user environment and the service provider, or the support of secure end-to-end transmission between the user terminal and the service provider application (e.g., secure socket layer and ciphering technologies).

7.1.1 Integrity aspects

NOTE – For information about responsibilities for ensuring maintenance of network integrity in an interconnected environment see [B-6].

Network integrity is a question of network management and the ability of the network to maintain certain characteristics with regard to performance and reliability.

Network integrity is a key issue when a network relationship is established between the PTN and the SP. The opening of the PTNO's networks to the SP involves the broadening of access to stored data/information. Data shall be adequately protected by use of passwords and partitioning, so that the integrity and privacy is not compromised.

Network integrity also involves ensuring the integrity of the network elements and providing an acceptable level of service. Vulnerabilities associated with system integrity may result in service denial or disruption, or the unauthorized modification of user or network information and network services.

The evolution of the PTNO's networks needed to support the enhanced services of the SPs creates the need for planning the growth of real-time switch capacity in concert with the emergence of this new access service. In order to cope with this issue, PTNOs and SPs should negotiate traffic engineering aspects to ensure that adequate network capacity is available. If PTNOs and SPs do not adequately plan for increase capacity, the public network will be vulnerable to disruption and denial of service problems.

The following aspects should be considered:

– A gateway function between the PTN and the SP, specially the charging/billing messages and their parameters.

– The protection mechanism in order to ensure that the SPs do not negatively affect the services provided in the PTN.
– The authentication/ciphering mechanisms to protect the PTN from the vulnerabilities due to the SPA.
– On the other hand, in order to maintain network integrity, the following requirements exist:
  • Compatibility measures should ensure that networks and the SPs with different levels of performance work together correctly.
  • Mechanisms to support conformance testing procedures should exist in order to verify PTN and SP interoperability.
  • SPA increases the potential for vulnerabilities associated with feature interaction problems in case there is no sufficient level of expertise to deal with this problem. Feature interaction could disrupt a needed service or be targeted for intentional abuse by computer intruders. Appropriate measures should be implemented to avoid this kind of risk.

The range of services offered by SPs is likely to lead to different interface types used for SPA. These different types of interfaces may require different sets of functionalities within the gateway at the network boundary.

In future implementations, the viewpoints of PTNOs, SPs and users/subscribers/customers have to be taken into consideration.

7.1.2 Authentication aspects

Within the framework of "Who has to authenticate himself against whom" several sub-aspects have to be considered:

– the user versus an SP and/or PTNO (e.g., in case of access);
– the SP versus the PTNO;
– one PTNO versus another (e.g., when packet-based networks are involved, where virtual connections including tunnelling are involved); and
– also SPs (mutually) if they use different levels ("semi-products") of the value-added chain.

Furthermore, there is also kind of a "passed-through authentication" based on priority rights (e.g., in case of emergency communications). In general, the verification process itself and the pass-through mechanism have to be distinguished, i.e., who verifies and how the result can be understood among the partners in the "authentication chain".

Typical means of authentication are PINs and SIM cards or digital signatures (e.g., in the context of mobile communications).

In future implementations, the viewpoints of PTNOs, SPs and users/subscribers/customers should be given particular consideration.

7.1.3 Confidentiality

Confidentiality is an essential requirement in doing business. Safeguarding confidentiality in the case of face-to-face meetings where only the partners directly involved are present, may be relatively simple. This does not, however, necessarily hold true, in the case of a public telecommunication via third parties like PTNOs and SPs (or third party facilities). Several levels of safeguarding confidentiality may be distinguished. With increasing difficulty of guaranteeing confidentiality these are:

Level 1: Contracts are exchanged by letter post or, e.g., by fax. In the first case, the 'secrecy of mails', in the second the 'secrecy of telecommunications' guarantees a certain degree of confidentiality.

Level 2: Contracts are exchanged via Internet (e.g., e-mail).

Level 3: Negotiations on contracts are done via communication networks as well.

If telecommunications are involved, it has to be distinguished whether the networks are public networks or company-networks (closed user groups).

E-commerce is a particularly good example illustrating the importance of confidentiality.

A well-known measure used to guarantee confidentiality is the use of electronic signatures.

7.1.3.1 Public telecommunication network operator's viewpoint

A PTNO may contribute to the maintenance of confidentiality by taking care that authorized persons only can tap communication facilities (see Lawful Interception).

7.1.3.2 Service provider's viewpoint

A typical, maybe even the most important, example of an action where the SP plays a confidentiality relevant role is E-commerce.

7.1.3.3 User's/subscriber's/customer's viewpoint

The u/s/c is interested in absolute confidentiality.

The higher the degree of confidentiality offered to him, the higher the remuneration the u/s/c will be prepared to pay for it.

7.1.4 Fraud protection

Fraud protection is an essential aspect of E-commerce as:

i) there is much at stake; and

ii) many points of possible attack exist.

7.1.4.1 Public telecommunication network operator's viewpoint

A PTNO is interested in receiving an adequate payment if "his" network facilities are used by somebody. Sources of fraud may be u/s/cs, SPs as well as other PTNOs involved in the whole communication process.

7.1.4.2 Service provider's viewpoint

An SP wishes the services he offers to be used only by authorized persons, i.e., by those having a corresponding contract with him.

An SP would like to be paid for every paying service being used.

7.1.4.3 User's/subscriber's/customer's viewpoint

A u/s/c would like to avoid situations where somebody else uses a service at his expense, e.g., by using his identification (PIN).

7.1.5 Lawful interception

Lawful Interception (LI) is not a subject for the ITU insofar as there is no intergovernmental authority to mandate it at the UN level (ITU Charter).

However, the reference points for interconnection and their corresponding interfaces (ITU-T Rec. Y.140) should be designed in such a way that national requirements regarding LI are taken into account and should not prevent (exclude) per se the implementation of related national measures, if they exist.

For economical reasons **SPs** and **PTNOs** do not wish to be forced to put unnecessary effort in possible realizations.

Users do not want to be too affected by necessary LI implementation measures.

A certain guidance on LI requirements and possible LI solutions may by found in the ETSI publications [10] and [9].

7.2 Service interaction aspects

In an environment where an end user subscribes to a range of services from more than one provider, adverse interactions may occur between services and service features. This implies the need for additional functionality to manage the interaction aspects to enable integrated and coherent service delivery.

Further study is needed for service interaction aspects, including the adverse interactions that may occur between the PTNO's and SP's equipment, when more than one of the parties involved in the call handling requires to be able to control the call.

A major example of such service interaction issues is provided by the combination of number portability and service providers access requirements. For instance, several requirements state that an SP-related action may be triggered on the basis of a call with the calling party's Calling Line Identification in a specific numbering range. Due to the service portability mechanisms, the detection of such numbering range is not a guarantee that the call will have to be processed by the SP to which the numbering range was initially allocated.

7.3 Charging/billing aspects

The standard charging mechanisms allow the charging of a successful call, e.g., between the called party's answer and the release of the call. Some requirements from service providers imply the usage of the PTNO's network outside this standard case, and the implementation of a related charging mechanism between the PTNO and the SP is, therefore, necessary in order to cover such a usage. This is the case for instance for the following requirements of SPs:

– requesting the opening of a backward in-band message path to the original calling party immediately upon the arrival of a confirmation of the call set-up, without returning an "answer" signal;
– conveying an indication of an unsuccessful call from the terminating PTN, i.e., either when an indication other than "ringing" is returned to the calling party, or when a "no reply" situation occurs;
– providing call destination and routing information for controlling the destination and routing of the call;
– interacting with the service user before any service charging begins;
– sending data to and receiving data from the service user's NTP without an alert signal, such as a ringing.
– call charging and billing aspects, as seen from the PTNO's perspective, are considered in ETSI EG 201 807.

In the case where end-user charging is suspended, delayed, altered or is different in other ways from standard call charging mechanisms, the appropriate event has to be created for possible logging e.g., thus providing the necessary data for appropriate accounting between the SP and PTNO.

For example, demand is emerging in the market place for:

– subscription-based billing for Internet access;
– included minutes in pre-pay subscription for fixed and mobile service; and
– pay-per-use without having a subscription.

All these cases require real-time accounting (hot billing) over a secure data interface.

National and European legislation and regulations, where appropriate, need to be taken into account when charging mechanisms are designed and implemented, e.g., to provide advice of charge to a service user.

7.3.1 Public telecommunication network operator's viewpoint

– Signalling tools for billing and (real-time) charging, advanced traffic information signals;

– Transmission of (real-time) charging information over the networks;

– Networks and service providers require tracing of real-time billing information and non-repudiation that the bill was received, that it was correct, with data integrity that is exact and unaltered;

– Special attention has to be paid to the precision of the network clock itself and to the accuracy of its transmission, in particular if more than one PTN is involved.

7.3.2 Service provider's viewpoint

– Generation and submission of (real-time) charging information for the customer.

7.3.3 User's viewpoint

– Receipt of (real-time) charging/billing information.

– The users/subscribers require traceability of what they are to be billed for and that the service was in fact used at the time claimed (service ticketing, advice of charge, billing itemization are potential solutions).

– Aspects of particular importance for the user are the accuracy of the bill and a reasonable "quantization" of the intervals on which billing is based (the narrower they are, the better).

7.4 Service availability

Service availability is an issue of policy, user-to-service provider, and service provider-to-network operator, and what they agree to in the service offer.

One relevant key item here is "preference scheme".

7.5 Access to a network address

NOTE – Though not shown in Figure 1 the relationships between different players imply naming and addressing aspects. These aspects may or may not fall under the jurisdiction of a regulatory authority.

Typical applications where an SP may need access to a network address are directory services, online inquiries, forwarding services, etc.

The access to networks, network services and applications requires that adequate numbers and numbering ranges are provided for all publicly available electronic communication services and that these can be assigned in an objective, transparent and non-discriminatory manner.

7.6 Management aspects

Figure 2 illustrates a reference architecture showing the RPIs between SPs and PTNOs. It may be used to determine both parties' requirements with regard to the exchange of management information via the interfaces corresponding to the RPIs.

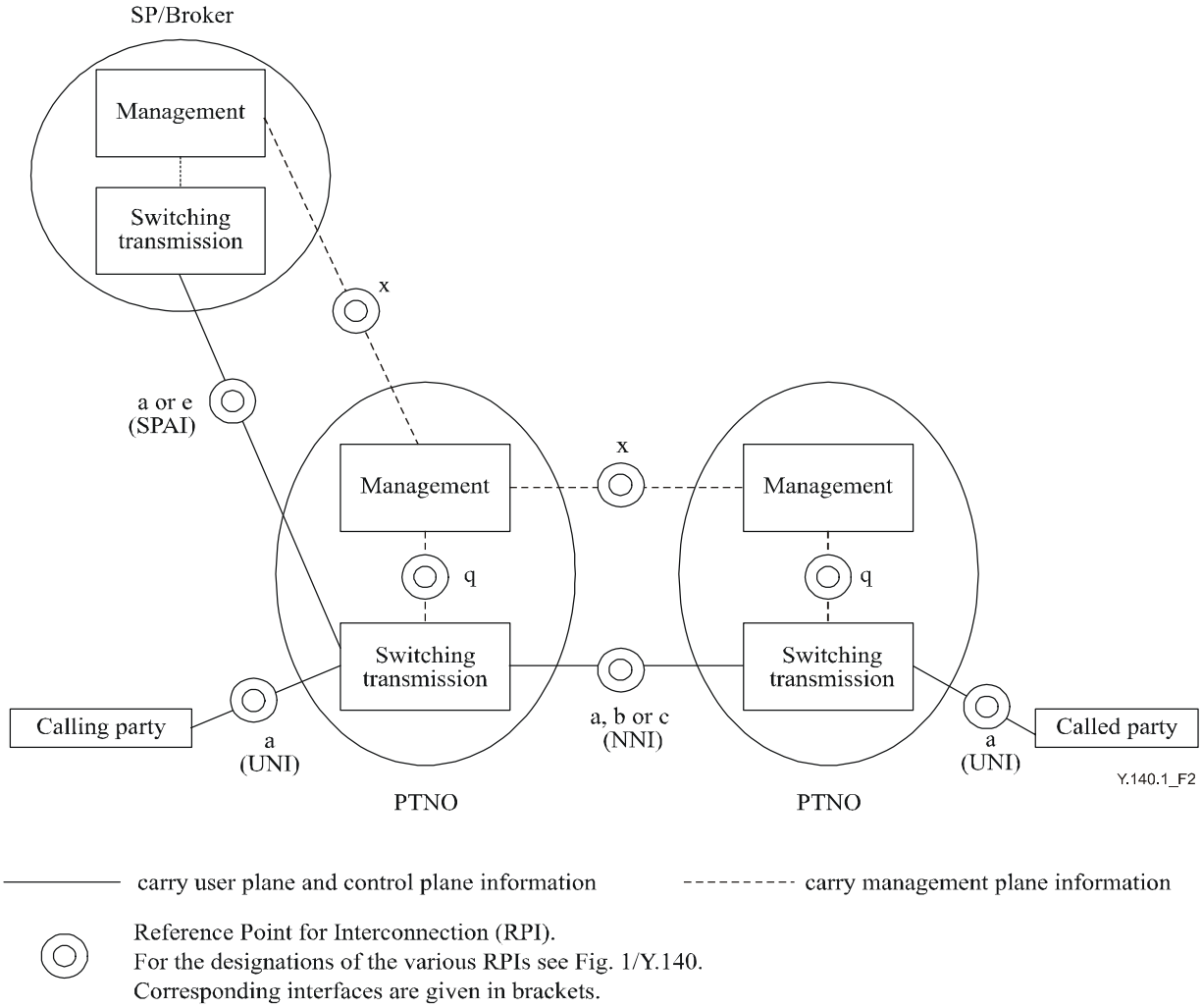

Figure 2/Y.140.1 – Reference architecture for SP-PTNO management requirements

A detailed analysis of the situation can be found in [18]. It deals with the management plane interface between the service provider equipment and the public telecommunication network operator equipment. Each requirement is based on the SPAR studies as published in [12] to [15]. [18] identifies whether each SPAR has a management implication. To fulfil these management requirements, appropriate protocols will be required, based on the information flows described in [18]. Where appropriate protocols are not available, either existing protocols will have to be enhanced or new protocols developed.

The management requirements covered in [18] can be split into:

– Traffic-related capabilities (e.g., setting switch triggers, datafill, etc.) necessary in order to fulfil, from an operational perspective, one or more of the Service Provider Access Requirements (SPAR).

– Performance management capabilities, e.g., monitoring performance of SP/PTN links, link reconfiguration, etc.

– Electronic bonding/ordering.

8 Requirements and their priorities at RPIs

Table 1/Y.140.1 – Priority of requirements at RPIs

Attributes	Viewpoint of			Remarks
	Public telecomm. network operator	Service provider	Customer subscriber end-user	
Service availability		High	High	
Correct billing	High	High		
Correct charging			High	
Network integrity	High			
Service integrity		High		
Access to a network address				
Management related requir.	High	High		

NOTE – The content of this table is not exhaustive, it is open for revision.

BIBLIOGRAPHY

[B-1] ITU Secretariat Publication, *Trends in telecommunication reform 2000-2001 – Interconnection and Regulation*.

[B-2] WTO Telecommunications Services Reference Paper (24 April 1996) http://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

[B-3] APEC Principles of interconnection (Annex 3 to [B-1]).

[B-4] CITEL Guidelines and practices for interconnection regulation (Annex 4 to [B-1]).

[B-5] Directive 97/33/EC "Interconnection in Telecommunications with regard to ensuring universal service and interoperability through application of the principles of Open Network Provision (ONP)" of the European Parliament and of the Council of 30 June 1997.

[B-6] CEPT/ECTRA Recommendation (98)01, *Set of Guidelines on Responsibilities for ensuring maintenance of Network Integrity (NI) in an interconnected environment*.

[B-7] http://www.itu.int/osg/spu/ni/security/links/news.html and http://www.itu.int/osg/spu/ni/security/links/misc.html.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	**Global information infrastructure, Internet protocol aspects and Next Generation Networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2004