TR 101 307 V2.2.2 (1999-03)

Technical Report

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements for service interoperability; Phase 2

Reference

DTR/TIPHON-01002 (c3o010pg.PDF)

Keywords

internet, network, protocol, telephony,

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet

secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

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 SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

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 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 Report (TR) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

Introduction

The objective of ETSI Project TIPHON is the specification of interoperability mechanisms and related parameters to enable multimedia communications to take place, to a defined quality of service, between switched circuit networks (SCN) and Internet Protocol (IP) based networks and their associated terminal equipment. The basis of the TIPHON work is the H.323 protocol suite [2] developed by ITU-T SG16. The requirements do not imply any changes in SCN.

The TIPHON environment has been divided into 4 interrelated scenarios as described in TR 101 300 [15].

The present document defines the initial requirements for scenario 1 and 2.

Scenario 1 is limited to real time voice communication between IP based terminals and terminals attached to the SCN, in which the call set-up is originated by the IP terminal user.

Scenario 2 covers real time voice communication between terminals attached to the SCN and IP based terminals in which the call is originated from a telephone connected to the SCN.

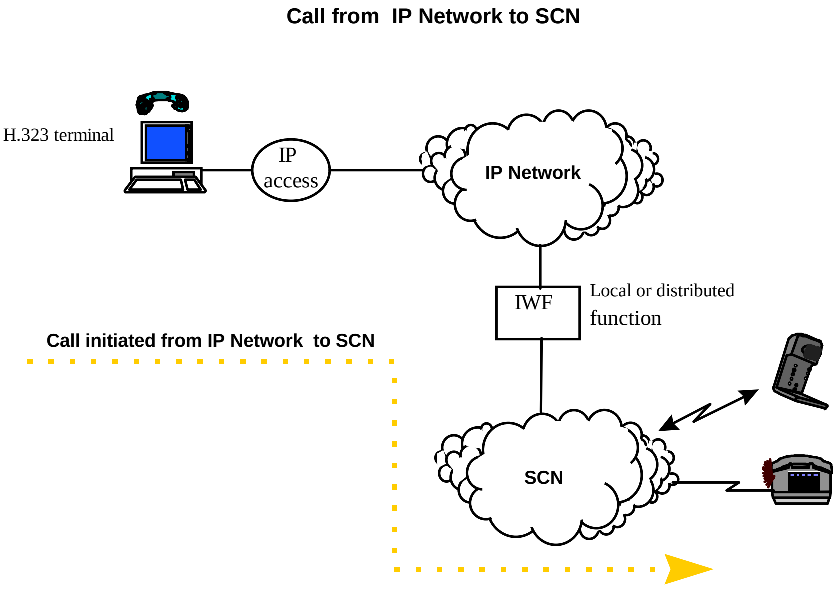
Other types of real time multimedia communication such as video, facsimile and data, conferencing and messaging services are not included. These are for further study.

It is recognized that the present document will require further amendment and extension to take account of further work and experience of scenario 1. It is intended that there will be further revisions of the present document.

1 Scope

The present document defines the scope, and mandatory requirements and optional requirements for the interworking function (IWF) to ensure service interoperability for TIPHON phase 2 systems (see clauses 6 to 10). This phase comprises the two scenarios described in the introduction.

Scenario 1 is limited to real time voice communication between IP based terminals and terminals attached to the circuit switched network (SCN), in which the call set-up is originated by the IP terminal user. This is illustrated in figure 1.


Call from IP Network to SCN
H.323 terminal
IP access
IP Network
IWF
Local or distributed function
Call initiated from IP Network to SCN
SCN

IWF: InterWorking Function

Figure 1: Definition of scenario 1

Scenario 2 covers real time voice communication between terminals attached to the SCN and IP based terminals in which the call is originated from a telephone connected to the SCN. This is illustrated in figure 2.

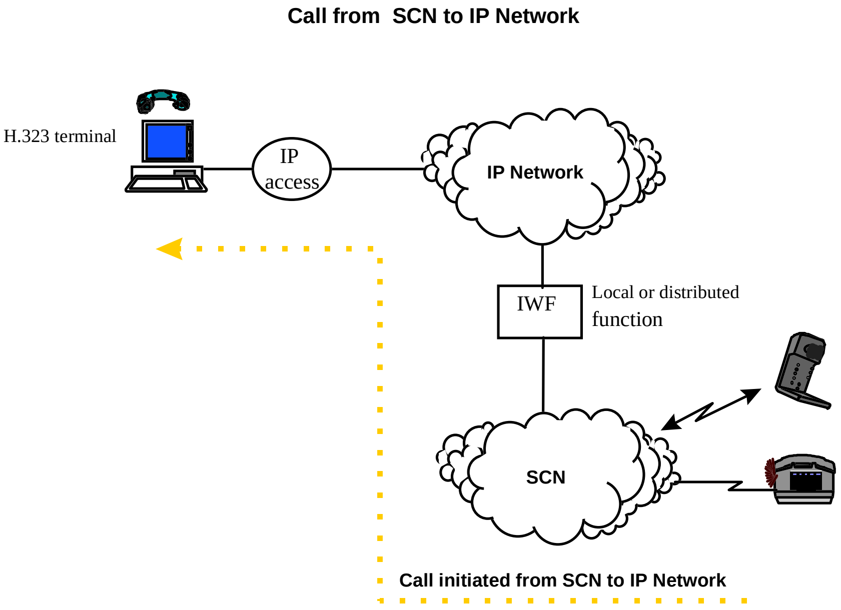

Call from SCN to IP Network
H.323 terminal
IP access
IP Network
IWF
Local or distributed function
SCN
Call initiated from SCN to IP Network

Figure 2: Definition of scenario 2

End-to-end video, fax and data transmission; voice, data and video conferencing; and messaging services are outside of the scope of the current version of the present document.

Where a requirement is optional or marked for further study in this release of the present document, this does not preclude the possibility that such a requirement may become mandatory in a future version of the present document.

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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ITU-T Recommendation E.164 (1997): "The international public telecommunication numbering plan".

[2] ITU-T Recommendation H.323 (1998): "Packet based multimedia communications systems".

[3] ITU-T Recommendation H.235 (1998): "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals".

[4] IETF RFC-791 (1981): "Internet Protocol".

[5] ITU-T Recommendation H.225.0 (1996): "Media stream packetization and synchronization on non-guaranteed quality of service LANs".

[6] ITU-T Recommendation H.245 (1998): "Control protocol for multimedia communication".

[7] ITU-T Recommendation H.246 (1998): "Interworking of H-Series of multimedia terminals with H-Series multimedia terminals and voice/voiceband terminals on GSTN and ISDN".

[8] IETF RFC-1884 (1995): "IP Version 6 Addressing Architecture".

[9] ISO/IEC 11571: "Information technology - Telecommunications and information exchange between systems - Numbering and sub-addressing in private integrated services networks".

[10] ETS 300 189: "Private Telecommunication Network (PTN); Addressing".

[11] Void.

[12] Telecommunications Information Networking Architecture Consortium, TINA-C deliverable: "Overall Concepts and Principles of TINA Version 1.0 (1995)".

[13] Telecommunications Information Networking Architecture - Consortium, TINA-C deliverable: "Business Model and Reference Points Version 4.0 (1997)".

[14] Void.

[15] TR 101 300: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of technical issues".

3 Definitions and abbreviations

3.1 Definitions

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

accounting: the process of collecting the call information data for purposes of attributing costs between service providers or network operators.

authentication: the process of proving identity within its context. This normally entails proving the possession of a secret (uniquely associated with the identification) to the authenticator.

authorization: the process of granting permission on the basis of identity, to access or use a service, or to access information. Authorization is performed by the entity that controls the resource, and, if payment is required, that same entity is responsible for accounting to the customer or other party.

backward call clearing: an ability for the called party to release a call during the call.

basic call: see the definition for call.

billing: the process of presenting the user with a request for payment e.g. based on network usage; possibly including supporting information such as call records.

call: point-to-point communication between two endpoints. The call begins with the call set-up procedure and ends with the call termination procedure. A call may be directly between two endpoints, or may include other H.323 entities such as a gatekeeper or Multipoint Control Unit (MCU). Typically, a call is between two users for the purpose of communication, but may include signalling-only calls. An endpoint may be capable of supporting multiple simultaneous calls.

charging: the process of determining the amount of money a user shall pay for usage of a certain service.

collect call: call paid for by the called party. Caller indicates a request for a collect call and the service provider asks the called party to accept.

credit card call: calls charged to a credit card user.

E.164 number: the international telephone number (as defined in ITU-T Recommendation E.164 [1]) composed of a variable length of decimal digits arranged in specific code fields as following:

Country Code + National Destination Number + Subscriber Number

eavesdropper: an unauthorized listening only participant in a communications channel.

firewall: a device (computer or software or both), used to restrict and monitor usage of computer(s) or the network.

forward call clearing: an ability for the calling party to release a call during the call.

free phone: a call which may be initiated for which the call originator is not charged, also known as a toll free call.

gatekeeper (GK): the gatekeeper is an H.323 entity on the network which provides address translation and controls access to the network for H.323 terminals, Gateways, and MCUs. The Gatekeeper may also provide other services to the terminals, Gateways, and MCUs such as bandwidth management and Gateway location.

gateway (GW): for the purposes of the present document, a gateway is understood to mean an H.323 gateway, as defined below.

H.323 gateway: an H.323 GW is an endpoint on a network which provides for real-time, two-way communications between H.323 Terminals on an IP based network and other terminals on a switched circuit network.

identification: an entity has identification within a specific context, and may therefore possess multiple identities; one for each context in which it has to be known. All identities within a particular context has to be unique. An Identification may consist of a simple string, or a name within a directory mechanism.

identity: information which uniquely identifies the user. Network operators require proof of identity for billing. Users require proof of identity before discussing sensitive information. Applications (e.g. audio response units) require proof of identity before allowing information to be accessed.

IP address: each network unit connected to an IP network needs to have a unique Internet or IP address. Today's IP addresses is based on IPv4 and are 32-bit numbers with its predefined structure. The IP address (IPv4) is written as four decimal numbers separated by a point.

IP endpoint: a device that originates or terminates the IP based part of a call. Endpoints include H.323 clients, and IP telephony gateways.

IP service provider: a company or organization which provides access to IP services which could be either access to a private IP network (Intranet) or to the Internet.

IPv4: the existing standard for IP, which uses a 32-bit address field.

IPv6 (or IPng): the next generation of IP, which uses a 128-bit address field.

Malicious Call IDentification (MCID): MCID is a supplementary service offered to the called party which enables the called party to request that the calling party be identified to the network and be registered in the network.

network operator: an organization which operates a telecommunications network.

non-repudiation: a security function that provides proof of the origination of information and serves as a deterrent to the originating party falsely denying the information.

premium rate call: calls made to access particular information, or services, for which an additional charge is made. The service provider charges the caller for the used services according to predefined rate.

privacy: the characteristic that only authorized entities are capable of access; e.g. eavesdropping is prevented.

Switched Circuit Network (SCN): a public or private switched telecommunications Network such as PSTN, N-ISDN, GSM or PISN. B-ISDN is not strictly a switched circuit, it exhibits some of the characteristics of a SCN through the use of virtual circuits.

Private Integrated services Network eXchange (PINX): a PISN nodal entity that provides automatic switching and call handling functions used for the provision of telecommunication services.

Private Integrated Services Network (PISN): a network serving a pre-determined set of users (different from a public network which provides services to the general public). The attribute "private" does not indicate any aspects of ownership.

3.2 Abbreviations

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

AD	Administrative Domain
AN	Access Network
C	Conditional
CHSP	Clearing House Service Provider
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CPE	Customer Premises Equipment
DTMF	Dual Tone Multiple Frequency
FFS	For Further Study
GK	GateKeeper
GSM	Global System for Mobile communications
GU	Global User service
GT	Global Transit service
GW	GateWay
ICP	InterConnectivity Provider
IETF	Internet Engineering Task Force
IN	Intelligent Network

IPAP	IP Access Provider
IPEU	IP End User
IPNP	IP Network Provider
ISDN	Integrated Services Digital Network
ITP	IP Telephony Provider
IWF	InterWorking Function
M	Mandatory
MCID	Malicious Call Identification
MCU	Multipoint Control Unit
NNI	Network Network Interface
NT	National Transit service
NU	National User Service
O	Optional
OAM&P	Operations, Administration, Maintenance, and Provisioning
PINX	Private ISDN eXchange
PISN	Private Integrated Services Network
PSTN	Public Switched Telephone Network
PU	Private User service
QoS	Quality of service
RFC	Request For Comments
ROA	Recognised Operating Agencies
SCEU	SCN End User
SCN	Switched Circuit Network
SCNP	SCN Network Provider
SDR	Service Detailed Records
TE	Terminal Equipment
UNI	User Network Interface

4 Assumptions

User services are defined independent of the version of the IP (e.g. IPv4, see IETF RFC-791 [4] and IPv6, see IETF RFC-1884 [8]).

Switched Circuit Networks (SCN) may be public networks (e.g. Public Switched Telephone Networks (PSTN), Integrated Services Digital Networks (ISDN), Global System for Mobile communications (GSM) networks) or Private Integrated Services Networks (PISN).

IP networks may be private or public IP networks.

The TIPHON architecture is defined with scaleability in mind. This means that the definition of functional entities and protocols is suitable for large systems, while smaller systems can be provided via a suitable combination of functional entities in physical entities.

In the definition of functional entities use outside of the TIPHON context is considered where applicable.

The focus of TIPHON is on voice communication. Upward-compatibility towards the support of multimedia is considered where applicable.

5 Extending the existing telephony service to IP network technology

5.1 The existing telephony service

The existing telephone service is based on the Switched Circuit Network (SCN), which consists of Customer Premises Equipment (CPE), Access Network (AN) and the Core Network.

The CPE may be single subscriber stations or one or more private integrated services network exchange (PINX), building private networks. The CPE is connected via the AN to the core network via a User-Network-Interface (UNI).

The core network consists of many networks operated by Administrations or so-called Recognized Operating Agencies (ROA). These networks are interconnected via Network-Network-Interfaces (NNI). Networks with CPE connected to them are called local networks or mobile networks, networks connecting local networks are called transit networks.

The entity using the telephone service is named user, subscriber or party. The entity setting up the connection or call is named originating or calling party (A-subscriber), the other side is named terminating or called party (B-subscriber). The network, where the calling party is connected to is the originating network, the network, where the called party is connected to, is the terminating network.

In public SCNs the terminating party is uniquely defined by the international E.164 number of the called party. In principle each subscriber connected to a public telephone network can be reached by any other subscriber via the international telephone service by dialling the E.164 number. The transit network(s) is (are) selected either be default or by carrier selection methods.

In private SCNs numbering schemes according to ISO/IEC 11571 [9] or ETS 300 189 [10] can be used. In principle each user connected to a private SCN can be reached by any other user in the private SCN by dialling a number in the private network numbering plan.

To interwork with the international telephone service in a consistent manner, a TIPHON compliant system needs to fulfil a basic set of requirements and provisions.. These can be summarized in two ways:

- from the point of the SCN operators on one hand the interworking must be very similar or equivalent with the interworking with other SCN;
- from the subscribers or users point of view, at least from the SCN-side, the service should look and feel like an extension of the existing service to the IP-network.

Before the requirements and provisions for inter-working can be defined, some definitions for the IP-side are necessary.

5.2 Business roles

It is intended that the following business roles can be supported by the TIPHON specifications. However, not every role listed below need to be present in all deployments or implementations.

a) IP end user;
A user who is connected to an IP network.

b) IP access provider;
A company or organization which provides access to IP services which could be either access to a private IP network (Intranet) or to the Internet.

c) IP network provider;
A company or organization which provides access to an IP network.

d) IP telephony service provider;
A company or organization which offers telephony services over IP networks.

e) interconnectivity provider;
A company or organization which offers services for interconnectivity between the telephony service on IP networks and Switched Circuit Networks.

f) SCN network provider;
A company providing a Switched Circuit Core Network.

g) SCN access provider;
A company providing a Switched Circuit Access Network.

h) SCN end user;
An end user who is connected to an Switched Circuit Network.

i) directory service provider;
A provider of directory information e.g. providing an E.164 number from an email address.

j) value added service provider;
Service provider which provides services beyond normal or traditional telephony services.

k) broker
Provider of a business service to facilitate the interworking between multiple IP service providers and SCN operators involved in the delivery of a telephony service. This includes accounting settlements.

Annex A gives further information about some of these business roles, and gives examples of different possible relationships between them.

An IP telephony administrative domain (containing possible combinations of business roles b, c, d, e) could provide different types of services, for which different sets of requirements apply:

- Global User Service – Type GU,
provides originating and terminating services for users with an E.164 Global Code number, which requires access to a Global IP-Telephony Directory Service.

- Global Transit Service – Type GT,
provides connectivity to any E.164 Global Code number user (when e.g. dialled from the SCN), which requires access to a Global IP-Telephony Directory Service.

- National User Service – Type NU,
provides originating and terminating services for users with an E.164 national numbers, with either geographic (home-related) or non-geographic (country based, with e.g. an IP specific prefix) scheme, depending on national regulations or customer demand.

- National Transit Service – Type NT,
provides transit and long distance carrier services (national and international), either between SCN's, between IP-based networks, or between a SCN and an IP-based network.

- Private User Service – Type PU,
provides originating and terminating services for users within its network.

A real IP administrative domain may provide one or more of these services.

To operate as an IP-Telephony provider, different kinds of agreements are necessary:

- agreements between Users and Providers (Terms of Subscription);

- agreements between Providers (Interconnect Agreements).

These agreements can be bilateral, but can also rely on the involvement of a Broker.

5.3 Types of Interconnections

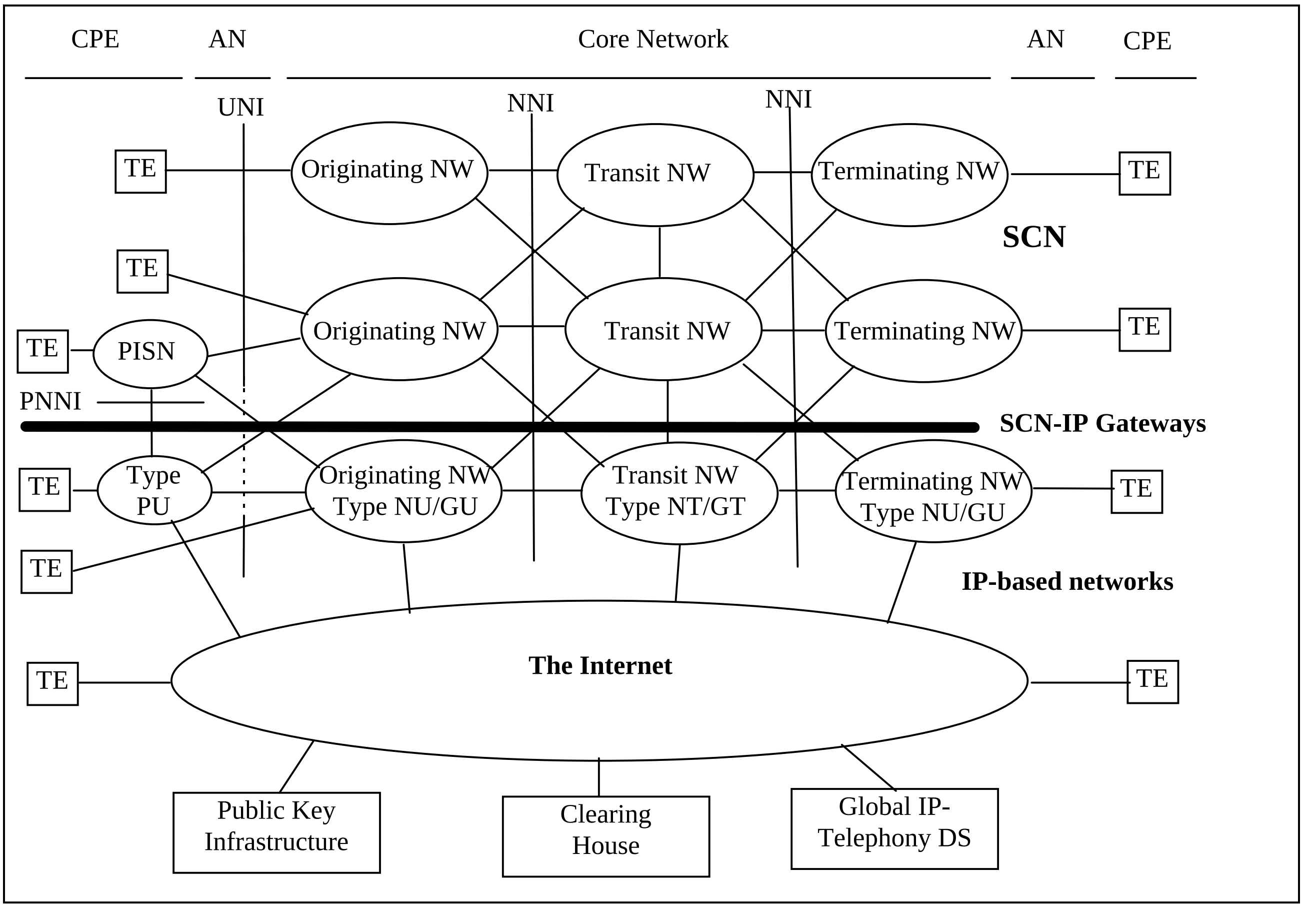
IP-Telephony administrative domains (AD's) must be able to inter-work with the SCN and with each other in different ways. Between administrative domains, whether using SCNs or IP networks, in principle three types of inter-working interfaces at protocol level are required:

- a Network-Network-Interface (NNI) between "public" networks;

- a User-Network-Interface (UNI) connecting single users and "private" networks to "public" networks (see note under figure 3);

- a Private Network-Network-Interface (Private NNI) between "private" networks, or entities within the same corporate network.

Figure 3 shows all types of AD's on the SCN and the IP network, and all possible types of interconnection:



NOTE 1: Not all possible connections are indicated in order not to overload the picture. However, Figure 4 contains all possible interfaces.

NOTE 2: The interfaces between PU Type and NU/GU Type IP-based networks, and between Private SCNs (PISN) and Type NU/GU IP-based networks are depicted as UNI in the figure. However, depending on implementation or interconnect agreements, the interface can be an NNI. In either case some aspects of the protocol, e.g. with respect to CLI number verification, may operate asymmetrically.

Figure 3: Types of interconnections

Figure 4 gives an overview of the different interworking and related interfaces between administrative domains that eventually will have to be covered.

		SCN			IP-based		
		Private SCN	Local SCN	Transit SCN	PU	NU/GU	NT/GT
SCN	Private SCN	PNNI	UNI	-	PNNI	UNI GW (note Fig.3)	-
	Local SCN	UNI	NNI	NNI	UNI GW	NNI GW	NNI GW
	Transit SCN	-	NNI	NNI	-	NNI GW	NNI GW
IP-based	PU	PNNI GW	UNI GW	-	PNNI* (+IP-GW)	UNI* (+IP-GW) (note Fig.3)	-
	NU/GU	UNI GW (note Fig.3)	NNI GW	NNI GW	UNI* (+IP-GW) (note Fig.3)	NNI* (+IP-GW)	NNI* (+IP-GW)
	NT/GT	-	NNI +GW	NNI +GW	-	NNI* (+IP-GW)	NNI* (+IP-GW)

Figure 4: Overview of the different interworking classes and related interfaces

In grey shading (with black text) are the interfaces presently specified. Between IP based networks (all interfaces with an *), in principle the same types of inter-working and interfaces apply. Also between IP network a gateway function might be needed, this is indicated by the (+IP-GW) entry in the table. The interfaces in addition to the already defined interfaces relevant within the context of TIPHON phase 2 have been given a grey shading with white text.

6 Services provided by a TIPHON compliant system

Major issues concerning the interoperability of IP telephony terminals are addressed within the ITU-T Recommendation H.323 [2], which is the basis of the TIPHON work. It is within the scope of the ETSI Project TIPHON to profile H.323 in order to ensure interworking between TIPHON compliant endpoints or terminals, including TIPHON compliant gatekeepers where applicable, and terminals connected to the SCNs. To accomplish this, the requirements expressed in ITU-T Recommendation H.323 [2] and supporting ITU-T Recommendations H.225.0 [5], H.245 [6], and H.246 [7] were reviewed. This review helped in the definition of the requirements listed in the present document.

In the rest of the present document requirements are presented in table format. The ID is a unique tag to refer to a requirement, its numerical value has no further meaning. In the "Req.Type" column it is indicated whether the requirement is optional or mandatory. The "Scen/ServType" column indicates for which of the TIPHON scenarios as described in clause 1 the requirements is applicable, and for which of the ServiceTypes defined in subclause 5.2. Default for the last column is applicable for all scenario and service types.

6.1 Basic services

ID	Requirement Description	Type	Scen./ Serv. Type
5	It shall be possible to setup calls from a TIPHON compliant H.323 client on an IP network to a terminal attached to a SCN.	M	Sc. 1
57	It shall be possible to setup calls from a terminal attached to a SCN to a TIPHON compliant H.323 client on an IP network.	M	Sc. 2
6	Backward call clearing shall be possible.	M	
7	Forward call clearing shall be possible.	M	
8	It shall be possible for the gatekeeper to clear a call.	O	
9	The detection of a non-recoverable failure of any of the critical resources (e.g. terminal, gateway, gatekeeper) involved in the call shall initiate the clearing of the call. The entity detecting the failure should initiate the clearing of the call.	ffs	
10	User services which make use of end-to-end bi-directional and unidirectional DTMF signalling shall be supported. e.g. voice mail applications, conference bridge applications, banking applications, controlling answering machine etc. Different application may apply in different scenarios.	M	
11	The calling party shall be informed of the state of the call e.g. by busy tone, alerting tone, congestion tone, etc.	M	
12	Inband audio tones and announcements to be received by the calling party before call setup into the public SCN shall be supported (e.g. special information tones, referral messages, etc).	C	Sc 1

6.2 Supplementary services/features

In order to allow early usage of TIPHON interoperability specifications, only requirements related to an initial set of supplementary services and features from an end-user perspective are defined in the present document.

ID	Requirement Description	Type	Scen./ Serv. Type
14	It shall be possible to provide the calling party or the party paying for the call with the ability to select intermediate carriers.		
58	The TIPHON architecture shall support the transport of identity information for use by e.g. calling line identification presentation and restriction services. At the interface between the IP domain and the public SCN, numbers shall be as defined in ITU-T Recommendation E.164 [1]; At the interface between a private IP domain to a private SCN within the same corporate network, numbers shall be in accordance with ISO/IEC 11571 [9] or ETS 300 189 [10].	M	
59	The TIPHON architecture shall support the transport of the calling line identification restriction information.	M	
60	It shall be possible for the calling party to provide a presentation number for use by the network in providing ID services.	M	
61	Malicious call tracing (MCID) for calls initiated from a IP based terminal shall be supported.	?	Sc 1

6.3 Quality of Service

ID	Requirement Description	Type	Scen./ Serv. Type
2	A TIPHON compliant system shall be capable of supporting one or more of the levels of Quality of Service (QoS) as defined by TIPHON.	M	
13	The calling party shall be able to select a level of QoS if more than one is available. This selection may be done per call or by subscription.	M	Sc 1,3

6.4 Mobility

NOTE: This subclause has not yet been completed, and protocol work will not be included in the TIPHON phase 2 deliverables. However, the requirements identified so far have been retained in this version of present document, in order to stimulate discussions by providing wider visibility to the present state of thinking on this subject within the TIPHON group.

Mobility in the TIPHON context is the possibility for a user (visitor) to connect to (register with) the gatekeeper of a foreign administrative domain. The foreign domain is also called the visited domain, the foreign gatekeeper is also called visited gatekeeper.

Only domains providing a user service may be home and visited domains. The user connecting to a visited domain must have a valid subscription in one administrative domain (the home administrative domain). Furthermore, the visited AD should allow the subscriber of the home AD to use resources in its domain. This is covered by a so-called "roaming agreement" between the home AD and the visited AD. These agreements can be bilateral, or can be done via a clearing house construction.

To recognize the home AD of a visitor, the identification of the home AD should be either contained intrinsic in the identification of the user or transferred additionally during the login procedure.

ID	Requirement Description	Type	Scen./ Serv. Type
48	Home Domain Identification A visited IP telephony provider shall have the possibility to identify the roaming users home domain or clearing house domain.	C (see note)	Sc 1 GU NU
49	User Identification A visited IP telephony provider shall have the possibility to identify the roaming user.	C (see note)	Sc1 GU NU
50	Visited Gatekeeper Discovery There shall be means for an IP terminal connected to the network on an arbitrary area, to locate a point of presence (Gatekeeper) of an IP telephony provider that can provide roaming services in that area.	C (see note)	Sc 1 GU NU
51	User Authentication There shall be means for the visited domain to securely authenticate the roaming user. Since the user's security profile may not reside in the visited domain, this may involve communication with the home domain. The authentication scheme shall be consistent with the H.235 and the TIPHON adopted security profiles.	C (see note)	Sc 1 GU NU
52	Authorization There shall be means for the visited domain to obtain authorization information from the home network. The authorization information needs to be standardized for interoperability. Authorization information may contain information concerning: - roaming services (reception of calls); - services in the visited network. Authorization for services could be required on a per call basis, or per registration session. The visited network might restrict the services provided, based on its own policies.	C (see note)	
53	Originating calls If authorized, it shall be possible for the roaming user to place IP originating call.	C (see note)	
54	Terminating calls If the roaming user is authorized, it shall be possible for a roaming user to receive calls from users in the IP network or SCN.	C (see note)	
55	Real time credit maintenance It shall be possible for a home network to keep a subscriber specific credit real-time up to date. If the credit is consumed, it shall be possible to terminate the ongoing call. It shall be possible for the home network to indicate (directly or indirectly) to the visited network that real time credit maintenance is required.	O	
56	Support for Virtual Home Environment It shall be possible for a ITSP or a VASP to offer provider specific services to their subscribers, also when they are roaming.	O	
NOTE: Conditional in the sense that support for mobility is optional, but if it is supported, the requirements listed here are mandatory.			

7 Addressing/Routing

ID	Requirement Description	Type	Scen./ Serv. Type
16	For applications involving public networks, it shall be possible for a call initiator in an IP network to use an E.164 number to identify and call a user of a SCN. This is independent of whether the number has been ported, and whether it refers to a terminal or a user. NOTE 1: It is assumed that if another naming scheme is used by the calling party, some type of database will be consulted to map the name to an E.164 number.	C	Sc 1
62	For applications within a private network context, it shall be possible for a call initiator in a private IP network to use the number of an SCN user in the private numbering plan (see [9] and [10]) to identify and call the called party. This is independent of the fact whether it refers to a terminal or user. NOTE 2: It is assumed that if another naming scheme is used by the calling party, some type of database will be consulted to map the name to a private numbering plan number.	C	Sc 1
17	Users who are connected to the IP network shall be able to use a terminal which has either a permanently or dynamically assigned IP address.		
18	For applications involving public networks it shall be possible for a call initiator in a SCN to use anE.164 number to identify and call an IP end user. This is independent of whether the number has been ported, and whether it refers to a terminal or a user. IP end users in the public domain will therefore have an E.164 alias. IP end users in a private domain might also have an E.164 alias, alternatively the dialled number might be a private numbering plan alias plus a prefix.	C	Sc 2
63	For applications within a private network context, it shall be possible for a call initiator in a PISN to use the number of the private numbering plan (see [9] and [10]) to identify and call an IP end user in a private IP network. This is independent of the fact whether it refers to a terminal or user.	C	Sc 2, PU
57	Service Provider Portability It shall be possible for a subscriber to switch ITSP without having to change his directory name or number.		NU GU

8 Security

This clause describes general security requirements for TIPHON services.

The requirements defined in this Section apply only if required by the business role.

Security is necessary to:

1) protect the network operator from abuse of the network (e.g. abuse of services/bandwidth);

2) protect the network operator from failures of the network caused by misbehaving terminals and network elements, accidental or on purpose;

3) protect the service user (subscriber) from theft.

Five protection services are relevant in the context of security:

- authentication;
- authorization;
- non-repudiation;
- privacy;
- integrity.

These services are worked out in more detail in the following subclauses. Each of the protection mechanisms may or may not be used for TIPHON calls. This may be decided on a per business deployment, and if needed, depending on the business role, it shall be possible to have it per subscription, or on a per call basis. See subclause 8.6 on security profiles. Therefore, all requirements in this clause are conditional, in the sense that they are mandatory depending on the supported security profile.

Basic requirements regarding security is in any case the following:

ID	Requirement Description	Type	Scen./ Serv. Type
19	TIPHON compliant systems shall use the security mechanisms as defined by ITU T Recommendation H.235	C	
1	Between business roles within the IP domain the use of a border element within a TIPHON compliant environment shall be possible. The functions of this border element can among other things be security, address translation and flow control.	O	

8.1 Authentication

ID	Requirement Description	Type	Scen./ Serv. Type
20	Authentication shall be supported. Both parties to a communication may require assurance of each other's identity. This may be between two systems across an untrusted communications link or end to end (user to user).	C	

8.2 Authorization

ID	Requirement Description	Type	Scen./ Serv. Type
21	Authorization of calls or resource usage shall be supported. Operators may require authorization of terminals to use facilities (for instance gateways). Several parties may be involved in such an authorization. For instance a terminal and/or IP enduser, a home operator (providing local services to the IP end user) and a remote operator (owning a gateway).	C	

8.3 Non-repudiation

ID	Requirement Description	Type	Scen./ Serv. Type
22	Non-repudiation should be supported. In other words, systems complying with this requirement shall be able to provide proof of use	C	

8.4 Privacy

Communication between TIPHON compliant products is likely to include confidential or proprietary information.

ID	Requirement Description	Type	Scen./ Serv. Type
23	TIPHON compliant systems shall have a mechanism for ensuring that eavesdropping on an IP link or on multiple IP links shall not result in the interception of the conversation.	C	
24	TIPHON compliant systems shall have a mechanism for ensuring that eavesdropping on an IP link or on multiple IP links shall not result in the determination of the identity and/or of the telephone number of one of the parties involved in the conversation.	C	

These statements imply the use of some kind of message encryption. Because encryption is a politically sensitive issue, two further requirements are derived from this:

ID	Requirement Description	Type	Scen./ Serv. Type
25	To allow commercial deployment in all countries, TIPHON shall support multiple encryption algorithms.	C	

8.5 Integrity

When there is a part of the network which might be physically accessible by unauthorized entities, there is the possibility that information may be altered on route from sender to receiver without authorization. Integrity is the provisioning of guarantees that information is received exactly as it was sent.

ID	Requirement Description	Type	Scen./ Serv. Type
27	TIPHON systems shall have a mechanism for ensuring integrity of signalling information and media information	C	

8.6 Security Profiles

Different deployments have different security requirements. For example, different levels of security may be required, and there are also varying penalties to be paid for the various security profiles. Also, there may be constraints to use a particular pre-existing security infrastructure.

Therefore, there shall be several different TIPHON security profiles that TIPHON systems can use. Each TIPHON security profile will fulfil a particular set of security requirements.

A TIPHON security profile shall contain the following elements:

1) a thorough discussion of the environment, application, or situation in which the profile can usefully be applied;

2) a discussion of which of the above 5 security services are provided, and at which level;

3) a list of which protocols, network elements, and communication channels are secured by the profile;

4) a discussion of known potential attacks, and what protection against them is offered by the profile;

5) a discussion of potential damage that might be incurred should the security measures in the profile eventually be breached;

6) a precise discussion of the mathematical and protocol algorithmic devices and technologies used, sufficient to ensure that two implementations complying with the profile can interoperate (if the profile offers parameters or choices, then two implementations choosing the same parameters have to interoperate, and the profile should discuss the implications of two implementations choosing different parameters).

ID	Requirement Description	Type	Scen./ Serv. Type
28	It shall be indicated to which TIPHON security profiles, in any, a TIPHON system complies	M	

8.7 Lawful Interception

Regulators and other legal bodies require real-time access to the entire telecommunications transmitted or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that are generated to process the call. The target should not be aware of the fact that his communication is intercepted.
Lawful interception is not part of a security profile, but the communication to and from the telecommunications system might require its own security profile. The fact that lawful interception shall be possible influences e.g. the media stream encryption the network can provide.

NOTE: This issue has not yet been studied in detail by TIPHON, but it has been agreed that this has to be supported as far as technically feasible. More detailed requirements will be identified for the next release of the present document.

ID	Requirement Description	Type	Scen./ Serv. Type
26	TIPHON systems shall have a mechanism for supporting Lawful Interception.	C	

9 Accounting/Billing/Charging

9.1 Introduction

If required by the business role, TIPHON systems shall support the accounting, charging and billing process through the collection and exchange of relevant information. Such information exchanges shall conform to the requirements identified below, including the overall principles, security, and service detail recording.

Billing is performed by a service provider towards end-users with whom they have a business relationship. In order to do so the service provider collects information for each call. If the service provider uses services from other business roles in order to perform the service for his subscriber, accounting information has to be transferred between domains.

9.2 Accounting

9.2.1 General requirements/principles

In the SCN, the following general principles apply:

1) Calling party pays, with the following exceptions: freephone, reverse charging, split charging.

2) The calling party should know in advance from the dialled number, what the price of the call will be. Therefore all surprises (additional costs, e.g. air time cost, the prize of the forwarding or roaming leg) have to be paid by the called party or by one or more providers involved in the call.

The same principles should apply to IP-based calls.

ID	Requirement Description	Type	Scen./ Serv. Type
29	Different domains needs to be able to exchange accounting information in a standardized manner		
30	The information exchange shall not constrain service to particular business models, but rather shall provide sufficient flexibility to support any reasonable business or administrative model (for example, user services, transit services, single administrative domains, bilateral peering, third party clearinghouse services, and roaming users).		
31	The method for information exchange shall be sufficiently powerful and flexible to support operation over the public Internet as well as private IP networks, and it shall support accounting between various business roles.		
32	The method for information exchange shall provide sufficient definition to ensure interoperability, yet permit easy extensibility for future and/or private extensions.		
33	The method for information exchange shall be flexible enough to support various modes of operations (per-call, or "hot billing" for example, as well as bulk processing).		

9.2.2 Security

ID	Requirement Description	Type	Scen./ Serv. Type
34	Notwithstanding the security requirements for actual calls, the method of exchange of pricing, authorization, and usage information shall support (but not require) mutual authentication, confidentiality, and non-repudiation of all communications.		
35	The method of information exchange must support (but not require) operation through firewalls and/or proxy servers.		

9.2.3 Clearinghouse/Broker scenarios

Accounting

Business roles can agree to do accounting via a Broker, rather than via bilateral agreements. In this scenario the same requirements as identified under subclause 9.2 apply.

Authorization/Pricing

A Broker service can also be actively involved in exchange of authorization and pricing information.

ID	Requirement Description	Type	Scen./ Serv. Type
36	Pricing exchange shall provide a method for operators to indicate the prices they charge for services. The pricing information shall indicate the billing method and service unit, and the services whose prices are indicated shall be sufficiently and unambiguously defined so as to permit consistent interpretation for multiple operators.		
37	Authorization exchange shall provide a method for operators to request authorization to use a service.		

9.2.4 Service Detail Records for accounting

ID	Requirement Description	Type	Scen./ Serv. Type
38	If exchange of usage information is required, that information shall be contained within service detailed records (SDR) for each call.		
39	Accounting information shall be collected for successful and non-successful calls. The information can be used for statistics as well, but will not be profiled towards this use.		
40	For reasons of interoperability, the content and format of SDR's should be standardized. The format should support private extensions and provide a way to ensure that private extensions from different sources can be unambiguously distinguished from each other.		

41	The SDR shall support, at a minimum, the following service scenarios:
	a) basic call (calling party pays by subscription);
	b) free phone / toll free (800 call);
	c) operator assisted call/collect call;
	d) premium rate call;
	e) credit card call.		

Below the requirements for the usage information to be provided by an IP telephony administrative domain, and exchanged with other domains, are collected. Since the information may be exchanged not only bilateral, but also via a clearing house, each component needs to be able to be self-contained and therefore should include all necessary information. The information is grouped in:

- basic Information;
- location Information;
- timing Information;
- details of Telecommunication Services used;
- charge Information.

The Telecommunication Services are either Basic Services or Supplementary Services. Only Basic Services are considered in the present document.

ID	Requirement Description	Type	Scen. / Serv. Type
43	Basic Information in an SDR:		
a	Identification of the charged domain This identification uniquely identifies the charged administrative domain. In case of a mobile subscriber, this could be the home administrator domain.	M	
b	Identification of the administrative domain raising the information This identification uniquely identifies the administrative domain raising the record. This is necessary for the receiving domain or the clearing house to properly distribute the charges.	M	
c	User Identification This information uniquely identifies the user, at least to the administrative domain owning the user *in case of roaming user this is necessary for the home domain to properly charge the user.	C*	
d	TransactionID If a clearinghouse in involved in the transaction, it might issue a transactionID to which the SDR eventually produced shall refer to.	O	
44	Location Information in an SDR This information may be necessary for calculation of checking of charges and for control purposes.		
a	Identification of the recording entity This information is used for tracing purposes. In GSM SDRs this identity is transported between operators, although one might argue that this information can stay within a domain, since this information can always be retrieved via the callID.	O	
b	Incoming location Identification of the incoming entity (e.g. a Gateway) and the identification of the incoming trunk group and circuit (e.g. CIC). This information is needed for accounting with fixed network operators. For H.323 terminals the element EndPoint may be used.	O	

ID	Requirement Description	Type	Scen. / Serv. Type
c	Outgoing location Identification of the outgoing entity (e.g. a Gateway) and the identification of the outgoing trunk group and circuit (e.g. CIC). This information is needed for accounting with fixed network operators. For H.323 terminals the element EndPoint may be used.	O	
45	Timing information in an SDR This information is necessary for checking of charges, for billing to the user and for call detail information to the user.		
a	Charging time stamp of the event Date and time (UTC) of the event to be charged. The time stamp may either be the Answer or the Disconnect time. It is proposed to use the disconnect time.	M	
b	Chargeable duration Chargeable duration of the event. In case of a basic call this is the time from Answer to Disconnect. Default is Seconds.	M	
c	Call setup duration * in case SCN operators do accounting on the basis of trunk seizure time	C*	
d	Cause value In order to distinguish between successful and non-successful calls, the Cause value in Q.931 or ISUP signalling is provided. The billing system could make a distinction between unsuccessful calls because of e.g. network congestion and subscriber busy. *in case SDR produced for unsuccessful call.	C*	
46	Detailed information of the Telecommunication Service in an SDR This information is necessary for additional data related to the service used. The information may be different for each type of service used.		
a	ServiceID Indicated the type of service being reported. In this case basic internet telephony service.	M	
b	CallID H.323 CallID	M	
c	Calling Party Address As used in Q.931 or ISUP signalling *if different from User Identification	C*	
d	Called Party Address (dialled digits) As used in Q.931 or ISUP signalling.	M	
e	Incoming Network Indicator Identification of the network offering the call.		
f	Outgoing Network Indicator Identification of the network the call is delivered to.		
g	QoS requested by the user *if more levels of QoS available to the user.	C*	
h	QoS as provided by the network *if information available	C*	
47	Charge information in an SDR This information indicates the amount of charge raised by the administrative domain creating the record.		
a	Charged amount Gives the full amount what is charged for this component.	M	
b	Currency Currency used with the amount *if different from fictive currency used by ROA's	C*	
c	Currency Exchange rate	ffs	
d	Tax Rate Defines the tax applicable to the charge in the country of the administrative domain creating the ticket (for tax refund by corporate subscribers).	ffs	
e	Tax Treatment Indicates whether the charges are inclusive or exclusive tax.	ffs	

9.3 Charging/Billing

10 Items for further study

10.1 Operations, Administration, Maintenance, and Provisioning (OAM&P)

This will include the function of an SDR collection system.

10.2 Conferencing

10.3 Interoperability with Intelligent Networks (INs)

10.4 Support for users with disabilities

Annex A (informative): Business scenarios

This annex describes several potential relationships between business roles identified in clause 5. The annex intends merely to assist in the understanding of the business roles. It is not an exhaustive list of business relationships, nor is it a detailed specification of business models (one such specification, for example, is available from the c (TINA) [12], and [13]). Additional relationships may be added in later revisions of the present document.

NOTE: These relationships are not exclusive of each other. For example, a local operator may negotiate bilateral agreements directly with other operators in some calling areas, yet still rely on a broker service to complete calls to other calling areas.

A.1 Relations between business roles involved in basic call

The figure below gives the most common relationships between the different business roles (identified in clause 5) involved in a basic call between SCN and IP network. The following points apply:

- relationships other than the depicted ones might be possible;
- not all relationships might apply at same time, e.g. ICP-IPAP and ICP-IPNP;
- different business roles can be combined into administrative domains;
- most business roles are applicable in the private domain as well as the public domain.
- multiplicity of business roles, e.g. ITSP's, IPNP's, SCNP's is not depicted in the figure.
  Rest of the Annex provides scenarios on how different IP Service Providers and ICP's could interoperate.

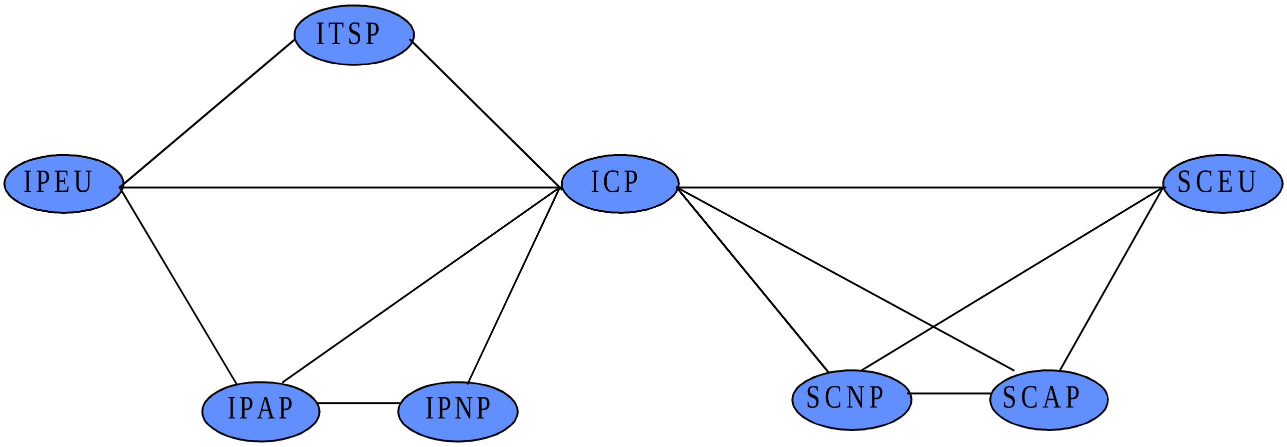


Figure A.1

The most common relationships between the different business roles involved in a basic call between SCN and IP network; IP end user (IPEU), IP Telephony Service Provider (ITSP), Interconnectivity Provider (ICP), IP access provider (IPAP), IP network provider (IPNP), SCN network provider (SCNP), SCN access provider (SCAP), SCN end user (SCEU).

A.2 Single IP telephony local operator

A single IP telephony local operator acts as an IP access provider, IP network provider, gatekeeper service provider, and internetworking function provider. It relies on a SCN access provider for connectivity. The operator owns or operates all IP endpoint devices in a closed network. Such a network may still rely on additional IP network providers (such as the public Internet) for physical connectivity, but only those devices in the operator's network are permitted to communicate with each other.

A.3 Multiple IP telephony local operators (bilateral agreements)

By negotiating directly with other operators, one IP telephony local operator can expand its service. In this case, each local operator acts as described in clause A.1. The participating operators simply agree to permit each other's devices to access their own devices. Such operators should use a common IP network provider, possibly the public Internet. In case of user mobility, subscribers of one operator can appear in networks of other operators it has an agreement with. The visited operator contacts the home network operator, which it finds by information provided by the visiting subscriber (e.g. smart card).

A.4 Backbone operator

A backbone operator provides physical interconnection between IP telephony local operators (as defined in clause A.1). The backbone operator acts as IP network provider and, potentially as a directory service provider and value added service provider. As a directory service provider, the backbone operator may provide functions that allow one local operator to locate another local operator. The backbone operator may also provide authorization services between the local operators.

A.5 Franchise/consortium

A franchise or consortium offers local operators (see clause A.1) a way to expand service without physically expanding their networks. The franchise provider acts as a directory service provider so that its franchisees may locate each other, and it may also provide authorization services. By joining a franchise, a local operator gains access to endpoint devices belonging to other franchise members. Although superficially similar to a broker (see clause A.5), a franchise is typically more restrictive and more tightly controlled. A local operator, for example, may purchase franchise rights for a specific calling area. Such a purchase would prohibit the franchiser from supporting other local operators in the same calling area, and all calls to that area would have to use the assigned local operator. In case of user mobility, subscribers of one operator can appear in networks of other operators of the consortium. One scenario is that the visited operator contacts the home network operator, which it finds by information provided by the visiting subscriber (e.g. smart card), or via a lookup in a database maintained by the consortium.

A.6 Broker service

A broker provides a subscription like service to multiple local operators. By subscribing to a broker, an operator gains access to other operators participating in the service. The broker acts as a directory service provider, and it provides authorization services for its subscribers. Broker services are typically designed to be much less restrictive than franchise or consortiums (although the technical operation may be very similar). Because of the less restrictive business relationship, though, broker service providers may require more stringent security measures. An example of a broker is a Clearing House Service Provider (CHSP).

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

- ITU-T Recommendation X.800 (1991): "Security architecture for Open Systems Interconnection for CCITT applications".

History

Document history		
V2.2.2	March 1999	Publication

ISBN 2-7437-2866-3
Dépôt légal : Mars 1999