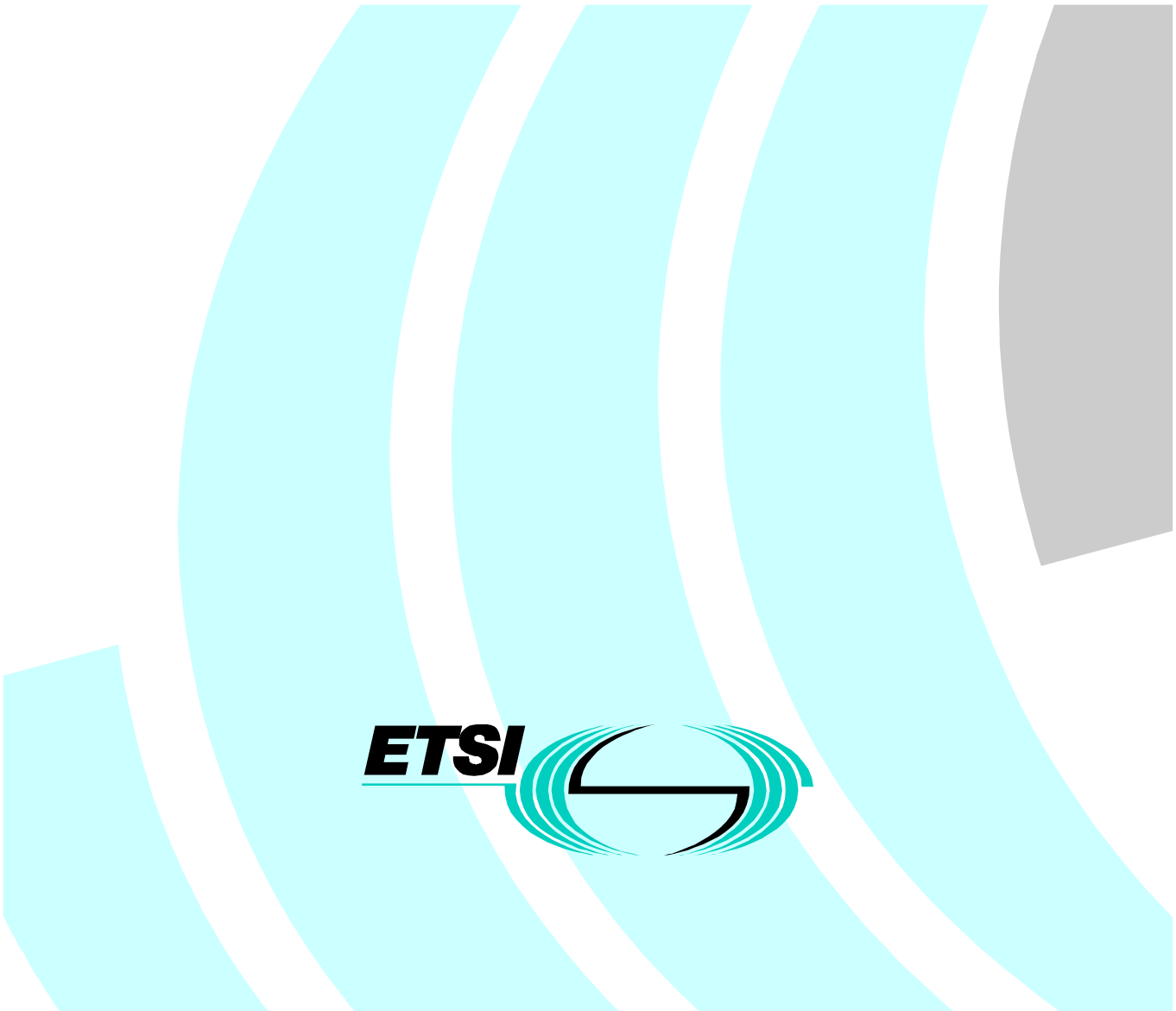
ETSI EG 201 807 V1.1.1 (2000-09)

ETSI Guide

Network Aspects (NA);
Intelligent Network (IN);
Network operators' requirements
for the delivery of service provider access



Reference
DEG/SPAN-061603

Keywords
access, NNI, protocol, regulation, service, UNI

ETSI

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

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

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

Contents

Intellectual property rights

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

Foreword

This ETSI Guide (EG) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN).

1 Scope

The present document lists the first set of requirements that public network operators have for the delivery of service provider access. These requirements are intended to facilitate a non-discriminatory access to public telecommunication networks for service providers.

The present document does not fully take into account the service capability requirements from a service provider's perspective, these aspects are defined in EG 201 722 [7]. The two documents EG 201 722 [7] and the present document should not be considered separately for implementation.

The scope of the present document is to present generic functional requirements regarding the service provider access. The priority of each requirement is based on the need perceived from the public network operator´s viewpoint. Service interaction aspects are outside the scope of the present document. To fulfil these requirements, appropriate protocols and/or provisions may have to be developed taking into account network integrity, security, charging, and other considerations expressed in the present document.

Clause 4 contains introductory text describing the background and motivations of the requirements of service provider access. Clause 5 contains a description of the functional requirements of the service provider access interface. These requirements need to be considered additional to the requirements specified in EG 201 722 [7].

The present document relates to the role of the service provider and the role of the public telecommunications network operator, with the realization that market players may act in multiple roles. This is in alignment with the current European legislation, which specifies that all capabilities utilized by a significant market power network operator's internal service provisional body, shall also be offered on equal terms to external entities.

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] CEPT/ECTRA Recommendation on network integrity, Rec(98)01, 12th May 1998.

[2] Directive 98/10/EC of the European Parliament and Council of 26th February 1998 on the application of Open Network Provisions to voice telephony and on universal service for telecommunications in a competitive environment.

[3] Directive 97/33/EC of the European Parliament and Council of 30th June 1997 on interconnection in telecommunications with regard to ensuring universal service and interoperability through the application of Open Network Provisions.

[4] ETSI ETR 322: "Intelligent Network (IN); Vocabulary of terms and abbreviations for CS-1 and CS-2".

[5] ETSI ETS 300 128 (1992): "Integrated Services Digital Network (ISDN), Malicious Call Identification (MCID) supplementary service; Service description".

[6] ETSI ES 201 158: "Telecommunications Security; Lawful Interception (LI); Requirements for network functions".

[7] ETSI EG 201 722: "Intelligent Network (IN); Service provider access requirements; Enhanced telephony services".

[8] ETSI EG 201 781: "Intelligent Network (IN); Lawful interception".

3 Definitions and abbreviations

3.1 Definitions

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

firewall: means of preventing external parties from directly accessing internal network resources. All signalling to internal network resources are directed via an entity dedicated to that purpose.

mapping: systematic way of converting messages from one signalling system to messages of another signalling system.

public telecommunications network: telecommunications network which provides telecommunications services to the general public [4].

public telecommunications network operator: entity which is responsible for the development, provisioning and maintenance of telecommunications services to the general public and for operating the corresponding networks [4].

public telecommunications network originating: PTN to which either the originating line is directly connected or in which an incoming call initiates a service.

public telecommunications network terminating: PTN to which either the terminating line is directly connected or in which the terminating line's user profile is stored.

screening: process involving intercepting signalling messages to check their contents before allowing them to continue, or rejecting them.

service provider: entity which provides services to its service subscribers on a contractual basis and who is responsible for the services offered. The same organization may act as a public telecommunications network operator and a service provider [4].

service provider originating: service provider that provides either services relating to the originating line (or to the originating profile), or services acting on the information coming from the originating or incoming call.

service provider terminating: service provider that provides either services relating to the terminating line (or to the terminating profile), or services acting on the call-related information coming from the terminating party's line.

service provider access: access facility that enables a service provider to access specific functionality of a public telecommunications network.

service provider access interface: interface between a public telecommunications network and a service provider´s equipment for enabling the service provider to access specific functionality of a public telecommunications network.

service provider access requirement: requirement for a service provider´s access to specific functionality of a public telecommunications network.

special network access: access at network termination points other than the more commonly provided network termination points, such as the conventional user-network interfaces (see Directive 98/10/EC [2]).

3.2 Abbreviations

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

CdPy	Called Party
CgPy	Calling Party
CLI	Calling Line Identity
EC	European Community
ECTRA	European Committee for Telecommunications Regulatory Affairs
ETP	European Telecommunications Platform
ETSI	European Telecommunications Standards Institute

ISDN	Integrated Services Digital Network
NRA	National Regulatory Authority
NTP	Network Terminating Point
PTN	Public Telecommunications Network
PTNO	Public Telecommunications Network Operator
PTNorig	originating Public Telecommunications Network
PTNterm	terminating Public Telecommunications Network
SP	Service Provider
SPorig	Service Provider originating
SPterm	Service Provider terminating
SPA	Service Provider Access
SPAR	Service Provider Access Requirements
UNI	User-Network Interface

4 Introduction

4.1 General

The aim of the present document is to define the requirements that need to be met when service providers wish to access functionality in the public telecommunication networks of PTNOs. Such requirements will generally apply to the interface between the PTNO and the SP. In EG 201 722 [7] the functional requirements which apply to this access interface from the perspective of service providers are specified.

The requirements in EG 201 722 [7] however do not adequately take into account the network integrity, charging or other aspects from a PTNO's perspective, that nevertheless needs to be clearly specified if the PTNO is to provide reliable and secure network access to the service provider. These technical conditions would in most cases be applicable to both the PTNO and the SP but there are clearly instances when the requirements may have to be given special and different treatment by the PTNO.

It is therefore important to ensure that the functional specifications defined in EG 201 722 [7] fully respect the technical criterion applicable to integrity, charging, and other key aspects that are of vital importance to both PTNOs and SPs. The requirements defined in the present document are from a PTNO's perspective and should therefore be read in conjunction with EG 201 722 [7].

4.2 Regulatory aspects

The present document outlines the current regulatory criterion which is applicable to service providers requesting "special network access" from the PTNO. These criteria primarily emanate from Article 16 of the Voice Telephony directive (see Directive 98/10/EC [2]) that places obligations on "significant market power" organizations to respond to "reasonable requests" for special network access.

Hence all NRAs in EU countries will be under an obligation to implement in national regulation the requirements of the EU directives and this means PTNOs nominated as having significant market power will need to comply with special network access requirements. It will be a matter for NRAs in each country to decide if they wish to go further and apply the EU requirements to "non-significant market power" organizations but there are clearly no obligations for member states to take these steps.

There are requirements in the directive to ensure that network integrity is fully respected and this means that both public telecommunication network operators and service providers will need to ensure that network integrity requirements are incorporated in their network facilities. The European Committee for Telecommunications Regulatory Affairs (ECTRA) recommendations on network integrity (see CEPT/ECTRA Recommendation (98)01 [1]) and the European Telecommunications Platform (ETP) guideline report on network integrity (see ETP guidline in Bibliography) outline broad regulatory and operational aspects of network integrity and are relevant to the present document.

Hence from the regulatory perspective PTNOs designated as operators having significant market power will be required to respond to "reasonable requests" for special network access. Those organizations designated, as having significant market power, shall in accordance with Article 16 of the Voice Telephony Directive adhere to the principle of non-discrimination (see Directives 98/10/EC [2] and 97/33/EC [3]). It will be a matter for both PTNO and SP to agree on what network services can be made available via special network access and whether such services are technically and economically feasible subject to regulatory oversight by the NRA.

The technical requirements of legal interception will need to accord with the specific regulations on security and interception that are in force in the respective countries (see EG 201 781 [8] and ES 201 158 [6]).

PTNOs willing to operate in one or more countries have to comply with the specific regulatory requirements of the NRAs of those countries. PTNOs are obliged to support the numbers being allocated to SPs by the NRA responsible for the respective country for the provision of the specific services offered by the SPs in that country.

4.3 Network integrity aspects

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 affect in a negative way the services provided in the PTN.
- The authentication/ciphering mechanisms to protect the PTN from the vulnerabilities due to the Service Provider access.

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.
- Service Provider access 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 risks.

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.

4.4 Security aspects

Security aspects of the SPA are briefly described in EG 201 722 [7].

4.5 Charging 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 for instance the case for the following SP's requirements, included in EG 201 722 [7]:

- 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 end user before any service charging begins;
- sending data to and receiving data from of the service user's NTP without an alert signal, such as a ringing.

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.

4.6 Guidelines for the service provider access requirements

In the specification of the service provider access requirements, the following aspects were taken into consideration:

- The definition of the SPA requirements needs to be based both upon service capability requirements from the viewpoint of SPs and related requirements of PTNOs, e.g. service operability, network integrity and security. EG 201 722 [7].
- The PTN restrictions which are due either to national regulations or to high-level network restrictions and barrings shall not be overridden by the SPs.
- The use of the SPA interface will not guarantee to the SP that service requests or responses can be passed across the boundaries of different PTNs.

5 Functional requirements for service provider access

5.1 Introduction

The requirements that service providers have for accessing functionality of a PTN are given in EG 201 722 [7]. Public telecommunications network operators have requirements for the delivery of service provider access. The existing interfaces were not specifically designed to meet the requirements of service provider access e.g. incorporate neither features to ensure network access integrity and security, nor provisions for charging and billing.

5.2 Calling party information handling requirements

The implementation of the service provider functional requirements relating to the CLI should be in conformance with the general EC (see Directive 97/33/EC [3]) and national regulations and with bilateral agreements where they exist, see subclause 4.2 and subclause 4.6 for details.

5.2.1 Relaying of the malicious call identification data of a received call

The terminating PTN needs to receive unchanged from the SP all the received call-specific information that can be used for malicious call tracing.

5.2.1.1 Priority

The priority of this requirement is high.

5.2.1.2 Example of usage

Malicious call tracing is an example.

5.2.1.3 Technical aspects

When a MCID interrogation or data logging is performed by the terminating PTNO, it is necessary that the information contained in the relevant data fields is correct and represents the true identity of the originating NTP. The SP therefore needs to forward to the terminating PTN all the received data necessary for this purpose (see ETS 300 128 [5]).

5.2.1.4 Information flow chart

In Figure 1, two message sequence scenarios are given. In scenario a, the MCID data is requested and delivered during the call set-up phase from the SP to the PTN. In scenario b, the MCID data is requested and delivered during the call phase from the SP to the PTN.

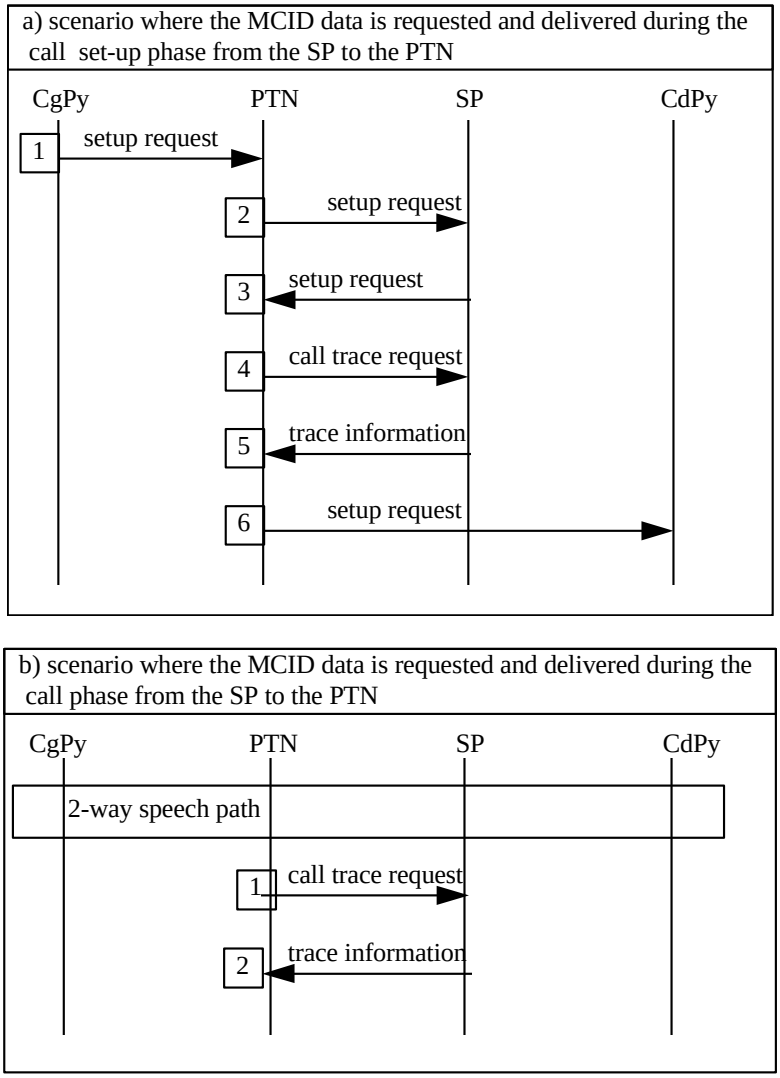


Figure 1: Relaying of the malicious call identification data of a received call

5.2.2 Application of the CLIR supplementary service

The PTN needs the ability to not pass to the SP the CLI, if the calling party has activated the CLIR supplementary service in accordance with national regulations, see text at beginning of subclause 5.2.

5.2.2.1 Priority

The priority of this requirement is high.

5.2.2.2 Example of usage

In the event that the CLIR supplementary service is activated, the CLI is conveyed through the networks involved in the call (originating, transit, terminating) but not presented to the called party. In this case of the SPA interface, the CLI shall not be passed to an SP where national regulations forbid the passing

5.2.2.3 Technical aspects

This applies both to "network-verified" and "user-provided" CLI.

In the event that an SP has an Emergency service role agreed by the national regulation authority, this requirement may be bypassed and the CLI may need to be transmitted even if the CLIR supplementary service is activated.

5.2.2.4 Information flow chart

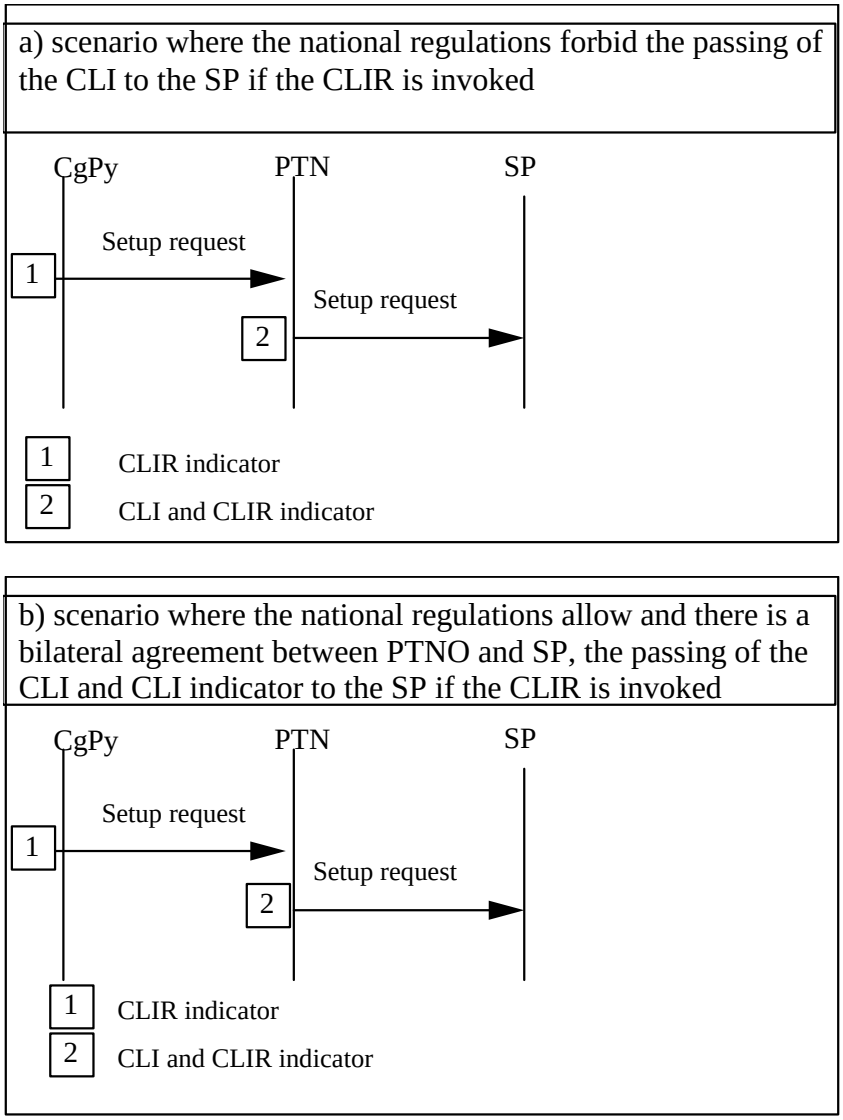


Figure 2: Application of the CLIR supplementary service

5.3 Basic call set-up and clear-down requirements

The implementation of the service provider functional requirements relating to the dialled digits should be in conformance with the general EC (see Directive 97/33/EC [3]) and national regulations and with bilateral agreements where they exist, see subclause 4.2 and subclause 4.6 for details.

5.3.1 Reception of the originally dialled digits

The PTN needs the ability to receive all originally dialled digits from the SP.

5.3.1.1 Priority

The priority of this requirement is low.

5.3.1.2 Example of usage

In case a SPorig has translated the dialled number and the SPterm needs the originally dialled digits, the SPorig needs to provide both the routing number and all originally dialled digits to be able to deliver these to the SPterm.

5.3.1.3 Technical aspects

This requirement is also valid when the dialled number has been translated before the PTN receives a call.

If the SPorig has translated the dialled number and the PTNterm requires the originally dialled digits, then the SPorig needs both the routing number and all originally dialled digits. Since the SPorig is connected to the speech path, the original dialled number is expected to be available in the set-up request that is provided by the SPorig to the PTNterm.

5.3.1.4 Information flow chart

The flowchart in Figure 3 presents a message sequence scenario from the viewpoint of the PTNterm when the dialled number is translated before the terminating PTN receives the call and in a situation where the call itself is connected to the SPs' equipment.

Since the SPorig is connected to the speech path, the original dialled number is expected to be available in the set-up request that is provided by the SPorig to the PTNterm. In this case the SPterm needs the originally dialled digits, the PTNterm needs to receive both the routing number and all originally dialled digits to be able to deliver these to the SPterm.

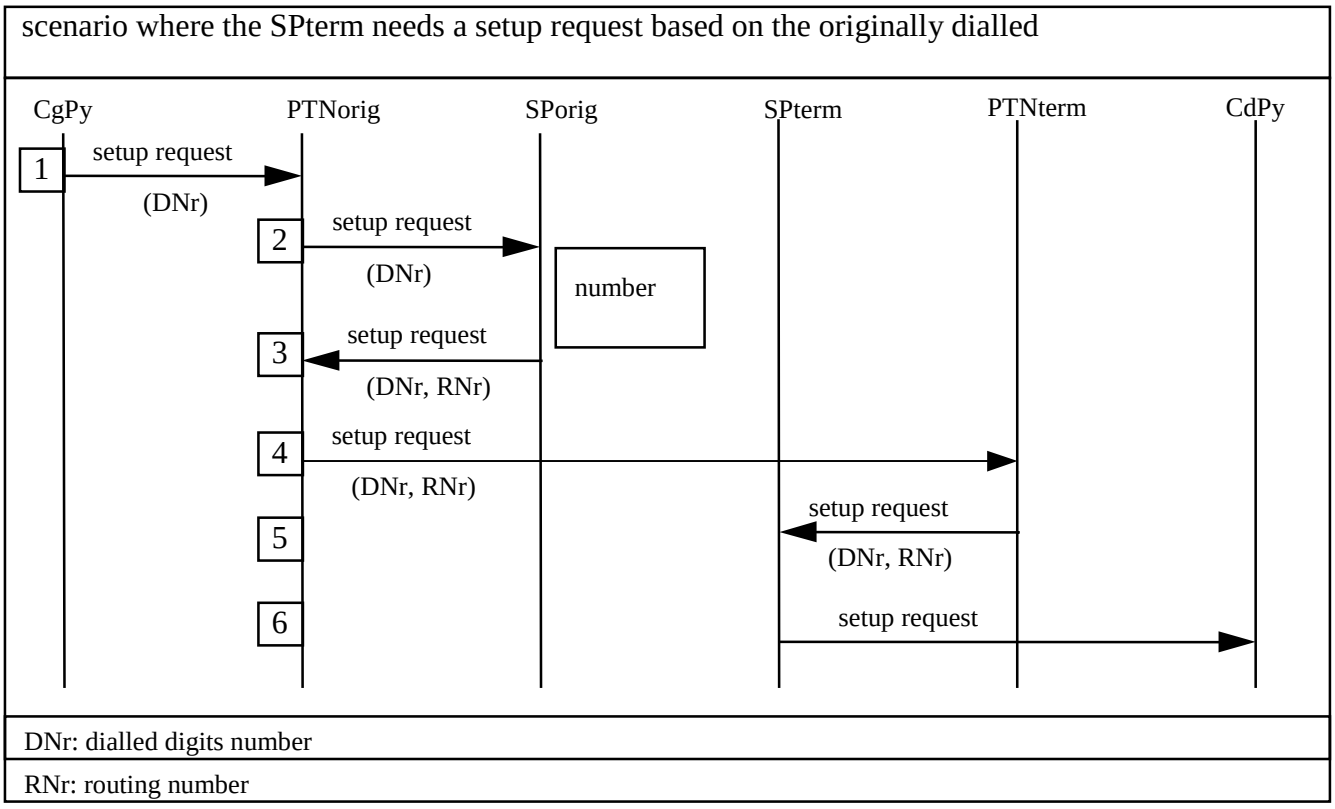


Figure 3: Reception of the originally dialled digits

5.3.2 Alternate routing of a call or the indication of a call to another "point of presence" of the SP

The PTN needs the ability to instruct the SP to route calls or the indications of calls to another "point of presence" of the PTN, if the first "point of presence" is not reachable.

5.3.2.1 Priority

The priority of this requirement is medium.

5.3.2.2 Example of usage

For reliability or capacity reasons, the PTNO may have several "points of presence", i.e. network interconnection points between the PTN and the SP's equipment. The capability to instruct a SP about the configuration of the routing of traffic to "points of presence" can be useful in case a particular "point of presence" is out of service e.g. in case of maintenance.

5.3.2.3 Technical aspects

This alternate routing is not needed on a call by call basis.

5.3.2.4 Information flow chart

The following flowchart in figure 4 presents the provision of the address data of another "point of presence" to the SP.

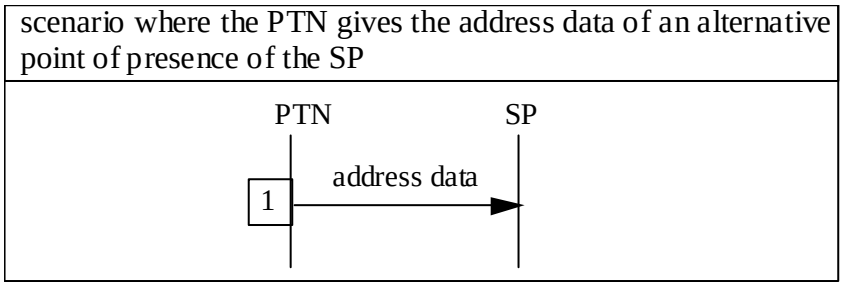


Figure 4: Alternate routing of a call or the indication of a call to another "point of presence" of the SP

5.4 Traffic-related and monitoring requirements

5.4.1 Event traceability

The PTNO needs the ability to perform event traceability with the SP, which should produce relevant call tracing data.

5.4.1.1 Priority

The priority of this requirement is high.

5.4.1.2 Example of usage

The PTNO needs event traceability in order to enable the combination of all the data of each call in off-line processing, e.g. for billing purposes or fault analysis.

Event traceability may also be useful for fraud prevention, so that the PTNO can identify that a call entering the network was originally originated within the same network.

5.4.1.3 Technical aspects

The utilization of a global call reference numbers would facilitate event traceability.

5.4.1.4 Information flow chart

In the message sequence scenario in Figure 5, call detail data is exchanged between the SP and the PTN.

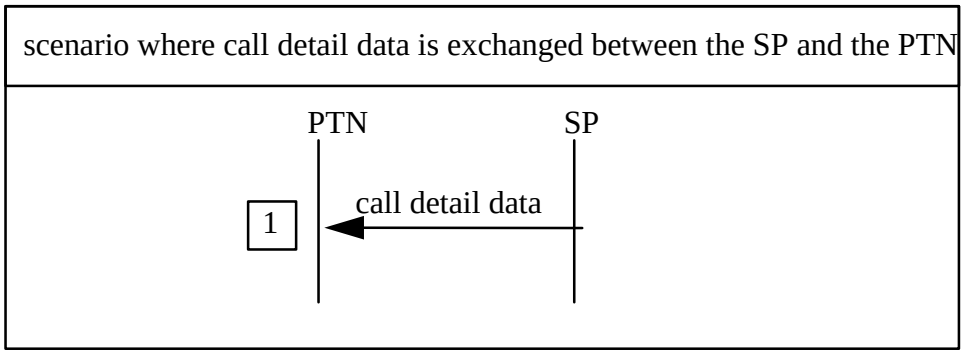


Figure 5: Exchange of call detail data for call event traceability

5.4.2 Traffic control

The PTNO needs the ability to control the signalling and call traffic between the SP's equipment and the PTN.

5.4.2.1 Priority

This priority of this requirement is high.

5.4.2.2 Example of usage

Traffic control capabilities may be needed at the time of overload or congestion.

5.4.2.3 Technical aspects

In order to ensure a sufficient quality of service for the carried traffic, the SP and PTNO may desire that the traffic between the PTN and SP's equipment does not exceed the dimensioned capacity of the related connection or the PTN/SP's equipment. Therefore, capabilities may be needed by the PTNO to control the signalling and call traffic between the SP's equipment and the PTN.

5.4.2.4 Information flow chart

In the message sequence scenario in Figure 6, traffic data is exchanged between the SP and the related PTN.

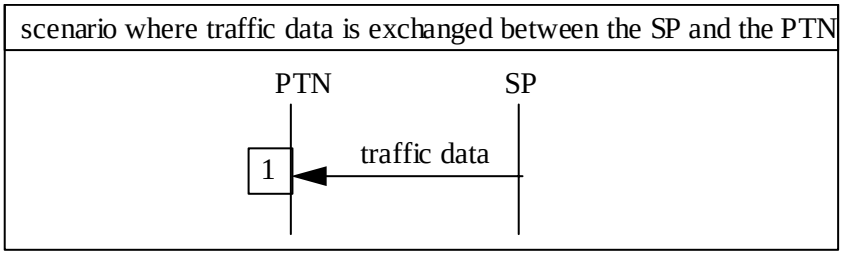


Figure 6: Exchange of traffic data for traffic control

5.4.3 Avoidance of the cyclical routing of a call

The PTNO needs the ability to detect and stop cyclical routing of a call between the PTN and the SP's equipment.

5.4.3.1 Priority

This priority of this requirement is high.

5.4.3.2 Example of usage

During the connection set-up phase of any single call, the call could be forwarded several times incorporating multiple number translations. In some situations, repeated call forwarding may cause undesirable cyclical routing of the call.

5.4.3.3 Technical aspects

To avoid undesirable cyclical routing, one alternative is that sufficient data is associated with the call (e.g. a "hop" counter of the forwarding operations performed).

5.5 Miscellaneous requirements

5.5.1 Application contents screening

The PTNO needs the ability to screen the messages sent and received across the SPA interface.

5.5.1.1 Priority

The priority of this requirement is high.

5.5.1.2 Example of usage

The ability to filter call gap messages and to pass notifications unchanged are examples of usage.

Services offered (e.g. based on IN technology), which need trigger and event detection points being dynamically armed by the SP.

5.5.1.3 Technical details

As far as the control plane interface is concerned, from the viewpoint of network integrity and security, an interworking function could be installed by the PTNO in order to perform:

- protocol screening, so that the full range protocol operations can be used, but only certain operations accepted, depending on which SP is sending the messages;

- messages translation, so that messages received at the reference point are converted into instructions that can be executed within the PTN.

Facilities for application screening functions are required in the connections between the PTN and the SP's equipment. These functions are required for messages, operations, and parameters, and can be specified as screening profiles defined per traffic relationship or destination. The screening profiles should be defined as a result of negotiation between the SP and the PTNO according to the national regulations and legislation.

Note that some SP-originated messages may destinate outside the PTN carrying content data of some service and using the PTN for transportation only. Screening does not apply to the contents of these messages.

Regarding notification messages, a PTNO should be able to require the SP to let notification messages pass unchanged. In general, the implementation and control of screening profiles will be a matter for bilateral agreements between the PTNO and the SP during the negotiation phase of a commercial contract and may also be subject to oversight by the NRA depending on national policy.

The technical specifications which define the screening parameters and profiles and which may be implemented during such commercial agreements will need to be developed by SPAN in accordance with the requirements of the present document.

For messages/operations/parameters these functions should be able to:

- let the message pass unchanged, or

- suppress the sending/receiving of the message/operations/parameters.

For parameter contents these functions should be able to:

- let the parameter content pass unchanged, or
- change the parameter content (within agreed range), e.g. in case of extending an CLI with the country code, or
- suppress the sending/receiving of the message.

When screening is performed, the sending party should be informed by the screening party, to allow the sending party to do the proper (re-)action in order to avoid e.g. resending of the message. This could be done by sending an error message with errorcode "ScreenedOut". In certain cases the action of screening may result in severe conditions that imply the cancellation of the relationship.

5.5.2 Charging mechanisms between SP and PTNO

There shall be technical mechanisms for the support of charging between the PTNO and the SP for the use of each other's resources.

5.5.2.1 Priority

This priority of this requirement is high.

5.5.2.2 Example of usage

In case that the SP use IVR units in the PTN or use announcement machines in the PTN, the PTNO may charge the SP for the use of its resources.

5.5.2.3 Technical aspects

The charging related requirements may be divided in the following categories, including:

- Call related:

  The PTNO needs the ability to, e.g.:

  - change the charging rate of a call, applied to the SP, during the call set-up phase;
  - change the charging rate of a call, applied to the SP, during the duration of the call;
  - charge the SP when the SP interacts with the end user before the charging of the end user begins;
  - charge the SP for delivering the PTN service "dropped-back calls".

- Data related:

  The PTNO needs the ability to charge the SP, e.g. when the SP sends data and receives data from the NTP of a service user without an alerting signal.

- Signalling related:

  The PTNO needs the ability to charge the SP for e.g.:

  - sending information to the SP (e.g. an indication of an originating or incoming call on the line of the SP's service user);
  - overriding any "incoming call barring" supplementary service activated on one of the SP's service user's line;
  - bypassing any "call diversion" supplementary service on one of the SP's service user's line;
  - "delivering" (to activate and to deactivate) a message waiting indication to a SP's service user's line.

Bibliography

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

ETP guideline on network integrity.

EC (1997): Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation Towards an Information Society Approach; COM(97)623, 3.12.97.

CEPT/ECTRA Rec(99)01: recommendation on the use of special network access, 3rd of March 1999.

Directive 97/66/EC of the European Parliament and Council on the processing of personal data and the protection of privacy in the telecommunications sector.

ETSI ETR 339 (1997): "Intelligent Network (IN); IN interconnect business requirements".

ETSI TR 101 664: "Intelligent Network (IN); IN interconnect security features".

ETSI TR 101 365: "Intelligent Network (IN); IN interconnect threat analysis".

ETSI ETS 300 089 (1992): "Integrated Services Digital Network (ISDN), Calling Line Identification Presentation (CLIP) supplementary service, Service description".

ETSI ETS 300 090 (1992): "Integrated Services Digital Network (ISDN), Calling Line Identification Restriction (CLIR) supplementary service; Service description".

ETSI ETS 300 200 (1994): "Integrated Services Digital Network (ISDN), Call Forwarding Unconditional (CFU) supplementary service; Service description".

History

Document history		
V1.1.1	June 2000	Membership Approval Procedure MV 20000818: 2000-06-20 to 2000-08-18
V1.1.1	September 2000	Publication