# TR 101 306 V1.2.3 (1998-02)

*Technical Report*

# Telecommunications and Internet Protocol Harmonization Over Network (TIPHON); Requirements for service interoperability; Scenario 1

*European Telecommunications Standards Institute*

Reference
DTR/TIPHON-01001 (c3c00iq4.PDF)

Keywords
Internet, protocol, telephony, network

***ETSI Secretariat***

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

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
secretariat@etsi.fr
http://www.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 ETR 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.fr/ipr).

Pursuant to the ETSI Interim 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 ETR 314 (or the updates on http://www.etsi.fr/ipr) 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 Network (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 circuit switched networks and Internet Protocol (IP) based networks and their associated terminal equipment.

The TIPHON environment has been divided into 4 interrelated scenarios as described in TR 101 300 [13].

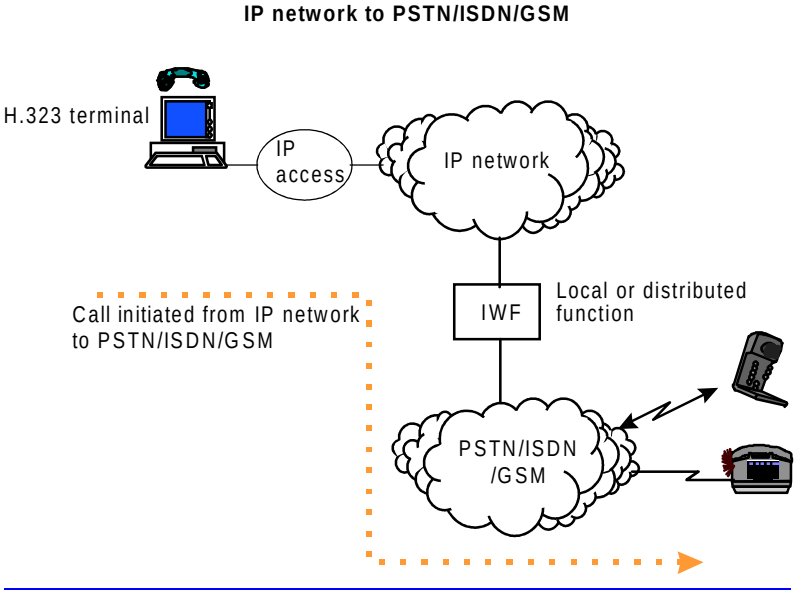
The present document defines the initial requirements for scenario 1, which is limited to real time voice communication between IP based terminals and terminals attached to circuit switced networks such as, Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN) and Global System for Mobile communications (GSM) terminals, in which the call set-up is originated by the IP terminal user.

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 mandatory and optional TIPHON requirements to ensure service interoperability for TIPHON scenario 1 systems (see clauses 6 to 10). This version of the present document specifies real time voice communications between users on Internet Protocol (IP) based networks and users on circuit switched networks where the call is originated on an IP based network. This is illustrated in figure 1.




IWF: InterWorking Function

**Figure 1: Definition of scenario 1**

End-to-end video, fax and data transmission; voice, data and video conferencing; and messaging services are not included in the current version of the present document.

It should be noted that where a requirement is optional or marked for further study in the first 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

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case 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.

## 2.1 Normative references

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

[2] ITU-T Recommendation H.323 (1998) (version 2): "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: "Internet Protocol, Jon Postel, USC/Information Sciences Institute, September 1981".

[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: "IP Version 6 Addressing Architecture", December 1995.

## 2.2 Informative references

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

[10] Telecommunications Information Networking Architecture - Consortium, TINA-C deliverable - "Overall concepts and principles of TINA", version 1.0.

[11] Telecommunications Information Networking Architecture - Consortium, TINA-C deliverable - "Domain types and basic reference points in TINA".

[12] Telecommunications Information Networking Architecture - Consortium, TINA-C deliverable - "TINA reference points", version 3.1.

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

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following 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.

**directory service provider:** A provider of directory information e.g. providing an E.164 number from an email address.

**E.164 number:** The international telephone number (as defined in ITU 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.

**gatekeeper service provider:** An IP service provider who offers services available from gatekeepers to the user.

**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 must be known. All identities within a particular context must 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.

**interconnectivity provider:** A service provider who offers services for access between IP and ISDN/PSTN/GSM networks.

**Internet Protocol (IP) access provider:** A company or organization which provides their customers with access to an IP network.

**IP address:** Each network unit connected to an IP network must 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 broker:** Provider of a business service to facilitate the exchange of IP traffic between multiple IP service providers and other network operators.

**IP end user:** A user who is connected to an IP network.

**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 network provider:** A company or organization which provides access to an IP network.

**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.

**IP telephony service provider:** A service provider who offers telephony services over IP networks.

**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.

**PSTN/ISDN/GSM end user:** A user who accesses the PSTN/ISDN/GSM services provided by Telecom companies.

**PSTN/ISDN/GSM network provider:** A company providing either PSTN, ISDN, or GSM network services.

**value added service provider:** Service provider which provides services beyond normal or traditional services. The extra services are normally informational services and are not part of the services which are offered traditionally by service providers.

## 3.2 Abbreviations

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

| | |
|---|---|
| CHSP | Clearing House Service Provider |
| CLIP | Calling Line Identification Presentation |
| CLIR | Calling Line Identification Restriction |
| DTMF | Dual Tone Multiple Frequency |
| GK | Gatekeeper |
| GSM | Global System for Mobile communications |
| GW | Gateway |
| IETF | Internet Engineering Task Force |
| IN | Intelligent Network |
| IP | Internet Protocol |
| ISDN | Integrated Services Digital Network |
| IWF | InterWorking Function |
| MCID | Malicious Call IDentification |
| MCU | Multipoint Control Unit |
| OAM&P | Operations, Administration, Maintenance, and Provisioning |
| PABX | Private Automatic Branch eXchange |
| PSTN | Public Switched Telephone Network |
| QoS | Quality of Service |
| RFC | Request For Comments |
| SDR | Service Detailed Records |

# 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]).

IP networks may be private or public IP networks.

# 5 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;

b) IP access provider;

c) IP network provider;

d) IP telephony service provider;

e) interconnectivity provider (including gatekeeper service provider);

f) PSTN/ISDN/GSM network provider;

g) PSTN/ISDN/GSM access provider;

h) PSTN/ISDN/GSM end user;

i) directory service providers;

j) value added service providers;

k) IP broker.

Annex A gives further information about some of these business roles.

# 6 General requirements

The terminals on IP based networks shall be compliant with ITU-T Recommendation H.323 [2]. Major issues concerning the interoperability of IP telephony terminals are addressed within the ITU-T Recommendation H.323 [2]. It is within the scope of the ETSI Project TIPHON to profile H.323 in order to ensure interworking between H.323 endpoints or terminals, including H.323 gatekeepers where applicable, and terminals connected to the circuit switched networks. 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.

1) The use of a firewall in a TIPHON compliant environment shall be possible.

2) A TIPHON compliant system shall be capable of supporting a minimum level of Quality of Service (QoS).

3) Scaleability - for further study.

4) Modularity - for further study.

# 7 Services provided by a TIPHON compliant system

## 7.1 Basic services

1) It shall be possible to setup calls which originate at a H.323 client on an IP-based network and terminate at terminals on PSTN/ISDN/GSM networks.

2) Backward call clearing shall be possible.

3) Forward call clearing shall be possible.

4) The detection of a non-recoverable failure of any of the critical resources involved in the call shall initiate the clearing of the call.

*5)* User services which make use of end-to-end bidirectional and unidirectional DTMF signaling shall be supported e.g. voice mail applications, conference bridge applications, banking applications, etc.

6) An inability to complete the call within the PSTN/ISDN/GSM network shall be detected and communicated to the calling party (e.g. busy tone). This can be done via either signalling or audio information.

7) The ability for inband audio tones and announcements to be received by the caller shall be supported (e.g. special information tones, referral messages, etc.)

## 7.2 Supplementary services

In order to allow early usage of TIPHON interoperability specifications, only requirements related to an initial set of supplementary services are defined in this version of the present document.

1) The call initiator 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.

2) It shall be possible to provide the call initiator or the party paying for the call with the ability to select intermediate carriers.

3) In order to preserve existing PSTN/ISDN/GSM service features, the TIPHON architecture shall support the following:

   a) the calling party may provide a presentation number, as defined in ITU-T Recommendation E.164 [1] format, which the network shall treat as additional CLIP information;

   b) the transport of the calling line identification;

   c) the transport of the calling line identification restriction;

   d) malicious call tracing for calls initiated from an IP based terminal.

# 8 Addressing

1) It shall be possible for a call initiator in an IP network to use the E.164 number of a PSTN/ISDN/GSM user to identify and call the called party. This is independent of whether the number has been ported, and whether it refers to a terminal or a user.

NOTE: 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.

2) 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.

# 9 Security

This clause describes general security requirements for TIPHON services.

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

One of the primary issues of security is protection of the network. Providers shall be able to protect their network against accidental or malicious failures caused by users or by interconnecting networks. This includes both network congestion and signalling type problems. These failures can be avoided by arrangements between interconnecting providers, either via authentication or trust. Both network operators and users need to be protected against abuse of the TIPHON equipment. This abuse might result in costs/losses for operators and/or users.

## 9.1 Authentication and authorization

More than one authentication and/or authorization mechanism may be required based on the business role.

1) TIPHON compliant systems shall use the security mechanism defined in ITU-T Recommendation H.235 [3].

2) Authentication shall be supported in TIPHON compliant systems. Not every call is required to use authentication, although it must be possible to use authentication on a per-call basis.
Authentication is the use of security techniques to prove identity. Both parties to a communication require assurance of each other's identity. The reasons, as well as the degree of authentication, differ for each party, e.g.:

   a) relevant parties in a call shall be able to authenticate themselves (e.g. users, services and preferably terminals);

   b) mutual authentication of calling and called user shall be supported.

3) Authorization of calls shall be supported in TIPHON compliant systems. Not every call is required to be separately authorized, although it shall be possible to authorize on a per-call basis. Authorization is the granting of permission to use resources and facilities. TIPHON services may not only identify remote operators, they may also provide authorization to use their facilities. This authorization is necessary because two subscribers may have no business relationship with each other. Before the remote operator will allow use of its facilities, it requires assurance that it will be compensated for that use.

4) Calls without authentication of the call shall be possible in TIPHON compliant systems. This allows for a certain class of services for subscribers without a relationship with the local IP telephony service provider, e.g. placing FreePhone calls.

5) Non-repudiation should be supported in TIPHON compliant systems. Non-repudiation provides proof of the origin of information, and it serves as a deterrent to one party falsely denying that they participated in a transaction.

6) It is desirable that end-to-end security should be supported in TIPHON compliant systems.

7) It shall be possible to ensure the authenticity of tokens in TIPHON compliant systems.

## 9.2 Message privacy

Communication between TIPHON compliant products is likely to include confidential or proprietary information. Protecting this information from eavesdroppers, particularly when the communication takes place across the public Internet, requires encryption.

Other specific requirements are:

- TIPHON 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.

- TIPHON 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 either the identity or the telephone number of one of the parties of a conversation.

- TIPHON systems shall have a mechanism for supporting lawful interception.
- Message privacy shall be possible.
- Detection of theft shall be possible. Theft is described as "service use that is outside the policy defined for some user by the service provider".

# 10 Accounting/charging/billing

1) If required by the business role TIPHON systems shall have a mechanism for providing Service Detailed Records (SDR) for each call, which can be used for accounting, charging, and billing for both successful and unsuccessful calls or service usage. The SDR may also be used for the generation of statistics.
2) The SDR shall at least be able to support the following scenarios/services:
   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.
3) The SDR shall contain information on the identity of the party to charge. It shall also be possible to configure the SDR to contain any of the following information:
   a) type of service (e.g. basic call, premium rate call, free phone call, use of supplementary service, etc.);
   b) the time of day (e.g. peak hours, quiet hours, working days, holidays, etc.);
   c) the source and destination of the call;
   d) the level of QoS;
   e) duration of call;
   f) resource utilization.

# 11 Items for further study

## 11.1 Operations, Administration, Maintenance, and Provisioning (OAM&P)

This will include the function of an SDR collection system.

11.2 Conferencing

11.3 Interoperability with Intelligent Networks (INs)

11.4 Support for users with disabilities

11.5 Operation with PABXs and private circuit switched networks

# Annex A: Business roles

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 Telecommunications Information Networking Architecture (TINA) [10], [11], and [12]). Additional relationships may be added in later revisions of the present document.

Note that 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 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 PSTN/ISDN/GSM 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.2 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.3 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.4 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.5 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).

# History

| Document history | | |
|---|---|---|
| V1.2.3 | February 1998 | Publication |
| | | |
| | | |
| | | |
| | | |

ISBN 2-7437-1990-7
Dépôt légal : Février 1998